Rivista elettronica di Diritto, Economia, Management

Numero 1 - 2017

Parte Prima: scritti nell'ambito dell'accordo SMAU-ANDIG

Parte Seconda: ambiente, CAD, sistemi intelligenti, robotica medica, qualità della scuola

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 VII, n. 1/2017
ISSN 2039-4926
Autorizzazione del Tribunale civile di Roma N. 329/2010 del 5 agosto 2010
Editor ClioEdu
Roma - Lecce

Indice

Editoriale

In questo numero pubblichiamo nella *Prima parte* i contributi elaborati nell'ambito dell'accordo SMAU-ANDIG. Il numero è curato da Massimo Farina che ha promosso l'accordo e cogliamo l'occasione per ringraziarlo per il lavoro svolto. Nella *Seconda parte* pubblichiamo articoli sull'ambiente, sulla trasparenza, sulla robotica medica, sulla Scuola della qualità, sulla opacità dei sistemi intelligenti, sulla riforma del Codice dell'Amministrazione Digitale.

Il Direttore della Rivista
Donato A. Limone

Autori di questo numero

Francesco Addante

Francesco Addante è nato a Bari dove risiede. Inizialmente da grande appassionato, poi da cultore e conoscitore, spinto dalla quasi irraggiungibile missione di far valere, a tutti i costi, i diritti di un semplice "*cittadino*", offre alla società, tramite il proprio sito web personale *http://www.francescoaddante.eu/* e articoli pubblicati su testate online autorevoli e specializzate, i risultati dei suoi esperimenti e ricerche di studio in materia di *Trasparenza* e *Anticorruzione* e nell'ambito specifico degli Appalti. Dopo la laurea Magistrale in "*Management ed E-Government delle Aziende Pubbliche*", (LM-63), conseguita con lode presso l'Università di Roma Unitelma Sapienza, nel 2015 consegue, con analogo profitto e nello stesso Ateneo, anche il Master di II livello in "*Organizzazione e Innovazione nelle Pubbliche Amministrazioni*", redigendo un Project work dal titolo *"Il nuovo D.lgs. 33/2013 con l'introduzione del F.O.I.A. in Italia. La verifica del sito web del Dipartimento della Funzione Pubblica prima e dopo il nuovo Decreto Trasparenza"* attraverso il quale ha fornito dei contributi operativi sugli obblighi informativi delle P.A. durante il processo di formazione che ha portato alla normazione definitiva del FOIA italiano

Edoardo Enrico Artese

Avvocato del foro di Milano; partner dello Studio AC Legal, con sede principale in centro a Milano e sedi distaccate a Bangkok ed Hong Kong; laureato in giurisprudenza con tesi in diritto industriale/ diritto d'autore; perfezionato in diritto societario presso l'Università degli Studi di Milano; membro dell'Associazione DirICTo. Specializzato in diritto commerciale ed esperto dei mercati asiatici.
Sito internet: www.ac-legal.eu – www.ithai.eu – www.diricto.it

Alessandro Bonu

Systems Infrastructure Engineer & Digital Forensics Expert presso ls Società Engineering. Nel corso della sua carriera ha conseguito diverse certificazioni e specializzazioni. É Microsoft Certified Professional, CTU, socio di CLUSIT (www.clusit.it) e AIP (www.aipnet.it).
Collabora col Network DirICTo e con il Laboratorio "ICT4 Law & Forensics" del Dipartimento di Ingegneria Elettrica ed Elettronica dell'Università degli Studi di Cagliari per attività legate alla Computer Forensics e Digital Investigation. Sito internet: www.diricto.it

Esmeralda Colombo

Laureata all'Università Cattolica di Milano nel 2011, ha conseguito un Master in Diritto dell'Unione Europea presso il Collège d'Europe di Bruges con una tesi in diritto dell'ambiente. Praticante abilitata, si occupa del legal di MyFoody, società volta alla riduzione degli sprechi alimentari.

Wanda D'Avanzo

Avvocato e dottore di ricerca in *Filosofia del diritto* presso l'Università degli studi di Napoli "Federico II". È docente a contratto dell'insegnamento di *Trattamento e protezione dei dati personali* del corso di Laurea Magistrale in Giurisprudenza dell'Università degli studi di Roma Unitelma Sapienza. Ha pubblicato le seguenti monografie: *L'e-government*, Movimedia, Lecce, 2007; *Partecipazione, democrazia, comunicazione pubblica. Percorsi di innovazione della Pubblica Amministrazione digitale*, Rubbettino, Soveria Mannelli, 2009; *Il sistema dei controlli nelle amministrazioni pubbliche*, ClioEdu, Lecce, 2011; *La filosofia del diritto nel Medioevo. Il pensiero di San Tommaso d'Aquino*, Arte tipografica, Napoli 2013; *Accordi volontari e* governance *ambientale*, Universitas studiorum, Mantova 2015.
E-mail: wanda.davanzo@unitelma.it

Paola De Lumè

Laureata nel 2003 in Lingue e Civiltà Orientali presso l'Università "Sapienza" di Roma, nel 2009 consegue una seconda laurea V.O. in Scienze della Formazione Primaria presso l'Università "Roma Tre". Inserita da tempo nel mondo della scuola, attiva diverse collaborazioni con istituti ed enti di formazione di Roma. Nel 2011 parte per Londra con una borsa di studio nell'ambito del progetto "Leonardo da Vinci – Job4Graduate" e collabora con la School of Oriental and African Studies della University of London. Nel 2013 rientra in Italia per la docenza del corso "Lingua inglese per l'Educatore Professionale di Comunità" presso il Dipartimento di Scienze della Formazione dell'Università "Roma Tre". Nel 2015 si trasferisce a Lecce dove, oltre all'attività di insegnamento, svolge altri incarichi presso diversi istituti scolastici della provincia. Nel 2016 consegue un Master di II livello dal titolo "Il ruolo dirigenziale: profilo manageriale e leadership educativa".

Salvo Dell'Arte

Avvocato dal 1992. Docente di diritto industriale e diritto dell'informazione e della comunicazione presso l'Università di Torino. Autore dei seguenti volumi monografici: "Fotografia e diritto",UTET, 2014, II° ed "Diritto dell'Immagine nella Comunicazione d'Impresa e nell'Informazione", UTET, 2014, II° ed "Manuale della nuova conciliazione", Experta, 2011, "Mettersi d'accordo senza giudice", Foschi editore, 2011, "I Marchio d'Impresa nella Comunità Europea", Experta, 2011, II° ed. "Modelli di contratti della fotografia e dell'immagine", Experta, 2004, "I Contratti della fotografia e dell'immagine", Experta, 2004. Autore di numerosi articoli sulle tematiche

del diritto industriale e della comunicazione. Direttore della Collana editoriale Temi di diritto dell'impresa, della comunicazione e dell'arte edita da Experta. Docente e relatore in numerosi corsi universitari, di formazione professionale e master nelle materie pertinenti alla sua docenza e specializzazione.

Massimo Farina

Dottore di ricerca in "Diritto e nuove Tecnologie" (Università di Bologna) e Docente "Diritto dell'Informatica e delle Nuove Tecnolgie" e di "Informatica Forense" presso l"Università degli Studi di Cagliari. Coordinatore del Laboratorio Universitario ICT4Law&Forensics (http://ict4forensics.diee.unica.it/). Ha conseguito il Master Universitario di II livello in "Diritto dell'Informatica e Teoria e Tecnica della Normazione" presso l'Università degli Studi di Roma "La Sapienza"; Dal 2004 al 2007 è stato titolare di borsa di ricerca in tema di "Firma digitale e Forma Telematica" presso l'Università degli Studi di Cagliari (sede di Nuoro). È arbitro, abilitato dal Registro del ccTLD ".it", per la risoluzione delle controversie relative ai "Domain Names". È autore di numerosi articoli su riviste cartacee e telematiche, nonché di varie monografie, tra le quali: "La sicurezza nella cyber dimension" (2016), "Fondamenti di Diritto dell'informatica"(2012), "La Nuova Privacy" (2011) "I contratti del Software (2011)". È fondatore del network DirICTo, che raggruppa esperti e studiosi, di tutta l'Italia, in materia di Diritto dell'Informatica e di Informatica Giuridica, con il fine di sviluppare attività di studio, ricerca e approfondimento su tematiche di interesse comune per il mondo giuridico e informatico.

Bruno Fiammella

Avvocato e professore a contratto di Informatica Giuridica presso la SSPL dell'Univ. Mediterranea dal 2009, esercita da circa 11 anni occupandosi anche di diritto penale e civile delle nuove tecnologie e computer forensics, www.fiammella.it. Ha pubblicato circa 20 contributi (14 articoli cartacei, 3 e-book e 3 libri) la maggior parte in tema di insider, criminalità informatica e testi per l'esame di Avvocato. E' docente da circa 8 anni in alcuni Master Universitari II liv., nonché per aziende e privati in tutta Italia su temi pratico - operativi connessi all'ICT.

Gianluigi Fioriglio

Dottore di ricerca in Scienze bioetico-giuridiche, è docente di "Informatica per le Scienze giuridiche" presso l'Università di Roma "Sapienza", Dipartimento di Scienze Politiche (Facoltà di Scienze Politiche, Sociologia, Comunicazione) e cultore di Filosofia del diritto nell'Università di Teramo (Facoltà di Scienze politiche). È stato Visiting Scientist presso il Massachusetts Institute of Technology, Max Weber Fellow presso lo European University Institute, assegnista di ricerca nelle Università di Roma "Sapienza" e Bologna, professore a contratto presso le Università di Roma "Sapienza", Polo di Pomezia, e di Teramo, oltre che docente in master, seminari, corsi di formazione e di dottorato (nazionali e internazionali). È stato relatore, *chair*

e *peer reviewer* in convegni e conferenze nazionali e internazionali (fra cui il XXVII e XXVIII Congresso mondiale IVR, il XXIX e il XXX Congresso Nazionale SIFD, Oxford Connected Life 2017 e i convegni ANDIG 2014 e 2016). È autore di cinque monografie (fra cui "Democrazia elettronica. Presupposti e strumenti", Cedam, 2017, e "Trasformazioni del diritto. Alla ricerca di nuovi equilibri nell'esperienza giuridica contemporanea", Giappichelli, 2017) e di numerose pubblicazioni.

Santo Gaetano

Avvocato in Reggio Calabria, Specializzato in Diritto Amministrativo e Scienze dell'Amministrazione, Cultore di Informatica Giuridica presso l'Università degli studi di Roma "Unitelma Sapienza".

Andrea Lisi

Docente nella Document Management Academy, SDA Bocconi, Milano, al MIS Academy - Management Information System – SDA Bocconi – IBM, nel Master in Management della cultura digitale, editoria, archivi e biblioteche nell'era del 2.0, Università di Verona e di UniDOC- Progetto di formazione continua in materia di documentazione amministrativa, amministrazione digitale, delibere degli organi e documenti informatici - COINFO - Consorzio interuniversitario sulla formazione - Università degli Studi di Torino. Ha fondato il Centro Studi&Ricerche Scint e la prima banca dati sul diritto dell'informatica (Scintlex). È stato Direttore della "RIVISTA DI DIRITTO ECONOMIA E GESTIONE DELLE NUOVE TECNOLOGIE", Nyberg Editore, Milano e attualmente dirige la Collana "DIRITTO, ECONOMIA E SOCIETÀ DELL'INFORMAZIONE", Cierre Edizioni, Roma. Oggi è direttore scientifico della rivista ECLOUD edita da Edisef e direttore editoriale della rivista IL DOCUMENTO DIGITALE pubblicata da Lex et Ars. Già componente del Comitato Scientifico nel Master in "DIRITTO DEL'INFORMAZIONE E DELL'INFORMATICA" presso l'Università di Messina (Direttore Prof. Trimarchi), oggi è nel Comitato Scientifico dell'Istituto Italiano per la Privacy (IIP) - http://www.istitutoitalianoprivacy.it, della Document Management Academy, SDA Bocconi, Milano, del DOCUBUSINESS (http://www.docubusiness.it), del Progetto e-HealthCare Forum (www.forumhealthcare.it), della Rivista Digital Document Magazine (edita da 4itGroup), del Centro Studi Themis Crime e di varie riviste giuridiche cartacee e telematiche ed è autore di diversi volumi e numerose pubblicazioni in materia di diritto delle nuove tecnologie. È stato, infine, docente in master dedicati al diritto dell'informatica presso la Business School del Sole24Ore, l'Università di Lecce, Taranto, Trento, Padova e Messina ed è iscritto all'Albo Docenti della Scuola Superiore dell'Amministrazione dell'Interno. Attualmente è arbitro di numerosi enti di risoluzione stragiudiziale delle dispute relative ai domini Internet ccTLD.it ed è Conciliatore Specializzato DM 23/07/2004 n. 222, è Esperto Valutatore IMQ per il servizio di attestazione Q&S_CS (Qualità e Sicurezza nella Conservazione Sostitutiva) e collabora in tutta Italia con università, enti camerali, centri di ricerca, primarie società fornendo progettazione, formazione,

assistenza e consulenza legale nell'e-business internazionale, nella privacy, nei servizi di conservazione digitale/fatturazione elettronica, nella realizzazione dei modelli organizzativi D. Lgs. 231/2001 e nel diritto delle nuove tecnologie, in genere.

Pietro Lucania

Laurea in Scienze Politiche e Scienze Economiche, Master in Psicologia Giuridica e Criminologia. È autore di numerose pubblicazioni e coautore della monografia "La sicurezza nella cyber dimension" (2016). Collaboratore della cattedra di "diritto dell'informatica e delle Nuove Tecnologie" presso l'Università di Cagliari e relatore nell'ambito del seminario di "Informatica Forense" organizzato dall'A.A. 2014/2015 presso la medesima università. Tra le aree di studio e di ricerca, si occupa in particolare di geopolitica, geoeconomia, *ciberstrategy*. Sito internet: www.diricto.it

Giovanni Maglio

Avvocato cassazionista del Foro di Lecce, consulente e docente in materia di nuove tecnologie, cultore della materia in Informatica giuridica presso la cattedra del Corso di Laurea in Scienze Politiche tenuto dal Prof. M. Mancarella all'Università del Salento, responsabile eHealth e Privacy del LeG (Laboratorio eGovernment) dell'Università del Salento - Area Ricerca, componente del Tavolo tecnico permanente sull'Amministrazione Digitale dell'Università del Salento, componente della Commissione informatica e P.C.T. dell'Ordine degli Avvocati di Lecce, componente del Comitato Scientifico dell'Osservatorio sull'Internet of Thing (IoT), istituito dalla SNAD (Scuola Nazionale di Amministrazione Digitale, Università degli studi di Roma Unitelma Sapienza) con il patrocinio di A.N.D.I.G. (Associazione Nazionale Docenti di Informatica Giuridica).

Giuliano Marconi

Avvocato; ha conseguito il Master Universitario di II livello in "Diritto del-l'Informatica e Teoria e Tecnica della Normazione" presso l'Università degli Studi di Roma "La Sapienza". Collaboratore di cattedra del corso "Diritto dell'informatica e delle Nuove Tecnologie" presso il Dipartimento di Ingegneria Elettrica ed Elettronica, dell'Università degli Studi di Cagliari. Membro del network DirICTo, per il quale ha ricoperto il ruolo di moderatore e coordinatore organizzativo nei seminari organizzati nella regione Marche.
Sito internet: www.diricto.it

Claudio Miotto

Praticante abilitato al patrocinio avanti alla Corte d'Appello di Milano; collaboratore dello Studio Legale Ferrari Artese, con sede principale in Milano e sedi distaccate in Madrid (E) e Shanghai (CH). Laureato in giurisprudenza con tesi sulla Commissione di Garanzia per l'attuazione della legge sullo sciopero nei servizi pubblici essenziali

presso l'Università degli Studi di Milano. Summer school in Sports Law presso University of Nantes.

Filippo Novario

Consulente Informatico Giuridico e Forense per Enti pubblici, Aziende, Istituti Bancari e di Credito, Studi legali, Forze dell'Ordine, Istituzioni. Docente nel programma University Relation di IBM area ICT security, già Docente a contratto d'Introduzione all'Informatica Giuridica presso l'Università del Piemonte Orientale, è relatore in convegni nazionali ed internazionali. È autore di pubblicazioni accademiche e professionali concernenti l'informatica giuridica, l'informatica forense, la sicurezza informatica e le tecniche di hacking, tra cui l'ultima opera *Le prove informatiche nel processo civile*, Giappichelli, Torino 2014.

Fabio Prolo

Praticante avvocato abilitato al patrocinio presso la Corte d'Appello di Milano; collaboratore dello Studio Legale Ferrari Artese; laureato in giurisprudenza, con tesi informatica giuridica; cultore della materia presso la cattedra di informatica giuridica ed informatica giuridica avanzata – Università degli Studi di Milano.

Pasquale Sarnacchiaro

Ricercatore Confermato di Statistica dal 2011 presso l'Università degli studi di Roma Unitelma Sapienza. Laureato con lode in Economia presso l'Università degli Studi di Napoli, successivamente ha conseguito nel 2003 presso la medesima Università il Dottorato di Ricerca in Gestione della Qualità Totale.
È attualmente titolare degli insegnamenti di Statistica, Statistica per le imprese e Modelli statistici per la Pubblica Amministrazione. Ha svolto attività di visiting professor presso l'Università degli studi di Bucarest Accademia degli studi Economici e l'Università di Montpellier.
Dal 2009 in seno alla Società Italiana di Statistica è stato eletto segretario del gruppo permanente "Statistica per la valutazione e la Qualità dei Servizi". È referee di diverse riviste internazionali di Statistica e Valutazione. È autore di pubblicazioni su riviste internazionali quali Journal of applied Statistics, Food Quality and Preference, Journal of Mental Health, Environment International, Australian and New Zealand Journal of Statistics e Corporate Social Responsibility
È stato relatore invitato a diversi convegni Nazionali e Internazionali. Ha partecipato come componente del comitato scientifico ed organizzativo alla realizzazione di Convegni e Scuole nazionali ed internazionali.
I suoi principali Campi di Ricerca sono Modelli ad Equazioni strutturali con variabili latenti. Analisi Statistica Multidimensionale dei Dati, Analisi della Co-Inerzia, Analisi delle Tabelle three-way. Analisi in componenti principali per variabili complesse. Piani sperimentali, Analysis of Means (ANOM), Analysis of Variance (ANOVA), Categorical Analysis of Variance (CATANOVA). Polinomi Ortogonali. Epidemiologia e

Statistica Medica. Misurazione della Customer Satisfaction e della Qualità dei Servizi con modelli multivariati. Controllo Statistico della Qualità.
È attualmente presidente del Comitato Strategico per gli studi economici. Ha partecipato in qualità di componente al progetto Europeo Tempus IV "Master programme in Applied Statistics" Call:EACEA N°28/09 Project number: 511140 - TEMPUS - 1 – 2010 - RS - TEMPUS JPCR
È stato consulente statistico per il Comitato Nazionale per la Valutazione del Sistema Universitario (CNVSU), la TESS – Costa del Vesuvio Regione Campania e Istituto Nazionale per la Valutazione del Sistema educativo di Istruzione e di formazione (INVALSI).

Gianluca Satta

Avvocato del foro di Cagliari e consulente in materia di diritto dell'informatica; Cultore della materia presso la cattedra di Diritto dell'Informatica e delle Nuove Tecnologie, Università degli Studi di Cagliari; componente del direttivo del network DirICTo; collaboratore per le attività di ricerca del Laboratorio "ICT4 Law & Forensics" del Dipartimento di Ingegneria Elettrica ed Elettronica dell'Università degli Studi di Cagliari. Sito internet: www.gianlucasatta.it e www.diricto.it

Marcello Tidore

Direttore del servizio promozione e governo delle reti di cura, già direttore dei Servizi Prevenzione, veterinaria, farmaceutico, accreditamenti dell'assessorato della sanità delka regione Sardegna. Già docente di diritto sanitario e organizzazione delle aziende sanitarie presso l'università degli studi di Cagliari e Sassari. Presidente dell'OIV della ASL n. 5 di Oristano, già membro dell'organo di indirizzo della AOU di Sassari

Sarah Ungaro

Avvocato, ha conseguito il diploma della Scuola di Specializzazione per le professioni legali. Collabora con il D&L Department dello Studio Legale Lisi occupandosi prevalentemente di e-government, formazione e conservazione digitale dei documenti informatici, cloud, fatturazione elettronica, privacy e della redazione di articoli e contratti.

PARTE PRIMA

Scritti nell'ambito dell'accordo SMAU-ANDIG

Introduzione

Questo numero speciale della rivista è una raccolta parziale dei seminari che l'Associazione Nazionale Docenti di Informatica Giuridica e diritto dell'informatica (ANDIG) ha organizzato nel biennio 2014/2015 in collaborazione con lo SMAU, lo storico salone dell'ICT dedicato all'innovazione per le imprese e le Pubbliche Amministrazioni.

Correva la fine dell'anno 2013 quando lo SMAU, la cui sede storica è Milano, decise di attivarsi per facilitare il processo di incontro tra i fornitori di tecnologia e gli imprenditori e manager di imprese e P.A., attraverso la realizzazione di eventi itineranti sul territorio italiano.

Fu così che ANDIG, il cui scopo è quello di promuovere l'introduzione e lo sviluppo dell'informatica giuridica e del diritto dell'informatica, con particolare attenzione al contesto della società dell'informazione e della conoscenza, decise di siglare un protocollo d'intesa con lo SMAU e partecipare, con ruolo attivo, alle tappe territoriali dello SMAU.

L'avvicinamento del mondo dell'insegnamento e della ricerca al mondo dell'impresa è stato un ottimo esperimento di contaminazione tra universi paralleli che ruotano intorno allo sviluppo delle tecnologie informatiche e telematiche.

I seminari ANDIG hanno portato nel territorio la consapevolezza dello stretto legame, ormai imprescindibile, che sussiste tra il mondo *ICT* e la Scienza Giuridica. Un connubio spesso trascurato dai protagonisti del mondo dello sviluppo tecnologico, che di sovente trascurano la valutazione dell'impatto normativo di ciò che viene progettato, prodotto e commercializzato.

I contributi, che fanno parte di questa raccolta, raccontano lo stato dell'arte, su alcune tematiche "calde" del Diritto dell'Informatica, dell'Informatica Giuridica e dell'Informatica Forense nel biennio 2014-2015, di conseguenza, per capirne il vero valore, non si può prescindere dalla collocazione temporale suddetta.

Oggi, molti di quei temi non hanno più un riscontro normativo attuale ma nonostante ciò in essi può scorgersi una lungimiranza degli autori, che per vari aspetti sono stati anticipatori delle novità che oggi sono attualità.

Augurando una buona lettura a tutti coloro che avranno il piacere di consultare questo numero speciale della rivista, in conclusione di questa breve presentazione voglio ringraziare sentitamente il Prof. Donato Limone e tutto il Direttivo ANDIG per aver sostenuto questa iniziativa, con l'auspicio che siano sempre più numerose le occasioni di incontro tra il mondo dell'insegnamento e della ricerca e il mondo dell'impresa.

Massimo Farina

Rivista elettronica di Diritto, Economia, Management

N. 1 - 2017 · pp. 14-18

"Cyber Strategy 2014": La strategia italiana per il cyber-spazio

Massimo Farina – Pietro Lucania

Abstract: Con il DPCM del 24 Gennaio 2014, il nostro Paese ha avviato un percorso di strutturazione della protezione dello "spazio cibernetico" nazionale, basato sulla pubblicazione di due documenti programmatici: il "Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico" con annesso il "Piano nazionale per la protezione cibernetica e la sicurezza informatica". Nel mese di febbraio di quest'anno, questi documenti sono stati pubblicati in Gazzetta Ufficiale, aprendo di fatto un nuovo capitolo della sicurezza del nostro paese.

1. Introduzione

Per la prima volta si pone l'attenzione sul fatto che la principale minaccia dello spazio virtuale è rivolta alla sicurezza del potenziale industriale nazionale rappresentato dal know-how scientifico, tecnologico ed aziendale con inevitabili ripercussioni del benessere sociale ed economico nazionale; per far fronte a ciò entrambi i documenti evidenziano un nuovo approccio per affrontare una problematica, una "strategia olistica", che consenta di individuare azioni congiunte tra il settore pubblico e privato finalizzate ad una idonea capacità di prevenzione, reazione, contrasto e contenimento.

La minaccia cyber è in continua evoluzione sia sotto il profilo tecnologico e sia sotto il profilo delle conseguenze e della varietà degli attori in campo (non solo minacce terroristiche ma anche e soprattutto mirate azioni di sabotaggio e/o spionaggio portate avanti da soggetti para-statali); inoltre sono sempre di più i Paesi che si stanno dotando di particolari capabilities che consentono loro di penetrare nelle reti nazionali di altri Stati sia con singoli attacchi cyber ma anche con più lungimiranti strategie realizzate grazie ad un efficientissima mobilitazione industriale (es. diffusione di hardware e software anche in importanti infrastrutture di rilevanza nazionale che presentano falle/back-door potenzialmente devastanti per tutto il sistema).

Si parla quindi di minacce alla capacità di funzionamento delle nostre strutture critiche che può essere contrastata attraverso lo sviluppo di capacità di prevenzione di eventi assicurando contestualmente una azione efficace di contenimento delle conseguenze rispetto a diverse tipologie di eventi.

Si tratta di capacità che possono essere espresse solamente attraverso una "adeguata

Articolo pervenuto il 16 Febbraio 2017, approvato il 20 Marzo 2017

formazione, sensibilizzazione e responsabilizzazione del personale, mediante l'adozione di misure di sicurezza fisiche, logiche e procedurali".
Tornando al focus dei due documenti programmatici va sottolineato come Il Quadro Strategico individua 6 strumenti per il potenziamento delle "capacità cibernetiche":

1) miglioramento, delle capacità tecnologiche, operative e di analisi degli attori istituzionali interessati;
2) potenziamento delle capacità di difesa delle Infrastrutture Critiche nazionali e degli attori di rilevanza strategica per il sistema-Paese.
3) incentivazione della cooperazione tra istituzioni ed imprese nazionali;
4) promozione e diffusione della cultura della sicurezza cibernetica;
5) rafforzamento delle capacità di contrasto alla diffusione di attività/contenuti illegali on-line;
6) rafforzamento della cooperazione internazionale in materia di sicurezza cibernetica

Tra gli elementi di assoluta novità, riscontrati in analoghi documenti predisposti da altri Paesi, vi è quello di individuare nelle Università e negli istituti di ricerca, gli interlocutori privilegiati per quel che riguarda la diffusione della cultura della sicurezza che ci si auspica possa entrare a far parte del bagaglio formativo di studenti/ricercatori.
Per il conseguimento dei 6 indirizzi strategici sono stati identificati 11 indirizzi operativi, contenuti nel "Piano nazionale per la protezione cibernetica e la sicurezza informatica":

1) potenziamento capacità di intelligence, di Polizia e di difesa civile/militare;
2) implementazione organizzazione e modalità di coordinamento a livello nazionale tra soggetti pubblici e privati;
3) promozione e diffusione della cultura della sicurezza informatica, formazione/addestramento;
4) Rafforzamento cooperazione internazionale ed esercitazioni;
5) Operatività del CERT Nazionale unitamente al CERT-PAe ai CERT dei vari dicasteri;
6) Interventi legislativi e compliance con obblighi internazionali;
7) Compliance a standard e protocolli di sicurezza.
8) Supporto allo sviluppo industriale e tecnologico;
9) Comunicazioni strategiche;
10) Ottimizzazione della spesa nei settori della cyber-security e cyber-defence;
11) Implementazione di un sistema integrato di Information Risk Managment nazionale.

2. Criticità

Struttura:
L'architettura istituzionale individuata dal decreto si sviluppa su tre livelli d'intervento: uno politico per l'elaborazione degli indirizzi strategici, affidati al Comitato interministeriale per la sicurezza della Repubblica; uno di supporto operativo ed amministrativo e a carattere permanente, il Nucleo per la Sicurezza Cibernetica presieduto dal Consigliere Militare del Presidente del Consiglio; uno di gestione di crisi, affidato al Tavolo interministeriale di crisi cibernetica.

Ruoli/Responsabilità:
In questo ambito dunque, una moltitudine di soggetti istituzionali vengono posizionati su pari livello di "capacità decisionale" per affrontare un tipo di minaccia che ben poco si presta ad essere gestita da strutture burocratiche e piramidali.
Allo stato attuale, l'approccio interministeriale (attraverso il ruolo decisivo riconosciuto al CISR Comitato Interministeriale per la Sicurezza della Repubblica) sembra essere l'unico possibile, anche se la partecipazione in egual misura dei vari Ministeri riflette una tipica concezione nazionale e ne consegue che, ad esempio, l'infrastruttura presa di mira da un attacco cyber, diviene competenza (per erroneo convincimento e per un primo lunghissimo momento) del Ministero di riferimento anziché di un Comando integrato di Difesa/Intelligence.

Definizione dei concetti di base.
Nonostante gli enormi passi in avanti compiuti grazie al decreto preso in esame, non esiste una definizione e classificazione condivisa di Infrastruttura Critica (spesso nelle relazioni vengono prese come riferimento quelle dei manuali statunitensi, inglesi, UE) con la conseguenza che senza sapere cosa difendere è impossibile qualsiasi forma di pianificazione efficace; allo stesso tempo è indispensabile chiarire dove inizia e dove finisce un attacco cibernetico ad una infrastruttura critica.

Assenza di un unico CERT (Computer Emergency Response Team).
Allo stato ne sono previsti tre:
1) Il CERT Nazionale presso il MISE
2) Il CERT della Pubblica Amministrazione presso l'Agenzia per l'Italia Digitale
3) Il Nucleo di Sicurezza Cibernetica presso l'Ufficio del Consigliere Militare alla Presidenza del Consiglio dei Ministri.

3. Modelli Comparativi

Alla fine del 2013 solo 17 dei 28 Stati membri dell'UE avevano pubblicato una Cyberstrategy e solo 29 dei 196 Stati sovrani a livello internazionale avevano fatto la stessa cosa.
Difficile l'esercizio di uno studio comparativo stante la presenza di una lunga serie

di variabili (budget a disposizione, entità dei dati da proteggere, peso internazionale, struttura governativa) che di fatto rendono complesso tale esercizio.
L'esempio della Confederazione Svizzera con il suo centro di coordinamento che interagisce con il CERT governativo e parallelamente con l'intelligence, le forze armate e riversa gli "alert" alle aziende (che a loro volta segnalano intrusioni ed attacchi) costituisce un modello contraddistinto da linearità, semplicità ed efficacia.
Diversa la posizione USA che tra il 2009 e il 2010 ha creato e reso operativo l'US Cyber Command (USCYBERCOM) che di fatto assume il controllo delle operazioni nello spazio cibernetico, organizza le risorse informatiche esistenti e sincronizza la difesa delle reti militari statunitensi; il Comando inoltre ha il compito di mettere insieme le risorse del cyberspace con la creazione di sinergie e la sincronizzazione di effetti di combattimento per difendere l'ambiente cibernetico e l'integrità delle informazioni (capacità proattiva).
Si tratta di due esempi che interessano due attori completamente diversi tra loro, in mezzo, tutta una serie di situazioni fatte da singoli Paesi consapevoli di far parte di una information society globale che si basa su sistemi operativi, protocolli di comunicazione e software totalmente insicuri, ove il più sprovveduto rischia di ritrovarsi in balia del più feroce ed astuto.

4. Prospettive

Pensare di affrontare le nuove minacce applicando vecchi schemi considerando lo spazio cibernetico semplicemente come un'altra dimensione di interazione strategica appare riduttivo e fuorviante; il cyberspazio agisce come "luogo" per raggiungere le altre dimensioni e un attacco informatico può rapidamente e facilmente passare dal mondo virtuale a quello reale.
Approcciarsi con metodo a questa realtà, è necessario per una corretta comprensione della minaccia e per favorire un'appropriata pianificazione della difesa cibernetica; l'adozione dei sistemi difesa ad hoc potrà quindi contribuire in maniera vantaggiosa alla salvaguardia del benessere e della sicurezza di tutti noi.
La direzione da percorrere è quella di una "global cyberstrategy" che tenga conto delle esigenze di difesa dei singoli ed individui le azioni di contrasto in una dottrina sempre più complessa; una strategia della sicurezza globale all'interno della quale siano chiari i ruoli e le responsabilità nelle attività gestionali, i cui costi siano compatibili con le risorse disponibili e che riunisca in un coordinamento efficace tutte le normative ed i documenti finora emanati.

Bibliografia

- European Commission, Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 2013, in http://www.eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf
- Cyber minacce e sicurezza. La relazione del COPASIR sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dallo spazio cibernetico, 2010, in http://www.parlamento.it/documenti-repository/commissioni/bicamerali/COMITATO%20SICUREZZA/Doc_XXXIV_n_4.
- Governo Italiano, Relazione sulla politica dell'informazione per la sicurezza 2012, 2013, pagg. 37-47, in http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2013/02/relazione-2012.pdf
- P. Lucania: Il Manuale di Tallin: diritto e cyber war – CESI Centro Studi Internazionali, 2013, in http://www.cesi-italia.org/europa/item/668-il-manuale-di-tallin-diritto-e-cyber-war.html

N. 1 - 2017 · pp. 19-27

Ricette e contromisure per la sicurezza delle informazioni

Alessandro Bonu - Massimo Farina

Abstract: Per anni ci si è concentrati su problemi legati alla sicurezza delle informazioni. Oggi più che mai è di fondamentale importanza cercare le soluzioni che mirino a creare sistemi più robusti e sicuri per salvaguardare i nostri dati. Tuttavia occorre considerare anche il rovescio della medaglia, ovvero che ci si è concentrati di più sul cercare di capire chi ci attacca, perdendo quindi di vista quello che è l'obiettivo principale: progettare e implementare sistemi sicuri. Si cerca pertanto di offrire un ricettario di contromisure da adottare per creare difese forti usando ingredienti comuni.

Parole chiave: andig, diricto, smau, formazione, sicurezza, sistema informativo

1. Introduzione

Con la rapida evoluzione delle tecnologie dell'informazione e della comunicazione, i sistemi informatici hanno assunto importanza centrale nell'assetto organizzativo e funzionale di imprese e Istituzioni. La diffusione delle tecnologie, fondate su quello che oggi rappresenta Internet, ha poi favorito il ridisegno dei confini organizzativi dell'impresa, sempre più aperta e connessa con altri soggetti e sistemi informatici.
In questo contesto, l'adozione di efficaci politiche di sicurezza informatica assume una rilevanza cruciale, in quanto da essa possono dipendere le stesse sorti dell'impresa/istituzione. Si tratta pertanto di un compito di non facile portata, in ragione soprattutto dei continui cambiamenti delle tecnologie e dell'elevato impegno operativo, organizzativo e finanziario richiesto a tutti i livelli della struttura aziendale.
Quando si parla di sicurezza in ambito informatico, occorre considerare un aspetto importante: **non esiste certezza della sicurezza delle informazioni** e relativa efficacia delle contromisure adottate dall'azienda/organizzazione per salvaguardare dati. Avere questa certezza significherebbe ridurre l'usabilità dei dati della medesima percentuale, ovvero non utilizzare i nostri dati. Per fare un banale paragone è come acquistare una auto nuova e tenerla ferma nel nostro garage, si tratta pertanto di una soluzione del tutto inapplicabile. Ciò che si può fare, in una realtà così tecno-

Articolo pervenuto il 16 Febbraio 2017, approvato il 20 Marzo 2017

logicamente complessa e "connessa" è cercare un equilibrio tra questi due aspetti: **sicurezza** e **usabilità**.
Alcuni recenti dati estrapolati da Ansa recitano che in Italia solo il 10% delle aziende è al passo con i tempi per la protezione. Tra perdite di dati sensibili per guasti o errori e interruzioni inattese dei sistemi informatici, le aziende italiane negli ultimi 12 mesi hanno perso 11,2 miliardi di euro, a livello mondiale la perdita è stata di 1.700 miliardi di dollari.
In uno scenario nazionale in cui l'80% delle aziende intervistate ha registrato, negli ultimi dodici mesi, un blocco inaspettato nei propri sistemi informatici o una perdita di dati sensibili che hanno portato:

- per il 38% a una perdita della produttività
- per il 22% a un decremento del fatturato
- per il 36% al ritardo nello sviluppo di un prodotto

Emerge inoltre dall'inchiesta che il 79% dei professionisti IT delle aziende italiane non nutre piena fiducia nella propria capacità di recuperare le informazioni a seguito di un incidente.
Si evince pertanto da questo scenario che il problema sulla sicurezza dei dati è importante e che le aziende devono investire e considerare questi aspetti come prioritari per le strategie di business.

2. Riservatezza, Integrità e Disponibilità delle informazioni

Una volta accettata la premessa che la sicurezza al 100 per cento non è raggiungibile, la strategia principale per attuare delle buone contromisure è quella di far percepire all'attaccante sconveniente e troppo oneroso condurre un'attività in questo senso.
Il sistema informatico rappresenta oggi per moltissime aziende il «**sistema nervoso**». Tanto più sensibili sono le informazioni detenute, tanto più è necessario dotarsi di SISTEMI, PROCEDURE E RISORSE che li «mettano al sicuro. Va inoltre ricordato che la tutela dei dati oggi non è più facoltativa ma obbligatoria, la «Legge sulla Privacy» impone rigorose e idonee misure di sicurezza perché i dati trattati non vengano utilizzati in modo improprio o diffusi indebitamente. L'informazione deve essere accessibile solo a chi è autorizzato, difesa da manomissioni e modifiche, disponibile quando necessario.
Ciò significa che non è pensabile, per un'impresa che voglia proteggere i propri dati, guardare alla sicurezza informatica come un'attività "una tantum" ma come un insieme di attività che tengano conto, per esempio, di azioni quali l'identificazione delle aree critiche, la gestione dei rischi, dei sistemi e della rete, delle vulnerabilità e degli incidenti, il controllo degli accessi, la gestione della privacy e la valutazione dei danni.
I seguenti aspetti focalizzano l'attenzione sulla corretta e adeguata gestione della

sicurezza informatica che prima di tutto devono rispettare i seguenti principi:

1) **INTEGRITÀ:** garanzia che l'informazione non subisca modifiche o cancellazioni a seguito di errori o di azioni volontarie, ma anche a seguito di malfunzionamenti o danni dei sistemi tecnologici.
2) **RISERVATEZZA:** gestione della sicurezza in modo tale da mitigare i rischi connessi all'accesso o all'uso delle informazioni in forma non autorizzata.
3) **DISPONIBILITÀ:** rendere fruibili le informazioni, con la garanzia di accesso e usabilità dei dati. Da un punto di vista di gestione della sicurezza significa ridurre a livelli accettabili i rischi connessi all'accesso alle informazioni (intrusioni, furto di dati, ecc.).

3. Le strategie

Per proteggere efficacemente le informazioni da minacce, siano queste interne piuttosto che esterne all'organizzazione, oggi le aziende devono adottare un modello di sicurezza operativo che sia basato sul rischio, sensibile ai contenuti, reattivo alle minacce e impostato sul attività mirate ad automatizzare le procedure di gestione e controllo.
Da un punto di vista strategico di gestione della sicurezza, per ridurre i rischi è necessario considerare i seguenti aspetti:

1. **Protezione dell'infrastruttura:** ottimale è senza dubbio una gestione centralizzata di tutti i sistemi in modo che sia possibile gestirli e proteggerli con efficacia. In pratica, tutto questo significa strutturare correttamente la rete e fortificare tutti gli endpoint/host, proteggere le e-mail, difendere i server interni critici, oltre a garantire il backup e recupero sicuro dei dati. È necessario quindi creare un ambiente protetto e rapidamente gestibile in caso di problemi.
2. **Gestione dei sistemi:** la sicurezza deve rendere la vita più semplice per mezzo di standardizzazione e automazione, aspetti semplici che è possibile porre in essere per fare in modo che il software per la sicurezza si occupi del lavoro più impegnativo, dalla gestione delle patch ai controlli di conformità periodici.
3. **Analisi e applicazione delle policy:** grazie alla classificazione dei rischi e alla definizione di adeguate policy a livello aziendale, le organizzazioni possono applicarle in modalità centralizzata con maggiore efficacia e con funzioni integrate di automazione e prevenzione.

4. **Protezione proattiva delle informazioni:** i tradizionali approcci alla sicurezza erano mirati alla protezione del perimetro di rete. Attualmente invece le organizzazioni stanno concentrando l'attenzione sui dati e le informazioni per comprendere in primis dove risiedono, chi vi accede, come vengono utilizzate e, soprattutto, come impedirne proattivamente la perdita. In quest'ambito, ragionare in termini di gestione della sicurezza significa garantire il massimo livello di riduzione del rischio per applicare automaticamente la conformità alle policy di sicurezza dei dati e consentire alle organizzazioni di "governare e controllare" il comportamento del personale.

4. L'approccio alla gestione della sicurezza

Come prima evidenziato, oggi più che mai il rischio di violazione dei dati è maggiore rispetto al passato. In parte la ragione è che gli attacchi mirati contro le aziende e lo sviluppo di codice nocivo hanno raggiunto il loro massimo storico. Da un punto di vista tecnologico, la tendenza in ambito Security Management è quello di adottare sistemi integrati che consentano una gestione completa, unificata e multilivello della sicurezza, con particolare attenzione agli aspetti di automazione non solo per la rilevazione di intrusione e vulnerabilità ma anche per gli scostamenti dalle policy di sicurezza da parte di endpoint, applicazioni e server cruciali nell'intera azienda.
Adottare un approccio centralizzato con tecnologie integrate e console di gestione uniformate garantisce alle aziende vantaggi in termini di:

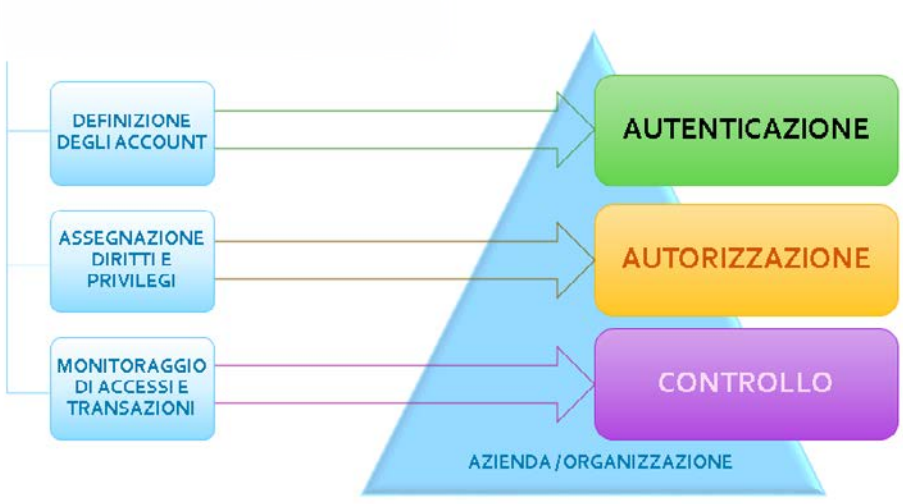
1. accuratezza nella gestione e controllo delle informazioni sulla sicurezza grazie a una maggiore visibilità a livello aziendale tramite sistemi di monitoraggio, gestione degli eventi, generazione di alert e report;
2. semplificazione della gestione con vantaggi significativi sul risparmio di costi e tempo, oltre a una maggiore produttività ed efficienza amministrativa con l'ottimizzazione e l'automazione delle operazioni di routine.

5. Persone, tecnologie e processi

Altro modo per mettere in atto delle efficaci contromisure e quello di variarne la natura. Un bravo hacker può essere in grado di bypassare una nostra regola di firewall ma potrebbe non essere in grado di evitare un secondo livello di controllo (processo di auditing) condotto da personale dedicato che ha il compito di analizzare minuziosamente tutti gli eventi anomali nel contesto del sistema informativo.
Si attua quindi una separazione dei compiti dove ognuno riveste un ruolo ben preciso all'interno dell'organizzazione. Più che di separazione dei compiti in questo caso si deve parlare di collaborazione e coordinamento del personale, evitando quindi sovrapposizioni e/o collusioni tra ruoli e competenze diverse, facendo in modo che

tale stratificazione incrementi il in egual misura il livello di sicurezza anche in relazione agli investimenti sulle risorse impegnate.

Altro elemento fondamentale nella progettazione della sicurezza è poter capire chi sono gli attori principali che andranno ad utilizzare le risorse[1] del sistema informativo. Andremo pertanto ad **autenticare** coloro che tecnicamente definiremo "account" del sistema, a seguire passeremo ad **autorizzare** i soggetti autenticati per dare la possibilità a questi account di poter accedere alle risorse aziendali con determinati privilegi delle politiche aziendali e infine **controllare**, accessi, processi e transazioni degli stessi account. Occorre evidenziare l'importanza del controllo in quanto questa attività riveste una duplice funzione: da un lato consente di avere evidenza degli eventi di accessi e transazioni ovvero di quello che succede durante le attività e dall'altro consente di individuare eventuali carenze o anomalie nel nostro piano strategico così da potervi immediatamente porre rimedio.



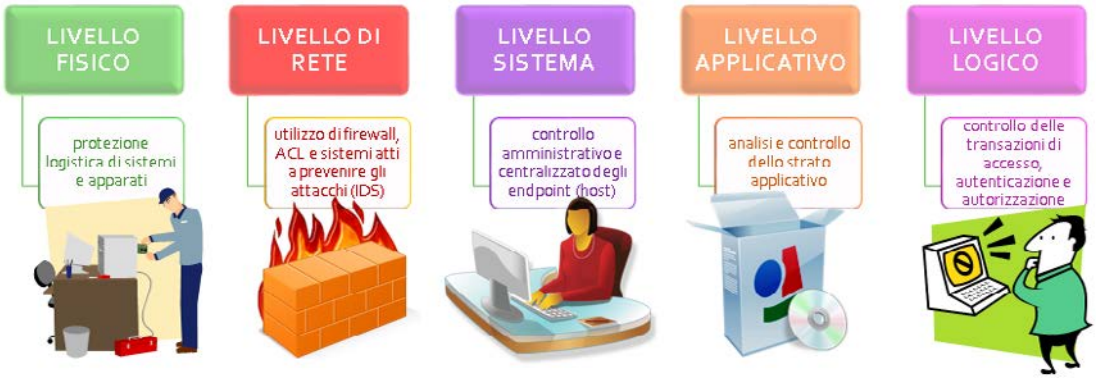
È utile notare come l'attuazione puntuale di tutte le opportune strategie mette in atto

[1] Le risorse di un sistema informativo sono l'insieme delle entità (dagli operatori alle componenti hardware, dal software di base a quello applicativo) necessarie al suo funzionamento.

quanto affermato all'inizio, ovvero si mettono in atto tutta una serie di ostacoli che pur non garantendo una sicurezza del 100 per cento, costringe i soggetti intenzionati ad attaccare la nostra organizzazione a dover "investire" e spendere di più per poterli superare e portare a compimento i loro malevoli intenti. Altro elemento importante da considerare è il fatto che non sempre è necessario implementare sistemi complessi e articolati per garantire più sicurezza e prevenzione. E' come pensare che installare più sistemi antivirus garantisca una maggiore protezione dei nostri sistemi. Da un lato potrebbe essere vero, ma occorre valutare anche l'altra faccia della medaglia, ovvero che da un lato andiamo ad investire di più e in secondo luogo dobbiamo impegnare più risorse per la gestione, aggiornamento e configurazione. In ultimo potrebbe risentirne anche la produttività e le performances se il carico di queste soluzioni fosse eccessivo.

6. Ambiti di applicazione delle contromisure

Vediamo ora quali sono gli ambiti sui quali applicare le contromisure:



1. **Livello fisico**: il primo aspetto da considerare è quello di proteggere adeguatamente sistemi e apparati di rete anche dal punto di vista logistico, in primis per un problema di accessi e autorizzazioni, in secondo luogo per un discorso di fruibilità e manutenzione. In questo contesto va anche valutato un adeguato sistema di climatizzazione.
2. **Livello di rete**: implementazione di tutte le protezioni adeguate nel perimetro di rete come firewall, ACL e IDS. Da evidenziare che nonostante l'attenzione vada posta sugli accessi esterni all'organizzazione, non bisogna sottovalutare gli accessi da parte di chi sta all'interno del perimetro aziendale ovvero degli endpoint.
3. **Livello di host/endpoint**: dietro le mura non ci si deve mai sentire completamente al sicuro, una strategia di controllo e gestione centralizzata degli endpoint è certamente da mettere in primo piano e considerare necessaria per una corretta e puntuale gestione.

4. **Livello applicativo**: anche in questo caso una gestione centralizzata delle applicazioni ci consente di ridurre al minimo problemi legati a carenza di patch e aggiornamenti che possono determinare importanti vulnerabilità sia in termini di sicurezza che di produttività.
5. **Livello logico**: è il livello di controllo non solo di accessi e transazioni ma anche della funzionalità di policies e procedure. Importante aspetto dal quale scaturiscono le attività "reattive" in relazione ad eventuali anomalie o problemi che si dovessero verificare, di fondamentale importanza per riportare in tempi rapidi la situazione alla normalità e ridurre pertanto al minimo i disservizi o le vulnerabilità evidenziate.

7. Gestione del rischio

La gestione del rischio informatico si svolge attraverso un articolato processo che mira a identificare le vulnerabilità del sistema informatico, le possibili minacce, la capacità di affrontarle e gestirle senza infine tralasciare una stima dei potenziali danni.
Data la natura incerta e l'evoluzione continua della tecnologia, la gestione del rischio IT rappresenta una sfida strategica in qualsiasi azienda e a riguardo si possono individuare quattro fasi che devono essere attuate in maniera ciclica e puntuale:

1. **Analisi del rischio** attraverso un'attenta analisi che mira a valutare tutte le potenziali fonti di rischio per lo specifico contesto in cui si opera.
2. **Implementazione di procedure,** tutte le attività da porre in essere e necessarie a prevenire, individuare e capaci di rispondere a situazioni di criticità per limitare i danni.
3. **Monitoraggio e controllo**, attenta analisi dei processi e delle transazioni dalle quali si evincono le dinamiche di funzionamento o non funzionamento delle procedure implementate per garantire la sicurezza del sistema informativo.
4. **Intervento e correzione** delle procedure applicate in presenza di anomalie o

7. Formazione e Informazione

Per realizzare un'efficace politica di sicurezza informatica è necessario che le risorse umane coinvolte nei vari processi aziendali siano attentamente formate, informate e sensibilizzate sugli aspetti tecnico-funzionali del sistema informativo e soprattutto sulle procedure che ne garantiscono la sicurezza.
Va infatti rimarcato che qualunque presidio di sicurezza tecnico-organizzativo adottato può essere vanificato da comportamenti dannosi posti in essere, in modo intenzionale o meno, dal personale dell'azienda che ha un rapporto privilegiato con gli strumenti.
Le risorse umane sono il vero patrimonio aziendale, intendendo la capacità della persona di assicurare riservatezza, disponibilità e integrità, nonché uso legale delle informazioni che tratta.
Ai fini del miglioramento di tale capacità, assumono rilievo le seguenti attività aziendali:

1. **Selezione accurata del personale** (in termini di competenze, conoscenze, capacità e qualità personali).
2. **Formazione e addestramento** sui diversi aspetti della sicurezza informatica attraverso il coinvolgimento nelle attività di routine ma anche attraverso l'organizzazione di corsi, modulati in relazione ai ruoli e alle competenze dei partecipanti, su argomenti quali: la normativa sulla privacy; le leggi e le normative aziendali in tema di sicurezza; gli standard di riferimento e le metodologie di analisi del rischio; la progettazione delle misure di protezione; i principi di audit.
3. **Precisa definizione delle attività** e delle responsabilità dei diversi ruoli che prevedono interventi sulle risorse informatiche aziendali.
4. **Progettazione** attenta dei processi aziendali in modo da ridurre la possibilità che le singole risorse si trovino in posizione critica.
5. **Introduzione di ridondanze** delle competenze specialistiche nei ruoli critici. Alcuni ruoli specialistici rappresentano punti di criticità nel senso che l'assenza delle persone che li ricoprono potrebbe compromettere lo svolgimento dei processi aziendali.
6. **Proceduralizzazione e la documentazione** delle diverse attività in relazione alle normative vigenti.
7. **Previsione di un piano sanzionatorio** che prevede misure disciplinari nei confronti di chi non rispetta il regolamento aziendale.

La promozione della cultura della sicurezza presso il personale deve essere considerata un fattore fondamentale per la protezione del patrimonio informativo aziendale. La consapevolezza e il coinvolgimento del personale devono essere assicurati attraverso idonei interventi di sensibilizzazione e comunicazione che mirino a valorizzare, nell'ambito della missione aziendale, le attività di sicurezza rendendo tutti partecipi dell'importanza che riveste l'osservanza delle procedure di protezione del sistema informativo.

8. Conclusioni

Possiamo pertanto riassumere in conclusione quanto segue:

1. Non esiste certezza nel progettare delle contromisure che siano efficaci al 100 per cento, l'unico modo per garantire un più alto livello di sicurezza è quello di bilanciare al meglio l'usabilità e il livello di sicurezza applicato attraverso le policies aziendali. Anche queste non rispondono a univoci standard ma vanno valutate e pianificate di volta in volta dopo attenta analisi del contesto in cui si opera.
2. Uno dei tanti meccanismi che mitigano il rischio è quello di diversificare ostacoli e strategie di intervento in modo tale da costringere chi attacca, o chi cerca di penetrare nel sistema informativo, a dover superare più ostacoli, scoraggiandone da un lato le intenzioni ma dall'altro creando una stratificazione di contromisure.
3. Semplicità e chiarezza in primo piano. In genere chi attacca cerca strade più semplici e in mancanza di queste le attenzioni potranno essere rivolte ad altri bersagli. In secondo luogo diventa inutile e complesso anche da gestire implementare sistemi complessi o sopravalutare condizioni di rischio. Piani semplici ed efficaci, attentamente valutati in un determinato contesto, danno luogo a maggiore efficienza in termini di sicurezza e fruibilità delle informazioni.

N. 1 - 2017 · pp. 28-40

L'utilizzo illecito di software contraffatti in ambito aziendale

Edoardo E. Artese[1] – Claudio Miotto[2]

Sommario: 1. Il concetto di software, genesi e definizione – 2. Breve introduzione al diritto d'autore. La tutela generale prevista dall'ordinamento italiano – 2.1 L'art. 171 bis LdA e le sue parole chiave – 2.1.1 Duplicazione – 2.1.2 Profitto – 2.1.3 Programmi – 2.1.4 Scopo commerciale – 2.1.5 Contrassegno SIAE – 3. Conclusioni.

1. Il concetto di *software*: genesi e definizione

Un primo passo, prima di affrontarne la disciplina nel panorama giuridico italiano, è quello di comprendere il significato del termine *software*.

Il termine *software* ha un'origine abbastanza lontana nel tempo: nasce durante la Seconda Guerra Mondiale allorquando un gruppo di studiosi inglesi[3], capitanati da Alan Turing[4], furono incaricati dai servizi segreti britannici di decrittare i codici nazisti elaborati con il progetto noto con il nome di Enigma[5].

Il primo macchinario utilizzato per crittografare i messaggi bellici (dal 1941 in avanti) era composto da due parti: una "dura" detta *hardware*, materialmente riconducibile alla struttura della macchina utilizzata dai tedeschi per scrivere i messaggi cifrati; una "morbida", detta appunto *software*, che permetteva di posizionare l'*hardware* nella composizione del messaggio.

L'influenza delle teorie di Turing, così come le sue previsioni relative allo sviluppo dell'informatica, portarono negli anni all'affermarsi, nell'immaginario collettivo, di

---

[1] Avvocato del Foro di Milano. Titolare dello Studio Legale Artese. Membro dell'Associazione DirICTo.

[2] Dottore in Giurisprudenza. Membro dell'Associazione DirITCo.

[3] Il c.d. gruppo di Bletchley Park (o Stazione X) dalla tenuta situata nel paese di Bletchley ove vennero radunati i più brillanti crittoanalisti del Regno Unito durante la Seconda Guerra Mondiale.

[4] Alan Turing (Londra 23.06.1912 – Wilmslow 07.06.1954) matematico, logico e crittografo britannico considerato uno dei padri fondatori dell'informatica moderna e dell'intelligenza artificiale (già dal medesimo teorizzata negli anni 30 del secolo scorso) ed in assoluto tra i più grandi matematici del XX secolo.

[5] Ovvero la macchina elettro-meccanica per cifrare e decifrare messaggi in codice, sviluppata prima per utilizzi commerciali e poi utilizzata dalle forze armate tedesche durante il secondo conflitto mondiale. Facile da usare e ritenuta indecifrabile venne in realtà violata da scienziati polacchi prima dello scoppio del conflitto e, soprattutto, dai britannici durante la guerra. Grazie a tale lavoro di intelligence le forze alleate riuscirono a carpire importantissime informazioni militari che contribuirono in modo determinante alla sconfitta della Germania nazista.

Articolo pervenuto il 16 Febbraio 2017, approvato il 20 Marzo 2017

un'analogia affascinante, un parallelismo secondo il quale l'*hardware* sarebbe stato al *software* di un personal computer, come il corpo alla mente negli esseri umani.
Il termine *software*, dopo la sua nascita, venne poi formalizzato nel senso moderno tra il 1957 e 1958 dallo statistico statunitense J.W. Tukey[6], arrivando oggi a significare, in ambito informatico, l'informazione ovvero le informazioni utilizzate da uno o più sistemi informatici e memorizzate su uno o più supporti informatici[7].
Solitamente vengono effettuate classificazioni del *software* in base alle caratteristiche dello stesso (per esempio per funzione, *software bacht* ovvero online, da installare o *portable*, ad interfaccia testuale o grafica, etc.) ovvero in base alla gerarchia (*firmware*, *software* di base come i sistemi operativi, *driver*, applicativi e strutturati come le più complesse *suite*).
Nonostante le differenze che intercorrono nel panorama sopra descritto, tutti gli esempi sopra riportati rientrano appieno nel concetto di *software*.

2. Breve introduzione al diritto d'autore. La tutela generale prevista dall'ordinamento italiano

Nell'ordinamento giuridico italiano vi è, ormai dal lontano 1941, una previsione normativa posta a tutela del diritto d'autore nelle sue più svariate forme e manifestazioni, ivi compresi anche prodotti dell'ingegno tra i quali è sempre stato pacificamente ricompreso, fin dalle sue prime manifestazioni, il *software*.
La norma guida è rappresentata dalla L. n. 633/1941[8] (di poi per semplicità "**Legge sul Diritto d'Autore**" o anche solo "**LdA**"), oggetto di vari interventi novativi.
L'oggetto della tutela è l'opera dell'ingegno descritta in via generale dall'art. 1 LdA[9] come espressione dell'attività creativa dell'uomo.
Il *software* è entrato relativamente da poco nell'ambito di tutela del diritto d'autore,

---

6 J.W. Tukey ,The Teaching of Concrete Mathematics, , American Mathematical Monthly, 1958.

7 Tali informazioni possono essere quindi rappresentate da uno o più programmi, oppure da uno o più dati, oppure da una combinazione dei due.

8 Il sistema italiano prevede una tutela del diritto d'autore sia sotto il punto di vista morale che patrimoniale con la previsione sia di rimedi civilistici sia di norme di stampo penale (queste ultime però poste a tutela dei soli diritti patrimoniali, lasciando al diritto "morale" d'autore la sola tutela civilistica).

9 Art. 1 L.d.A: "*sono protette ai sensi di questa legge le opere dell'ingegno di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma di espressione. Sono altresì protetti i programmi per elaboratore come opere letterarie ai sensi della convenzione di Berna sulla protezione delle opere letterarie ed artistiche ratificata e resa esecutiva con legge 20 giugno 1978, n. 399, nonché le banche di dati che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore.*"

e per la precisione con il D. Lgs. 518/92, che recepisce la Direttiva 91/250, e che ha emendato l'articolo 1 della l. 633/41 inserendo il seguente capo: "*sono altresì protetti i programmi per elaboratore come opere letterarie ai sensi della convenzione di Berna*[10] *sulla protezione delle opere letterarie ed artistiche ratificata e resa esecutiva con legge 20 giugno 1978, n. 399, nonché le banche di dati che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore*".
Il doppio profilo della tutela (morale e patrimoniale) riconosce, da un lato, all'autore il diritto di paternità dell'opera (ivi compreso il diritto di inedito, il diritto di modificare l'opera ed il diritto di anonimato) e, dall'altro lato, il diritto esclusivo allo sfruttamento economico della stessa[11].
Il rispetto dei suddetti diritti è presidiato dall'art. 171 LdA intitolato "*tutela penale dell'opera dell'ingegno in generale*" che, mediante le numerose riforme della norma, ha subito un costante aggiornamento parallelo con l'evoluzione dei mezzi tecnologici, disciplinando in tal modo fenomeni quali la fotocopiatura o la riproduzione grafica di opere dell'ingegno[12].

2.1 - L'art. 171 bis LdA: analisi della norma

La tutela del *software* originariamente introdotta ha subito successive modifiche da parte del legislatore.
In particolare, la riforma realizzata con la legge n. 248/2000, effettuata dal legislatore sotto i forti impulsi della giurisprudenza nonché della comunità internazionale, ha introdotto una serie di articoli specifici tesi a regolamentare la disciplina relativa al *software*[13].
Tale novella ha sostanzialmente modificato la portata dell'art. 171bis LdA.
Recependo gli orientamenti dottrinali e giurisprudenziali all'epoca prevalenti, il legislatore decise di tutelare il *software* come opera letteraria piuttosto che come invenzione industriale.
L'articolo introduce una tutela di natura penale perseguendo una serie di condotte a danno di programmi per elaboratore quali duplicazione, riproduzione, commercializzazione, etc.
L'art. 171bis, co. I, LdA recita infatti: "*chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed*

[10] La Convenzione di Berna, adottata nel lontano 1896 dopo 10 anni di lavori, è stata soggetta a numerose revisioni, dovute allo sviluppo tecnologico fino all'ultima versione, ratificata a Parigi il 24.07.1971 recepita in Italia con legge n. 399/1978, ed ha la finalità di armonizzare il diritto d'autore a livello internazionale.

[11] Salvo il limite temporale dei 70 anni dalla morte dell'autore posto dall'art. 25 LdA.

[12] Si veda, a titolo esemplificativo, la nuova formulazione dell'art. 68 LdA.

[13] Cfr. artt. 64-64 bis e ss. LdA.

editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da lire cinque milioni a lire trenta milioni".

Le pene previste sarebbero dunque assai aspre, poiché la norma prevede congiuntamente sia la reclusione sia la multa.

La medesima pena è altresì prevista ove ad un programma per elaboratore si applichi "*qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori*".

Questa formulazione, oggetto di alcune critiche (in quanto forse poco chiara e comunque non tassativa), intenderebbe punire i traffici relativi a *cracks*[14], *key-generators* (più noti come "*keygen*"[15]) ed alla duplicazione abusiva di chiavi *hardware*[16] (realizzate per sostituire quelle originali).

In tal modo parrebbe effettuarsi una chiara anticipazione della tutela penale, in quanto si punirebbe anche solo l'intenzione di commettere un illecito, ben prima che si possa anche solo configurare una ipotesi di tentativo[17].

È dunque evidente come la norma posta a tutela di un utilizzo illecito di programmi per elaboratore sia molto stringente.

Passando ad un'analisi dettagliata ed accurata del testo dell'art. 171bis LdA, emergono

---

[14] La *crack* (o il *crack*), in informatica, è un'applicazione che aggira le protezioni di un programma in modo da permetterne l'uso anche non avendolo acquistato. Esistono vari tipi di crack, generalmente suddivisi in: *Patch*: quando si modifica il software per non richiedere l'attivazione. L*oader* (o *memory loader*): programmi che modificano il software durante il caricamento per superare i controlli CRC (Cyclic redundacy check). *Dropper*, file modificati che vengono sostituiti a quelli originali. *API-Bridge*, un tipo di crack usato solo per le librerie DLL, sostituendo a una DLL un file che funzionerà come la DLL, segnalando però che il software è stato registrato. I *No-CD/DVD* , tipo di crack che evita di dover inserire il CD o DVD originale nel lettore. I *NoLimit,* crack che modificano la data di sistema per allungare all'infinito il periodo di prova di un software.

[15] Il keygen o generatore di chiavi o codici è un programma creato appositamente per registrare in maniera fraudolenta un programma commerciale a pagamento. A differenza dei crack il keygen non modifica assolutamente il programma, ma si limita a sbloccarlo mediante una serie di codici appositamente confezionati. Il *Keygen* è spesso un programma complesso cui, oltre al *cracker* (colui che disassembla il programma al fine di trovare i codici e gli algoritmi di registrazione), lavorano anche grafici, musicisti e programmatori, spesso raggruppati in un gruppo dove ognuno ha il suo scopo preciso.

[16] Essenzialmente piccole penne USB che devono essere inserite all'interno dell'apposita porta affinché la macchina possa lanciare il programma, o addirittura farlo funzionare. Questo per evitare che si usi lo stesso programma, con un'unica licenza, contemporaneamente in più PC; ed inoltre per impedirne la duplicazione illegale dal momento che non è possibile scaricare da internet le suddette chiavi. Il programma fa una cosa molto semplice: in precisi momenti (all'avvio nel primo caso sopra citato, o ad intervalli regolari nel secondo) controlla che nella porta USB sia inserita una pennetta al cui interno deve essere presente il chip richiesto dal programma. La presenza fisica del chip rende ardua (seppur non impossibile) la duplicazione dal momento che per creare fisicamente una seconda chiave occorrerebbe fondamentalmente aprire l'originale, prelevare il Chip, copiarne la Rom, e poi rimontare la chiave. Costi e difficoltà tali che mediamente rendono più vantaggioso l'acquisto di una seconda licenza.

[17] Il sistema penale punisce il tentativo ex art. 56 c.p.; tuttavia per tentativo si intende un delitto che non è giunto alla sua consumazione perché non si è verificato l'evento voluto dal reo o perché, per ragioni indipendenti dalla sua volontà, l'azione non è comunque giunta a compimento. Sono però necessari atti idonei, diretti in modo non equivoco a commettere tale delitto.

alcune parole chiave utilizzate dal legislatore, sulle quali maggiori sono stati e sono tutt'ora i dubbi interpretativi espressi da giurisprudenza e dottrina. Tali *keywords*, sono riassumibili nei concetti di:duplicazione;

- profitto;
- programma;
- scopo commerciale;
- contrassegno SIAE.

2.1.1. La interpretazione del termine "duplicare" all'interno dell'art. 171Bis LdA

La prima parola chiave individuata risponde alla voce "duplicazione" inserita dal legislatore al primo comma dell'art. 171bis LdA. Con tale termine, in riferito ai programmi per elaboratore elettronico, **si intende la riproduzione totale degli stessi nel loro medesimo formato originario**.
Quindi costituisce duplicazione non solo la produzione di una copia di un supporto (cd/dvd/blu-ray, etc.) dal contenuto identico a quello originario, bensì anche la semplice produzione di un file (ovunque esso venga poi posizionato) altrettanto identico a quello di partenza.
Se ne deduce come possa rientrare pienamente in tale concetto anche la famosa operazione "*copia-incolla*" di un file presente in un PC[18].
Ne deriva l'applicabilità del dettato normativo ad una pressoché infinita casistica di ipotesi.
Non a caso, si possono contare già numerose pronunce giurisprudenziali.
Stabilisce infatti la Cassazione come "*costituisce abusiva duplicazione di un programma informatico altrui anche la mera opera di adattamento del* software *a diverse esigenze in senso soltanto quantitativo, per essere stato il medesimo realizzato sfruttando, per lo sviluppo, essenzialmente la sequenza dei comandi del codice sorgente dell'originario programma*"[19].
E ancora la Suprema Corte afferma come "*integra il reato di cui all'art. 171 bis l. n. 633 del 1941 non solo la condotta di abusiva integrale duplicazione dell'opera informatica altrui, ma altresì qualsiasi attività di sviluppo di tale opera in assenza dell'autorizzazione dell'avente diritto che ne implichi anche solo parzialmente la*

---

[18] Tale modo di duplicare costituisce la base dell'utilizzo di tutti i programmi di condivisione Peer-to-peer (o P2P) ovvero un'architettura logica di rete informatica in cui i nodi non sono gerarchizzati unicamente sotto forma di client o server fissi (clienti e serventi), ma sotto forma di ***nodi equivalenti* o *paritari*** (in inglese *peer*) che possono cioè fungere sia da cliente che da servente verso gli altri nodi terminali (host) della rete. Essa dunque è un caso particolare dell'architettura logica di rete client-server. Mediante questa configurazione qualsiasi nodo è in grado di avviare o completare una transazione. I nodi equivalenti possono differire nella configurazione locale, nella velocità di elaborazione, nella ampiezza di banda e nella quantità di dati memorizzati. L'esempio classico di P2P è la rete per la condivisione di file (il cd. *file sharing*).

[19] Cass. Pen. n. 38325/2011.

riproduzione" e come "l'illecita duplicazione dei programmi al fine dell'utilizzo degli stessi su molteplici apparecchi costituisce una violazione prevista dalla prima parte del primo comma dell'art. 171-bis della legge 22 aprile 1941, n. 633»[20].

2.1.2. Il termine "profitto" nell'art. 171Bis LdA.

Il secondo intervento catalizzatore effettuato dalla Legge n. 248/2000 sull'articolo 171bis è rappresentato da un'importante modifica, fortemente voluta dai produttori di *software* e supporti multimediali, ossia la sostituzione del termine "lucro" con il termine "**profitto**".
Tali termini, che a prima vista possono sembrare quasi sinonimi, hanno in realtà un significato profondamente diverso.
Il termine "lucro" indica un vantaggio di tipo patrimoniale, ossia un incremento effettivo del patrimonio che può verificarsi per effetto di un negozio con la consegna di una somma di denaro, di un bene o di un servizio.
Nel diritto commerciale il lucro è infatti definito quale risultato effettivo di una transazione (ossia all'interno del "bilancio contabile" rappresenta la differenza tra il valore di ciò che si consegna e di ciò che si riceve).
Alla luce di ciò, qualora si consideri uno scambio di beni di pari entità (ad es. cd-rom piratato in cambio di un altro cd-rom piratato dello stesso valore commerciale) non si potrà parlare dell'esistenza di alcuna forma di lucro dal momento che i soggetti che hanno realizzato lo scambio non ci guadagnerebbero nulla.
In maniera analoga, non vi sarà lucro nemmeno in caso di scambio tra un film pirata e la somma di denaro usata per acquistare il supporto vergine su cui il medesimo viene riprodotto nonché i costi dell'energia utilizzata per realizzare la duplicazione.
Diversamente, il termine "profitto" prescinde dal risultato effettivo ed economicamente quantificabile raggiunto dal negozio e consiste in qualsiasi tipo di vantaggio venga conseguito, anche di natura non patrimoniale.
Non è quindi il risultato contabile di una transazione, bensì qualsiasi tipo di "entrata", vantaggio ovvero semplice miglioria dal precedente *status quo* che venga realizzata tramite la condotta oggetto d'esame.
È pertanto evidente l'impatto scaturito dell'utilizzo del termine profitto in luogo di quello di lucro all'interno della previsione normativa, con la conseguente estensione della portata penale della tutela ad una – decisamente - più ampia casistica di condotte dei consociati.
Di tale portata (anche in questo senso) fortemente ampliativa del novero delle fattispecie perseguibili si è accorta anche la giurisprudenza.
Svariate volte, infatti, i Giudici di merito e di legittimità sono intervenuti proprio sul punto.
Particolarmente esemplificativo, in questo senso, è quanto stabilito dalla Suprema

[20] *Idem*.

Corte di Cassazione nel 2008, laddove ha evidenziato come "*per l'applicazione dell'art. 171-bis, comma 1, legge 633/41, non è più previsto il dolo specifico del* "fine di lucro" *ma quello del* "fine di trarne profitto"; *si è, quindi, determinata un'accezione più vasta che non richiede necessariamente una finalità direttamente patrimoniale ed amplia quindi i confini della responsabilità dell'autore*", arrivando a chiarire come "*la detenzione e l'utilizzo di numerosi programmi* software*, illecitamente riprodotti, nello studio professionale rende manifesta la sussistenza del reato contestato, sotto il profilo oggettivo e soggettivo*" sancendo quindi come "***la condotta di duplicazione abusiva di un programma per elaboratore è punita, dall'art. 171 bis, comma 1, della legge sul diritto d'autore, a titolo di dolo di profitto il quale, più ampio dei previgente dolo di lucro, comprende anche l'intento di destinare la copia all'uso in uno studio professionale Non rileva, pertanto, lo scopo commerciale o imprenditoriale previsto per l'ipotesi della detenzione***"[21].

La tesi illustrata è poi stata ripresa e chiarita sempre dalla Suprema Corte allorquando nel 2011 si è espressa nel seguente modo: "*le differenti espressioni, adoperate dal legislatore nella diversa formulazione degli art. 171 bis e ter, hanno esplicato la funzione di modificare la soglia di punibilità del medesimo fatto, ampliandola allorché sia stata utilizzata la espressione "*a scopo di profitto*" e restringendola allorché il fatto sia stato previsto come reato solo se commesso "*a fini di lucro*"*; la Corte prosegue affermando come *"si rileva che con tale ultima espressione deve intendersi un fine di guadagno economicamente apprezzabile o di incremento patrimoniale a favore dell'autore del fatto, non identificabile con qualsiasi vantaggio di altro genere. Pertanto, non integra una condotta penalmente rilevante la diffusione di una trasmissione criptata in un pubblico esercizio nella vigenza del "*fine di lucro*" se i clienti all'interno del locale non sono numerosi*"[22].

2.1.3. Il termine "programma" nell'art. 171Bis LdA.

La terza parola chiave individuata nella lettera dell'art. 171bis LdA è rappresentata dall'utilizzo del termine programma per elaboratore, soprattutto in considerazione del fatto che una definizione univoca e precisa di cosa si intenda con tali parole ancora non esiste nel panorama normativo italiano.

In questa lacuna normativa, accorre in aiuto la definizione formulata dall'Organizzazione Mondiale Proprietà Intellettuale (o W.I.P.O.)[23], secondo la quale il programma o *software* è "*l'espressione di un insieme organizzato e strutturato di istruzioni (o simboli) contenuti in qualsiasi forma o supporto, capace direttamente o*

[21] Cass. Pen. 25104/2008.

[22] Cass. Pen. 29535/2011.

[23] Agenzia specializzata delle Nazioni Unite creata nel 1967 con la finalità di incoraggiare l'attività creativa e promuovere la protezione della proprietà intellettuale nel mondo. Attualmente è composta da 187 stati membri, regola 24 trattati internazionali ed ha sede a Ginevra, in Svizzera.

indirettamente, di far eseguire o far ottenere una funzione, un compito od un risultato particolare per mezzo di un sistema di elaborazione elettronica dell'informazione".
Stando alla definizione, infatti, si avrà insieme organizzato e strutturato di istruzioni capace di far eseguire o ottenere una funzione ogniqualvolta si tratti, non solo con un sistema operativo o una *suite* di applicativi, bensì con ogni singolo file[24].
Si potrebbe allora propendere per una classificazione che consideri, quali parametri di riferimento adeguati a distinguere cosa sia *software* da cosa non lo sia, i destinatari delle istruzioni.
La discriminante tra file e software potrebbe risiedere nell'autonomia del secondo, e viceversa, nella necessità del primo di venire "letto" da un interprete in mancanza del quale il medesimo non potrà essere eseguito[25].
Anche tale argomentazione, a ben guardare non appare dirimente, dal momento che qualsiasi *software* complesso richiede un interprete ovvero il Sistema Operativo in cui è installato, e senza il quale non può venir avviato[26].
La distinzione tra file e *software* non può vertere nemmeno sul concetto di originalità e creatività, perché se risiedesse nelle istruzioni (codice sorgente) e nelle finalità del programma, la distinzione non sarebbe possibile perché entrambi possiedono le stesse predette caratteristiche.
L'estrema conseguenza del ragionamento porta quindi a considerare programmi tutti i *file*, dal prodotto di un altro *file* a quelli "strutturali"[27] che servono al funzionamento di tutti gli altri.
Quindi anche gli mp3, così come qualsiasi *file* frutto della compressione di immagini e suoni (divx, jpg, midi, wav, etc.), dovrebbero essere considerati dei programmi, a prescindere dell'effettiva opera che rappresentano.
Inoltre si consideri che la normativa in esame non parla semplicemente di esecuzione, bensì di duplicazione (nell'ampia accezione sopra descritta), importazione, distribuzione, vendita e detenzione, con la conseguenza che, per far scattare i meccanismi sanzionatori previsti dall'art. 171bis LdA, basterebbe che il *file* abusivamente condiviso (se considerabile *software* a tutti gli effetti) sia semplicemente presente nel PC perché sia integrato il reato di cui all'art. 171bis LdA.

---

[24] Per esempio, possiamo considerare Microsoft Excel un software, ed invece non considerare tale il file in formato «*.xls» creato dallo stesso Excel? Nonostante istintivamente si potrebbe rispondere affermativamente, rileggendo la definizione fornita dalla W.I.P.O. ci si accorge come anche il file prodotto dal celebre software di calcolo in realtà rientri perfettamente nei parametri richiesti contenendo esso stesso un insieme di istruzioni a cui fa conseguire un risultato per mezzo di un sistema di elaborazione elettronica (la visualizzazione di un foglio di calcolo, nonché i risultati di funzioni inserite, i grafici, i tabulati e tutti gli altri output propri del programma che ha elaborato il suddetto file).

[25] Restando all'esempio precedente, il file «*.xls» non è fruibile da solo, ma richiederà necessariamente un interprete, un programma in grado di leggere le sue istruzioni, o meglio, il suo codice sorgente.

[26] Medesimo discorso può essere fatto per il Sistema Operativo che abbisogna per potersi caricare del software di Bios o comunque di Boot necessari all'avvio della macchina.

[27] Tra cui le librerie, ossia i file "dll".

2.1.4. Il significato del termine "scopo commerciale" nell'art. 171Bis LdA.

Altro aspetto di fondamentale importanza, forse in ultima analisi quello che più sta avendo un impatto sugli operatori del diritto chiamati a giudicare nel caso concreto, risiede nella scelta, operata dal legislatore, del termine "*scopo commerciale*" quale requisito per configurare l'ipotesi di illecito di cui all'art. 171bis LdA.
Tale distinzione è però riferita esclusivamente alla detenzione, avendo il legislatore escluso le altre ipotesi contemplate (escludendo quindi duplicazione, distribuzione, etc.).
Ciò chiarito, passiamo ora ad analizzare la definizione di "scopo commerciale"; secondo una definizione classica, si dovrebbe intendere "*ogni attività finalizzata allo scambio di beni e servizi*".
Nel caso di specie, tuttavia, si è creato un rilevante dibattito giurisprudenziale, reso ancora più complesso se analizzato congiuntamente alla sostituzione terminologica con "*profitto*" al posto di "*lucro*" nell'art. 171bis LdA, sopra analizzata.
Da tale scelta semantica del legislatore sembra, infatti, desumibile la preferenza dell'ordinamento nei confronti di una "*finalità dell'attività commerciale*" tendente in direzione del profitto, quindi di ogni tipo di vantaggio, anche non patrimoniale, che possa venir conseguito.
La detenzione a scopo commerciale, per configurare il reato previsto ex art. 171bis LdA, potrà quindi concretizzarsi con il semplice posizionamento di un programma nella cartella del PC condivisa dal programma P2P (pronto per la duplicazione)[28].
Nonostante quanto sopra illustrato, va rilevato come di tutte le *keywords* finora esaminate, questa risulti essere quella che conserva un maggiore spazio di manovra in capo all'organo giudiziario, risultando la lettera della legge meno diretta e più interpretabile.

---

[28] Da un'applicazione *stricto sensu* della normativa in esame all'utente di una rete P2P che condivide qualsiasi file con altri utenti potrà quindi venir contestato:
- il reato di duplicazione di programma per conseguire il vantaggio (nel senso ampio di profitto) di poter scaricare da altri utenti qualsiasi tipo di dato informatico, ex art. 171 bis;
- il reato di ricettazione ex art. 648 c.p., se il file scaricato e/o condiviso è "*crackato*" (da 2 a 8 anni oltre multa, o fino a 6 anni se fatto di particolare tenuità) perché riceve e/o fa ricevere, sempre al fine di ottenere il predetto profitto, il prodotto del reato ex art. 171bis di rimozione abusiva dei dispositivi di protezione del programma. Si ricorda inoltre come per condividere un file basti condividere una cartella del proprio PC (spesso la stessa cartella dei file scaricati dalla rete) ciò significa che non appena si scarica un file, se non si sono specificamente modificate le impostazioni di default, lo stesso diventa disponibile per tutti gli altri utenti del network. Tale scenario potrebbe condurre, anche a causa del diffuso fenomeno dei *fake* (file dal contenuto diverso da quello che sembrano avere ad un primo esame superficiale) a situazioni anche penalmente assai rilevanti potendosi configurare, e addirittura magari senza nemmeno rendersene conto stante la condivisione automatica anche di contenuto non completamente scaricati, il reato di diffusione di materiale pedopornografico, sanzionato ex art. 600-ter, II c., con la reclusione da uno a cinque anni e con la multa da euro 2.582 a euro 51.645 (eventualità tutt'altro che scolastica, stante quanto successo in Cass. Pen. 10491/2014 in cui la difesa dell'imputato è riuscita a dimostrare l'insussistenza del dolo dell'agente solo al termine di tutti e tre i gradi di giudizio).

La giurisprudenza ha infatti dato dimostrazione di una visione più concreta di quella proposta dal legislatore, avendo modo più volte di ridurre la portata applicativa (nel senso di una maggiore selezione delle condotte penalmente rilevanti) delle pesanti sanzioni previste ex art. 171bis LdA e applicandole (parrebbe) solamente a quelle situazioni veramente meritevoli di una più forte tutela e repressione.
Una innovativa giurisprudenza di merito ha infatti reinterpretato la locuzione "*scopo commerciale*" collegandolo alla modalità imprenditoriale dell'azione. Stabilisce infatti il Tribunale di Bolzano come: "*l'illecito si concretizzerebbe non dall'uso del programma da parte di un imprenditore, (altrimenti sarebbe per es. legittimo qualsiasi uso del* software *da parte di Onlus o simili) bensì nella condotta illegittima posta in essere esercitando in modalità imprenditoriale la riproduzione, distribuzione, vendita, commercializzazione o importazione di opere protette dal diritto d'autore*"[29].
Anche la giurisprudenza di legittimità ha dato il proprio contributo sancendo a più riprese come l'attività libero-professionale non rientri nel concetto di attività commerciale richiamato dalla norma.
Stabilisce infatti la corte di Cassazione come "è *da escludere la responsabilità penale del legale rappresentante di uno studio associato che detiene* software *privi del marchio Siae. Per configurare il reato di cui all'art. 171bis l. n.633/41 non è sufficiente il fine di trarre profitto dall'uso del software-pirata; la detenzione di programmi senza licenza da parte del professionista non integra la fattispecie criminosa perché manca lo scopo commerciale o imprenditoriale sanzionato dalla norma incriminatrice*".[30]
E ancora, "*il reato previsto dall'art. 171 bis comma 1 primo periodo seconda ipotesi l. n. 633 del 1941 (illecita detenzione, a scopo commerciale o imprenditoriale, di programmi per elaboratore privi di contrassegno Siae) laddove richiede che la detenzione avvenga "*a scopo commerciale o imprenditoriale" *non si riferisce anche alla detenzione ed utilizzazione nell'ambito di una attività libero professionale, alla quale pertanto non si applica la norma in esame*" ricordando inoltre come di primaria importanza debba risultare anche in materia di tutela del diritto d'autore la partecipazione dell'agente alla commissione del reato, al punto da stabilire che "*non commette reato chi sia in possesso di software abusivamente duplicato senza prova che abbia effettivamente, in forma materiale o morale, concorso nella duplicazione sanzionata*"[31].

[29] Tribunale Bolzano 31 maggio 2005, in Il Sole 24ore, www.ilsole24ore.com (18/01/15).

[30] Cass. Pen. 42429/2010.

[31] Cass. Pen. 49385/2009.

2.1.5. L'indicazione del "contrassegno SIAE" nell'art. 171Bis LdA.

Ultimo elemento da analizzare, non tanto per i dubbi interpretativi, quanto dalle problematiche pratiche di applicazione dei precetti italiani e di coordinamento tra normative nazionali e internazionali spesso molto diverse tra loro, riguarda l'istituzione del c.d. contrassegno SIAE.
Tale strumento, previsto dalla LdA, assolve a funzioni di autenticazione e di garanzia, sia nei confronti delle Forze dell'Ordine che dei consumatori, con l'effetto (quantomeno auspicato) di rendere facilmente distinguibile i prodotti legittimi da quelli piratati o comunque abusivi e di permettere altresì l'immediata individuazione di chi produce o commercializza prodotti contraffatti.
In forza di tali principi, la norma stabilisce, all'art. 181bis LdA, che su ogni supporto contenente programmi per elaboratore od opere multimediali, nonché su ogni supporto (CD, cassette audio e video, CD-Rom, DVD, ecc.) contenente suoni, voci o immagini in movimento che reca la fissazione di opere o di parti di opere protette dalla legge sul diritto d'autore (art. 1, primo comma, legge n.633/1941) destinati al commercio o che vengano ceduti in uso a qualunque titolo a fine di lucro, deve essere apposto un contrassegno.
Il problema degli effetti dell'apposizione o meno del contrassegno SIAE sui supporti contenenti opere protette dal diritto d'autore è da sempre uno dei profili più delicati della LdA, e rappresenta uno degli aspetti strettamente tecnici affrontati dalla legge di riforma n. 48/2000 (e successivo decreto attuativo d.P.C.M. 338/2001).
La regolamentazione italiana, già sufficientemente complessa ed articolata, per anni non si è mai integrata all'interno della normativa europea di riferimento e non ha mai rispettato le prescrizioni da questa richiesta, rivolte ad uniformare il mercato comune in un settore ad altissimo tasso di compenetrazione, al punto di costringere all'intervento la Corte di Giustizia della Comunità Europea (o ECJ).
Gli inadempimenti dell'Italia ai vincoli comunitari hanno portato la Corte a stabilire come "*la direttiva del Parlamento europeo e del Consiglio*[32]*, che prevede una procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione, debba essere interpretata nel senso che le disposizioni nazionali - quali l'obbligo previsto in Italia di apposizione del contrassegno SIAE sui supporti in vista della loro commercializzazione nello Stato membro - stabilite successivamente all'entrata in vigore della direttiva europea*[33] *che prevede una procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche, "costituisce una regola tecnica che, qualora non sia stata notificata alla Commissione, non può essere fatta valere*

[32] Direttiva 22 giugno 1998, 98/34/CE come modificata con direttiva del Parlamento europeo e del Consiglio 20 luglio 1998, 98/48/CE.

[33] Direttiva del Consiglio 28 marzo 1983, 83/189/CEE.

nei confronti di un privato"[34].

L'inerzia italiana di fronte ad una direttiva comunitaria del 1983 aveva infatti generato delle discrepanze non più tollerabili all'interno del mercato comunitario, costringendo la Corte di Giustizia ad un intervento tanto invasivo quanto inevitabile e giustificato.

Dopo circa 34 anni passati in attesa di una normativa attuativa che disciplinasse e regolamentasse la notificazione alla Commissione Europea delle regole tecniche richieste dall'Italia agli operatori commerciali del mercato unico, l'ECJ non ha potuto che sancire la non opponibilità ai terzi delle norme italiane non rispettose dei precetti europei.

A seguito della sentenza Schwibbert, anche la Suprema Corte di Cassazione si è dovuta pronunciare sulla stessa linea, stabilendo che: "*il giudice nazionale deve disapplicare la regola interna che impone l'obbligo di apporre sui supporti il marchio SIAE in vista della loro commercializzazione fino al momento in cui sarà perfezionata la procedura di notifica*"[35].

La conseguenza di tale doppio intervento giurisprudenziale è stato il venir meno, con effetto retroattivo, della rilevanza penale di tutte le fattispecie di reato che includevano il contrassegno SIAE quale elemento costitutivo della condotta tipica dell'agente[36].

Tale situazione è stata finalmente risolta con l'entrata in vigore, nel 2009 – e quindi a 36 anni dalla direttiva europea 83/179 - della norma di approvazione e notificazione delle regole tecniche[37] in materia di contrassegno SIAE, che ha finalmente condotto ad una normalizzazione della materia.

---

[34] Corte di Giustizia Europea, Sentenza Schwibbert – 8/11/2007.

[35] Corte di Cassazione Sezione 3 Penale Sentenza del 22 giugno 2010, n. 23914

[36] Esclusivamente però per quanto atteneva al bollino SIAE, rimanendo quindi vietata qualsiasi attività che comportasse l'abusiva diffusione, riproduzione o contraffazione delle opere dell'ingegno, così come correttamente statuito, in altra occasione sempre dalla Corte di Cassazione, che ha stabilito infatti come: "A seguito della sentenza della Corte di giustizia Ce 8 novembre 2007, Schwibbert, che ha qualificato l'apposizione del contrassegno Siae sui supporti non cartacei come regola tecnica, da notificare alla Commissione europea in base alle direttive comunitarie n. 83/189/Cee e 98/34/Ce, sussiste l'obbligo per i giudici nazionali di disapplicare le norme che prevedono quale "elemento costitutivo del reato" la mancata apposizione del predetto contrassegno, ovviamente per i fatti commessi anteriormente alla comunicazione della suindicata regola tecnica, che è successivamente intervenuta (d.P.C.M. 23 febbraio 2009 n. 31). Tale conclusione si riflette sull'ambito di operatività dell'art. 171 bis, comma 1, l. 22 aprile 1941 n. 633, dove si prevede come fattispecie alternativa di reato l'abusiva duplicazione di programmi per elaboratore, allo scopo di trarne profitto, o, ai medesimi fini, l'importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale, concessione in locazione di programmi contenuti in supporti non contrassegnati dalla Siae. **Peraltro, rispetto a tali condotte incriminatrici, occorre considerare che, in quella dell'abusiva duplicazione di programmi per elaboratore al fine di trarne profitto, il contrassegno Siae non è elemento costitutivo del reato, sicché la pronuncia della Corte di giustizia non esplica alcun effetto sulla configurabilità di tale fattispecie**. Al contrario, la mancanza del contrassegno Siae è elemento costitutivo di tutte le altre ipotesi previste dal citato art. 171 bis, comma 1, l.n. 633 del 1941, con la conseguente inapplicabilità della norma ai fatti commessi anteriormente alla comunicazione della regola tecnica da parte dello Stato italiano» (Cass. Pen. 42429/2010).

[37] D.p.c.m. n. 31/2009.

3. Conclusioni.

Alla luce di quanto sopra illustrato si possono trarre le seguenti considerazioni.
La normativa al momento in vigore in Italia ha operato un deciso "giro di vite" inasprendo le fattispecie penali e soprattutto ampliando notevolmente, alle volte in modo forse eccessivo, i casi concreti a cui applicare le previsioni normative più stringenti.
Come sopra analizzato, infatti, la normativa attualmente vigente sanziona in modo molto aspro l'utilizzo di *software* contraffatto in ambito professionale.
L'utilizzo di una terminologia non propriamente tecnica, la presenza di termini indefiniti quali "detenzione", "profitto" e "scopo commerciale" hanno infatti esteso l'applicabilità della disciplina penale a dismisura.
Ne deriva che l'utilizzatore di *software* in ambito aziendale dovrà muoversi con una piena consapevolezza sia nel senso di un richiamo ad una comprensione delle licenze dei programmi prima del loro utilizzo (onde evitare di porre in essere condotte non legittime), sia verso una maggiore apertura, anche solo concettuale, al mondo delle licenze *freeware* ed *open source*.

N. 1 - 2017 • pp. 41-47

Cloud computing e privacy: criticità e vantaggi

Saveria Coronese

Abstract: Il cloud computing, inteso come modello flessibile ed economico di fornitura di servizi ICT, rappresenta non solo uno strumento di risparmio e razionalizzazione delle risorse informatiche ma anche e soprattutto un nuovo metodo di progettazione, realizzazione e gestione di sistemi informativi. Affianco ai tanti vantaggi il cloud presenta però anche dei rischi per la privacy dei dati conservati, rischi che occorre valutare con attenzione per poter prevenire possibili conseguenze negative.
Parole chiave: cloud computing, privacy, trattamento dati, lock in, accountability.

Il *cloud computing*[1] si presenta come uno strumento dalle molteplici qualità. Esso, infatti, da un lato consente il risparmio e la razionalizzazione delle risorse informatiche, dall'altro la progettazione, realizzazione e gestione dei sistemi informativi delle aziende e delle pubbliche amministrazioni, permettendo un'organizzazione più efficiente ed economica di risorse, dati e informazioni.
La capacità di utilizzo del cloud è svariata e questo strumento fornisce a chi lo usa la possibilità di compiere diverse attività, alcune fra tutte l'accesso on line da qualsiasi client alla potenza di
elaborazione, alle piattaforme, ai servizi, ai software e ai documenti immagazzinati sulla nuvola virtuale gestita dal *cloud service provider.*
Tale ventaglio di funzioni ne spiega la diffusione sempre maggiore tra imprese, banche, singoli utenti e soprattutto pubbliche amministrazioni[2], le quali tramite il

---

[1] *"I sistemi cloud sono grandi contenitori di risorse virtuali di facile utilizzo e accesso (che mettono a disposizione vari software, ma anche l'hardware, le piattaforme di sviluppo e/o di servizio, la potenza di calcolo). Queste infrastrutture informatiche possono essere dinamicamente riconfigurate per adattarsi a un carico di lavoro variabile (scalabilità), consentendo anche un'utilizzazione ottimale delle risorse. Questo sistema è impiegato tipicamente secondo il modello pay-for-use nel quale tutto è garantito dal provider dell'infrastruttura tramite SLA personalizzati".* Definizione dell'ACM Computer Communication Review , in "*A Break in the Clouds: Towards a Cloud Definition*", di L. M. Vaquero, L. Rodero-Merino, J. Caceres, M. Lindner, Vol. 39, N. 1, January 2009.

[2] In linea con l'assunto che l'utilizzo di sistemi cloud riveste per le Pubbliche Amministrazioni una notevole importanza, nasce il progetto europeo *Cloud for Europe,* con il quale si incentiva l'uso del cloud computing nella Pubblica Amministrazione. Diversi sono i partner internazionali del progetto (Ministerie van Financiën Directoraat-generaal Belastingdienst -Paesi Bassi, Entidade de Serviços Partilhados da Administração Pública -Portogallo, The National Institute for Research & Development in Informatics - Ministry for Information Society -Romania, Ministry of Finance of the Slovak Republic-Slovacchia). L'obiettivo della gara è quello di stimolare le aziende, i centri di ricerca e le università a inviare (entro il 20 febbraio 2015) i progetti, di loro ideazione, per la realizzazione di piattaforme Cloud delle amministrazioni pubbliche europee.

Articolo pervenuto il 16 Febbraio 2017, approvato il 20 Marzo 2017

cloud conseguono più agevolmente gli obiettivi di efficacia, efficienza, trasparenza, partecipazione, condivisione, cooperazione, interoperabilità e sicurezza nell'agire amministrativo.
In effetti, i servizi di cloud costituiscono uno dei mezzi più economici per realizzare sia quanto previsto dal sistema di *eGovernment* delineato dal Codice dell'Amministrazione Digitale sia quanto disposto con l'art. 47 della legge n. 35/2012 (di conversione del D.L. n. 5/2012), il quale pianifica il programma di misure da adottare per il perseguimento degli obiettivi dell'Agenda digitale italiana: infatti, alla lett. d) dell'art. 47 della suddetta legge si parla proprio di "promozione della diffusione e del controllo di architetture di cloud computing per le attività e i servizi delle pubbliche amministrazioni".
L'utilizzo dei sistemi cloud, però, fa sorgere alcune problematiche, soprattutto in tema di asimmetria informativa, riservatezza, lock in, internazionalità dell'accordo, licenze software, deleghe di servizi, interruzioni di servizio, Privacy e accountability. Uno dei problemi principali inerisce soprattutto alla questione della sicurezza dei dati personali che gli utenti immettono quotidianamente in tali sistemi.
Se per un verso il Cloud è considerato uno strumento in grado di offrire opportunità particolarmente vantaggiose, dall'altro non è di difficile intuizione il rischio che grava sui dati in esso contenuti.
Una pianificazione poco attenta della gestione organizzativa dei dati potrebbe in effetti dare luogo a una diffusione incondizionata degli stessi che potrebbero pervenire a qualsiasi utente del web.
Sul punto sono state elaborate diverse fasi operative che consentono di raggiungere l'obiettivo finale della protezione dei dati. Nello specifico le fasi consistono nel:

- selezionare l'insieme dei dati che si intende trasferire nel *cloud*, individuandoli in seguito a una analisi dei vantaggi e delle criticità, tenendo conto della natura dei dati che si intende esternalizzare;
- classificare le informazioni critiche della pubblica amministrazione o dell'azienda, individuando i dati sensibili o strategici, i dati personali, i dati biometrici, i dati identificativi, ecc;
- individuare l'ambito geografico di circolazione delle informazioni e i soggetti coinvolti, stabilendo così la normativa alla quale il trattamento dei dati è assoggettato e gli aspetti relativi alla legge applicabile a quel rapporto contrattuale avente a oggetto il *cloud storage* di quei dati.

Come detto in precedenza, l'utilizzo del sistema di Cloud computing avvantaggia la PA, conferendole un risparmio in termini di capitali e di risorse umane e tecnologiche. Contestualmente, l'adozione di un sistema cloud da parte di una PA fa emergere in primis la questione relativa alla modalità di gestione dei dati pubblici e ai conseguenti diversi profili di responsabilità che possono configurarsi sia in capo ad alcuni organi della PA stessa, sia in capo ai diversi soggetti che intervengono nella catena di erogazione dei servizi cloud in favore di tali enti.

Quando una PA si trova a stipulare un contratto con un Cloud Provider[3], è necessario che questa compia una preliminare analisi comparativa (anche in virtù di quanto previsto dall'art. 68 del Codice dell'Amministrazione Digitale[4]) con la quale mira a individuare i possibili modelli di cloud implementabili. Inoltre, nella scelta del Cloud Provider si deve tenere conto dei sistemi di qualificazione del concorrente basati su elevati standard qualitativi, alla stregua dei quali l'aggiudicatario sarà individuato secondo il criterio dell'offerta economicamente più vantaggiosa.
La PA contraente dovrà, pertanto, valutare attentamente la presenza, nel contratto, di una garanzia dei livelli di servizio e il rispetto della disciplina sulla tutela dei dati personali. Ancora, dovrà essere chiaramente stabilita la responsabilità contrattuale del Cloud Provider e degli altri soggetti eventualmente coinvolti nell'erogazione dei servizi in modalità cloud, nel caso in cui si verifichino violazioni o danni alla stessa PA contraente o a soggetti terzi.

---

[3] Il *Cloud Provider* costituisce uno dei ruoli che si delineano in seno alla PA in seguito allo svolgimento di servizi cloud. Ulteriori figure consistono nel:
• *Cloud Provider* (che acquisisce e gestisce le infrastrutture di elaborazione necessarie a fornire i servizi attraverso la rete e assicura l'esecuzione dei programmi che consentono i servizi),
• *Cloud Consumer* (ossia l'utente o l'organizzazione che sottoscrive un contratto con il Cloud Provider),
• *Cloud Auditor* (che è il soggetto che può eseguire un controllo indipendente sui servizi erogati da un Cloud Provider con il fine di esprimere un parere, ad esempio in merito alla sicurezza, all'impatto sulla privacy e al livello delle prestazioni),
• *Cloud Broker* (è il soggetto che gestisce l'impiego, le prestazioni e l'erogazione dei servizi cloud e cura le relazioni tra il Cloud Provider e il Cloud Consumer)
• *Cloud Carrier* (il quale agisce come un intermediario, fornendo la connettività e il trasporto di servizi cloud tra il Cloud Consumer e il Cloud Provider, nonché l'accesso al Cloud Consumer attraverso le reti e i dispositivi).

[4] Viene riportato qui di seguito il testo dell'art 68 del D.lgs. n.82/2005, recante il Codice dell'Amministrazione Digitale (CAD)
"Analisi comparativa delle soluzioni.
1. Le pubbliche amministrazioni, nel rispetto della legge 7 agosto 1990, n. 241, e del decreto legislativo 12 febbraio 1993, n. 39, acquisiscono, secondo le procedure previste dall'ordinamento, programmi informatici a seguito di una valutazione comparativa di tipo tecnico ed economico tra le seguenti soluzioni disponibili sul mercato:
a) sviluppo di programmi informatici per conto e a spese dell'amministrazione sulla scorta dei requisiti indicati dalla stessa amministrazione committente;
b) riuso di programmi informatici, o parti di essi, sviluppati per conto e a spese della medesima o di altre amministrazioni;
c) acquisizione di programmi informatici di tipo proprietario mediante ricorso a licenza d'uso;
d) acquisizione di programmi informatici appartenenti alla categoria del software libero o a codice sorgente aperto;
e) acquisizione mediante combinazione delle modalità di cui alle lettere da a) a d).
2. Le pubbliche amministrazioni nella predisposizione o nell'acquisizione dei programmi informatici, adottano soluzioni informatiche, quando possibile modulari, basate sui sistemi funzionali resi noti ai sensi dell'articolo 70, che assicurino l'interoperabilità e la cooperazione applicativa e consentano la rappresentazione dei dati e documenti in più formati, di cui almeno uno di tipo aperto, salvo che ricorrano motivate ed eccezionali esigenze".
2-bis. Le amministrazioni pubbliche comunicano tempestivamente al DigitPA l'adozione delle applicazioni informatiche e delle pratiche tecnologiche, e organizzative, adottate, fornendo ogni utile informazione ai fini della piena conoscibilità delle soluzioni adottate e dei risultati ottenuti, anche per favorire il riuso e la più ampia diffusione delle migliori pratiche. (*Omissis*).

La figura del Cloud Provider, infatti, ha un impatto più pesante in merito alla sicurezza, in quanto è a lui che spettano le scelte sui luoghi di circolazione dei dati allocati su server e sui soggetti atti a elaborarli (c.d. subfornitori).
Per quanto riguarda l'area bancaria[5], una scelta orientata verso l'uso di sistemi cloud comporta, principalmente, il conseguimento di un risparmio economico e della c.d. *scalabilità*.
Il risparmio economico si traduce in:

- una riduzione delle spese correnti complessive;
- una più idonea ripartizione dei costi (poiché le spese del servizio saranno rapportate esclusivamente alla sua effettiva utilizzazione);
- una maggiore possibilità di dedicare le risorse tecniche allo sviluppo di attività strategiche.

La scalabilità, invece, va considerata in base alla:

- possibilità di commisurare la richiesta di fornitura di servizi informatici alle esigenze effettivamente nutrite dall'azienda;
- integrazione con l'infrastruttura informatica esistente.

Come detto in precedenza uno dei problemi cardine che influenzano la decisione di affidare i propri dati a sistemi cloud è costituito dalla sicurezza.
Anche in merito a tale argomento il Garante per la protezione dei dati personali[6] ha delineato, nel provvedimento del 12 maggio 2011, n. 192, delle misure di sicurezza specifiche che le banche sono tenute ad adottare per evitare il verificarsi di situazioni che legittimino reclami "*in tema di trattamento di dati personali della clientela effettuato dalle banche in ordine ai temi della "circolazione" delle informazioni riferite ai clienti all'interno dei gruppi bancari e della "tracciabilità" delle operazioni*

---

[5] Torna particolarmente utile la consultazione del manuale sui *Servizi di Cloud Computing e protezione dei dati personali in ambito bancario,* di L. BOLOGNINI, E. PELINO, a cura dell'Istituto Italiano per la privacy e la valorizzazione dei dati, del 19 gennaio 2015.

[6] Il Garante Privacy ha dettato alcuni consigli in materia di cloud che si sostanziano:
• nell'individuazione corretta delle misure di sicurezza adottate dal cloud provider per proteggere i dati;
• nell'identificazione del reale fornitore del servizio in cloud;
• nel verificare i piani di business continuity -in particolare i tempi di ripristino - e disaster recovery;
• nell'accertarsi che sia consentito un accesso a tutto il sistema o parte di esso anche in caso di problemi di connettività a Internet;
• nel controllo del rispetto della riservatezza garantita mediante la separazione dei data base rispetto all'utilizzo comune con altre società dei server forniti nel servizio cloud;
• nella determinazione dello Stato in cui sono conservati i dati immessi nella "nuvola";
• nell'accertare l'esportabilità del database in caso di cessazione del servizio fornito;
• nel concordare con il cloud provider forme di risarcimento in caso di perdita di dati e precisare i livelli di servizio forniti;
• nel ricordarsi che la responsabilità in caso di violazioni privacy commesse dal cloud provider è esclusivamente del titolare del dato;
• nella nomina del cloud provider come responsabile del trattamento;
• nella verifica del livello di professionalità del personale del cloud provider;
• nella verifica dei livelli di accountability forniti dal cloud provider.

bancarie effettuate da incaricati del trattamento di tali dati"[7].
A livello europeo, invece, l'utilizzo dei sistemi cloud viene visto in un'ottica favorevole e l'Unione Europea si è sempre espressa incentivandone l'adozione da parte di imprese ed enti pubblici.
Sul tema è intervenuta anche la Commissione Europea[8], la quale, a fine giugno 2014, ha pubblicato delle Linee Guida con lo scopo di supportare la categoria dei soggetti fruitori del cloud, coadiuvandoli nella scoperta di questo nuovo "mondo" e garantendo loro un approccio quanto più protetto possibile.
Nello specifico, le Linee Guida sono state realizzate da un gruppo di lavoro dell'European Cloud Strategy, il *Cloud Select Industry Group,* il cui operato è finalizzato all'incremento della predisposizione degli utenti e delle imprese verso l'utilizzo dei servizi cloud, in considerazione degli ingenti benefici che questi ultimi sono in grado di apportare.
In effetti, l'utente che intende servirsi delle capacità fornite da un sistema cloud potrebbe essere scoraggiato da una serie di circostanze critiche che spesso sono presenti nei contratti relativi alle forniture dei provider.
Dalle suddette Linee guida emerge quindi la volontà della Commissione di porre le fondamenta di un sistema comune di accordi (c.d. Service Level Agreements, SLA) che armonizzi la disciplina dei servizi erogati dai fornitori di cloud ed elimini le differenze nelle terminologie utilizzate dai diversi fornitori di servizio.
Solo mediante la predisposizione di basi solide e certe gli utenti saranno maggiormente incentivati a fruire dei servizi offerti dalla "nuvola", eliminando quegli elementi che causano un allontanamento dei possibili utenti dalla fruizione del sistema.
Emerge, inoltre, fra gli aspetti negativi maggiormente disapprovati dagli utenti, la scarsa chiarezza delle clausole contrattuali, di solito non caratterizzate da certezza ed inequivocabilità, bensì da terminologie ambigue e poco comprensibili che suscitano preoccupazione in capo agli utenti e non li aiutano ad usufruire del servizio in maniera tranquilla e consapevole.
Spesso la terminologia relativa agli SLA differisce da un fornitore di servizi cloud a

---

[7] *Ibidem*. Si veda inoltre http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1813953

[8] Nel febbraio 2013, la *European Commission Directorate General for Communications Networks, Content & Technology (DG Connect)*, organismo in linea con le politiche dell'UE volte a realizzare la crescita dell'Unione Europea attraverso il contributo delle tecnologie digitali, ha istituito il *Cloud Select Industry Group-Subgroup* sui *Service Level Agreement* (C-SIG-SLA) per lavorare su questi aspetti. Il sottogruppo C-SIG SLA ha preparato questo documento per fornire una serie di Linee guida di standardizzazione per i fornitori di servizi cloud e i loro clienti.
Tuttavia viene specificato nel Preambolo delle Linee Guida che questa iniziativa avrà il massimo impatto se la standardizzazione stessa avverrà a livello internazionale, piuttosto che a livello nazionale o regionale. Le norme internazionali, come ISO / IEC 19086, vengono considerate come un valido punto di partenza per raggiungere questo obiettivo.
Tenendo conto di ciò, il Sottogruppo C-SIG SLA ha istituito un collegamento con l'ISO *Cloude Computing Working Group* per fornire contributi concreti e presentare a livello internazionale la posizione europea. Le linee guida serviranno come base per l'ulteriore lavoro del C-SIG SLA e per un contributo al progetto ISO / IEC 19086.

un altro, impedendo all'utente di effettuare un confronto tra gli stessi
La scelta di un cloud provider si basa sulla presenza di alcune sue caratteristiche che lo qualifichino in maniera seria e professionale. L'utente valuterà se il cloud sia in grado di soddisfare alcune sue esigenze, (ad esempio, il rispetto dei livelli di servizio garantiti e degli impegni contrattuali, la presenza di eventuali certificazioni, l'esperienza maturata sul mercato e la stabilità economica e finanziaria).
Dal punto di vista formale il testo delle Linee Guida è suddiviso in sei paragrafi che riprendono i punti focali che si è inteso approfondire, suddivisi in quest'ordine:

1. Principles for the development of Service Level Agreement Standards for Cloud Computing – paragrafo relativo ai principi intorno ai quali ruota lo sviluppo del sistema comune di accordi per il Cloud Computing;
2. Cloud SLA Vocabulary – paragrafo contenente i termini più frequentemente adoperati con le relative definizioni;
3. Performance Service Level Objectives Overview – paragrafo inerente agli obiettivi riferiti alle prestazioni del cloud;
4. Security Service Level Objectives Overview - paragrafo dedicato agli obiettivi che si vogliono conseguire in tema di sicurezza;
5. Data Management Service Level Objectives Overview – paragrafo incentrato sugli obiettivi da conseguire nella gestione dei dati;
6. Personal Data Protection Service Level Objectives Overview – paragrafo indirizzato alla contemplazione degli obiettivi da perseguire in materia di protezione dei dati personali.

L'ultimo paragrafo delle Linee Guida, come si può notare, è dedicato interamente alla protezione dei dati personali.
Non a caso, la problematica privacy (da intendersi come garanzia di un corretto trattamento dei dati personali) è una delle note più dolenti del cloud computing e prioritaria causa di apprensione da parte degli utenti.
Sul punto, le Linee guida sottolineano che il cliente del servizio di cloud ha il diritto di valutare la legittimità del trattamento dei dati personali nel cloud, scegliendo un fornitore di servizi di cloud che rispetti la normativa in tema di protezione dei dati. Inoltre, sono previsti in capo al fornitore di servizi degli obblighi di informazione nei confronti del cliente circa il diritto di quest'ultimo di richiedere la cancellazione dei propri dati (e con essi i file temporanei e le versioni precedenti) non appena questi non risultino più necessari agli scopi prefissati, rendendolo edotto dell'esistenza di circostanze che lo obbligano a rivelare i dati su richiesta dell'Autorità governativa competente.
Sempre ai fini della trasparenza, il fornitore è tenuto a informare il cliente del servizio cloud circa la presenza di eventuali subappaltatori[9] del servizio.

[9] Il testo delle Linee guida chiarisce anche che, per quanto riguarda il trasferimento dei dati personali dei clienti ai subappaltatori del provider, nel Parere del WP29 si sottolinea la necessità che i contratti tra il fornitore di servizi di cloud e i subappaltatori riflettano, in termini di disposizioni sulla protezione dei dati, le clausole del contratto tra clienti e provider. Inoltre, il consenso del cliente del

Dalla presente, non esaustiva, trattazione è emerso come alcuni soggetti (privati e pubblici), optando per un servizio di cloud computing ricaverebbero esclusivamente benefici di varia natura.
Accanto ai vantaggi apportati dal sistema, però, si profilano delle criticità, prime fra tutte la sicurezza e la protezione dei dati personali che vengono inseriti nelle "nuvola".
Questi aspetti problematici producono il risultato di inficiare la scelta dell'utente che, nell'incertezza sulla tutela dei suoi dati, preferisce fare a meno dei servizi cloud rinunciando parallelamente anche ai vantaggi forniti dal sistema.
Dall'Europa, invece, è chiaro l'indirizzo che imprese, banche, pubbliche amministrazioni e singoli utenti devono seguire, basato proprio sull'utilizzo dei servizi cloud per incrementare le risorse e il risparmio. Sembra necessaria, quindi, un'azione che miri a garantire una maggiore certezza e chiarezza dei contratti cloud, per realizzare quello che possiamo definire uno degli scopi principali delle *Cloud Service Level Agreement Standardisation Guidelines* del giugno 2014.

servizio cloud (che può assumere la forma di un generale consenso principale) è necessario per il subappalto e il cliente può opporsi ai cambiamenti nella lista dei subappaltatori. Al fine di attuare queste disposizioni, l'elenco dei subappaltatori deve essere nella disponibilità del cliente.

N. 1 - 2017 · pp. 48-58

Digital Business Security
informatica, sicurezza e diritto

Filippo Novario

Abstract: La gestione dei dati aziendali attraverso tecnologie informatiche implica una maggiore attenzione alla loro essenza digitale, per ottimizzare sicurezza e reperimento di prove d'illeciti. L'obiettivo è generalmente perseguito attraverso la disposizione di tre discipline: *ICT Security*, Diritto e *Risk Management*. La complessità tecnico-giuridica delle attività da disporre, fusa con l'avanzamento tecnologico e delle condotte illecite, impongono una nuova concezione di tutela dei sistemi informativi: il *Digital Business Security*. Questo fonde le attitudini di *security*, giuridiche e d'amministrazione d'azienda in una figura professionale, il Consulente Informatico Giuridico e Forense, atto al raggiungimento della *compliance* e della *performance* aziendali. Molte questioni informatico-aziendali mostrano profili d'influenza per questo nuovo corso informatico giuridico, in particolare la *Digital Privacy*.

Corporate digital data implies an high level of attention to them informatics essence, in order to optimize security and unlawful act's proof. The aim is perceived generally through coordination of three disciplines: ICT Security, Law and Risk management. Legal informatics complexity and technical implementations of unlawful acts create a new concept of informative system protection: Digital Business Security. The discipline merges Security, Law and Management aptitudes in a single expert professional – the Computer Forensics and Law Advisor – in order to have corporate compliance and performance. A lot of IT-Corporate questions show Digital Business Security profiles, first Digital Privacy.

Parole chiave: Informatica Giuridica per le aziende, *Computer Forensics*, *Privacy* Digitale, *ICT Security*, *Risk management*, Crittografia, *Digital Business Security*.

Articolo pervenuto il 16 Febbraio 2017, approvato il 20 Marzo 2017

1. *Legal Informatics, Information Technology* e *Business*

L'Informatica pervade il Diritto provocandone mutamenti[1], anche altre "sfere della vita pratica"[2] presentano però influssi informatici, cui necessitano estensioni d'applicazioni informatico giuridiche e forensi oppure l'elaborazione di nuove soluzioni tecnico-giuridiche. Tra queste la sfera economica, in particolare il campo aziendale e professionale, in altre parole il *Business*. Con questo termine si vuole intendere l'insieme d'elementi, personali, materiali ed intellettuali che consentono d'ottenere vantaggi economici per la produzione di un bene o la prestazione di un servizio, cui possono far parte Aziende, piccole-medie-grandi, Enti privati e pubblici, con o senza fini di lucro, Liberi Professionisti e *Manager*.
L'ambito aziendale ha visto aumentare l'impatto delle tecnologie informatiche: dalla mera elaborazione dei dati legata alla fatturazione sino alla gestione del *Business* attraverso *email* e sistemi informatici[3]. Tanto la Società dell'Informazione ha tramutato le informazioni da materiale grezzo a raffinato[4], quanto ha contribuito ad evolvere i problemi del *Business*, da questioni legate alla produzione di beni o servizi a questioni inerenti le informazioni tecnico-giuridico-economiche[5]. Sono di dominio pubblico le molteplici vertenze circa gli illeciti utilizzi di informazioni aziendali tra cui spiccano lo spionaggio industriale nel campo del *design* e dei nuovi progetti tecnologici, il caso *Apple vs. Samsung* può esserne l'emblema[6]. Le attività sono spesso effetto d'accessi illeciti o abusivi a sistemi informatici e della fruizione non consentita di flussi di dati veicolati via *Internet*, senza escludere la sottrazione di dati operata da soggetti interni all'ente o attraverso tecnologie digitali di tipo fisico, quali le memorie di massa esterne o la sottrazione di fascicoli[7]. Da una necessità produttivo-amministrativa, dunque, l'informatica aziendale si è trasposta nello strumento fulcro della sicurezza informazionale interna ed esterna all'ente, in *Digital Business Security*, disciplina che pone le sue radici nell'Informatica, nel Diritto e nell'Amministrazione aziendale.

---

1 Cfr. G. Sartor, *Corso di informatica giuridica*, Giappichelli, Torino 2018, pp. 12 ss.

2 F. Viola, G. Zaccaria, *Diritto e interpretazione*, Laterza, Roma-Bari 2014, p. 3.

3 Cfr. P. E. Ceruzzi, *A history of modern computing*, MIT, Chicago 2003, pp. 109 ss; G. Mangia, *Lo sviluppo dei sistemi informativi nelle organizzazioni. Teoria e casi*, Franco Angeli, Milano 2005, pp. 11 ss.

4 Cfr. G. O. Longo, *Il nuovo Golem*, Laterza, Roma-Bari 1998, pp. 27 ss.

5 Cfr. F. Miotto, *I sistemi informativi in azienda. Teoria e pratica*, Franco angeli, Milano 2001, pp. 123 ss; P. Galdieri, C. Giustozzi, M. Strano, *Sicurezza e Privacy in Azienda*, Apogeo, Milano 2001, pp. 1 ss.

6 Cfr. M. Hitt, R. Ireland, R. Hoskisson, *Strategic management*, Hitt, Ireland & Hoskisson, USA 2014, pp. 119 ss.

7 Cfr. AA.vv., *Hack Proofing*, McGraw-Hill, Milano 2002, pp. 131 ss; F. Novario, *Linux USB Live System's Forensics Analysis: KALI Tools and Hacking Tricks*, in *eForensics Magazine*, dicembre 2013.

2. Evoluzioni tecnico-giuridiche quali fonti del *Digital Business Security*

L'Informatica ha subito una peculiare evoluzione tecnico-giuridica cui è conseguenza la nascita del *Digital Business Security*. Nata negli anni '40 come disciplina accademica per applicazioni matematiche attraverso tecnologie meccaniche[8], la grande potenzialità archiviale dell'informatica è stata piegata dagli anni '70-'80 alle necessità del *Business* attraverso l'automazione dei trattamenti di dati mediante grandi elaboratori e *personal computer*[9]. La nascita delle reti di connessione tra elaboratori ha presentato un ulteriore momento evolutivo che ha migliorato le prestazioni professionali e la condivisione dei dati[10], nonché favorito la creazione di database e sistemi informativi aziendali complessi, associati a necessari nuovi approcci alla sicurezza aziendale. L'apporto della sicurezza informatica, c.d. *ICT Security*, insieme di tecniche, principi e prassi senzienti l'intera evoluzione tecnica del mezzo digitale, è stata a sua volta oggetto di evoluzioni tecnico-aziendali. Da un iniziale approccio alla sicurezza di tipo *fisico*, dove l'elaboratore poteva considerarsi difeso attraverso il suo isolamento, la sicurezza informatica è divenuta di tipo *connettivo*, poiché da qualunque elaboratore connesso ad una rete sarebbe stato possibile disporre atti illeciti su altri elaboratori connessi. L'avvento dell'interazione globale degli elaboratori, il fenomeno *Internet*, ha implicato l'elaborazione di un differente, e più alto, coefficiente di sicurezza: si è giunti così alla sicurezza informatica di tipo *digitale*, consistente nella creazione d'elementi *software-hardware* a tutela dei sistemi e in sviluppi logico-matematici per la crittazione dei flussi di dati[11]. L'evoluzione della sicurezza informatica non è riuscita a tramutare l'informatica in una scienza tecnologica completamente sicura, rappresentando però un importante deterrente per l'utilizzo abusivo e illecito di dati.

L'evoluzione tecnica informatico-aziendale è stata coadiuvata, quanto stimolata, da interventi giuridici, in particolare la legiferazione di normative nazionali ed internazionali per la tutela dei dati e dei sistemi[12]. Tra queste possono essere annoverate leggi circa la tutela del *software* e delle banche dati[13], in materia di *Privacy* e trat-

---

[8] Cfr. A. Turing, *On computable numbers, with an application to the Entscheidungsproblem*, in *Proc. London Math. Soc.* 1936, 42, pp. 230 ss; A. Turing, *Intelligenza Meccanica*, Bollati Boringhieri, Torino 2004, p. 29 ss.

[9] Cfr. F. Miotto, *I sistemi informativi in azienda. Teoria e pratica*, Franco angeli, Milano 2001, pp. 25 ss.

[10] Cfr. P. E. Ceruzzi, *A history of modern computing*, MIT, Chicago 2003, pp. 357 ss; D. E. Comer, *Computer Networks and Internets, with Internet Applications*, Pearson Education, New Jersey 2001, pp. 1 ss.

[11] *Firewall* e *antivirus,* nonché il *tunneling* e le reti di dati dedicate. Cfr. AA.vv., *Hack Proofing*, McGraw Hill, Milano 2002, pp. 16 ss. - 20 ss. e pp. 530 ss.

[12] Cfr. S. Amore, V. Stanca, S. Staro, *I Crimini informatici*, Halley, Matelica 2006, pp. 1 ss; B. Hlubik Schell, C. Martin, *Cybercrime: a reference handbook*, ABC Clio, California 2004, pp. 1 ss.

[13] Cfr. M. G. Jori, *Diritto, Nuove tecnologie e comunicazione digitale*, Giuffrè 2013, pp. 4 ss, 55 ss.

tamento dei dati[14], nonché la Responsabilità Amministrativa degli Enti[15]. Dal primo atto illecito "digitale" acclarato, tradizionalmente ricondotto ad un'infezione virale digitale accaduta nella seconda metà degli anni '80[16], l'attenzione del legislatore si è alternativamente concentrata sull'obbligo di sicurezza dei sistemi e sulla repressione degli illeciti. Questa duplice attitudine legislativa ha mostrato importanti riflessi giudiziali, quanto informatici ed aziendali. Sotto un profilo informatico giuridico, infatti, la creazione e configurazione dei Sistemi Informativi aziendali si è evoluta: dal mero sviluppo di Sistemi Informativi ci si è orientati alla creazione di Sistemi Informativi sicuri, poi giuridicamente corretti e, ad oggi, tali da consentire la loro accertabilità attraverso attività investigative producibili in giudizio quali elementi digitali di prova. Quest'ultimo tassello è cuore e anima del *Digital business Security*.

3. Il *Digital Business Security*

Il *Digital Business Security* è un'attitudine multidisciplinare che pervade il *Business*. Un bilanciamento, aderente e dipendente dal caso concreto, di diversi elementi: previsioni di Legge, tecnicità Informatica, necessità Giudiziali, esigenze performative di Sistemi Informatici e Sicurezza. Consta di una complessa amalgama tra aree aziendali – amministrazione, produzione, informatica e ufficio legale – il cui scopo è radicare e sviluppare una cultura della Sicurezza. Leggi nazionali ed internazionali, nonché ragioni informatiche ed aziendali, impongono *standard* di sicurezza performanti e differenti a seconda degli ambiti lavorativi[17]. Non deve essere solo e concreto rispetto delle normative lo scopo dell'ente, bensì la reale sicurezza del proprio *business*, fondata sulle norme di legge ma atta ad una performante ottimizzazione dei risultati. Solo una gestione armonica della sicurezza, associata alle esigenze giuridiche, informatiche e manageriali d'azienda può raggiungere reali e alti livelli di *performance*. Questo tipo di gestione presenta profili tecnici, culturali ed aziendali distinti, difficili da amalgamare in realtà aziendali di grandi dimensioni e ad organizzazione complessa, fondati sulla fusione di *know-how* giuridico, informatico e aziendale, al fine di disporre attività di sicurezza, prevenire attività illecite o digitalmente pericolose e consentirne la prova in giudizio. La concentrazione in un'unica disciplina di tre

---

[14] Cfr. S. Rodotà, *Il mondo nella rete. Quali diritti, quali vincoli*, Laterza, Roma-Bari 2014; R. Razzante, *Manuale di diritto dell'informazione e della comunicazione. Privacy, diffamazione e tutela della persona. Libertà e regole nella rete*, Cedam, Padova 2014.

[15] Cfr. M. Levis, A. Perini, *La responsabilità amministrativa delle società e degli enti*, Zanichelli, Bologna 2014.

[16] Cfr. h*ttp://archiviostorico.corriere.it/2011/gennaio/21/primo_virus_per_arrivo_anni_co_10_110121020.shtml*

[17] Cfr. M. De Cata, *La responsabilità civile dell'internet service provider*, Giuffrè, Milano 2010, pp. 1 ss; P. Bontempi, *Diritto Bancario*, Giuffrè, Milano 2009, pp. 1ss., L. McCarthy, *IT security: risking the corporation*, Prentice Hall, New Jersey 2003, pp. 20 ss; *http://www.symantec.com/index.jsp*; *http://www.mcafee.com*; *http://www.rsa.com/*.

attitudini differenti è necessaria quanto complessa: l'osservazione dalla sola prospettiva giuridica, informatica od economica può infatti portare ad una parziale soluzione delle questioni problematiche. L'osservazione globale dei molteplici profili di sicurezza del *business* digitale, invece, consente, pur non garantendo un assoluto risalutato, di meglio ponderare cause ed effetti delle misure tecniche, giuridiche ed aziendali, da disporre o già disposte, attraverso una dialettica tra le aree aziendali, atta allo sviluppo di policy coerenti, corrette e concrete.
Oggetto principale del *Digital Business Security* è la Sicurezza, in quanto conoscenza che l'evoluzione di un sistema non produrrà effetti indesiderati, cui è eco la c.d. "scienza della sicurezza", disciplina che studia il rischio nelle sue varie forme con l'obiettivo di ridurlo, fino ad annullarlo o controllarne le conseguenze attraverso il c.d. Rischio residuo[18]. La scienza della sicurezza si fonda su tre concetti: *safety*, incolumità della persona; *security*, sicurezza delle informazioni; *emergency*, misure da porre in essere in caso di fallimento di *safety* e *security*. L'applicazione di tecniche e prassi di sicurezza prende le mosse da due momenti tecnico-giuridici: 1) Analisi del rischio, da svolgersi attraverso attività d'osservazione, *audit* e elaborazioni statistiche; 2) Percezione del rischio, concernente la sua individuazione e consapevolezza da parte dell'ente, dei suoi dipendenti e dei collaboratori[19]. Il raggiungimento della sicurezza consta nell'applicazione d'un c.d. "ciclo virtuoso", composto da alcuni momenti tecnico-giuridici: 1) *Analisi*, studio legislativo, normativo, ambientale, personale, professionale, delle attività e dei processi; 2) *Misure*, attive e passive, strutturali, amministrative o disciplinari, di tipo preventivo o protettivo; 3) *Gestione*, al fine di mantenere viva la sicurezza attraverso studi, aggiornamenti, formazione, piani di sicurezza, adeguamenti[20]. Gli strumenti suindicati sono il fondamento del *Digital Business Security* e del suo scopo: la disposizione di tutele digitali di tipo preventivo per ridurre i rischi di violazione dei Sistemi Informativi attraverso il rispetto di *policy* legali, informatiche ed aziendali, alzando il livello di rischio residuo e consentendone una migliore circoscrizione attraverso controlli di sicurezza e possibilità di far valere le proprie ragioni in sede giudiziale. Quest'ultima attitudine è centrale non soltanto per quanto concerne le violazioni subite attraverso tecniche di *hacking* e *cracking*, ma anche per la mostrazione della corretta e coerente strutturazione dei sistemi informativi.

---

[18] Cfr. P. Slovic, *The Psychology of Risk*, in *Saude e Sociedade*, 19/2010, 4, pp. 731 ss.

[19] Cfr. A. Crescentini, A. Sada, L. Giossi (a cura di), *Elogio della sicurezza: tra scienza e pratica*, in Vita e pensiero, Milano 2007, pp. 111 ss; S. Dohle, C. Keller, M. Siegrist, *Examining the Relationship between affect and implicit association: Implications for risk perception*, in *Risk analisys*, 30, 7/2010, pp. 1116 ss.

[20] Cfr. F. Novario, *Computer Forensics – tra Giudizio e Business*, Cortina Torino, Torino 2012, pp. 162 ss.

4. La *Computer Forensics* Aziendale e il Consulente Informatico Giuridico e Forense

La disposizione di *policy* di *Digital Business Security*, e loro violazioni, possono essere oggetto di cristallizzazione in copie forensi dei dati, che consentono l'osservazione *in vitro* delle dinamiche digitali svolte sugli elaboratori[21]. Se ritualmente acquisite e assunte nel processo, l'analisi di suddette copie può fornire elementi di prova relativi ai sistemi informativi. Le tecniche *forensics*, generalmente disposte da Forze dell'Ordine a fatto illecito digitale acclarato[22], possono anche essere disposte dalle aziende, attraverso professionisti, e indipendentemente dalla formalizzazione di notizie di reato, allo scopo di ricerca d'elementi di rischio per la sicurezza o per controlli sulla correttezza del trattamento digitale dei dati. Le attività, che vedono la disposizione di tecniche di *Corporate Computer Forensics*[23], generalmente, non possono essere disposte da dipendenti della stessa azienda per motivi giuslavoristici, in particolare la necessità di un contratto di lavoro *ad hoc* comprendente come onere la difesa dell'ente in giudizio, nonché processuali, per il minor valore probatorio in sede giudiziale delle attività svolte. Le tecniche *forensics* devono essere disposte attraverso attività d'indagine preventive e difensive e la nomina di un Consulente Tecnico Informatico Giuridico e Forense. La loro valenza probatoria è elemento importante e ampiamente trattato dalla dottrina[24], la loro attitudine al perfezionamento dei Sistemi Informativi aziendali, invece, è una nuova attitudine che deve essere meglio esplicata. La cristallizzazione dei dati in copie forensi consente di poterne osservare il trattamento digitale e le violazioni, attraverso le ricostruzioni effettuate dal consulente, a fini di miglioramento delle *performance* di sicurezza e di modificazione delle infrastrutture informatiche.

Gli importanti riflessi delle attività di *Corporate Computer Forensics*, nonché le tutele del *Digital Business Security*, possono essere disposte da una nuova figura aziendale di tipo libero professionale: il Consulente Informatico Giuridico e Forense. Le tecniche forensi digitali implicano il coinvolgimento da parte dell'ente di un tecnico-giurista, a fini tanto informatici quanto probatori. La fase d'analisi dei dati, successiva a quella d'acquisizione, rappresenta il momento più complesso dell'attività

---

[21] F. Novario, *Le prove informatiche nel processo civile*, Giappichelli, Torino 2014, pp. 17 ss – 260 ss; F. Novario, *Prove penali informatiche*, Libreria Cortina Torino, Torino 2011, pp. 21 ss.

[22] Cfr. A. Ghirardini, G. Faggioli, *Digital Forensics*, Apogeo, Milano 2013, pp. 9 ss.

[23] Cfr. L. Lupària, G. Ziccardi, *Investigazione penale e tecnologia informatica*, Giuffrè, Milano 2007, pp. 89 ss.

[24] Cfr. F. Novario, *Le prove informatiche nel processo civile*, Giappichelli, Torino 2014; F. Novario, *Le prove informatiche*, in P. Ferrua, E. Marzaduri, G. Spanger, *La prova penale*, Giappichelli, Torino 2013, pp. 121 ss; G. Vaciago, *Digital Evidence*, Giappichelli, Torino 2012; F. Novario, *Prove penali informatiche*, Cortina Torino, Torino 2011; L. Luparia, *Sistema penale e criminalità informatica*, Giuffrè, Milano 2009; L. Lupària, G. Ziccardi, *Investigazione penale e tecnologia informatica*, Giuffrè, Milano 2007.

consulenziale, consentendo una ricostruzione spazio-temporale degli eventi digitali dell'elaboratore, garantendo la non manipolazione dei dati originali e la fidefacienza dei dati analizzati in copia. La delicata fase tecnico-giuridica deve essere intesa come atto corale dell'intera struttura aziendale, al fine di ridurne i tempi e favorire la corretta disposizione tecnica mediante il passaggio di *know-how* dalle aree aziendali al Consulente, che dovrà comunque effettuare una completa osservazione dei luoghi digitali. Le peculiarità del *Digital Business Security* mettono in evidenza le attitudini della consulenza Informatico Giuridica e Forense: competenza tecnica e giuridica, interdisciplinarietà, attitudine al coordinamento e alla gestione di progetti/gruppi di lavoro. Queste tramutano il Consulente nel fulcro delle operazioni di sicurezza digitale aziendale, senza per altro intaccare l'operato, le competenze e la responsabilità di uffici legali e responsabili IT aziendali. Il consulente non è né un puro giurista né un puro tecnico informatico, è una figura "ibrida", in grado di svolgere un'osservazione informatico-giuridica preliminare, così da consentire a legali e tecnici una migliore comprensione delle questioni problematiche, riservandosi l'eventuale attività di *Problem Solver* qualora necessario e richiesto.

5. Attività tecnico-giuridiche del *Digital Business Security*

L'apporto informatico giuridico, proprio dell'analisi dei sistemi, risulta elemento secondario rispetto all'apporto informatico forense, che garantisce la corretta acquisizione degli elementi di prova per la loro produzione in giudizio. L'acquisizione di elementi digitali può svolgersi su qualunque tipo di elaboratore, *client* o *server*, attraverso copia fisica o logica dei dati: *disk to disk* o via rete[25]. L'operazione tecnica possiede generalmente una caratura "straordinaria", presentando reali elementi di rischio. In ambito giudiziale, il carattere straordinario delle operazioni di *Computer Forensics* è implicato dall'estraneità degli inquirenti all'ambiente investigativo digitale. In ambito aziendale, invece, la straordinarietà è un mero rischio, che può essere annullato, o contenuto, considerando le attività tecniche come "ordinarie". La costante disposizione di tecniche *forensics* sui sistemi informatici aziendali, a fronte di adattamenti tecnico-giuridici, può consentire un nuovo corso nello sviluppo dei Sistemi Informativi, sotto il profilo *hardware* e *software*. Elementi essenziali da inserire e sviluppare nelle infrastrutture informatiche aziendali sono: 1) Tecnologie di *Write Block*, al fine di scongiurare l'alterazione dei dati; 2) L'uso di *software forensics* compatibili con i sistemi operativi e informativi; 3) La gestione accentrata e sicura di *password* e credenziali di sicurezza dei sistemi; 4) Le modalità di gestione dei *log* riconducibili a *computer server* e *client*.

[25] Cfr. A. Ghirardini, G. Faggioli, *Computer Forensics*, Apogeo, Milano 2007, pp. 45 s. e pp. 69 ss.

L'importante profilo d'indipendenza del Consulente Informatico Giuridico e Forense, sotto il profilo giuslavoristico e consulenziale, si arricchisce di un ulteriore dettaglio: il delicato bilanciamento tra la tutela dell'ente e la segretezza degli elementi di prova rinvenuti. Il consulente dispone attività per il rinvenimento di elementi di prova e la comunicazione di notizie di reato alle Autorità, nonché per la tutela dalle violazioni di dati o del loro trattamento. Tanto può essere importante la rilevanza giuridica e giudiziale di elementi rinvenuti, quanto, spesso, può essere essenziale la volontà dell'azienda di sottacere eventi lesivi la sua immagine pubblica: ad esempio deficit di *ICT Security* o vulnerabilità dei Sistemi Informativi. L'analisi informatico giuridica aziendale dei dati può far emergere responsabilità sia di terzi sia dell'ente, a fronte delle prerogative digitali dell'Archivio Informatico, che tutto ritiene e difficilmente oblia[26]. Qualora i dati implichino responsabilità dell'ente, ai fini di una performante tutela giuridica, è possibile disporre non già l'occultamento dei dati bensì una strategia d'inazione giuridica e giudiziale. Questa consente, attraverso una decisione armonica di *management*, ufficio legale e Consulente, di non portare a conoscenza delle Autorità atti che potrebbero danneggiare l'ente, senza per altro procedere alla loro distruzione e senza violare leggi vincolanti la comunicazione di illeciti o la produzione di prove, provvedendo invece a sanare la lacuna tecnico-giuridica. Sotto quest'aspetto, i dipendenti dell'ente sono vincolati da un mero "segreto aziendale", mentre il Consulente è soggetto ad un "segreto professionale", con un più profondo coefficiente di riservatezza, che nasce dal tipo di rapporto lavorativo – indipendente e di tipo libero professionale – tale da garantire l'ente da eventuali fughe di notizie inopportune.

6. *A Digital Business Security case study*: Digital Privacy

Il *Digital Business Security* ha ricadute concrete in molti ambiti aziendali, giuridici e informatici, in particolare per quanto concerne la gestione dei dati personali, ex Codice Privacy. Il substrato giuridico della Privacy Digitale è ravvisabile nelle direttive 95/46/CE e 2002/58/CE[27], e per il territorio italiano principalmente nel d.lgs. 196/2003, "Codice della Privacy"[28]. Quest'ultimo si presenta come una disciplina organica per l'acquisizione, la gestione e la custodia dei dati inerenti persone fisiche, tale da consentirne il corretto trattamento secondo la classificazione disposta nel d.lgs. all'art. 4. In via generale: dati personali, sensibili e c.d. supersensibili[29].

---

[26] F. Novario, *Computer Forensics – tra Giudizio e Business*, Cortina Torino, Torino 2012, pp. 24 ss.

[27] Cfr. R. Wacks, *Privacy: A Very Short Introduction*, Oxford University Press, Oxford 2010, pp. 51 ss.

[28] Cfr. N. Arnaboldi, *Codice della privacy e DPS*, Giuffrè, Milano 2010.

[29] Cfr. D. Giannini, *L'accesso ai documenti*, Giuffrè, Milano 2013, pp. 113 ss; E. Casetta, *Manuale di*

Ex art. 7 d.lgs. 196/2003, il trattamento dei dati si fonda su un'architettura "quadro" secondo cui l'interessato, cioè il soggetto cui si riferiscono i dati, possiede il diritto di conoscere l'origine, le finalità e le modalità di trattamento, nonché il titolare, i responsabili e le persone che possono venire a conoscenza dei dati. Ha diritto altresì all'aggiornamento dei dati, alla loro cancellazione e può opporsi al loro trattamento. I diritti e le modalità di gestione dei dati sono oggetto di un'informativa che il titolare del trattamento deve portare a conoscenza del soggetto interessato, salvo particolari casi[30], in forma orale o scritta a seconda dei tipi di dati, e che deve essere accettata esplicitamente. Ex art. 13 e 141 ss d.lgs. 196/2003, la violazione delle indicazioni di legge apre a sanzioni amministrative e, se dall'illecito trattamento deriva danno, anche civili e penali. L'illiceità del trattamento dei dati è fondata ad oggi non solo sulle violazioni formali alle regole del Codice della Privacy, ma anche su anomali processi digitali di trattamento dei dati.
Con il termine "trattamento", ex art. 4 d.lgs. 196/2003, deve essere inteso "qualunque operazione o complesso di operazioni, effettuate anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in banche dati". Il trattamento rappresenta dunque qualunque manipolazione, fisica ed informatica, dei dati da parte del titolare, del responsabile o degli incaricati. Le operazioni "tecniche" sono garantite attraverso la prescrizione di "misure di sicurezza", presenti nel Codice della *Privacy* all'art. 31 s. e nell'allegato B "Disciplinare tecnico in materia di misure minime di sicurezza". I dati personali devono essere oggetto di custodia e controllo, secondo gli sviluppi del progresso tecnologico, la natura dei dati e le caratteristiche del trattamento, in modo da ridurre al minimo errori, perdite e illeciti utilizzi di dati, attraverso l'adozione di preventive misure di sicurezza. Il trattamento dei dati attraverso strumenti elettronici non può prescindere da alcuni elementi cardine: 1) Presenza d'autenticazione informatica; 2) Procedure di gestione delle credenziali d'autenticazione; 3) Sistema d'autorizzazione; 4) Aggiornamento periodico di incaricati al trattamento e addetti a gestione o manutenzione; 5) Protezione di strumenti elettronici e dati; 6) Procedure di custodia per copie di sicurezza; 7) Processi per il ripristino dei dati e dei sistemi; 8) Adozione di cifratura o codici identificativi per determinati trattamenti di dati[31].

diritto amministrativo, Giuffrè, Milano 2011, pp. 460 ss.

[30] Trattamento dati a scopo statistico, storico e scientifico ex art. 24 ss. d.lgs. 196/2003.

[31] Cfr. N. Arnaboldi, *Codice della privacy e DPS. Flussi processuali*, Giuffrè, Milano 2010, pp. 27 ss.

6.1 *Privacy* Digitale: tra Sicurezza, Crittografia e *Computer Forensics*

Il d.lgs. 196/2003, all'art. 31, subordina il corretto trattamento dei dati "anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento", mentre all'art. 34 subordina "solo" particolari tipi di dati sanitari all'adozione di tecniche di cifratura o di codici identificativi. L'adozione della crittografia non può considerarsi limitata al solo ambito di dati di tipo sanitario, può altresì essere utilizzata a protezione dei dati in base alle necessità del caso concreto. La crittografia, unione delle parole κρυπτός (nascosto), e γραφία (scrittura), è una disciplina che ha ad oggetto l'offuscamento dei messaggi, attraverso cifratura con chiavi simmetriche o asimmetriche[32], nonché certificati digitali in caso di crittazione informatica[33], al fine di non renderli comprensibili a soggetti non autorizzati[34]. Le tecniche di crittografia sono oggi considerate elementi propri della sicurezza dei Sistemi Informativi e delle comunicazioni, per la garanzia del trasferimento e conservazione di dati[35]. La crittazione informatica è il più sicuro metodo di custodia dei dati, nonostante possa presentare profili di rischio qualora sia smarrita o non utilizzabile la chiave di decrittazione: i dati risulterebbero, infatti, irrimediabilmente persi. A tutela dell'eventualità, ex art. 22-34 d.lgs. 196/2003 e art. 23 ss allegato B, è necessario che i titolari del trattamento sviluppino e dispongano concrete procedure per il *backup* dei dati e il loro ripristino. Gli stessi *backup*, qualora necessario, potrebbero però essere oggetto di crittazione a fini di sicurezza: tautologia tecnico-giuridica inevitabile quanto risolvibile attraverso un ragionamento informatico giuridico e forense. Il Codice della *Privacy* è teso ad impedire indebite influenze nella sfera personalissima dei soggetti, attraverso l'oscuramento di dati comuni, personali e sensibili. I dati oscurati devono subire un trattamento performante, implicando rischi di divulgazione e perdita dei dati scongiurati dalla disposizione di procedure di sicurezza e *backup*. Lo scopo fondante la tutela della *Privacy* è però la non divulgazione di alcuni tipi di dati, piuttosto che il loro mantenimento in archivi e copie di *backup*. Qualora infatti un dato sia perso, è generalmente possibile richiederlo a enti o al soggetto interessato. Qualora invece un dato risulti sottratto, diviene impossibile riottenerne la segretezza. La crittazione dei dati fornisce dunque una tecnica performante ex d.lgs. 196/2003 anche qualora la chiave di decrittazione sia persa, secretando i dati in via definitiva e impedendone la divulgazione.
La disposizione di strumenti per la crittazione dei dati influenza in modo non marginale la disposizione di tecniche *forensics* digitali: raramente, qualora non in pos-

[32] Cfr. A. De Rosa Cattello, *Sistemi di cifratura*, Maggioli, Santarcangelo di Romagna 2009, pp. 13 ss.

[33] Cfr. Jon Erickson, *L'arte dell'hacking*, II, Apogeo, Milano 2009, pp. 193 ss.

[34] Cfr. A. Languasco, A. Zaccagnini, *Introduzione alla crittografia*, Hoelpi, Milano 2004, pp. 89 ss; N. Ferguson, B. Shneiner, *Crittografia pratica*, Apogeo, Milano 2005, pp. 17 ss.

[35] Cfr. A. De Rosa Cattello, *op.cit*, Maggioli, Santarcangelo di Romagna 2009, pp. 13 ss.

sesso di chiavi di decrittazione, è possibile svolgere indagini informatico giuridiche e forensi sui dati crittati[36]. Considerando però le attività di *Computer Forensics* quali procedure ordinarie di *Digital Business Security*, il rischio di un difficoltoso accertamento tecnico digitale può essere ridotto. Attraverso *policy* e strutture tecnico-informatiche è possibile pianificare e sviluppare procedure atte al *bypass* del sistema crittografico. In particolare, mediante la conservazione sicura delle credenziali d'accesso o l'elaborazione di procedure celate e parallele per la decrittazione, è possibile garantire profondi profili di sicurezza associati a performanti sistemi di ripristino dei dati e attività *forensics*. Lo sviluppo di Sistemi Informativi e *policy* attraverso linee guida Informatico Giuridiche e Forensi possono rendere coerente giuridicamente, e concreto informaticamente, il trattamento dei dati soggetti a tutela della *privacy*, attraverso una commistione di: sicurezza, via crittazione digitale; controllo, via attività *forensics*; sviluppo/configurazione dei sistemi, via indicazioni informatico giuridiche.

7. Conclusioni

Il *Digital Business Security*, attraverso la nuova figura professionale del Consulente Informatico Giuridico e Forense, possiede importanti riflessi tanto aziendali quanto difensivi. L'effetto trasversale l'intera attività aziendale che tange qualunque settore, dalla produzione di beni alla fornitura di servizi, permette di considerare la sicurezza digitale del *business* come un nuovo elemento essenziale l'economia moderna, non tanto quale servizio reso alle aziende, ma quale possibilità, per queste ultime, di ottimizzare le loro *performance* attraverso la configurazione e lo sviluppo di sistemi informatici rispettosi delle norme di legge e delle migliori regole tecnico-informatiche, atte all'armonizzazione delle aree aziendali e alla loro collaborazione/coordinazione.

[36] Cfr. G. Consalvo, *Perizia informatica 2.0 – metodi e strumenti per al computer forensics*, *http://books.google.it/books?id=gK_jAgAAQBAJ&pg=PA105&dq=computer+forensics+cifratura&hl=it&sa=X&ei=vFexU_T7JsOV7Aah_YDADg&ved=0CCgQ6AEwAA#v=onepage&q=computer%20forensics%20cifratura&f=false*, pp. 105 ss.

Rivista elettronica di Diritto, Economia, Management

N. 1 - 2017 · pp. 59-70

Le prove informatiche nel contesto aziendale

Filippo Novario

Abstract: La totale informatizzazione dei processi aziendali, di enti pubblici e privati, implica un'importante rilevanza delle prove informatiche a fini d'indagine e tutela giudiziale. Le infrastrutture aziendali digitali e telematiche si presentano complesse, difficili da difendere e scarsamente orientate all'accertamento dei fatti. L'approfondimento delle attitudini proprie della *Computer Forensics* – disciplina atta all'acquisizione, custodia e analisi dei dati con rilevanza giuridica e giudiziale – associata alle dinamiche informatiche degli enti e ai loro sistemi informativi, consente una maggiore tutela sotto i profili informatico, giuridico e probatorio. Attraverso la comprensione di modi, luoghi e tempistiche per il reperimento delle prove informatiche in azienda è possibile addivenire a differenti soluzioni informatico giuridiche: dall'elaborazione di prassi e processi per l'acquisizione *forensics* dei dati alla strutturazione di sistemi informativi "*forensics by design*".

Public and private companies computerization imply needs of corporate digital evidence, for investigative and judicial reasons. Digital and telematics corporate structures, therefore, are complex, difficult to defend and not oriented to ascertain happened facts. Focusing Computer Forensics aptitudes - discipline for data acquisition, custody and analysis with juridical and judicial relevance - linked to corporate informatics dynamics and informative systems, it can confer a strong safeguard in the fields of ICT, law and proof in court. Through the comprehension of ways, places and timing to obtain digital evidence in companies, we can have different Legal Informatics solutions: from the develop of praxis and process to the data forensics acquisition in order to develop corporate informative systems "forensics by design".

Parole chiave: Informatica Giuridica per le aziende, Prove informatiche, *Computer Forensics*, *ICT Security*, Consulente Tecnico.

Articolo pervenuto il 16 Febbraio 2017, approvato il 20 Marzo 2017

1. Introduzione

L'Informatica è sempre più addentro alle dinamiche aziendali per l'ormai totale gestione di dati e informazioni attraverso sistemi informatici. La digitalizzazione delle informazioni aziendali prende le mosse dalle alte performance di gestione informatica quanto da alcune prescrizioni di legge, ultime in ordine di tempo la fatturazione elettronica per la liquidazione di crediti verso le PA e la Conservazione sostitutiva dei documenti fiscali[1]. La dematerializzazione delle informazioni, a fronte di agevolazioni nella gestione dei dati, è altresì fonte di questioni problematiche: su tutte la sicurezza dei dati[2]. Questa mostra profili di inevitabilità - è di pubblico dominio come sia impossibile ottenere e sviluppare una soluzione digitale completamente sicura - che possono essere mitigati attraverso approcci informatico giuridici e forensi, *in primis* legati ad attività giudiziali ma anche stragiudiziali, nonché preventive. Elemento tecnico-giuridico trasversale a qualunque approccio sono le prove informatiche, quale attività tecnica atta al rinvenimento di evidenze rilevanti giuridicamente e giudizialmente[3] per questioni aziendali concrete. Substrato informatico giuridico aziendale, concetto di *Digital Forensics*, effetti aziendali informatico giuridici e forensi, selezione del consulente/*advisor*, sono questioni fondanti per una piena comprensione del fenomeno delle prove informatiche in azienda e una concreta tutela di informazioni, dati e sistemi informativi aziendali..

2. Informatizzazione aziendale: sicurezza, diritto e prova

L'Informatica ha subito una peculiare evoluzione tecnico-giuridica. L'*ICT* vede la genesi della sua moderna concezione negli anni '40, quale disciplina accademica sviluppata per applicazioni matematiche svolte concretamente attraverso tecnologie meccaniche[4]. Dagli anni '60 inizia la parabola aziendale dell'informatica, a fronte della sua grande potenzialità archiviale. Dalla potenzialità dei grandi computer dei

---

1 Cfr. M. Fiammelli, *La fattura elettronica alla PA*, Maggioli Editore, Santarcangelo di Romagna 2014. *http://www.fatturapa.gov.it/export/fatturazione/it/index.htm*; *http://www.agid.gov.it/agenda-digitale/pubblica-amministrazione/conservazione*

2 Cfr. C. Gallotti, *Sicurezza delle informazioni: valutazione del rischio; i sistemi di gestione per la sicurezza delle informazioni; la norma ISO/IEC 27001:2013*, Ebook 2014, 101 ss.

3 Cfr. F. Novario, *Prove informatiche nel processo civile*, Giappichelli, Torino 2014, pp. 17 ss; F. Novario, *Prove penali informatiche*, Cortina Torino, Torino 2011, pp. 16 ss

4 Cfr. A. Turing, *On computable numbers, with an application to the Entscheidungsproblem*, in *Proc. London Math. Soc.* 1936, 42, pp. 230 ss; A. Turing, *Intelligenza Meccanica*, Bollati Boringhieri, Torino 2004, p. 29 ss.

primi anni, orientati alla gestione di dati e *database*, i cd. *Mainframe*, si è passati negli anni '70 e '80 all'automazione dei trattamenti di dati mediante elaboratori, c.d. *Midrange*, e *personal computer*[5]. La nascita delle reti di connessione tra elaboratori ha fornito un ulteriore momento evolutivo della tecnologia, tale da migliorare le prestazioni professionali e la condivisione dei dati[6], favorendo la creazione di database e sistemi informativi aziendali complessi e interconnessi. Il momento connettivo, attraverso i suoi profili positivi, di gestione dei dati, e negativi, di vulnerabilità degli stessi durante il loro trasferimento, ha comportato la nascita di un nuovo approccio alla sicurezza aziendale: la Sicurezza Informatica. La c.d. *ICT Security* - insieme di tecniche, principi e prassi senzienti l'intera evoluzione tecnica del mezzo digitale[7] - è stata a sua volta oggetto di evoluzioni tecnico-aziendali. Da un iniziale approccio alla sicurezza di tipo fisico, fondato sull'isolamento dell'elaboratore al fine di scongiurare accessi fisici indesiderati, la sicurezza informatica si è tramutata in connettiva, al fine di tutelare elaboratori e *computer* connessi in rete. Il fenomeno *Internet* ha reso centrale la questione della sicurezza connettiva aziendale, implicando un più alto coefficiente di sicurezza che si è espresso nella sua evoluzione allo stadio digitale, mediante la creazione di *software e hardware* a tutela dei sistemi nonché lo sviluppo logico-matematico di sistemi per la crittazione dei flussi di dati[8].
L'*ICT Security* non tramuta l'informatica in una scienza-tecnologica completamente sicura, rappresenta però un importante deterrente per l'utilizzo abusivo e illecito di dati. L'alea di rischio è oggetto di interventi giuridici, in particolare attraverso normative nazionali ed internazionali per la tutela dei dati e dei sistemi[9]. Dal primo atto illecito "digitale" acclarato, tradizionalmente ricondotto ad un'infezione virale digitale accaduta negli anni '80[10], l'attenzione del legislatore si è concentrata sia sull'obbligo di sicurezza dei sistemi sia sulla repressione degli illeciti. Questa duplice attitudine mostra importanti riflessi giudiziali, quanto informatici ed aziendali. Sotto un profilo informatico giuridico, infatti, la creazione e la configurazione dei Sistemi Informativi si è evoluta gradualmente: dal mero sviluppo di Sistemi Informativi si è passati alla creazione di Sistemi Informativi sicuri, poi giuridicamente corretti e, per ultimo, tali da consentire la loro accertabilità attraverso attività investigative, i cui risultati siano producibili in giudizio quali elementi digitali di prova. Quest'ultimo tassello è oggi il cuore dell'*ICT Security* aziendale, fondato su una disciplina tecnico-giuridica, fin ora, di interesse prettamente giudiziale: la *Computer Forensics*.

---

[5] Cfr. F. Miotto, *I sistemi informativi in azienda. Teoria e pratica*, Franco angeli, Milano 2001, pp. 25 ss.

[6] Cfr. P. E. Ceruzzi, *A history of modern computing*, MIT, Chicago 2003, pp. 357 ss; D. E. Comer, *Computer Networks and Internets, with Internet Applications*, Pearson Education, New Jersey 2001, pp. 1 ss.

[7] Cfr. C. P. Pfleeger, S. L. Pfleeger, *Security in computing*, Pearson Education, New Jersey 2003, pp. 1 s.

[8] *Firewall* e *antivirus,* nonché il *tunneling* e le reti di dati dedicate. Cfr. AA.vv., *Hack Proofing*, McGraw Hill, Milano 2002, pp. 16 ss. - 20 ss. e pp. 530 ss.

[9] Cfr. S. Amore, V. Stanca, S. Staro, *I Crimini informatici*, Halley, Matelica 2006, pp. 1 ss; B. Hlubik Schell, C. Martin, *Cybercrime: a reference handbook*, ABC Clio, California 2004, pp. 1 ss.

[10] Cfr. *http://archiviostorico.corriere.it/2011/gennaio/21/primo_virus_per_arrivo_ anni_co_ 10_110121020.shtml*

3. Prove digitali: la *Computer Forensics*

Dalla tecnicità informatica è possibile desumere l'oggetto delle prove informatiche: i dati, descrizioni elementari di cose o fatti, da soli o nel loro insieme rilevanti per il diritto[11]. Il dato è un componente *software*, necessariamente contenuto in componenti *hardware*, che possiede alcune caratteristiche: è digitale, è variamente rappresentabile ed è immateriale. In base a queste caratteristiche le prove informatiche possono essere classificate sotto diversi profili teorico-pratici. Riguardo al profilo tipologico queste sono riconducibili alla categoria delle prove tecniche e scientifiche, quali prove derivate dall'impiego di tecnologie informatiche[12]. Sotto il profilo del loro apporto probatorio, possono invece essere ricondotte nell'alveo delle cosiddette prove storiche: il dato risulta di per sé idoneo a rappresentare cose o fatti[13]. Sotto il profilo rappresentativo, possono altresì essere ricondotte alla categoria delle prove dirette: i dati recano atti compiuti da un utente, registrati e immagazzinati da programmi *software* in supporti *hardware*, dunque essi stessi fatti, seppur non immediatamente intelligibili poiché rappresentati in codice binario[14]. Sotto il profilo materiale, infine, l'essenza digitale del dato permette di ricondurre le prove informatiche alla categoria delle prove documentali: il dato infatti è un'informazione codificata in numeri, riconducibile al concetto di testo in quanto successione di simboli, anche se immateriale[15].

Le caratteristiche tecniche degli oggetti di prova informatici hanno una forte influenza sulla pratica investigativa e giudiziaria. I dati sono rappresentabili mediante diversi tipi di *file*: di registro, testuali, di immagine, multimediali, di programma, etc. La loro rilevanza probatoria può interessare un intero *file*, una porzione o un insieme di *file*. L'immaterialità del *software* impedisce una materiale individuazione del dato, anche se legato all'*hardware*, e ne rende facile la manipolazione. Queste caratteristiche comportano problemi giuridici legati all'individuazione dei dati, alla necessità di apprezzare il contenuto dei supporti *hardware* e all'instabilità dei contenuti *software*. Per ovviare a tali questioni l'*Information Technology* è stata asservita ai fini probatori, mediante la creazione di una disciplina informatico-giuridica in grado di far collimare esigenze di indagine, garanzie probatorie e tecnologia informatica: la *Computer Forensics*.

La *Computer Forensics*, o Informatica Forense[16], è la disciplina che studia il valore, inteso come resistenza alle contestazioni in sede giudiziale, che un dato correlato ad

---

[11] Cfr. G. Sartor, *Corso di informatica giuridica*, Giappichelli, Torino 2008, pp. 121 s.

[12] Cfr. M. Taruffo, *La prova dei fatti giuridici*, in *Tratt. Dir. Civ. e Comm.*, Milano 1992, vol. III, 2, 1, 440s.

[13] Cfr. F. Cordero, *Procedura penale*, Giuffrè, Milano 2003, pp. 581 s.

[14] Cfr. F. Carnelutti, *Teoria generale del diritto*, Società Editrice del Foro italiano, Roma 1951, pp. 379 s.

[15] Cfr. G. Sartor, *Corso di informatica giuridica*, Giappichelli, Torino 2008, p. 121.

[16] C. Maioli, *Introduzione all'informatica forense*, in P. Pozzi, *La sicurezza preventiva dell'informazione e della comunicazione*, Franco angeli, Milano 2004, pp. 108 s.

un sistema informatico o telematico può avere in ambito giuridico, attraverso l'estensione alla tecnologia informatica di teorie, principi e prassi proprie delle scienze forensi. Coinvolge tre settori tecnico-giuridici con competenze differenti: informatica, procedura giudiziale e prassi investigative[17]. La sua applicazione è trasversale ad illeciti penali, civili ed amministrativi, anche tradizionali, compiuti, in tutto o in parte, tramite le tecnologie informatiche[18]. Scopo della *Computer Forensics* è conservare, identificare, acquisire, documentare e interpretare dati rilevanti per il diritto, senza loro alterazione o modificazione, obiettivo perseguito attraverso l'utilizzo di *Tool Forensics*, *software* e *hardware* in grado di fornire supporto tecnico per l'osservazione in sola lettura dei supporti di memoria, l'acquisizione della copia forense dei dati e la loro analisi[19], e *Best Practices*, procedure e prassi degli operatori tecnico-giuridici concernenti la scansione temporale delle attività tecniche[20]. *Tool Forensics* e *Best Practices*, attraverso una disposizione congiunta, consentono l'acquisizione, la custodia e l'analisi dei dati rilevanti per il caso giudiziale concreto. Emblema dell'attività tecnico-giuridica d'informatica forense è l'acquisizione della copia forense dei dati: la c.d. *bitstream image*.

3.1 Copia forense, analisi dei dati ed effetti probatori

La fase d'acquisizione forense dei dati consta nella creazione di un'immagine digitale, c.d. *bitstream image* o *mirror image*, dei supporti di memorizzazione o dei flussi di dati. Nel secondo caso l'acquisizione è possibile solo durante lo scambio dinamico dei dati, nel primo caso, invece, la copia può avvenire *in loco* o, a causa di difficoltà tecniche, in un laboratorio *forensics*. L'immagine forense non è una semplice copia ma un esatto duplicato, *bit* per *bit*, dei dati, comprendente porzioni di *file*, *file* danneggiati, frammenti di *file* e aree non occupate dei supporti. Risultato dell'operazione è un'immagine clone dei dati[21]. L'architettura *software-hardware* dei *Tool Forensics* è orientata alla genuina apprensione e custodia delle fonti di prova digitali. La procedura informatica di copia forense è, per questo motivo, associata a due particolari misure tecnico-giuridiche. La prima riguarda l'approccio del *Tool Forensics* al calcolatore da clonare, mediante un algoritmo a bassa complessità computazionale o un *hardware* che permetta di osservare i supporti di memoria in con-

---

[17] L. Luparìa, G. Ziccardi, *Investigazione penale e tecnologia informatica*, Giuffrè, Milano 2007, pp. 31s; A. Ghirardini, G. Faggioli, *Computer Forensics*, Apogeo, Milano 2009, pp. 1 s.

[18] Cfr. E. Casey, *The need for knowledge sharing and standardization*, in *Digital Investigation*, 2004, 1, 1-2.

[19] Per un approfondimento sulle tecnologie di *Write Blocker* si veda J. R. Lyte, *A strategy for testing hardware write block devices*, in *Digital Investigation*, 3, 2006, pp. 3.

[20] L. Lupària, G. Ziccardi *Investigazione penale e tecnologia informatica*, Giuffrè, Milano 2007, pp. 55 s e pp. 103 s; F. Novario, *Prove penali informatiche*, Libreria Cortina Torino, Torino 2011, pp. 21 s; E. Casey, *Digital Evidence and Computer Crime. Forensics science, computer and the internet*, Ed. II, Elsevier, San Diego 2004, pp. 211 s.

[21] Cfr. A. Ghirardini, G. Faggioli, *Computer Forensics*, Apogeo, Milano 2009, pp. 97 s..

dizione di sola lettura, per scongiurare volontarie o involontarie manipolazioni dei dati. La seconda riguarda la genuinità del risultato dell'immagine forense: il calcolo dell'valore dell'algoritmo di *hash*, funzione matematica unidirezionale che univocamente consente il calcolo delle dimensioni dell'immagine forense da una sequenza di *bit*. Questo è effettuato sui dati originali prima dell'inizio delle operazioni e sulle copie al termine delle operazioni, se coincidente sancisce l'identità dell'immagine forense con l'originale. In alcuni casi le modifiche dei dati possono essere inevitabili. La corretta applicazione delle misure tecnico-giuridiche da parte degli investigatori permette di superare l'*impasse* rendendo queste ipotesi residuali[22].
La fase di analisi dei dati è generalmente successiva a quella di acquisizione[23], è svolta sulle copie forensi per non modificare irrimediabilmente l'originale ed operare su un terreno di analisi cristallizzato e garantito. Anche in questa fase è notevole l'apporto tecnico dei *Tool Forensics*, che consentono di disporre molteplici opzioni per la ricerca, l'individuazione e l'analisi dei dati, sfruttando le loro caratteristiche informatiche: criteri di ricerca per nomi e proprietà dei *file*, recupero di informazioni strutturali, riesumazione di dati cancellati, ricostruzione di sequenze di eventi, decrittazione di *file*, etc. Per le operazioni suddette sono stati sviluppati *software* onnicomprensivi e specifiche *release*[24], i casi concreti, però, presentano spesso particolari problemi che devono essere affrontati con *Tool ad hoc*[25]. Elemento sotteso a qualunque attività tecnica forense digitale è la compatibilità dei Tool utilizzati con l'*hardware* e il *software* del *computer* da clonare, o della rete da osservare, per ridurre al minimo la possibilità di errore della copia forense[26]. Questione tutt'ora aperta per la disposizione d'attività di *Digital Forensics*, invece, è l'uso di *Tool* proprietari o *opensource*: i primi, spesso certificati da organizzazioni investigative di livello mondiale, nascondono i propri codici sorgente; i secondi, spesso gratuiti, sono invece trasparenti sugli algoritmi utilizzati[27]. La trasparenza dei passaggi tecnici è un elemento essenziale delle fasi investigative. In questo particolare caso, però, la disputa è da chiudere in favore dei *software* proprietari per un motivo pratico: la certificazione del *software* è il principale indice su cui un giudice possa fondare la validità di un attività tecnica. Ciò non preclude, altresì, il possibile utilizzo di *softwa-*

---

[22] Cfr. F. Novario, *Computer Forensics - Tra Giudizio e Business*, Cortina Torino, Torino 2012, pp. 41 s.

[23] È anche possibile, seppur scarsamente utilizzata per i rischi di compromissione dei dati originali, la disposizione d'attività quali l'ispezione e la perquisizione informatica, in un momento antecedente alla fase di copia dei dati e in concreto sui dati originali. Cfr. S. Aterno, F. Cajani, G. Costabile, M. Mattiucci, G. Mazzaraco, *Computer Forensics e Indagini Digitali*, Vol. I, Experta, Forlì 2011, pp. 393 ss.

[24] tra cui EnCase, CAINE, Autopsy. Cfr. *http://www.guidancesoftware.com/encase-forensic.htm; http://www.caine-live.net/; http://www.sleuthkit.org/autopsy/.*

[25] tra cui è possibile annoverare Ethetcop, VmWare, Grep, etc. Cfr. L. Lupària, G. Ziccardi, *Investigazione penale e tecnologia informatica*, Giuffrè, Milano 2007, pp. 85s.

[26] Cfr. *www.cybercrimes.it*; A. Ghirardini, G. Faggioli, *Computer forensics*, Apogeo, Milano 2009, pp. 209 s.

[27] Cfr. V. Mangini, *Manuale breve di diritto industriale*, Cedam, Padova 2009, pp. 87 s.

re opensource qualora posseggano una certificazione.[28].
L'apporto tecnico della *Computer Forensics* influisce anche sul merito dell'analisi delle fonti di prova. I dati reperiti possono essere rappresentati come porzioni o agglomerati di *file* che mantengono le proprie caratteristiche tecniche. La loro analisi consente una ricostruzione digitale dei fatti o di elementi rilevanti per lo svolgimento delle indagini[29]. È possibile osservare l'attitudine probatoria dei *file* suddividendoli in due categorie: evidenze informatiche – *file* testuali, multimediali o di archivio – la cui sola presenza può far riscontrare l'evento o la condotta di un illecito; programmi/registrazioni, *file* che necessitano di un'analisi per divenire evidenti. Nel caso delle evidenze informatiche le proprietà dei *file* – data, ora e utente di creazione, cancellazione e modificazione – possono divenire informazioni utili per la ricostruzione cronologica dei fatti e la corretta attribuzione di responsabilità dell'utente. Tra I *file* di programma/registrazione, che possono essere applicativi o di sistema, un tipo risulta particolarmente rilevante: i *log*. Questi sono generati in automatico da programmi attivi nel sistema *software* e presenti nelle memorie di massa, sono di tipo testuale e contengono la registrazione di tutte le informazioni sul programma che li ha generati e sulle sue attività. Le informazioni non sono immediatamente intelligibili, devono essere analizzate da un esperto che le interpreti. I *file* di *log* sono facilmente manipolabili e sovrascritti dal sistema in breve tempo, così da renderne utile l'analisi solo a breve termine dalla commissione dell'illecito[30]. La ragione che spinge a superare questi ultimi ostacoli tecnici è il risultato di analisi: un'esatta ricostruzione cronologica delle operazioni avvenute nel sistema o in programmi applicativi, associate all'utente che le ha compiute.

4. Impatto della *Digital Forensics* in azienda

Come risulta evidente dalle righe precedenti, un approccio informatico giuridico e forense mostra profili tecnico-giuridici peculiari, importanti, pervasivi e concreti, soprattutto se associato a possibilità di prova digitale e tutela legale. Una più specifica analisi di queste attitudini in campo aziendale mette in luce, a fronte della necessaria organizzazione sottesa all'ente per il raggiungimento di scopi economici e/o sociali, una ampia e concreta possibilità di attività tecnico-giuridiche volte alla prevenzione di attività illecite, atte sia a scongiurare, sia a meglio approntare, questioni giudiziarie. Attività stragiudiziali, preventive e giudiziali, infatti, sono strettamente legate nella tutela informatico giuridica e forense di un ente: qualora l'attività preventiva non sia svolta, o sia stata svolta in modo non corretto, questa può recare pregiudizio

[28] Cfr. F. Novario, *Prove penali Informatiche*, Libreria Cortina Torino, Torino 2011, pp. 21 s.

[29] Cfr. F. Novario, *Prove Informatiche*, in P. Ferrua, E. Marzaduri, G. Spangher, *La prova penale*, Giappichelli, Torino 2013, pp. 127 s.

[30] Cfr. A. Ghirardini, G. Faggioli, *Computer Forensics*, Apogeo, Milano 2009, pp. 347 s.

ad un'eventuale attività giudiziaria. Comprendere quali siano le attività preventive disponibili, a fronte dei loro effetti e peculiarità, risulta dunque essenziale e propedeutico a qualunque attività tecnico-giuridica di tutela dell'ente.
La *Digital Forensics* consente di disporre svariate attività tecniche con diversi effetti giuridici o probatori. *In primis* è possibile ottenere la prova digitale di violazioni subite dall'ente, con tutele ed effetti a contrasto di *cyber*-attacchi alle infrastrutture informatiche, *computer crime* e atti illeciti digitali. È altresì possibile ottenere prove circa violazioni informatiche, con riflessi anche extra informatici, compiute dell'ente stesso, cui esempio possono essere il mancato rispetto di prescrizioni giuridiche a tutela del consumatore oppure l'illecito scambio di informazioni tra aziendale. Ulteriormente, l'attività informatico giuridica e forense può essere fonte di reperimento di tracce digitali concernenti processi informatici approntati dall'ente, del tutto illeciti o tecnicamente non corretti rispetto alle generali indicazioni di legge, cui esempi possono essere la violazione delle c.d. Misure minime di sicurezza ex art. 33 ss. del d.lgs. 196/2003 (Codice della Privacy) e suo allegato B. Infine, l'attività di prova digitale aziendale può fornire tracce digitali di processi informatici, e processi aziendali legati all'uso delle tecnologie *IT*, considerabili virtuosi, cui esempio può essere la prova della corretta conformazione e concretezza delle tecnologie e dei processi sviluppati ex d.lgs. 231/2001 (Responsabilità Amministrativa degli Enti)[31].
L'impatto della *Digital Forensics*, e più in generale di un approccio informatico giuridico concreto, alle aziende, consente l'elaborazione di soluzioni tecnico-giuridiche di tipo preventivo, proattivo e gestionale, secondo due paradigmi fondamentali: l'*Assessment* e la Consulenza. Il primo rappresenta una c.d. *second opinion* elaborata da un *Professional* o da un Ente terzo sullo stato di *security* infrastrutturale e gestionale di un ente, al fine di indicare elementi di rischio e di futuro sviluppo, oppure orientato al controllo della *compliance* aziendale rispetto alle regole tecnico-giuridiche inerenti l'informatica, il diritto e l'economia aziendale. La Consulenza invece, attività più tradizionale, rappresenta l'individuazione di un *Professional* o di un Ente per lo sviluppo di soluzioni tecnico-giuridiche tali da rendere l'ente *compliance* per quanto concerne profili informatici, giuridici e aziendali, in particolare attraverso l'elaborazione di progetti tecnico-giuridici, la gestione dei lavori e delle attività in concreto. Le due attività hanno ad oggetto, in via non esaustiva e non necessariamente alternativa, l'uniformazione dei sistemi *ICT* e la loro riconfigurazione, la creazione di sistemi informatico giuridici e forensi "*by design*", la gestione delle emergenze e dei rischi aziendali, nonché l'attività di Consulenza Tecnica a fini stragiudiziali e giudiziali. Come evidente, sia l'*Assessment* sia la Consulenza pongono le radici della loro effettiva e performante disposizione nell'individuazione di *Professional*, riconosciuti e stimati professionisti della materia, che possono essere liberi professionisti come afferenti ad aziende che ne gestiscono o promuovono l'operato. Individuare, valutare e apprezzare un *Professional* informatico giuridico e forense risulta un passaggio

[31] Cfr. F. Novario, *Computer Forensics. Tra Giudizio e Business*, Cortina Torino, Torino 2012, pp. 170 ss.

essenziale, meritevole d'attenzione in quanto momento dirimente la riuscita delle attività tecniche disposte in azienda.

5. Il Consulente Informatico Giuridico e Forense

L'informatica giuridica e forense è una materia di nuova genesi e concezione, non sostenuta ad oggi da un'organica formazione accademica come da Ordini o Collegi Professionali[32]. Questa, altresì, è spesso considerata una "fetta di mercato" inesplorata dove, a fronte della necessaria essenza artigianale per lo svolgimento delle attività tecnico-giuridiche, generici consulenti informatici, giuridici, ma anche semplici millantatori, possono inserirsi, con possibili conseguenze negative per enti e loro utenti. Il profilo di "artigiano tecnico-giuridico", associato alla necessaria attitudine al "*problem solving*" proprio della materia e dell'attività d'*Assessment*/Consulenza, rende complessa l'individuazione di un *Professional* in questo campo. La complessità è altresì aumentata dalla necessaria ponderazione delle attitudini professionali da parte dell'ente interessato alla prestazione professionale, spesso non avvezzo alla disciplina e quindi più orientato a propendere verso soggetti che vantino rapporti di fiducia con l'ente, individuati attraverso un "passa parola" tra aziende *partner* nonché attraverso *provider* di generici servizi di *assessment* o consulenziali. Alcuni elementi essenziali per ponderare la professionalità informatica giuridica e forense, sistematizzati in una griglia valutativa, possono fornire quanto meno una solida base sulla quale l'ente possa svolgere una concreata e indipendente scelta di un *Professional*.

I macro parametri da osservare sono principalmente tre: *Situazione personale/Formazione accademica e professionale*; *Esperienza professionale*; *Impatto sulla comunità scientifica e professionale*. Ogni macro parametro ritiene almeno quattro essenziali questioni cui ottenere delucidazioni, estrapolabili dal *curriculum vitae* e professionale del soggetto individuato o da individuare, nonché sviscerabili in sede di colloquio conoscitivo, momento per altro irrinunciabile per giungere ad una chiara comprensione circa le competenze del *Professional*.

Il parametro *Situazione personale/Formazione accademica e professionale* ha ad oggetto questioni inerenti alla condizione personale e di formazione del professionista:

- se il soggetto sia incensurato: al fine di appurarne la credibilità in ambito giudiziale ma anche stragiudiziale, nonché la riservatezza e sicurezza nella gestione dei dati aziendali.
- se il soggetto possieda una formazione universitaria: al fine di comprenderne la

[32] Eccezion fatta per il Collegio Toscano Periti Esperti Consulenti, che vanta un registro per le professionalità di Computer Forensics giudiziale e aziendale e Informatica Giuridica per le PA e le Aziende. Cfr. *http://www.collegiotoscanoperiti.org/index.php*

formazione e la sua compatibilità circa l'attività tecnico-giuridica di cui dovrebbe essere incaricato.
- se il soggetto possiede specializzazioni accademiche e professionali: di particolare rilevanza sono, in ordine decrescente di importanza, Dottorati di ricerca, Master universitari e corsi di formazione professionale, così da sondare l'effettiva e certificata preparazione teorica e tecnico-giuridica afferente l'attività professionale che deve essere svolta.
- se il soggetto è iscritto a Ordini o Collegi Professionali: per ottenere una certificazione delle competenze tecnico-giuridiche. Essenziale è che il Collegio o l'Ordine preveda una particolare categoria o registro per l'informatica giuridica e forense, e che il *Professional* vi sia iscritto.
Il parametro *Esperienza professionale*, invece, ha ad oggetto questioni inerenti alla pratica disposizione di attività tecnico-giuridiche e all'esperienza concreta del professionista:
- se il soggetto possiede un'esperienza professionale almeno settennale nei separati ambiti dell'informatica, del diritto o aziendale: al fine di comprendere l'attitudine pratica verso la soluzione di questioni tecniche, giuridiche e aziendali considerate quali elementi distinti.
- se il soggetto possiede un'esperienza professionale almeno settennale nel campo dell'informatica giuridica e forense: al fine di comprendere l'attitudine pratica verso la soluzione di questioni tecnico-giuridiche, in particolare nel campo dell'informatica giuridica e forense.
- se il soggetto collabora, ha collaborato o ha fatto parte delle Forze dell'Ordine: al fine di evidenziare peculiarità concernenti la comprensione delle responsabilità e la pratica disposizione delle metodologie di lavoro in campo d'indagine.
- se il soggetto collabora o ha collaborato con Procure della Repubblica e Magistrati giudicanti: al fine di evidenziare peculiarità concernenti la comprensione dei ragionamenti giuridici e giudiziari, nonché la pratica gestione delle attività tecniche in sede giudiziale.
Il parametro circa l'*Impatto sulla comunità scientifica e professionale*, infine, ha ad oggetto la considerazione teorica e pratica del professionista tra colleghi, altri professionisti e accademici, afferenti all'area d'informatica giuridica e forense oppure ad altre aree interessate da quest'ultima:
- se il soggetto ha ricoperto incarichi di docenza universitaria: intendendo con ciò attività per cui sia stato concesso l'uso del titolo di Docente a contratto, Docente associato e Docente ordinario, per insegnamenti inerenti l'informatica giuridica e forense, oppure per la professionalità vantata. Ciò al fine di ottenere la prova del possesso di un approccio metodologico scientifico sotteso anche all'attività professionale.
- se il soggetto è autore di saggi, scritti, articoli: pubblicati su riviste accademiche e professionali, da parte di editori d'ambiti compatibili con la professionalità vantata. Ciò al fine di ponderare l'attitudine al lavoro in staff.
- se il soggetto è autore di monografie: accademiche o professionali, pubblicate da

editori d'ambiti compatibili con la professionalità vantata. Ciò al fine di ponderare l'attitudine al lavoro individuale.
- se il soggetto è, o ha ricoperto, la figura di Direttore scientifico e/o Coordinatore di progetti formativi od editoriali di ricerca: in particolare nel campo dell'informatica giuridica e forense, ciò al fine di ponderare l'attitudine alla gestione di gruppi di lavoro.
Feed back positivi alla totalità delle questioni suindicate mostrano la totale competenza personale, formativa, professionale e accademica del *Professional*, tale da poter essere considerato come *Peritus peritorum* nel campo dell'informatica giuridica e forense. *Feed back* negativi ad alcune voci comportano, invece, la necessaria ponderazione in concreto delle attitudini del *Professional* che, da una possibile considerazione quale *Peritus peritorum* può divenire, in un'ottica decrescente, prima perito, poi consulente, ancora semplice esperto e, infine, "inesperto" nell'informatica giuridica e forense. Quest'ultima attitudine evidenzia come il soggetto possa essere preparato e competente su alcune attività professionali, ma non per specifiche attività d'informatica giuridica e forense.
La griglia valutativa qui illustrata è riportata in copia nell'allegato 1 del presente articolo.

6. Conclusioni

Le prove informatiche sono elementi ormai fondanti il substrato aziendale, a scopo di tutela dell'ente, garanzia dell'utenza e tutela dei sistemi informativi. L'essenza tecnico-giuridica della materia, fusa con la totale informatizzazione di processi aziendali, implica una sempre più costante attenzione e fruizione di attività di *Computer Forensics* Aziendale, che possono essere disposte attraverso attività d'*Assessment* e Consulenze, da soggetti che devono essere selezionati secondo severe linee guida a fronte della peculiare riservatezza e complessità dell'attività lavorativa da svolgere.
Il fenomeno informatico giuridico e forense aziendale è dunque realtà. I suoi sviluppi non sono ad oggi completamente prevedibili. Nonostante ciò è possibile considerare l'espansione della materia, e la sua costante elaborazione teorico-pratica, come inevitabile nel panorama tecnico-giuridico aziendale.

Allegato 1

CRITERI SELEZIONE CT/CTU/PERITI INFORMATICA GIURIDICA E FORENSE		
Questioni	**No** Valore 0	**Sì** Valore 1
Formazione accademica/professionale		
1) E' incensurato.	☐	☐
2) Possiede una laurea.	☐	☐
3) Possiede specializzazioni accademiche o professionali nel campo. (dottorato, master, formazione professionale)	☐	☐
4) E' iscritto ad un collegio od ordine professionale con specializzazione in Informatica Giuridica e Forense.	☐	☐
Esperienza professionale		
5) Possiede un'esperienza professionale almeno settennale in campo informatico/ giuridico/aziendale.	☐	☐
6) Possiede un'esperienza professionale almeno settennale in Informatica Giuridica e Forense.	☐	☐
7) Collabora o ha fatto parte delle Forze dell'Ordine.	☐	☐
8) Collabora con Tribunali, Corti d'Appello e Procure della Repubblica.	☐	☐
Impatto sulla comunità scientifica		
9) E' stato docente universitario (a contratto, associato o ordinario) nel campo della Informatica Giuridica e Forense.	☐	☐
10) E' autore di articoli e saggi in riviste accademiche e collettanee del settore.	☐	☐
11) E' autore di monografie del settore.	☐	☐
12) E' direttore/coordinatore di progetti formativi/ricerca nel campo d'Informatica Giuridica e Forense per Enti di ricerca od Editori.	☐	☐
Punteggio		
Risultati		
0-4: **inesperto** (formato nel campo ma non avvezzo alle applicazioni pratiche)		☐
5-6: **esperto** (conoscitore della materia, atto all'elaborazione di pareri su argomenti di dettaglio)		☐
7-8: **consulente** (conoscitore della materia, atto a consiglio e assistenza nello svolgimento d'atti, pratiche o progetti attraverso informazioni, pareri e soluzioni)		☐
9-11: **perito** (profondo conoscitore della materia, atto, oltre che al consiglio e all'assistenza, alla supervisione e al controllo di atti pratici, progettuali e soluzioni, nonché alla formazione professionale)		☐
12: **peritus peritorum** (estremo conoscitore della materia, atto all'insegnamento e all'evoluzione della materia, allo sviluppo di soluzioni innovative, oltre che al consiglio, all'assistenza, alla supervisione e al controllo di atti pratici, progettuali e soluzioni, nonché alla formazione accademico-professionale)		☐

Rivista elettronica di Diritto, Economia, Management

N. 1 - 2017 · pp. 71-78

Le nuove professioni digitali: il Responsabile della conservazione e il Responsabile del trattamento dei dati personali

Andrea Lisi e Sarah Ungaro

Abstract: La progressiva digitalizzazione di enti e aziende pone l'accento sul bisogno, negli enti privati e ancor di più in quelli pubblici, di professionalità specifiche, che siano in grado di gestire in modo ottimale e corretto dal punto di vista normativo questa fase di passaggio dalla carta al digitale e sappiano mettere a pieno regime la gestione digitale di documenti, dati e informazioni. Tra queste assumono un ruolo di spicco il Responsabile della conservazione e il Responsabile del trattamento dei dati.

Parole chiave: Responsabile della conservazione, Responsabile del trattamento, accreditamento conservatori, AgID, regole tecniche.

1. Il Responsabile della conservazione e l'accreditamento dei conservatori

Le recenti novità normative in tema di digitalizzazione hanno posto l'attenzione sul Responsabile della conservazione, figura che risulterà ancor più imprescindibile e strategica a seguito dell'entrata in vigore dell'obbligo di fatturazione elettronica verso le pubbliche amministrazioni[1].Queste, infatti, dovranno provvedere alla conservazione digitale a norma sia delle fatture elettroniche, sia del Registro unico delle fatture[2], visto che tali documenti informatici devono comunque essere conservati digitalmente, in conformità al Decreto Ministeriale n. 55/2013 e agli art. 43 e ss. del

[1] Obblighi che sono decorsi dal 6 giugno 2014 per Ministeri, Agenzie fiscali ed Enti nazionali di previdenza e decorreranno dal 31 marzo 2015 per le altre Amministrazioni pubbliche, tra cui gli enti locali, come disposto dal Decreto legge 24 aprile 2014, n. 66, convertito con modificazioni dalla L. 23 giugno 2014, n. 89.

[2] La cui adozione è prescritta dal DL 24 aprile 2014, n. 66, convertito, con modificazioni, dalla Legge 23 giugno 2014, n. 89 (in G.U. 23/06/2014, n. 143).

Articolo pervenuto il 16 Febbraio 2017, approvato il 20 Marzo 2017

Codice dell'Amministrazione digitale (D. Lgs. 82/2005), insieme - ovviamente - a tutti gli altri documenti digitali prodotti o ricevuti dall'ente pubblico o dall'azienda.
Alla gestione e al coordinamento del processo di conservazione, il legislatore ha preposto il Responsabile della conservazione, figura professionale prevista dalla legge a cui sono attribuiti, appunto, il compito di sovraintendere il processo di conservazione a norma di dati e documenti digitali.
Nello specifico, già il comma 1-*bis* dell'art. 44 del Codice dell'Amministrazione digitale stabilisce espressamente che il sistema di conservazione dei documenti informatici sia gestito dal Responsabile della conservazione, il quale deve operare d'intesa con il Responsabile del trattamento dei dati personali (di cui all'articolo 29 del D.Lgs. 30 giugno 2003, n. 196), e, nelle pubbliche amministrazioni, con il Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi (di cui all'articolo 61 del DPR 28 dicembre 2000, n. 445)[3].
Inoltre, anche nelle nuove Regole tecniche sui sistemi di conservazione, emanate con il DPCM 3 dicembre 2013, il legislatore ha inteso valorizzare la figura del Responsabile della conservazione, peraltro specificando che nelle pubbliche amministrazioni tale ruolo debba essere svolto da un dirigente o da un funzionario formalmente designato.
In effetti, come previsto dall'art. 6 del DPCM 3 dicembre 2013, il Responsabile della conservazione ha il compito, in estrema sintesi, di definire e attuare le politiche complessive del sistema di conservazione e di governarne la gestione con piena responsabilità e autonomia, in relazione al modello organizzativo adottato.
In particolare, ai sensi dell'art. 7 del citato DPCM, il Responsabile della conservazione è competente per lo svolgimento dei seguenti compiti (art. 7):
a) definire le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente;
b) gestire il processo di conservazione e garantirne nel tempo la conformità alla normativa vigente;
c) generare il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
d) generare e sottoscrivere il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
e) effettuare il monitoraggio della corretta funzionalità del sistema di conservazione;
f) assicurare la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adottare

[3] Come peraltro previsto anche dal recentissimo DPCM 13 novembre 2014, recante le "*Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005*", pubblicato nella Gazzetta Ufficiale n. 8 del 12 gennaio 2015.

misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adottare analoghe misure riguardo all'obsolescenza dei formati;
h) provvedere alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
i) adottare le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12 del DPCM 3 dicembre 2013;
j) assicurare la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
k) assicurare agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
l) provvedere, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti;
m) predisporre il manuale di conservazione di cui all'art. 8 e curarne l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.
Nello specifico, inoltre, ai sensi dell'art. 44, comma 1-*ter* del Codice dell'Amministrazione digitale, è possibile implementare il sistema di conservazione all'interno della struttura organizzativa dell'azienda o della pubblica amministrazione di appartenenza oppure si può scegliere di affidarlo a un soggetto esterno - il Conservatore - mediante contratto o convenzione di servizio, che preveda comunque l'obbligo di rispettare il Manuale della conservazione predisposto dallo stesso Responsabile[4]. Sul punto, è opportuno porre in evidenza, inoltre, che nel caso in cui il Responsabile della conservazione affidi il processo di conservazione a un soggetto esterno, in base all'espressa previsione dell'art. 6 del DPCM 3 dicembre 2013, costui assume *ope legis* il ruolo di Responsabile del trattamento dei dati personali relativi ai documenti oggetto di conservazione (ai sensi dell'art. 29 del D.Lgs. 196/2003)[5].
In argomento, tuttavia, è necessario specificare che l'art. 5 del DPCM 3 dicembre 2013 dispone che i Responsabili della conservazione delle pubbliche amministrazioni che intendano affidare il sistema di conservazione a Conservatori esterni all'ente di appartenenza possano individuare per tale incarico solo Conservatori accreditatisi presso l'Agenzia per l'Italia digitale, ossia soggetti - pubblici o privati - che offrano

[4] Inoltre, ai sensi dell'art. 44, comma 1-*ter*, del Codice dell'Amministrazione digitale e dell'art. 7 del DPCM 3 dicembre 2013, il Responsabile della conservazione può chiedere di certificare la conformità del processo di conservazione a soggetti, pubblici o privati, che offrano idonee garanzie organizzative e tecnologiche, ovvero a soggetti a cui è stato riconosciuto il possesso dei requisiti di cui all'art. 44-bis, comma 1, del D.Lgs. 82/2005, distinti dai conservatori o dai conservatori accreditati.

[5] Resta ferma la competenza del Ministero dei beni e delle attività culturali in materia di tutela dei sistemi di conservazione degli archivi pubblici o degli archivi privati che rivestono interesse storico particolarmente rilevante.

le maggiori garanzie organizzative e tecnologiche, così come previsto dall'articolo 44-bis, comma 1, del Codice dell'Amministrazione digitale.
Tutti i Conservatori, dunque, che intendessero fornire i loro servizi alle PPAA o che vogliano in ogni caso dimostrare di possedere i requisiti organizzativi e tecnologici di livello più elevato per offrire servizi più qualificati sul mercato, devono procedere alla richiesta per ottenere il riconoscimento di "Conservatore accreditato" presso l'Agenzia per l'Italia digitale[6] (AgID). A tal fine, dovranno osservare quanto prescritto sia dalle nuove Regole tecniche (DPCM 3 dicembre 2013), sia dalla Circolare AgID n. 65 del 10 aprile 2014[7], che definisce le modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici, di cui all'art. 44-*bis* del D.Lgs n. 82/2005 (Codice dell'Amministrazione digitale).
Inoltre, proprio in relazione alla Circolare 65/2014, è stato pubblicato un documento dedicato ai profili professionali[8] che devono essere presenti nella struttura organizzativa del Conservatore che intenda conseguire l'accreditamento presso l'AgID. In tale documento, nello specifico, si stabilisce la formazione e le esperienze minime, le attività associate al ruolo, nonché la tipologia di rapporto contrattuale richiesti per il Responsabile della conservazione e per le altre figure professionali che con questo devono collaborare, tra cui il Responsabile del trattamento dei dati personali.
Da ultimo, nell'allegato alla Circolare 65/2014 di AgID, per la figura professionale del Responsabile della conservazione che opera nella struttura organizzativa del Conservatore accreditato si richiede il possesso della laurea e di esperienza lavorativa di almeno 5 anni in questo ruolo o, in assenza di laurea, esperienza in un ruolo analogo di almeno 8 anni. Inoltre, si prescrive che il rapporto contrattuale in essere tra il Responsabile della conservazione e la struttura organizzativa del soggetto - pubblico o privato - che svolge attività di conservazione dei documenti informatici e intende conseguire il riconoscimento dei requisiti di livello più elevato, in termini di qualità e sicurezza, come previsto dall'art. 44-*bis*, comma 1, del Codice dell'Amministrazione digitale, sia a tempo indeterminato o della durata di almeno 3 anni.
In sintesi, anche dalle norme più recenti emerge in maniera ancora più incisiva che un sistema di conservazione - così complesso, delicato ed essenziale per tutelare il patrimonio documentale di una pubblica amministrazione - non può essere affidato a chiunque, ma ha bisogno di essere gestito internamente attraverso specifiche

---

[6] Qualora avessero già presentato domanda di accreditamento in vigenza delle precedenti Regole tecniche (di cui alla Deliberazione CNIPA n. 11/2004) e della Circolare di DigitPA n. 59/2011, i Conservatori dovranno provvedere a integrare la documentazione eventualmente già presentata con gli ulteriori requisiti imposti dalle disposizioni del DPCM 3 dicembre 2013 e dai suoi allegati, nonché con quelli previsti dalla Circolare AgID n. 65 del 10 aprile 2014 e dai Documenti dalla stessa richiamati.

[7] La nuova Circolare AgID n. 65/2014 è disponibile sul sito dell'Agenzia per l'Italia digitale all'indirizzo http://www.agid.gov.it/sites/default/files/circolari/circolare_accreditamento_conservatori_n_65_10-04-2014.pdf

[8] Disponibile sul sito dell'AgID all'indirizzo http://www.agid.gov.it/sites/default/files/documentazione/profili_professionali_per_la_conservazione.pdf

figure professionali o di essere, invece, affidato in outsourcing a soggetti che siano davvero in grado di garantire la correttezza di tali processi. In questi sistemi, quindi, risulta strategico il ruolo del Responsabile della conservazione, ossia una figura professionale specifica che oggi può essere valorizzata e tutelata grazie alla legge n. 4/2013.

2. I compiti e le funzioni del Responsabile del trattamento

Come innanzi illustrato, le nuove Regole tecniche sulla conservazione (di cui al DPCM 3 dicembre 2013) e la Circolare AgID n. 65 del 10 aprile 2014 hanno introdotto molte importanti novità per tutte quelle organizzazioni che intendono fornire i loro servizi di conservazione alle PPAA (o ad aziende private) e che vogliono ottenere il riconoscimento di "Conservatore accreditato" presso AgID.
Con specifico riferimento alla protezione dei dati di cui si effettua il trattamento, il legislatore attribuisce un ruolo centrale al Responsabile del trattamento dei dati personali (di cui all'art. 29 d.lgs. 196/2003, c.d. Codice Privacy).
Nel campo della digitalizzazione documentale, in particolare, questa figura svolge una funzione molto importante e delicata, poiché gestisce il trattamento elettronico di tutti i dati personali nei vari flussi informativi e documentali di un'azienda, pubblica amministrazione, associazione o studio professionale, facendo in modo che venga garantita la *compliance* normativa sia in riferimento alla privacy, sia alle altre norme che direttamente o indirettamente la richiamano. In base all'art. 30 del D.Lgs. 196/2003, il Responsabile privacy occupa, pertanto, una posizione di staff e supporto al Titolare del trattamento, definendo e implementando le procedure organizzative per il trattamento, curando l'applicazione di misure di sicurezza (minime, idonee e necessarie) e coordinando tutti gli adempimenti normativi mediante la predisposizione di un modello organizzativo di privacy interna (e le relative privacy policy) che possa garantire un corretto trattamento dei dati personali di titolarità propria o di terzi.
In effetti, alla base della corretta gestione digitale di dati vi è l'attenzione per l'aspetto organizzativo, in modo tale da garantire che il trattamento dei dati personali sia sempre aderente alle diverse normative che regolano la dematerializzazione documentale, avendo riguardo non solo di quanto stabilito dal Codice Privacy, ma anche da tutte le disposizioni emanate in tema di digitalizzazione (dunque in termini di sicurezza e privacy, dematerializzazione e archiviazione digitale, continuità operativa e recupero dati, adeguamento ai modelli organizzativi 231, etc.). Ciò ancor di più se si considera la sempre crescente applicazione di nuove tecnologie in svariati campi (dalla sanità alle banche, dalle pubbliche amministrazioni al settore privato), che comporta inevitabilmente un incremento di rischi e minacce per i flussi di infor-

mazioni immateriali, soprattutto se sensibili, e il pericolo di una loro alterazione o di un accesso abusivo agli stessi.
Nello specifico, l'attuale Codice Privacy stabilisce che il Responsabile del trattamento dei dati personali può essere la "*persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo*" a cui il Titolare del trattamento può affidare una serie di responsabilità e compiti operativi molto specifici.
Il Titolare del trattamento, perciò, una volta selezionati i Responsabili, deve provvedere a nominarli per iscritto (pena la nullità del conferimento dell'incarico), definendo nel dettaglio attività, modalità e ambito di trattamento che intende delegare loro (ai sensi dell'art. 29, comma 4, del Codice, infatti, "*i compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare*") e deve organizzarsi per la verifica del rispetto delle funzioni delegate e delle istruzioni impartite (art. 29, comma 5, del Codice).
Sul punto, come già ricordato, lo stesso articolo 44 comma 1-*bis* del d.lgs. 82/2005 (Codice dell'Amministrazione Digitale), che disegna un sistema di conservazione gestito da un Responsabile della conservazione che opera d'intesa con il Responsabile del trattamento dei dati personali e il Responsabile del servizio per la tenuta del protocollo informatico, ci ricorda come nell'ambito della dematerializzazione e della digitalizzazione documentale sia necessaria la compresenza e la collaborazione tra professionalità che devono possedere specifiche competenze.
In particolare, il Responsabile del trattamento dei dati personali deve essere dotato di competenze legali, informatiche e organizzativo-gestionali e deve quindi possedere conoscenze specifiche che possono essere acquisite solamente attraverso un adeguato percorso formativo e una buona dose di esperienza sul campo.
Proprio alla luce di queste specifiche competenze e delle responsabilità che gli possono essere affidate, nella normativa italiana attualmente in vigore il Responsabile per il trattamento dei dati, da intendersi nella sua accezione più ampia, può essere considerato un vero e proprio "Data Protection Officer" o "Privacy Officer" (figure previste e disciplinate in altri paesi dell'UE e nella bozza di Regolamento europeo sulla privacy recentemente votata, ma che si trova – purtroppo - ancora in attesa di approvazione definitiva), e presta il suo servizio alle imprese o pubbliche amministrazioni che sempre più spesso si trovano a dirimere le intricate problematiche interpretative derivanti sia dalla legislazione italiana in materia di digitalizzazione (si veda, a titolo esemplificativo, il d.lgs. n. 33/2013, c.d. Decreto Trasparenza), sia dalle specifiche prescrizioni contenute nei provvedimenti emanati dall'Autorità Garante per la protezione dei dati personali.
Tuttavia, alla luce delle sorti incerte del nuovo Regolamento europeo in materia di privacy, sembra opportuno focalizzare la nostra attenzione e valorizzare la figura professionale emergente del Responsabile del trattamento, che prenderà sempre più piede all'interno delle aziende e delle pubbliche amministrazioni. Sul punto, in effetti, pare corretto ritenere che la nomina di un Responsabile del trattamento, seppure in alcuni contesti formalmente facoltativa, oramai in molti ambiti sia diventata

di fatto obbligatoria[9] (molto spesso in provvedimenti emanati dell'Autorità Garante è possibile notare, in effetti, come l'affidamento di alcuni servizi a soggetti interni o esterni, che comporta dei rischi in capo agli interessati nelle varie fasi del trattamento dei loro dati, preveda - quale misura di "sicurezza necessaria" - la nomina degli stessi a responsabili ai sensi dell'art. 29 d.lgs. 196/2003).
È opportuno sottolineare inoltre che, tra le figure professionali obbligatorie per i Conservatori accreditati nel documento allegato alla Circolare 65/2014 non è richiamato il c.d. privacy officer, una figura di cui non c'è traccia nella normativa vigente, ma che è tuttora oggetto di speculazioni. In effetti, basandosi sul dato normativo, l'unica figura professionale che il nostro ordinamento prevede espressamente come preposta al trattamento dei dati personali e che svolge una funzione prevalentemente organizzativa e metodologica, pur applicando la normativa, è il Responsabile del trattamento, di cui all'art. 29 del D.Lgs. 196/2003. Si ritiene, infatti, che il ruolo e i compiti del Responsabile del trattamento - se opportunamente disegnati per le specifiche esigenze della struttura organizzativa del titolare del trattamento - ben potrebbero comprendere tutti i compiti del "privacy officer"[10] che forse - presto o tardi - potrebbe essere ufficialmente sancita in sede europea in virtù del Regolamento europeo.
Appara utile ricordare, inoltre, alla luce delle recenti novità normative, che chiunque voglia gestire e implementare un sistema di conservazione a norma e garantire così la correttezza dei processi sviluppati, non può prescindere dal ruolo strategico del Responsabile del trattamento dei dati personali, figura professionale specifica che oggi può essere valorizzata e tutelata anche grazie alla legge n. 4/2013 e che - a differenza di altre ancora incerte figure per le quali pure esistono vari corsi o certificazioni - è soggetta per espressa previsione di legge a obblighi di aggiornamento, analogamente agli iscritti a qualsiasi Albo professionale.
A sottolineare l'importanza della corretta gestione del trattamento dei dati, infine, nell'allegato "Documentazione per accreditamento conservatori", alla lettera p), tra i "Documenti tecnici e organizzativi generali", emerge un ulteriore e non secondario requisito che bisogna possedere per accreditarsi, ovvero la presentazione di una specifica "dichiarazione di aver ottemperato a quanto previsto dalla normativa inerente il trattamento dei dati personali". Pertanto, alla luce di questo ulteriore adem-

---

[9] La non obbligatorietà della designazione del responsabile del trattamento dei dati personali, prevista dall'art. 29 del D.Lgs. 196/2003, è giustificata esclusivamente dal fatto che il titolare del trattamento può essere sia una persona fisica che una persona giuridica pubblica o privata. Considerato l'attuale sviluppo delle nuove tecnologie in ambito aziendale privato e pubblico e l'attuale necessità di avere un controllo costante sui dati personali trattati, è da considerarsi sicuramente imprudente la scelta di non avvalersi di questa figura, alla luce anche delle pesanti sanzioni in sede civile, amministrativa o in ambito penale a cui può andare incontro il Titolare del trattamento.

[10] Occorre quindi fare le dovute distinzioni tra la figura professionale del Responsabile del trattamento, valorizzata sia nel Codice dell'amministrazione digitale sia nella citata Circolare AgID, e quella del privacy officer, anche in relazione ai vari percorsi formativi tendenti a fornire delle nozioni in ambito privacy, ma che non possono certificare o riconoscere una figura come quella del privacy officer che attualmente non trova spazio nelle norme vigenti.

pimento che certifichi la *compliance* aziendale alla normativa in materia di privacy, tutti coloro che vorranno accreditarsi presentando la relativa domanda dovranno valutare attentamente e individuare in maniera corretta il soggetto deputato a ricoprire il ruolo di responsabile del trattamento, il quale avrà – tra le altre cose - il compito di curare all'interno della struttura organizzativa tutti gli adempimenti in materia di privacy e i necessari audit, in modo da rendere la sua struttura veramente conforme ai principi del Codice Privacy e agli specifici provvedimenti emanati dall'Autorità Garante, in relazione ovviamente alla natura dei dati e alle modalità del trattamento. In conclusione, la tutela dei dati personali risulta sempre più strategica e delicata in ogni organizzazione: pertanto, è indispensabile che le figure professionali che incidono in qualche modo sul corretto trattamento di dati - anche personali - collaborino tra loro in maniera costante, al fine di garantire un continuo controllo e una gestione corretta, controllata e sicura dei dati e delle informazioni.

N. 1 - 2017 • pp. 79-91

Illecito 2.0: Reati e Illeciti Civili sui *Social Network*

Edoardo E. Artese[1] – Fabio Prolo[2]

Abstract: Il presente elaborato si basa su un intervento presentato nell'ambito della fiera SMAU e si propone di analizzare i rapporti intercorrenti tra le figure di illecito disciplinate dal nostro ordinamento e l'utilizzo dei più diffusi social network, fra tutti Facebook e Twitter.
Si inizierà definendo tecnicamente l'argomento *social network*, analizzando tutti gli illeciti configurabili in tale ambito. Verranno poi analizzate una serie di casistiche giurisprudenziali italiane.

1. Il concetto di Web 2.0.

L'espressione "*Web* 2.0", creata dallo studioso irlandese Tim O'Reilly[3] nel 2004, ha lo scopo di sottolineare l'evoluzione in senso "*social*" e di condivisione vissuta dalle tecnologie *Internet* a partire dal nuovo millennio. Non a caso viene scelta la sigla 2.0, solitamente usata per distinguere le versioni di un *software*.

---

[1] Avvocato del Foro di Milano; titolare dello Studio Legale Ferrari Artese.

[2] Praticante abilitato al patrocinio presso la Corte d'Appello di Milano.

[3] Per un maggior approfondimento si vedano A. Fini – M. E. Cicognini "*Web* 2.0 e *Social Networking*", F. Mini, "*Social Media – Introduction*", in " *Internet Case Study Book", R. Ford* – J. Wiederman, Taschen, Koln, 2010.

Articolo pervenuto il 16 Febbraio 2017, approvato il 20 Marzo 2017

Tale nomenclatura, tuttavia, può trarre in inganno, poiché, a differenza di quel che avviene comunemente tra le diverse *release* di un *software*, in questo l'architettura del *World Wide Web* rimane la medesima, bensì cambia la filosofia alla base e, in particolare, la modalità di utilizzo.
L'utente passivo (ovvero il cd. "utente 1.0") si trasforma e diventa un utente attivo: da mero fruitore di contenuti diventa **creatore** di contenuti, cd. *User Generetad Content* (U.G.C.). Al contempo - presupposto indispensabile - si passa da siti ipertestuali statici di mera consultazione, a siti dinamici modificati dalle produzioni degli stessi utenti.
I tratti peculiari del *Web* 2.0 vengono riassunti dal cd. paradigma delle tre P:

- **Pubblicazione**: l'utente diventa editore del proprio spazio;
- **Partecipazione**: possibilità di aggregazione senza limiti spazio temporali;
- **Personalizzazione**: possibilità di modificare secondo esigenza le funzioni di un servizio.[4]

In questo ampio contesto si inseriscono *blog*, *forum*, piattaforme *wiki*, piattaforme di condivisione di contenuti (*YouTube, Flicker*, etc.) e, ovviamente, i *Social Network*.

2. Il concetto di *Social Network.*

In ambiente informatico, il termine *Social Network* si riferisce a qualsiasi piattaforma *Web* che permetta al suo interno la creazione un identità sociale individuale e la gestione di una propria rete di contatti. Queste piattaforme rappresentano lo stadio più avanzato di *Web 2.0* come sopra descritto e, per tale ragione, alcuni studiosi optano per la nomenclatura "*Web 2.5*".
Il concetto di rete sociale, tuttavia, non è un concetto informatico, bensì sociologico. Per tale ragione sarebbe più corretto l'utilizzo del termine *Social Media*, che nasce dall'unione di *Social Network* e *new media*, tuttavia di scarso utilizzo nel linguaggio comune.
Le innovazioni portate dall'informatica in ambiente sociologico sono notevoli, basti pensare alla "violazione" della regola di Dunbar, o regola dei 150, che affermerebbe che le dimensioni di una rete sociale in grado di sostenere relazioni stabili siano limitate a circa 150 membri. Inutile dire come *Social Network* quali Facebook o Twitter superino con facilità queste previsioni.
La definizione di rete sociale telematica è dunque stata ridefinita su modelli più attuali. Come hanno rilevato le ricercatrici americane Danah Boyd e Nicole Ellison nel 2007, i *Social Network* (o *social media*) sono caratterizzati da tre elementi:

- la presenza di uno spazio virtuale (forum) in cui l'utente può costruire ed esibire un proprio profilo. Il profilo deve essere accessibile, almeno in forma parziale, a tutti gli utenti dello spazio;

[4] Cfr. G. M. Riccio "*Social Networks* e responsabilità civile", Dir. Informatica, 2010, 06, 859.

- la possibilità di creare una lista di altri utenti (rete) con cui è possibile entrare in contatto e comunicare;
- la possibilità di analizzare le caratteristiche della propria rete, in particolare le connessioni degli altri utenti.

Le interazioni tra i soggetti che frequentano queste reti, o meglio queste comunità, creeranno – così come avviene in ambienti non virtuali – dei contrasti suscettibili di essere apprezzati da un punto di vista giuridico. In altre parole, gli utenti commetteranno illeciti a discapito degli altri membri della comunità.

3. Il concetto di illecito nell'ordinamento giuridico italiano: brevi cenni.

Prima di analizzare i rapporti intercorrenti tra *Social Network* e le singole fattispecie, pare opportuno, per i non giuristi che saranno fruitori non del presente elaborato, definire sinteticamente il concetto di illecito.

In diritto, il termine illecito indica un comportamento umano contrario all'ordinamento giuridico, che si sostanzia nella violazione di un dovere o di un obbligo imposto da una norma giuridica. L'ordinamento giuridico, invece, è l'insieme di norme che regolano la vita di una comunità.

Il comportamento che costituisce l'illecito può essere commissivo, quando viola un obbligo o dovere negativo (di non fare), oppure omissivo, quando invece viola un obbligo o dovere positivo (di fare).

Le condotte illecite assumono una rilevanza giuridica differente a seconda dell'ambito nel quale sono poste in essere. In particolare, nell'Ordinamento Italiano possono essere individuate tre diverse tipologie di illeciti:

- civili (consistono nella violazione di una norma posta a tutela di un interesse privato alla quale consegue una sanzione risarcitoria);
- penali (detti anche reati, sono costituiti dalle condotte che violano le norme poste a tutela dell'interesse pubblico ed attinenti, quindi, all'ordine etico-politico-sociale dello Stato; al compimento di tali condotta verrà comminata una sanzione);
- amministrativi (modellati sulla struttura del reato, ma sono sanzionati dalla pubblica amministrazione e non dall'Autorità Giudiziaria. Prevedono l'applicazione di sanzioni pecuniarie, che possono poi essere accompagnate anche da misure accessorie di diversa natura).

Tale differenziazione si effettuata in relazione alla norma violata, al tipo di sanzione che ne consegue o alle modalità per la sua irrogazione ed è pertanto di fondamentale importanza, nel caso concreto, potere ricondurre il fatto ad una singola categoria.

Come è ovvio, anche al mondo "*virtuale*" e, dunque, a quello dei *social netwrok*, si applicano questi criteri.

4. Classificazione degli illeciti configurabili nell'ambito dei *Social Network*.

4.1. Premessa.

La casistica di illeciti configurabili nell'ambito dei *social network* è assai ampia e, per chiarezza espositiva, si ritiene opportuno effettuare una ulteriore distinzione:

- gli illeciti commessi direttamente dai *social network*;
- illeciti commessi da agenti terzi all'interno e/o per tramite dei *social network*.

4.2. Illeciti commessi dai *Social Network*.

In tale sono ricompresi quegli illeciti che vengono commessi esclusivamente dalle società che possiedono e gestiscono la piattaforma.
In tale categoria, per completezza divulgativa, si citano gli illeciti societari autonomi, che tuttavia non riguardano il presente elaborato.
Per quanto qui concerne, invece, si riscontrano una serie di illeciti connessi ai peculiari servizi che un *social network* offre e, dunque, ipotesi relative alla responsabilità dell'*Internet Service Provider* (le aziende che forniscono servizi in rete) in relazione ai contenuti che vengono pubblicati dagli utenti loro tramite.
Al riguardo, pur non essendo ancora stata raggiunta una posizione unanime, si può affermare che in linea di massima non esista un obbligo di controllo preventivo posto a carico del *provider*[5], ma un obbligo di intervento successivo a segnalazione che è fonte di responsabilità qualora venga disatteso[6].

4.3. Illeciti commessi da agenti terzi all'interno e/o per tramite dei *Social Network*.

Assai ampia risulta la casistica di illeciti configurabili tramite azioni di terzi effettuate all'interno e/o per il tramite dei servizi offerti dal *Social Network*.
Tali ipotesi possono essere classificate in:

- utilizzo illecito del *Social Network* che travisa le funzioni della piattaforma;

---

[5] Cfr. Art. 17 D. Lgs. 70/2003; CGE n. 360/10; Cass. Pen. sez. III del 2014 numero 5107.

[6] Cfr. Art. 16 D. Lgs. 70/2003. Sul punto si veda G. Comandè, "*Al via l'attuazione della direttiva*" cit., 812 ss. e anche L. Bugiolacchi, *"(Dis)orientamenti giurisprudenziali in tema di responsabilità degli internet provider (ovvero del difficile rapporto tra assenza di obblighi di controllo e conoscenza dell'illecito)*", Resp. civ. prev., 2010, 1586, spec. nota 35, Tosi, Le responsabilità civili cit., 578 s. L'autore, in particolare, rileva che «*non essendo precisate - come invece sarebbe stato opportuno - né le modalità né le fonti della "conoscenza" del fatto illecito: criticità che non mancherà di riverberare effetti sulla prima giurisprudenza successiva all'entrata in vigore della nuova normativa*».

- utilizzo illecito del *Social Network* che non travisa le funzioni della piattaforma;
- utilizzo lecito del *Social Network* considerato illecito dall'ordinamento.

Nel primo caso (utilizzo illecito che travisa le funzioni), il *Social Network* è utilizzato come mero veicolo per il raggiungimento di un fine illecito che va al di la delle tradizionali funzioni permesse dalla piattaforma: la caratteristica principale che accomuna gli illeciti appartenenti a questa famiglia infatti è quella di deviare l'originaria concezione degli strumenti predisposti dalla piattaforma[7].

Nella seconda categoria (utilizzo illecito che non travisa le funzioni della piattaforma) possono essere ricondotte tutte quelle azioni illecite che, pur configurando comunque un utilizzo contrario agli standard e alle *policies* del *Social Network*, non travisano le finalità tipiche dei mezzi comunicativi con la conseguenza che potrebbero essere considerate apparentemente lecite[8].

Nella terza categoria (utilizzo lecito del *Social Network*, ma contrario all'ordinamento), infine, sono da ricondursi tutte quelle azioni che sono considerate illecite solo dal nostro ordinamento, ma che sono perfettamente in linea con le condizioni di utilizzo dei *Social Network* e con i loro *standard*[9].

5. Casistica di illeciti civili nell'ambito dei *Social Network*.

5.1- Premessa. Cenni di illeciti di natura contrattuale.

Gli illeciti in ambito civile si distinguono in contrattuali ed extra contrattuali.

Individuare fattispecie della prima ipotesi all'interno di un *Social Network* non è semplice. Le piattaforme sociali, infatti, rivolgono le loro funzioni principali alla comunicazione e/o pubblicazione tralasciando quasi completamente gli aspetti di *e-commerce*.

A ben vedere, gli unici soggetti interessati a sottoscrivere contratti (di utilizzo) con gli utenti e amministratori di un *social media* potrebbero essere le società sviluppatrici di "*App*".

---

[7] Si potrebbero far rientrare in questa categoria le seguenti ipotesi delittuose: spamming, raccolta e l'utilizzo indebito di dati persona, accesso abusivo a sistema informatico, utilizzo dei contatti per trasmettere volutamente virus informatici, utilizzo dei contatti per acquisire abusivamente codici di accesso per violare sistemi informatici.

[8] Possono rientrare in questa categoria: ipotesi di concorrenza sleale, lo scambio di immagini pedopornografiche che integra gli estremi del reato di cessione di materiale pedopornografico, pubblicazione o invio di messaggi di incitamento all'odio e alla discriminazione razziale, la diffamazione, furto di identità e usurpazione di titoli e onori, reati di vilipendio, minacce, concorrenza sleale, *stalking* e *cyber-bulling*.

[9] In questa categoria si configurano i reati di peculato e di violazione di misure cautelari.

Sul punto, tuttavia, non esiste alcuna pronuncia giurisprudenziale e, pertanto, si dovrà ritenere che ogni aspetto contrattuale sia da ricondurre modello classico previsto dal codice civile ovvero alle disposizioni previste dalla Direttiva 2000/31/CE che disciplina il commercio elettronico in territorio comunitario.
Assai più ampie sono le ipotesi di illeciti extracontrattuali.

5.2. Illeciti di natura extracontrattuale.

5.2.1. La concorrenza sleale ex art. 2598 c.c.[10]

Le grandi potenzialità comunicative proposte dai *Social Network* non hanno tardato ad attribuire a tali piattaforme un ruolo privilegiato anche in campo commerciale. Grazie a quest'ultime è infatti possibile arrivare a promuovere la propria attività in prima persona, a costo zero e senza la canonica necessità di affidarsi ad un intermediario esterno.
La mole di utenti che tocca un *Social Network* da forte rilevanza concorrenziale a questi nuovi sistemi di comunicazione: tale aspetto non è sfuggito alla giurisprudenza che ha operato un raccordo tra normativa vigente in materia di concorrenza sleale e *new media*.
Prendendo ad esempio il *Social Network* per eccellenza, Facebook, non è raro che le società sfruttino per fini promozionali strumenti messi a disposizione dal sito quali le Pagine Pubbliche o i Gruppi.
Al riguardo, il Tribunale di Torino ha precisato come «*i gruppi di Facebook, ove usati nell'ambito di un'attività economica, svolgono la funzione d*i *segni distintivi atipici*», garantendo così ogni tutela prevista dal Codice Civile[11]. Questo provvedimento stabilisce un principio che potrà poi essere esteso ad altri strumenti e *Social Network*.
In conclusione, le pagine delle società presenti sui *Social Network* sono considerati segni distintivi atipici, suscettibili dunque di tutela contro l'interferenza confusoria. Tale interpretazione è coerente con le recenti statuizioni della Suprema Corte[12] che hanno attribuito rilievo generale all'uso di segni distintivi atipici in *Internet* (nel

---

[10] Art. 2958 c.c.: "*ferme le disposizioni che concernono la tutela dei segni distintivi [2563-2574] e dei diritti di brevetto [2584-2594], compie atti di concorrenza sleale chiunque: 1) usa nomi o segni distintivi idonei a produrre confusione con i nomi o i segni distintivi legittimamente usati da altri, o imita servilmente i prodotti di un concorrente, o compie con qualsiasi altro mezzo atti idonei a creare confusione con i prodotti e con l'attività di un concorrente; 2) diffonde notizie e apprezzamenti sui prodotti e sull'attività di un concorrente, idonei a determinarne il discredito, o si appropria di pregi dei prodotti o dell'impresa di un concorrente; 3) si vale direttamente o indirettamente di ogni altro mezzo non conforme ai principi della correttezza professionale e idoneo a danneggiare l'altrui azienda*".

[11] Cfr. Tribunale di Torino, Ordinanza del 7 luglio 2011, consultabile su http://www.altalex.com/index.php?idnot=54083 (14 agosto 2014).

[12] Cfr. Cass. Civ. n.24620 del 3 dicembre 2011.

caso specifico, il dominio delle pagine *Web*) qualora sia ravvisabile una funzione pubblicitaria e suggestiva del segno, finalizzata ad attrarre il consumatore nell'orbita dell'imprenditore.

5.2.2. Ipotesi di violazione del diritto d'autore.

Nel nostro ordinamento, il diritto d'autore è tutelato dalla legge n. 633 del 22 aprile 1941 - "*Protezione del diritto d'autore e di altri diritti connessi al suo esercizio*" - nonché dal Titolo IX del Libro Quinto del Codice Civile.
Pare opportuno precisare che, benché la materia giuridica del diritto d'autore si considerata usualmente una materia civilista, alcune condotte assumono una rilevanza anche dal punto di vista penale; ed invero, anche la stessa L.d.A. stabilisce pene detentive in caso di violazione della normativa.
Ciò posto, il fine precipuo della disciplina è la tutela del diritto allo sfruttamento economico dell'opera d'ingegno.
Nello specifico, i principali strumenti messi a disposizione dal legislatore sono:

1. azioni di accertamento cautelare e con funzione inibitoria;
2. azioni per la distruzione o rimozione della violazione;
3. azione per il risarcimento del danno;
4. azioni strumentali all'esercizio delle difese civili ex art. 161 L.D.A.

Da un punto di vista penale, invece, la violazione del diritto d'autore è considerata un delitto e comporta pene detentive che, nei casi più gravi, arrivano ai 3 anni di reclusione[13].
I rapporti tra questa fattispecie e i *Social Network* sono molteplici, così come le pronunce in merito. Sul punto, infatti, si è arrivati ad orientamenti piuttosto consolidati che ci permettono di affermare che:

- «*il gestore di un Social Network non è tenuto a predisporre un sistema di filtraggio delle informazioni per prevenire la violazione dei diritti d'autore*[14]» ;
- l'utente sarà comunque responsabile delle proprie condotte e – oltre alle conseguenze giuridiche – potrebbe essere escluso dall'utilizzo del *Social Network* in caso di violazione dei diritti d'autore altrui.

In sede penale, gli orientamenti sono piuttosto severi: si è addirittura arrivati a stabilite che sia «*da ritenersi penalmente responsabile chiunque diffonda anche solo parzialmente opere protette attraverso la pubblicazione delle stesse su Social Network senza citarne espressamente il co-autore*» e che sia sufficiente il dolo generico per la configurazione dell'illecito[15].

---

[13] A disciplinare tali aspetti è la stessa Legge sul Diritto d'Autore che dall'art. 171 ss. riporta le singole fattispecie nonché le relative pene detentive e pecuniarie.

[14] Cfr. CGE, Sez. III, sentenza n. 360 del 16 febbraio 2012.

[15] Cfr. Tribunale di Genova sez. I 3443 del 13 luglio 2012.

5.2.3. Il diritto all'oblio.

Prima di concludere la parte dedicata alle fattispecie civilistiche, merita qualche breve cenno (l'argomento infatti è assai vasto e oggetto di dibattito) una particolare forma di garanzia, sviluppatasi con l'evoluzione del Web in senso 2.0. ed a una sempre maggior attenzione degli studiosi al tema della *privacy*, ossia il cd. **diritto all'oblio**. Quest'ultimo può essere tradotto nel «*diritto a non restare indeterminatamente esposti ai danni ulteriori che la reiterata pubblicazione di una notizia può arrecare all'onore e alla reputazione, salvo che, per eventi sopravvenuti, il fatto precedente ritorni di attualità e rinasca un nuovo interesse pubblico all'informazione*»[16].
In particolare, il diritto all'oblio è ricompreso nei cd. diritti inviolabili, ossia in quei diritti che pur non avendo esplicito riconoscimento costituzionale, sono comunque garantiti da disposizioni a carattere generale. In Italia, la sua tutela è garantita dall'art. 2 della Costituzione, secondo cui *"la Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità"*.
In sede giurisprudenziale, il diritto all'oblio è ormai pacificamente riconosciuto anche dalla Suprema Corte, che – da ultimo – nel 2013 ha affermato che «*per reiterare legittimamente notizie attinenti a fatti remoti nel tempo, è necessario il rilevante collegamento con la realtà attuale e la concreta utilità della notizia, da esprimersi sempre nei vincoli della cd. continenza espositiva*»[17].
L'organo di tutela principale è il Garante della Protezione dei Dati Personali, che è un'autorità amministrativa indipendente e che, pertanto, non è competente per le richieste di risarcimento danni, affidate invece ai Tribunali Ordinari.
All'interno dei *Social Network*, le violazioni del diritto all'oblio potranno essere compiute:
- **da singoli utenti**, tramite la pubblicazione di una notizia all'interno dello spazio personale che la piattaforma mette a disposizione degli iscritti (ad es. bacheca).
- **dalle pagine pubbliche o profili social dei quotidiani** - sempre presenti sui *Social Network* - che si occupano della continua pubblicazione delle notizie.

Il problema principale delle violazioni che concernono il diritto all'oblio, tanto genericamente sul Web quanto specificamente sui *Social Network*, non è tanto la rimozione dei contenuti dalle singole piattaforme, quanto la rimozione dell'indicizzazione operata dai motori di ricerca.
Al riguardo, un importante passo avanti è stato fatto in sede comunitaria con la sentenza ECJ – C131/12 del 13 maggio 2014 che ha stabilito che "*i providers di servizi di ricerca sul Web sono titolari dei dati personali indicizzati anche se pubblicati su siti di terzi"*.
Questa affermazione implica che l'interessato possa rivolgersi ai motori di ricerca

[16] Luca Fazzo, "Mario Chiesa ha diritto all' oblio" in la Repubblica, Roma, 2 febbraio 2005.

[17] Cfr. Cass. Civ., Sez. III, sentenza n. 1611/13.

per impedire l'indicizzazione delle informazioni riguardanti la sua persona, pubblicate su pagine web di terzi, facendo valere la propria volontà che tali informazioni non siano conosciute dagli utenti di Internet, ove egli reputi che la loro divulgazione possa arrecargli pregiudizio o desideri che tali informazioni siano dimenticate, anche quando si tratti di informazioni pubblicate da terzi lecitamente (artt. 12 e 14 CE 95/46).

6. Breve cenni di ipotesi di Illecito amministrativo connesso all'attività di *Social Network*.

Unica pronuncia rilevabile nel panorama giuridico del nostro ordinamento, relativa alla violazione di fattispecie amministrative connessa all'utilizzo di un *Social Network*, riguarda i cd. illeciti da tifoseria e, in particolare, l'incitazione all'odio in occasioni di manifestazioni sportive ex art. 6, co. I, L. 401/1989.
Tale articolo, prevede che *«l'autorità di pubblica sicurezza (possa) sempre ordinare il divieto di accesso ai luoghi dove si svolgono competizioni agonistiche alle persone che vi si rechino con armi improprie, o che siano state condannate o che risultino denunciate per aver preso parte attiva a episodi di violenza in occasione o a causa di manifestazioni sportive, o che nelle stesse circostanze abbiano incitato o inneggiato alla violenza con grida o con scritte*.»
Il provvedimento di divieto è il cd. D.A.SPO., acronimo di divieto di accedere a manifestazioni sportive. Competente per la sua emissione è il questore, la sua durata può andare da uno a cinque anni e può essere accompagnato (e quasi mai manca di esserlo) dall'obbligo di presentazione ad un ufficio di polizia in concomitanza temporale con la manifestazione sportiva vietata.
Relativamente alla configurazione di detto illecito per il tramite dell'utilizzo di un *Social Network* è stato stabilito che "*sia illegittima la misura del divieto di accesso a manifestazioni sportive – cd. DA.SPO – nei confronti del tifoso che ha utilizzato, tramite, un Social Network, espressioni che ancorché sommamente sgradevoli, non si può sostenere costituiscano un'induzione e/o un incitamento diretto e specifico alla violenza, né che risultino direttamente espresse in occasione, o comunque nell'ambito di competizioni sportive, a pena, in caso contrario, del rischio di una dilatazione eccessiva dell'ambito applicativo delle ipotesi contemplate dall'art. 6, co. 1, della l. 401/1989 che invece risultano tassative ed insuscettibili di interpretazioni analogiche od estensive*"[18].

[18] Cfr. T.A.R. per la Toscana, sez. II, sentenza n. 98/2012.

7. Casistiche di reati nell'ambito dei *Social Network*.

7.1. Fattispecie tipiche di reati informatici: *Stalking* e *Cyber-Stalking*.

Attraverso il decreto legge n. 11 del 23 febbraio 2009[19], rubricato "*misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori*", è stato introdotto nel codice penale il reato di atti persecutori[20], ovvero di *stalking*.

A questa nuova figura vengono tipicamente ricondotte diverse altre ipotesi criminose previste autonomamente quali i reati di minaccia e di molestia[21], ingiuria, diffamazione, violazione di domicilio, violenza e maltrattamenti di varia natura. Lo *stalking* viene solitamente considerato un estensione delle citate fattispecie[22].

L'elemento distintivo tra gli atti persecutori e le altre figure è la reiterazione dei comportamenti offensivi. Lo *stalking* è un reato abituale, a forma libera, di danno e di evento.

In particolare, per la sua configurazione è richiesto che le condotte cagionino alternativamente:

- un perdurante e grave stato di ansia;
- un fondato timore per l'incolumità propria o di un prossimo congiunto;
- una sensibile modificazione delle abitudini di vita.

Per quanto riguarda i *Social Network*, "*integrano la condotta tipica del delitto di atti persecutori, di cui all'articolo 612 bis c.p., le molestie perpetrate attraverso il reiterato invio alla persona offesa di sms, mail oppure di messaggi di posta elettronica postati sui Social Network (ad esempio Facebook) [...]*"[23].

Con questa pronuncia la Corte Suprema ha affrontato per la prima volta il nuovo fenomeno del *cyber-stalking* ovvero "*dell'impiego spregiudicato e sempre più insidioso delle nuove tecnologie in funzione persecutoria e assillante ai danni della vittima prescelte*". La giurisprudenza di merito, ha poi ampliato la portata dell'art.612-bis c.p. introducendo la figura del cd. *stalking* vigilante, che si adatta perfettamente ai mo-

---

[19] Meglio noto come Decreto Maroni, dal nome del ministro che lo promosse, convertito nella L. 38 del 23 aprile 2009.

[20] Cfr. art. 7 del Art 7 del decreto legge n. 11 del 23 febbraio 2009, poi rubricato all'art. 612-*bis* del codice penale.

[21] Previste rispettivamente dagli art. 612 c.p. e 660 c.p.

[22] Cfr. C. Minnella *op. cit.*; A. Bastianello, "Il reato di *stalking* ex art. 612-bis c.p." in Giur. Merito 2012, 3, 673;F. Agnino, "*Delitto di atti persecutori e ricerca per tipo di autore dello stalker*" sempre in Giur. merito 2011, 9, 2237.

[23] Cfr. Cass. Pen. Sez. VI, n. 32404 del 16 luglio 2010.

delli di utilizzo di un *Social Network*. Al riguardo, infatti, il Trib. Termini Imerese ha stabilito che *"integrano l'elemento materiale del delitto di atti persecutori le condotte riconducibili alle categorie del cd. stalking vigilante (controllo sulla vita quotidiana della vittima), del cd. stalking comunicativo (consistente in contatti per via epistolare o telefonica, Sms, scritte su muri ed altri messaggi in luoghi frequentati dalla persona offesa) e del cd. cyber stalking, costituito dall'uso di tutte quelle tecniche di intrusione molesta nella vita della vittima rese possibili dalle moderne tecnologie informatiche e, segnatamente, dai Social Network»*[24].

7.2 Altre ipotesi di reato configurabili nell'ambito dei *Social network*.

7.2.1. Ingiuria e diffamazione.

I delitti di diffamazione ed ingiuria, rispettivamente disciplinati dagli artt. 595 e 594 del codice penale, sono senza dubbio i reati maggiormente commessi dagli utenti dei *Social Network*.
Non essendo emerse particolari questioni dottrinali o giurisprudenziali sulla configurabilità di queste fattispecie sulle piattaforme *social*, pare più opportuno concentrarsi sul lungo dibattito che ha interessato la distinzione tra le due. In breve, l'interrogativo era il seguente: l'offesa sul *Social Network* configura un reato di ingiuria ovvero di diffamazione?
Nella tradizionale concezione delle due figure di reato, ovvero quella appartenente al mondo reale, a fare da spartiacque è la presenza della persona offesa al momento dell'azione lesiva. In buona sostanza: se il soggetto destinatario delle affermazioni lesive è presente sarà configurato il reato di ingiuria; se assente, sarà configurato il reato di diffamazione.
Sui *Social Network* e più in generale sul Web, tuttavia, tale distinzione diventa molto offuscata. Da un lato, infatti, il destinatario delle affermazioni lesive potrebbe in astratto sempre percepire direttamente l'offesa; dall'altro lato, invece, che la presenza virtuale di un soggetto perde di importanza nell'indistinta massa di utenti che ha per definizione una piattaforma sociale.
Come spesso accade nel diritto informatico, ogni questione è stata superata applicando modelli reali al mondo virtuale: se l'affermazione lesiva sarà comunicata in privato (ad es. in chat) sarà integrata la fattispecie dell'ingiuria; se sarà, invece, comunicata pubblicamente, sarà integrata la diffamazione (ad es. un cd. *wall*).
La diffamazione, tuttavia, sarà sempre da ritenersi aggravata ai sensi del comma 3 dell'art. 595 c.p. integrando il *Social Network* – e più in generale Internet - i requisiti

[24] Cfr. Tribunale di Termini Imerese, Ordinanza del 9 febbraio 2011.

per essere considerato «mezzo di pubblicità» al pari di una testata giornalistica.[25]

7.2.2.La sostituzione di persona.

L'art. 494 c.p. così recita: "*chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona , o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici , è punito, se il fatto non costituisce un altro delitto contro la fede pubblica, con la reclusione fino ad un anno*".
La sostituzione di persona è un reato plurioffensivo, richiedendo contemporaneamente una lesione della pubblica fede e un vantaggio all'agente o un danno ingiusto alla persona offesa.
L'elemento soggettivo è il dolo specifico: la sostituzione deve essere illegittimamente voluta e ricercata e deve concretizzarsi in atti fraudolenti; l'elemento oggettivo, invece, è l'induzione in errore che deve fondarsi su un atto commissivo.
Benché nel novero delle decisioni degli organi giurisdizionali del nostro paese non siano – ancora – ravvisabili pronunce direttamente riguardanti i *Social Network*, la fattispecie oggetto del presente paragrafo può essere affrontata - più in generale - alla luce di quanto stabilito dalla sentenza n. 46674/2007 della Corte di Cassazione[26].
Secondo la Suprema Corte "*integra il reato di sostituzione di persona la condotta di colui che crei ed utilizzi un account di posta elettronica, attribuendosi falsamente le generalità di un diverso soggetto, inducendo in errore gli utenti della rete Internet nei confronti dei quali le false generalità siano declinate e con il fine di arrecare danno al soggetto le cui generalità siano state abusivamente spese[...]*[27]".
L'estensione di tale pronuncia anche alle piattaforme sociali è di immediata intuizione per due ragioni:

- al momento della registrazione ogni *Social Network* richiede che per l'accesso venga fornito un indirizzo mail valido;
- i *Social Network* consentono, per definizione, la creazione di un alter ego virtuale che agisce nella comunità.

7.3. La violazione di misure cautelari.

Con l'inedita sentenza n. 37151 del 29 settembre 2010, avente ad oggetto l'utilizzo di Facebook, la seconda sezione della Corte di Cassazione Penale ha esteso anche al contesto dei *Social Network* l'ambito di operatività delle previsioni contenute al comma 1 dell'art. 276 c.p.p.

---

[25] Cfr., *in primis*, Cass. Pen., sez. V n. 4741 del 27 dicembre 2000.

[26] Cfr. Corte di Cassazione, sez. V penale, n. 46674 in data 8 novembre 2007.

[27] Tale pronuncia è stata positivamente confermata anche dall'enunciato della sentenza n. 12479 emessa dalla III Sezione Penale della Corte di Cassazione il 15 dicembre 2011.

Qualora infatti il soggetto cui è stato imposto il divieto di "comunicare con persone diverse dai familiari conviventi", a norma del comma 2 dell'art. 284 c.p.p. utilizzi Facebook per comunicare con terzi non annoverati tra i conviventi andrà incontro ad un inasprimento delle misure a suo carico[28].
L'utilizzo di *Internet* da parte del condannato, tuttavia, come precisato dal supremo collegio in una successiva pronuncia conforme[29], non è proibito tout court:, la giurisprudenza riconosce un importante ruolo rieducativo e conoscitivo al Web, limitandosi ad impedire le sole comunicazioni illecite con terzi.
Al riguardo, infatti, il tribunale di Varese con la sentenza in data 8 novembre 2012 ha riconosciuto all'imputato sottoposto alla misura cautelare degli arresti domiciliari la possibilità di comunicazione tramite *Social Network* con terzi estranei al nucleo familiare ai fini dell'apprendimento scolastico.

8. Conclusione.

Quanto sopra riepilogato è, senza alcuna presunzione di completezza, una panoramica di fattispecie di illecito configurabili e verificatesi nel mondo dei *Social Network*, in base alla vigente normativa italiana e/o comunitaria.
Viene da sé che, in base all'argomento trattato e le evoluzioni tecnologiche (e sociologiche) che si verificano in tale contesto, nuove e variegate ipotesi di illecito saranno probabilmente configurabili.

[28] Cfr. A. Natalini, "Agli arresti domiciliari vietato accedere a "facebook" (ed a qualunque altro mezzo di comunicazione con l'esterno)" in Diritto e Giustizia 2010, 0, 468 nota alla sentenza Cass. Pen. sez. II, , n. 37151.

[29] Cfr. Cass. Pen. Sez. II, sentenza n. 4064, del 6 dicembre 2011

N. 1 - 2017 • pp. 92-102

La comunicazione di impresa su Internet: regole e tutela

Salvo Dell'Arte

Abstract: La comunicazione è elemento fondamentale se non essenziale per lo sviluppo economico delle imprese perché è il mezzo col quale si raggiungono i soggetti target che l'imprenditore vuole conquistare per proporre i propri beni o servizi. Internet permette di affinare, approfondire i vecchi sistemi di comunicazione e di inventarne di nuovi alla ricerca della catalizzazione dell'attenzione del consumatore. Scopo del presente articolo è quello di verificare se e quali regole devono essere applicate nella comunicazione di impresa sulla rete sia a tutela dell'imprenditore che a tutela del consumatore.

1. Introduzione

Prima di affrontare gli aspetti prettamente giuridici dell'argomento che ci occupa vorrei prendere le mosse da un simpatico aneddoto relegatoci da David Olgivy, guru della pubblicità nel secolo scorso: un merluzzo depone migliaia di uova e resta in silenzio, di contro la gallina depone un solo uovo e starnazza così che tutti possano notare il singolo uovo. Qual'è la differenza tra il merluzzo e la gallina? La seconda ha fatto pubblicità al proprio prodotto mentre nel silenzio del merluzzo nessuno potrà mai venire a conoscenza dei migliaia di prodotti da lui generati.
L'importanza della comunicazione di impresa è quindi immediatamente percepibile sia come fenomeno sociologico ed economico sia, di conseguenza, sotto l'aspetto tecnico-giuridico. In linea generale il fenomeno della comunicazione di impresa si estrinseca in tutte le forme di marketing che si differenziano tra loro come diverse manifestazioni pur avendo tutte lo scopo di promuovere l'attività di impresa e di persuadere i consumatori all'acquisto dei prodotti o dei servizi commercializzati.
Per una migliore comprensione del fenomeno giuridico è necessario avere una visione globale e unitaria dei principali strumenti di comunicazione intergrata che compongono il così detto *marketing communication mix*[1] .

[1] Per maggiori approfondimenti si rinvia a S. Dell'Arte in "*Diritto dell'Immagine nella Comunicazione d'Impresa e nell'Informazione*" parte quarta, seconda edizione, UTET 2014. Cfr. AA.VV., Nuovo dizionario illustrato della Pubblicità e Comunicazione, Lupetti, 2001, pag.405: "*Marketing mix* è la composizione e il dosaggio degli strumenti ai quali il piano di marketing affida il successo. Così come la riuscita di un cocktail è legata all'intelligente combinazione di sapori diversi e alle giuste quantità di ciascuno di essi, allo stesso modo il raggiungimento degli obiettivi di marketing è legato

Articolo pervenuto il 16 Febbraio 2017, approvato il 20 Marzo 2017

2. La comunicazione d'impresa: inquadramento definitorio

La comunicazione d'impresa può essere suddivisa in due macro aree:

- la pubblicità tabellare o *above the line* (*sopra la linea*, in un certo senso *evidente*) che è la forma di pubblicità intesa in senso stretto, rappresentata da tutte le forme di *advertising diretto* costituite da: un messaggio pubblicitario che ha a oggetto prodotti o servizi (a) rivolto a incrementare direttamente la vendita del prodotto o servizio reclamizzato (b) e trasmesso su media e spazi pubblicitari tradizionali quali la stampa, le affissioni, la radio, la televisione e il cinema (c).
- la pubblicità *below the line* (*sotto la linea*) comprende tutte le forme di comunicazione pubblicitaria indiretta dove manca o è del tutto secondario un messaggio avente a oggetto i prodotti o i servizi dell'impresa e le loro caratteristiche, nella quale si trasmettono valori più ampi come l'immagine dell'impresa, i suoi segni distintivi o i valori nei quali essa vuole essere riconosciuta, dove manca la sollecitazione all'acquisto dei singoli prodotti e che occupa spazi non tradizionali di *advertising*; tra queste ricomprendiamo la sponsorizzazione, il mecenatismo, le manifestazioni a premio, il sito *web* istituzionale.

La comunicazione su internet può esplicarsi in entrambe le macro aree sopra definite; infatti il web è un *non luogo* che sviluppa le possibilità di comunicazione di impresa potenzialmente illimitate e senza confini. È bene subito premettere che in questo *non luogo* intangibile si devono applicare tutte le regole nel mondo tangibile e reale. Limitante sarebbe la definizione di internet come *media* perchè la rete propone, nelle sue pressoché illimitate variabili, tutte le sfaccettature dei media tradizionali: dalla parola scritta, alle immagini statiche o in movimento a tutte le combinazioni che la creatività degli operatori del settore possono immaginare.
Pertanto le norme di riferimento dovranno essere quelle tradizionali applicabili, a mo avviso, direttamente e non per analogia o per interpretazione estensiva.

3. Le nuove forme di pubblicità sulla rete

Come detto, internet permette nuove forme di comunicazione di impresa e fino a qualche lustro orsono non erano pensabili; basta una breve navigazione sul web per comprendere come la creatività dei comunicatori si sia sviluppata in funzione del nuovo strumento e dei nuovi media che la rete offre in continuazione.
Gli aspetti innovativi della comunicazione sul web riguardano in primo luogo la modifica strutturale della comunicazione superando le tradizionali forme per sperimentarne di nuove che permettono di raggiungere un target potenzialmente

alla scelta degli strumenti adeguati e alla corretta distribuzione dell'investimento tra di essi".

illimitato con uno sforzo economico limitato. In particolare vi è stata una evoluzione dall'*advertising* tradizionale, che ha lo scopo di persuadere direttamente il consumatore focalizzandolo sul prodotto o sul servizio, alla più moderna evoluzione dell'*advertainment* che consiste in una forma di intrattenimento più ampio fino a coinvolgere direttamente il consumatore nella diffusione virale della pubblicità.
La nascita dei *social network* ha permesso un nuovo modo di comunicazione veloce ed essenziale con il coinvolgimento diretto dei consumatori che diventano a loro volta i ripetitori del messaggio pubblicitario.
L'evoluzione di supporti quali gli smartphone e i tablet amplificano l'importanza di internet come strumento per la comunicazione d'impresa del XXI secolo; sicché l'evoluzione parallela della tecnologia software e hardware ha concentrato l'attenzione degli esperti della comunicazione nella loro direzione.
Basti pensare che grazie ai moderni *devices* il consumatore è potenzialmente perennemente collegato in rete e, quindi, può essere potenzialmente raggiunto dal messaggio in qualunque momento e in ogni luogo. L'attitudine a dipendere sempre più dalla connessione è, ad oggi, ben diversa dalle abitudini tradizionali del lettore di riviste o giornali quotidiani o dello spettatore televisivo; per non parlare della cartellonistica stradale che oramai nel rumore quotidiano delle immagini on the road non attira più l'attenzione del consumatore che anche nei trasferimenti è assorto dal suo tablet o cellulare connesso ai *social network* o comunque in rete.
Il consumatore inizia a svolgere un ruolo attivo: produce, realizza e ripubblica contenuti e viene così definito col termine di *prosumer* e cioè soggetto attivo che non subisce più passivamente la comunicazione pubblicitaria, ma ne prende parte attiva.
Alcuni esempi chiariranno la visione del quadro di insieme.
Tra le forme più innovative di comunicazione pubblicitaria, nel rispetto della sintesi del presente lavoro, mi limito a ricordare i video virali e l'e-buzzing.
Il termine Marketing Virale fu utilizzato per la prima volta da Tim Draper per definire il successo avuto dal servizio di posta elettronica Hotmail nella seconda metà del 1996 e per tutto il 1997[2]. Il concetto di Marketing virale supera quello di passaparola che ha caratterizzato la rete fino ad allora.
Un video può essere definito virale quando supera un determinato numero di visualizzazioni. L'aggettivo virale è riferito alla modalità di propagazione del messaggio: come in un virus, la diffusione esponenziale avviene da una cellula all'altra in modo rapido e utilizza le risorse delle cellule raggiunte per i propri scopi. La propagazione del "virus" è garantita dagli utenti stessi che, un volta visto il video, lo consigliano a loro volta da altri utenti o lo condividono sul *social network*. Il passaparola è un processo che si autoalimenta, in quanto si rafforza senza interventi esterni ma solo grazie alla naturale trasformazione dei destinatari in nuovi vettori del messaggio.

[2] A.Bazzoffia, Spot 2.0. L'uso di You Tube come mezzo pubblicitario

A differenza della pubblicità tradizionale, il messaggio virale non è avvertito come aggressivo in quanto proviene da amici o conoscenti che fanno parte della vita dell'utente e quindi il destinatario lo visualizza anche più volte. La commistione tra video virali e *social network* ha dato vita a quello che è stato definito il Social Video Advertising, ovvero una tecnica di distribuzione online del video che garantisce un certo numero di contratti grazie all'utilizzo dei social network.
Il termine "*buzz"* è stato utilizzato da Emabuel Rosen, nel suo libro *The anatomy of buzz. How to create word of mouth marketing,* per indicare il risultato aggregato dal passaparola intorno a un prodotto o servizio: *buzz* è l'insieme di tutti i commenti scambiati in un dato momento a proposito di un determinato prodotto.
L'*E-buzzing* diventa così un network composto da siti web, *influential blog*, social media, applicazioni per mobile, tablet e desktop in più di 90 paesi. Rappresenta una risorsa importante per il mondo dell'*advertising online*. Di questo fenomeno si sono avvalse molte grandi imprese per pianificare campagne pubblicitarie a basso costo.
Il *WOMMA (Word Of Mouth Marketing Association),* un'associazione di settore che si occupa di promuovere il passaparola e il social media marketing. Il *WOMMA* ha redatto la bozza di codice etico il 9 febbraio 2005. Nel 2010 la *Federal Trade Commission* americana ha riconosciuto la correttezza dei principi di tale codice. I valori su cui si basa sono:

- Fiducia: creare un ambiente di fiducia tra il consumatore e il venditore.
- Integrità: promuovere onestà e trasparenza e respingere qualsiasi forma di ingannevolezza.
- Rispetto: promuovere e rispettare pratiche che pongono al centro gli interessi del consumatore.
- Onestà: lasciare il consumatore libero di farsi una propria opinione e di condividerla senza imporlo.
- Responsabilità: prestare particolare attenzione alle comunicazioni pubblicitarie rivolta a minori, in quanto vulnerabili alla manipolazione e all'inganno.
- Privacy: rispettare la privacy dei consumatori e promuovere i mezzi di tutela.

Di fatto i principi sopra elencati non sono altro che una corretta applicazione pratica dei principi che si traggono dalle norme di legge che vedremo appresso nel dettaglio.
Da ultimo una breve menzione al banner il quale è una striscia pubblicitaria che può avere varie dimensioni e che si trova in diverse posizioni della pagina Web. Rappresenta il primo strumento di pubblicità online, comparso per la prima volta nel 1994 su "*Hot Wired"*, versione online della rivista "*Wired"*. Esso contiene in genere il nome, il logo o l'immagine dell'azienda inserzionista allo scopo di attirare l'attenzione degli utenti indicandogli ciò che troveranno ciccandoci sopra. Un banner ha quindi il compito di sintetizzare ciò che il navigatore troverà nel sito sponsorizzato e lo deve fare nel modo più attraente possibile[3], ma può anche risultare utile in

[3] Foglio A., E-commerce e web Marketing: strategie di web Marketing e tecniche di vendita in Internet, Milano, Angeli, 2002, pag. 502

termini di awareness[4].
L'efficacia di un banner viene misurata dal cosiddetto *Click Throungh Rates*, ovvero il rapporto tra il numero di visitatori che hanno avuto l'opportunità di vedere un annuncio (*impression)* e quello di coloro che hanno cliccato su di esso[5]. La naturale avversione dell'utente internet a tale forme di pubblicità invasiva ha fatto sì che il banner abbia perso di appeal e sia diventato oramai una forma residuale e secondaria.

4. Quadro normativo

Come abbiamo già accennato sopra, anche per tutte le forme di pubblicità tipica on line o atipica sviluppatesi *ad hoc* devono essere applicate le norme dettate in materia di comunicazione d'impresa.
Uno sguardo internazionale è d'obbligo perchè la caratteristica essenziale di internet è proprio la sua a-territorialità essendo fruibile in ogni dove purchè vi sia connessione. Per amore di sintesi ci limiteremo alle normative comunitarie e alla loro applicazione nell'ordinamento giuridico italiano.
La prima fonte normativa cui possiamo fare riferimento è la Direttiva 84/450/CEE in materia di pubblicità ingannevole, la quale, all'art. 2 recita: *"Ai sensi della presente direttiva si intende per "pubblicità", qualsiasi forma di messaggio che sia diffuso nell'esercizio di un'attività commerciale, industriale, artigianale o professionale, allo scopo di promuovere la fornitura di beni o servizi"*. Tale definizione è stata ripresa dalla normativa interna dal D. Lgs. 25 gennaio 1992 n. 74 di attuazione della predetta Direttiva e poi ripetuta quasi costantemente nelle formulazioni di successivi interventi de legislatore.
La materia è in continua evoluzione al pari del fenomeno sociale ed economico; a riprova gli ultimi interventi legislativi che prendono le mosse dalla Direttiva 2005/29/CE recepita nel D. Lgs. 6 settembre 2005 n. 206 Codice del Consumo hanno introdotto l'istituto delle cosiddette *"pratiche commerciali"* che comprende una nozione più ampia rispetto a quella di *"pubblicità"*. Restano ferme le norme riguardanti la pubblicità ingannevole e comparativa di cui al D. Lgs. 2 agosto 2007 n. 145 sulla pubblicità ingannevole e comparativa e le conseguenze sleali.
Il Codice del Consumo si applica nei rapporti tra le imprese ed i consumatori mentre il decreto sulla pubblicità trova il suo campo nei rapporti tra imprese; sicché possiamo affermare che nel nostro sistema giuridico la materia che ci occupa prevede un doppio binario di tutela: le norme destinate a regolare i rapporti tra consumatore e impresa e riguardano tutte le pratiche commerciali e le norme che regolano i rapporti tra imprese concorrenti e concernono la pubblicità.

---

[4] Harold D., Google Advertising Tools, New York, O'Reilly, 2006, pag. 84

[5] Pastore A., Vernuccio M., Impresa e comunicazione. Principi e strumenti per il management, Apogeo, 2008, pag. 491

Nel settore della comunicazione dei mezzi media audiovisivi e radiofonici, troviamo il Testo unico dei servizi media audiovisivi e radiofonici[6] che detta una disciplina particolare per le forme di comunicazione pubblicitaria televisiva e radiofonica.
Accanto alla disciplina legislativa statale dobbiamo altresì tenere conto di un *corpus normativo* particolare dettato dall'Istituto dell'Autodisciplina Pubblicitaria, organismo privato creato dagli operatori del settore e dalle associazioni di categoria, il quale ha emanato un Codice di Autodisciplina della Comunicazione Commerciale al quale devono aderire tutti gli iscritti[7].
Sinteticamente gli elementi costituivi e definitori della pubblicità che si traggono da corpus normativo di cui sopra sono:

- ***i)*** il mezzo della comunicazione, che consiste in un qualsiasi messaggio, diretto o indiretto, rivolto alla massa;
- ***ii)*** l'oggetto della promozione che è identificabile in beni o servizi determinati o determinabili;
- ***iii)*** lo scopo individuato nell'incremento dei profitti dell'imprenditore attraverso la promozione diretta della vendita di beni o servizi.

Tali elementi sono quindi applicabili anche alla comunicazione tramite internet.

5. Condizioni di liceità

Dalla lettura del complesso normativo vigente possiamo trarre agevolmente i principi cardine entro i quali la pubblicità e la comunicazione commerciale possono e devono svilupparsi.
Ai fini della tutela del consumatore e della concorrenza leale tra imprenditori la pubblicità deve rispettare i canoni di liceità che si traducono in: trasparenza, verità e correttezza.
Infatti la pubblicità *deve essere palese, veritiera e corretta*[8].
***Palese*:** la pubblicità deve essere immediatamente riconosciuta o riconoscibile come tale e come messaggio promozionale; l'art. 5 del D. Lgs. 145/2007 afferma che la pubblicità deve essere chiaramente riconoscibile come tale. La *ratio* del precetto normativo è quella di non creare confusione con le altre forme di manifestazione della libertà di informazione e comunicazione prima fra tutte l'informazione di cronaca o critica che hanno scopi intrinseci ben differenti come già visto. A conferma il citato art. 5 del D. Lgs. 145/2007 sottolinea che la pubblicità a mezzo stampa deve essere distinguibile dalle altre forme di comunicazione al pubblico con modalità grafiche

[6] Emanato col D. Lgs. 31 luglio 2005 n. 177 e successivamente modificato con D. Lgs. 15 marzo 2010 n. 44.

[7] Si veda per approfondimenti il sito istituzionale www.iap.it. La prima stesura del Codice risale al 1966 e viene aggiornato quasi annualmente.

[8] Art. 19 D. Lgs. 206/2005 e art. 1 D. Lgs. 145/2007.

di evidente percezione.
Il lato oscuro della pubblicità trasparente è dato dall'istituto della *pubblicità occulta* che si traduce in una forma di comunicazione al pubblico di contenuto commerciale senza che venga esplicitata la natura di pubblicità. Ad esempio la pubblicità redazionale che sotto la veste di articolo di giornale o di servizio informativo televisivo o radiofonico, nasconde messaggi pubblicitari dell'inserzionista committente.
Ciò posto, l'interprete del diritto deve applicare il principio in oggetto anche alle comunicazioni promozionali on-line; ne consegue che bisogna sempre rendere appalesato che si tratta di pubblicità. Sicché forme di pubblicità quali i video virali o l'e-buzzing dovrebbero sempre contenere un *disclaimer* che in qualche modo possa rendere edotto il ricevente del messaggio che si tratta di pubblicità.
Ancora: è vietata ogni forma di pubblicità subliminale.
La pubblicità subliminale (dal latino *sub*-sotto e *limen*-soglia) consisterebbe in quel messaggio pubblicitario al di sotto del confine del pensiero conscio, percepito cioè inconsciamente senz ala consapevolezza da parte del ricevente. L'istituto è nato nel 1957 dopo un esperimento di James Vicary, studioso di marketing, il quale ha inserito brevissimi frames all'interno di una pellicola di un film dal titolo Picnic (Joshua Logan, USA 1955) con un tempo di proiezione di 1/3000 di secondo sì da rendere impossibile la percezione degli spettatori. I frames contenevano incitazioni al consumo di Coca-Cola e di pop-corn; il risultato fu che si constatò un incremento di vendite di detti "alimenti". Non esistono studi scientifici che provino gli effetti della pubblicità subliminale né quali siano le modalità affinchè il messaggio possa sortire effetto sul consumatore. Si noti che l'esperimento di Vicary era realizzato durante la proiezione di un film la cui sceneggiatura ruotava attorno ad un picnic con ovvie scene di consumo di alimenti sicchè l'induzione all'acquisto di Coca-Cola e popcorn non è, a mio avviso, imputabile alla recondita efficacia dei frames sul subconscio degli spettatori.
In ogni caso il legislatore ha sancito il divieto assoluto di tale forma di pubblicità che vale anche per la rete.
***Veritiera*:** il messaggio contenuto nella comunicazione pubblicitaria deve corrispondere alla realtà delle informazioni contenute sia pure nella funzione promozionale intrinseca nella natura della pubblicità che deve persuadere il target all'acquisto del bene o del servizio.
All'uopo l'inserzionista può essere chiamato a dimostrare la veridicità dei dati, delle descrizioni e delle affermazioni del messaggio pubblicitario[9].
Ovviamente è consentita l'iperbole (figura retorica che consiste nell'esagerazione della descrizione della realtà tramite espressioni non credibili) cioè quella esagerazione delle qualità del prodotto tali da non essere credibili da parte del consumatore medio. È il caso di gran parte dei video virali i quali con eccesso di creatività cercano il sensazionalismo tramite fiction delle situazioni irreali.

[9] Così art. 8 D. Lgs. 145/2007 e art. 6 Codice IAP.

***Corretta*:** la correttezza del messaggio non si deve limitare esclusivamente alla verità dei contenuti, ma deve concretizzarsi in maniera tale da non creare nel percettore una falsa rappresentazione del bene o del servizio pubblicizzato. Deve rispettare i principi di diligenza professionale, non deve essere idonea a falsare in misura apprezzabile i comportamento economico del consumatore medio target[10].

6. Pubblicità ingannevole

La pubblicità ingannevole rileva sia nei rapporti tra inserzionista e consumatore sia in quelli diretti tra imprese concorrenti. Come si evince dal termine stesso, la pubblicità ingannevole è quella comunicazione commerciale idonea a indurre in errore il destinatario target e a pregiudicare il comportamento economico del medesimo o, in alternativa, a ledere un concorrente[11].
Dal punto di vista dell'elemento soggettivo del dolo o colpa dell'inserzionista occorre evidenziare che a nulla rileva l'esistenza o l'assenza di uno di questi elementi soggettivi ai fini della qualificazione della pubblicità come ingannevole. Basta che ricorrano gli elementi oggettivi della ingannevolezza senza considerare la volontarietà o la negligenza dell'inserzionista al fine di qualificare come illecita la comunicazione in sé.
Ai fini della prova dell'ingannevolezza non occorre verificare se la pubblicità abbia effettivamente indotto in errore il mercato né l'effettiva lesione del comportamento economico del consumatore essendo sufficiente la sua idoneità a pregiudicare la libera scelta economica del medesimo. Si tratta di illecito di pericolo che si concretizza con la mera decettività della pubblicità e non con l'effettivo evento lesivo e ingannevole.
Ritengo che l'interprete del diritto non debba limitarsi alla semplice lettura delle norme della fattispecie che lo occupa, ma debba leggere trasversalmente alla luce delle scienze che studiano la comunicazione e la ricezione del linguaggio e dei segni. È unanimemente riconosciuto che il processo di comunicazione è sempre a due vie sulla base del grafico che si definisce con l'acronimo EMR e cioè:
Leggiamo il grafico con le variabili che si applicano nelle ipotesi di pubblicità ingannevole: l'Emittente è la fonte della pubblicità e cioè l'imprenditore inserzionista; il Messaggio è il contenuto oggettivo della comunicazione e cioè la pubblicità; il Ricevente è colui che percepisce la comunicazione e cioè il mercato target della pubblicità.
La comunicazione si esplica con un percorso di andata dall'imprenditore al mercato target e con un percorso di ritorno dal mercato target all'imprenditore attraverso la scelta del consumatore guidata dalla capacità persuasiva della pubblicità. Ovviamente la scelta può essere positiva, traducendosi nell'acquisto del prodotto o

[10] Cfr. art. 2 D. Lgs. 145/2007 e art. 20 D. Lgs. 206/2005,

[11] Così la definizione dell'art. 2 del D. Lgs. 145/2007.

negativa concretizzandosi nella scelta di un prodotto concorrente o nella rinuncia all'acquisto; quindi particolare attenzione va rivolta ai ricettori della comunicazione. Ecco quindi che appare in tutta la sua importanza il fenomeno della percezione o della ricezione della pubblicità da parte del consumatore target. Ne consegue che *in primis* si dovrà individuare il consumatore medio target della pubblicità e valutare l'ingannevolezza alla luce dei suoi procedimenti percettivi e cognitivi. Tale percorso esegetico potrà risultare difficoltoso per la pubblicità su internet ma i criteri dovrebbero essere qualli guida della comunicazione tradizionale.
In buona sostanza per prodotti di largo consumo si dovrà fare riferimento al *consumatore medio* con le cognizioni e capacità decodificativa della pubblicità dell'uomo medio; diversamente per prodotti specializzati occorrerà procedere con la valutazione dell'esperienza del *consumatore specializzato* in possesso di elementi valutativi più specifici e capacità interpretativa superiore a quella del consumatore medio tanto che potremmo definirlo come *consumatore informato*[12].
Tali criteri devono essere letti alla luce della specificità del caso concreto che nelle fattispecie di internet hanno colori più forti. Ad esempio un consumatore che si sia informato tramite blog, social network e siti di informazione è certamente un utente più specializzato e di conoscenze diverse rispetto alla famosa "massaia di Voghera" tante volte richiamata in tema di confusione marchi.
Per quanto concerne l'idoneità a indurre in errore, l'interprete del diritto, applicando i criteri critici di lettura del consumatore target di cui sopra, dovrà operare un procedimento ermeneutico che deve valutare il messaggio in tutte e sue componenti (visive, - *headline*, testo, *claim* - percettive e concettuali) attraverso un procedimento di analisi che deve seguire il seguente schema logico.
Occorre in primo luogo considerare che il consumatore normalmente percepisce la pubblicità nel suo complesso e in maniera unitaria senza esaminare dettagliatamente le singole componenti che vengono percepite ed elaborate mentalmente nella loro organicità e unitarietà; è questa la *ratio* che impone all'interprete di passare attraverso un procedimento analitico, esaminando tutti i singoli elementi costitutivi della pubblicità, per giungere a una conclusione sintetica valutando la ingannevolezza con una visione olistica. A ben vedere, si tratta di principi di analisi che affondano le proprie radici nelle *Regulae ad directionem ingenii* di Cartesio (1628) il quale aveva individuato tra le regole fondamentali di un metodo quella dell'*analisi* e quella della *sintesi*.
La decettività deve essere valutata solo ed esclusivamente dagli elementi del messaggio in sé senza operare rinvii ad altre comunicazioni sia pure dello stesso inserzionista o ad altre fonti integrative esterne. Il consumatore non ha l'onere di documentarsi tramite un procedimento di ricerca. Ciò vale, ad esempio, per quelle modalità di rinvio nelle pubblicità ad eventuali siti istituzionali dell'inserzionista che

[12] Per maggiori approfondimenti sulla teoria della percezione del consumatore in materia di comunicazione d'impresa si rinvia a S. Dell'Arte, *I Marchi d'impresa nella Comunità Europea*, seconda edizione, 2011, pagg. 77 e segg.

dovrebbero fornire completezza alla comunicazione pubblicitaria.
L'ingannevolezza può tradursi sia in un comportamento attivo, l'inserzionista afferma elementi confusori, sia in un comportamento omissivo, l'inserzionista omette di comunicare elementi rilevati e determinanti tacendo sulla loro esistenza.
Per quanto riguarda gli elementi di valutazione l'art.3 del D. L.gs. indica che per determinare se la pubblicità è ingannevole se ne devono considerare tutti gli elementi, con riguardo in particolare: alle caratteristiche dei beni o dei servizi (quali la loro disponibilità , la natura, l'esecuzione, la composizione, il metodo e la data di fabbricazione o della prestazione, l'idoneità allo scopo, gli usi, la quantità, la descrizione, l'origine geografica o commerciale, o risultati che si possono ottenere con il loro uso); al prezzo o al modo di calcolo; all'identità, alle caratteristiche e ai diritti dell'inserzionista.
Per quanto concerne il secondo elemento costitutivo della pubblicità ingannevole e cioè il pregiudizio al comportamento economico del consumatore e la lesione del concorrente, come già detto, non è necessario che questi si concretizzino materialmente essendo sufficiente che la pubblicità sia virtualmente capace di cagionarli senza che sia necessaria la prova dell'effettivo danno patrimoniale concretamente subito dal consumatore in forza dell'acquisto indotto dall'ingannevolezza della pubblicità. In sostanza ai fini dell'illiceità della pubblicità non è necessario che il consumatore abbia effettivamente proceduto all'acquisto del prodotto o del servizio reclamizzato.

7. Pubblicità comparativa

La pubblicità comparativa può costituire un'utile forma di comunicazione al pubblico potendo fornire delle informazioni tra prodotti che possono rientrare nella scelta di consumo per soddisfare una medesima esigenza, ma si può trasformare in una premeditata azione lesiva ai danni sia dei consumatori che dei concorrenti qualora utilizzata spregiudicatamente e a fini illeciti. A fronte di questa sua dicotomia, il legislatore è intervenuto, a seguito della Direttiva 2005/29/CE delineando le condizioni di liceità della pubblicità comparativa[13].
In primo luogo la comparazione deve rispettare il principio di omogeneità e cioè deve confrontare beni o servizi che soddisfano gli stessi bisogni o si propongono gli stessi obiettivi. Nell'interpretare tale requisito occorre procedere in maniera restrittiva valutando con rigore tutti gli elementi della fattispecie concreta. Ad esempio comparare caratteristiche ed effetti di alimenti destinati ad un pubblico adulto con quelli destinati alla prima infanzia comporta un giudizio tra prodotti non omogenei benchè entrambi appartenenti al *genus* alimenti e soddisfino, in linea generale, gli stessi bisogni.
Il confronto deve avere ad oggetto specifico caratteristiche essenziali, pertinenti,

[13] Cfr. art. 4 D. L gs. 145/2007.

verificabili e rappresentative dei beni posti a confronto; il confronto deve essere oggettivo e può anche limitarsi ad alcune di queste caratteristiche e non necessariamente riguardare l'integrale essenza dei prodotti. Occorre precisare che il requisito della verificabilità s'intende soddisfatto quando gli elementi e i dati utilizzati per la comparazione deI prodotti sono suscettibili di dimostrazione.
Per quanto concerne il *competitor* coinvolto nella comparazione, l'inserzionista non deve ingenerare confusione nel mercato e non deve causare discredito o denigrazione sui segni distintivi, beni o servizi, attività o posizione del concorrente.
Inoltre, la pubblicità comparativa non deve diventare pretesto per trasformarsi in pubblicità parassitaria o per agganciamento essendo vietato trarre indebitamente vantaggio dalla notorietà del concorrente, del suo marchio o dei suoi segni distintivi.
Nè deve assurgere a *escamotage* per presentare i prodotti come imitazione o contraffazione di beni o servizi protetti da un marchio o da una denominazione commerciale depositati.
Infine, per i prodotti recanti denominazione d'origine ci si deve riferire esclusivamente a prodotti aventi la stessa denominazione.

8. Conclusione

La comunicazione d'impresa divulgata tramite la rete è soggetta alle norme dettate per la pubblicità tradizionale. Alla prova dei fatti, ritengo che il corpus normativo di riferimento sia ancora attuale anche per quanto riguarda le nuove forme di comunicazione in rete perchè i limiti della pubblicità, la cui violazione colorerebbe la comunicazione di illecito, sono precisi nella loro individuazione e generici nella loro applicazione in qualsiasi ambito.
Le forme di pubblicità divulgate e create per la rete presentano però delle peculiarità proprie che impongono all'interprete del diritto uno sforzo esegetico nell'applicare le norme in materia.
Tali peculiarità nascono sia dal sistema di internet che dalle diverse caratteristiche dei soggetti che attingono informazioni pubblicitarie dalla rete, con la conseguenza che potrebbero portare a conclusioni in parte differenti rispetto a fattispecie simili ma radicate nella realtà tangibile. mi rendo conto che tale conclusione non conforta il desiderio di certezza degli utenti del diritto ma non si discosta tanto dalla posizione che si avrebbe in materie giuridiche più tradizionali: come scienza umanistica il diritto non è rigore matematico, ma applicazione di principi certi alla luce dell'interpretazione più logica ed equa rispetto al caso concreto.

N. 1 - 2017 · pp. 103-110

Le "app" tra progettazione e trattamento dati personali, alla ricerca di una terza via

Bruno Fiammella ed Esmeralda Colombo[1]

(Relazione di sintesi dell'intervento svolto a SMAU Bologna 2014)

Abstract: Cosa sono realmente le applicazioni che scarichiamo sui nostri dispositivi mobile e come stanno cambiando la nostra vita di relazione, lavorativa e professionale ? Il progresso tecnologico sta davvero procedendo verso una direzione evolutiva della nostra vita quotidiana o siamo soltanto vittime di un sistema professionale e di vita relazionale più stressante ? Occorre cioè che l'individuo si domandi quali siano i concreti vantaggi nell'utilizzare alcune applicazioni per il proprio smartphone ? Per fare questo, occorre dare uno sguardo alla progettazione ed ideazione di questi software che, per fare business, deve essere ideata e concepita intorno all'uomo.

What really are the applications that we download on our mobile devices, and how are they changing our social and professional life? Is technological progress really moving towards an evolutionary direction of our daily lives, or are we victims of a system of professional and relational life that is just more stressful ? Should one ask him/herself what tangible advantages mobile applications bring about? To do this, one should take a look at the planning and design of this kind of software . Indeed, business is tobe conceived and designed for human beings, rather than machines.

Parole chiave: App, mobile phone, progettazione, trattamento dati personali, sicurezza e tecnologia, bussines, etica.

Diversi sono gli interrogativi di cui ci si potrebbe occupare quando si pensa alle nuove *app*, al loro modo di aver invaso il mercato, ed ai bisogni che vorrebbero soddisfare (e creare) nel tentativo di risolvere alcuni problemi quotidiani della vita di relazione dell'individuo.
Il più interessante probabilmente è proprio l'interrogativo finalizzato a comprendere

[1] Avv. Bruno Fiammella, Prof. a contratto di Informatica Giuridica presso la SSPL dell'Univ. Mediterranea dal 2009, esercita da circa 11 anni occupandosi anche di diritto penale e civile delle nuove tecnologie e computer forensics, *www.fiammella.it*. Ha pubblicato circa 20 contributi (14 articoli cartacei, 3 e-book e 3 libri) la maggior parte in tema di insider, criminalità informatica e testi per l'esame di Avvocato. E' docente da circa 8 anni in alcuni Master Universitari II liv., nonché per aziende e privati in tutta Italia su temi pratico - operativi connessi all'ICT. Dott.ssa Esmeralda Colombo, laureata all'Università Cattolica di Milano nel 2011, ha conseguito un Master in Diritto dell'Unione Europea presso il Collège d'Europe di Bruges con una tesi in diritto dell'ambiente. Praticante abilitata, si occupa del *legal* di MyFoody, società volta alla riduzione degli sprechi alimentari.

Articolo pervenuto il 16 Febbraio 2017, approvato il 20 Marzo 2017

se queste applicazioni software per *mobile phone* o per *tablet* cambino veramente la nostra vita di relazione, e ci consentano un miglioramento, o siano soltanto l'ennesimo prodotto del *business* che prima crea un bisogno, e poi ritiene di poterlo soddisfare, transitando per il portafoglio dell'individuo. Sono cioè realmente concepite e progettate intorno all'uomo queste applicazioni *software*, o soltanto intorno alle esigenze del mercato ?

Si dice che uno dei primi passi che il progettista di *software* debba compiere, riguardi la necessità di ridurre i rischi per la sicurezza dell'utente medio, prevedendo e prevenendo, sin dalla fase della scrittura del *software*, alcuni degli incidenti più comuni e dei rischi più conosciuti. In realtà, spesso, la programmazione rimane vittima di questo tipo di esigenze, dimenticando che lo scopo principale di una app è "servire", nel senso che, maggiore sarà la sua utilità pratica, maggiore sarà la possibilità che la stessa ottenga successo e venda.

Questo, quindi, il dilemma: stiamo veramente progettando e costruendo una tecnologia utile ed "amica" che possa risolvere i principali problemi dell'individuo, oppure la progettazione è soltanto schiava del mercato, delle esigenze del fatturato, del *business* e non guarda più verso alcuna direzione etica o funzionale, anche in termini esistenziali o di evoluzione (socio-comunicativa) dell'individuo ?

Esiste la possibilità di trovare una terza via, che non sia ispirata dal marketing o, per lo meno, non solo dal marketing, e che quindi favorisca l'utente ad aderire al trattamento dei suoi dati, senza il timore che questo gli si ritorca contro, apprezzandone, invece, i vantaggi ?

È noto che una app di successo, secondo i principali studi, dipenda dai seguenti fattori: se è utile, perché portatrice di un benessere concreto nella vita relazionale o professionale dell'individuo; se è semplice (più è facile usarla, più piacerà e verrà usata);se risponde ad una necessità della maggioranza delle persone (soddisfa un bisogno, anche apparente, delle masse); se è poco costosa o apparentemente gratuita, per cui l'individuo deve spendere poco per averla. La soluzione del progettista, pertanto, deve essere al tempo stesso brillante e creativa, tenendo presente il prezioso insegnamento in base al quale le migliori soluzioni, sono sempre quelle più lineari.

Accanto a questi principi, o linee guida, elementari ora lievemente tratteggiate, occorre contestualizzare queste premesse, forse un po' filosofico-sociali, fondendole con le principali problematiche pratico-opearative aventi risvolti giuridici di prim'ordine. Ad esempio: è ancora irrisolto il delicato problema di come possano essere ricomposti gli aspetti connessi alla utilizzazione dei *mobile phone* e dei relativi applicativi, da parte dei minori. Il bene infatti (il telefonino *latusensu* inteso) è di proprietà di un adulto, perché così deve essere all'atto dell'acquisto. La scheda telefonica, ugualmente, non può che essere intestata ad uno dei genitori, ma, in realtà, quante volte il dispositivo è materialmente, se non esclusivamente, utilizzato, e quindi in possesso esclusivo dal minore ?

Come risolvere le delicate esigenze connesse alle indagini penali (fondate sul principio espresso dall'art. 27 della Costituzione secondo cui la responsabilità penale è personale) o come risolvere, l'altrettanto delicato dilemma relativo alla necessità

della manifestazione del consenso "libero, consapevole ed informato", relativo ad alcune applicazioni (giochi, *et similia*), quando le stesse non vengono gestite o manifestate (il consenso e le autorizzazioni), di fatto, da un adulto ?
La tecnologia ancora non consente queste "sfumature identificative", sfumature che però hanno una rilevanza fondamentale dal punto di vista giuridico. Posso asserire con valenza giuridica di essere stato efficacemente e scientemente posto a conoscenza del fatto che l'ultimo videogioco sia solo parzialmente gratuito ?
Sul punto, ovvero sulle problematiche inerenti il rapporto tra privacy e trattamento dati degli utenti degli smartphone, l'attenzione del mondo istituzionale è vigile, tanto da essersi formalizzato un intervento dell'Ufficio del Garante della Privacy che si è espresso indicando al progettista- programmatore ed alle case produttrici, la necessità di una semplificazione e comprensione dei meccanismi di funzionamento dei *mobile phone*, raccomandando l'adozione di alcune linee guida cui le case produttrici dovrebbero attenersi.
Ma, le riflessioni cui questo intervento odierno vuole condurre, gli spunti che vuole sollecitare sono di più ampio respiro: come regolamentiamo il delicato problema delle app connesse al trattamento dei dati sanitari ? Può oggi, coscientemente, asserirsi che una app possa salvare la vita ? E' possibile sostituire con una app il medico di fiducia ? C'è da segnalare un effetto rilevante connesso al mondo della salute: la condivisione tra pazienti delle informazioni relative ad una patologia comune, può determinare una svolta o un'accellerazione della ricerca. In questo senso sono molte le iniziative atte a promuovere questa nuova forma di sperimentazione, se così possiamo definirla impropriamente. Certo è che la condivisione delle conoscenze in ambito medico e sanitario, magari tra utenti di differenti continenti, possa capovolgere parzialmente i criteri della ricerca, oggi blindata e secretata per scopi di profitto, indirizzandola, lato utente-paziente, verso una logica di condivisione. Il dato sanitario è evidentemente quello che rappresenta il più alto rischio in termini di trattamento.
In generale, i rischi evidenziati dal Parere espresso dalle Autorità Garanti Europee del 2013 riguardanti tutte le tipologie di dati contenuti negli smartphone e nei tablet, passa proprio per il delicato problema del trattamento: indirizzi, localizzazione geografica, informazioni bancarie, foto, video, sensori, bussole e dispositivi per tracciare gli spostamenti dell'utente, in una parola: geolocalizzazione. La legislazione della UE prevede che ogni persona abbia il diritto di decidere sul trattamento dei propri dati personali e le applicazioni, dunque, per trattare i dati degli utenti, devono prima fornire informative adeguate, in modo da ottenere un consenso che sia veramente "libero ed informato". Il parere delle Autorità Europee individua precisi obblighi, evidenziando che la protezione di dati personali e la sicurezza sono il risultato di azioni coordinate tra gli sviluppatori, i produttori dei sistemi operativi, i distributori; e sono azioni che devono durare nel tempo. Si sconsigliano quindi soluzioni forfettarie ed approssimative: la sicurezza, come è noto, è un processo, ed i dati, in questo senso, devono essere concepiti e trattati. In particolare ci si deve soffermare sugli obblighi dell'informativa e sul consenso riguardo l'archiviazione di informazioni sui terminali degli utenti, nonché sull'utilizzo, da parte delle app, di dati di localizzazione o delle

rubriche dei contatti. Si raccomanda l'adozione di *best practice* che devono essere operative sin dalle fasi iniziali e di sviluppo delle app: l'impiego di identificativi non persistenti, per ridurre al minimo il rischio di tracciamenti degli utenti per tempi indefiniti; la definizione di precisi tempi di conservazione dei dati raccolti; l'impiego di icone *user-friendly* per segnalare che specifici trattamenti di dati sono in corso.
Le app devono inoltre rispettare i requisiti previsti per qualsiasi campagna pubblicitaria. Le comunicazioni devono avvenire in modo trasparente, chiaro ed esaustivo. Un forte dissenso è stato espresso alla possibilità di sviluppare ipotesi di pubblicità ingannevole.
In ordine alle modalità di acquisizione del consenso, appare utile, in questa sede, sinteticamente riportare che, lo stesso, va ottenuto prima che qualsiasi dato venga acquisitoo processato dal dispositivo o dall'applicazione. Ad esempio, in tema di consenso **libero**, non è sufficiente una semplice casella da "spuntare" per poter proseguire, una volta presa visione della *privacy policy*, ma deve essere presente anche una esplicita opzione di uscita, che consenta all'utente di negare il consenso espresso e di "tornare indietro".
Ancora, il consenso deve esser "**informato**": la policy deve contenere alcune informazioni essenziali: l'identità del titolare del trattamento e le informazioni per poterlo contattare, l'indicazione precisa delle categorie di dati personali che la app raccoglierà e tratterà, gli scopi specifici della raccolta, la dettagliata previsione di eventuali soggetti terzi ai quali i dati verranno trasmessi, e infine le modalità di esercizio dei diritti di revoca del consenso e di cancellazione dei dati. Non è corretto raggruppare tutte le indicazioni in illeggibili condizioni legali, oppure fare utilizzo di numerosi collegamenti ipertestuali.
Il consenso espresso deve essere anche "**specifico**": nell'indicare le finalità del trattamento, evitare descrizioni troppo generiche od onnicomprensive. Un forte no si erge contro le indicazioni sommarie del tipo: "per ricerche di marketing" o "per innovare i prodotti". Questi i principi sintetizzabili dalle indicazioni e dalla normativa vigente.
L'attenzione delle autorità intorno a questi aspetti è tanto alta da essere stata proposta, proprio in questi giorni (maggio 2014), una iniziativa dal nome "Sweepday". Si tratta di una azione congiunta di 28 Authority europee che hanno svolto uno "sweep" (indagine a tappeto), scegliendo tra le 50 applicazioni più importanti disponibili su varie piattaforme (Android, iOs, Windows e altre) nel periodo compreso fra il 12 ed il 18 maggio del 2014. L'obiettivo era quello di verificare l'esistenza di comportamenti poco cristallini od irrispettosi della privacy degli utenti. Sono state sottoposte all'esame una serie di app, a campione, per accertarsi che non si impossessino di dati sensibili e non li girino a soggetti terzi ad insaputa dell'utente. L'ufficio del Garante Privacy italiano incentrerà la sua azione di verifica sulle applicazioni mediche. Purtroppo ad oggi non è dato conoscere i risultati che verranno probabilmente pubblicati nel mese di ottobre 2014.
E' dei giorni scorsi, tra l'altro, la notizia che l'Antitrust abbia aperto una istruttoria su alcuni noti operatori del settore. Si tratta di una indagine svolta su alcune società che sviluppano e pubblicano videogiochi scaricabili da internet, in merito alle app che

vengono proposte agli utenti - consumatori e che richiedono, dopo un primo *step* di accesso gratuito, una serie di acquisti successivi per poter continuare a giocare. Il procedimento dovrà verificare se i consumatori potrebbero essere indotti a ritenere che il gioco sia del tutto gratuito o, se comunque, siano effettivamente messi in grado di conoscere preventivamente gli effettivi costi dello stesso. Sussisterebbero, inoltre, carenze informative circa gli strumenti per escludere o limitare la possibilità di acquisti all'interno delle app e le relative modalità di attivazione.
Infine, uno sguardo alla sicurezza: secondo alcuni anche questo aspetto merita un'analisi approfondita: le misure di sicurezza potrebbero essere insufficienti. L'utilizzo delle principali piattaforme presenti sul mercato, apre il problema degli aggiornamenti del software connesso alla interazione tra i vari sistemi che lavorano su piattaforme differenti. Le esistenti differenze evolutive dei sistemi, potrebbero aprire falle di sicurezza, magari trascurate nella spasmodica ricerca della compatibilità e della soddisfazione del cliente.
Di recente, inoltre, si è sentito parlare dei primi *virus e malware* che potrebbero mascherarsi dietro delle finte applicazioni,concepiteappositamente per far credere all'utente di risolvere dei problemi di sicurezza, mentre in realtà, proprio queste applicazioni malevole li starebbero creando. Si aprirebbero nuove vie per delle tradizionali ipotesi di reato (truffa, frode informatica, accesso abusivo ad un sistema informatico o telematico).
Un'ultima riflessione la vorrei esprimere in merito alle difficoltà potenzialmente connesse all'uso promiscuo dello smartphone: lo stesso strumento utilizzato in azienda per lavoro,ed a casa o nella vita privata,per interessi personali. Ridefinire i limiti ed i perimetri della sicurezza, rivedere le policy, rideterminare le responsabilità in caso di incidente, diventerebbero allora delle priorità imprescindibili anche per il datore di lavoro, atteso che i rischi per i clienti dell'azienda e per i dipendenti darebbero alti, anche in termini di responsabilità giuridiche. La perdita di controllo diretto sui dispositivi esterni *mobile*, implica delle falle nell'ambito delle misure di sicurezza correlate.
Concludendo,sarebbe utile auspicare che il processo di informatizzazione di cui siamo protagonisti, vada sempre di pari passo ad un processo di informazione, sulle capacità e sui limiti dei dispositivi stessi da noi utilizzati, accompagnato da una buona dose di buon senso, quando si crea o progetta, e quando si esegue o utilizza.

Case study: l'esperienza di MyFoody in ordine alle necessità di un adeguato trattamento di dati da parte delle "app" – a cura di Esmeralda Colombo.
Myfoody è una start-up innovativa che si basa su di un portale web, accessibile anche tramite applicazione sul cellulare.Il software offre la possibilità alla grande distribuzione organizzata, piccola distribuzione, grossisti e ristorazione organizzata di vendere i propri prodotti alimentari in scadenza, ineccesso o con difetti estetici di confezionamento a prezzi scontati.Con un sistema intelligente di geolocalizzazione, il consumatore visualizza e acquista su MyFoody solo i prodotti della propria area urbana di riferimento.

Grazie ad un sistema mirato di prezzi, l'utente risparmia con questo strumento tra il 30% ed il 70%.Egli può farsi recapitare la spesa a casa con un servizio di consegna a domicilio ad impatto zero, su mezzi non inquinanti, risparmiando anche in termini di tempo.In alternativa, l'utente potrà decidere di "raccogliere" personalmente i prodotti acquistati, dirigendosi ai punti vendita dove essi si trovano.
MyFoody è anche un progetto a vocazione sociale. Di ciò che non viene acquistato sul portale, saranno ogni giorno avvisati telematicamente gli enti non profit alimentari, che provvederanno a raccogliere i prodotti di punto vendita in punto vendita.
Ciò che qui affronteremo è la progettazione della app in merito al trattamento dei dati dell'utente. Premettiamo che i dati che interessano questa app non sono di natura sensibile giuridicamente intesa[2].Ma è necessario, fore, un consenso specifico riguardo ai dati sulla geolocalizzazione dell'utente?
Occorre domandarsi se occorra un primo consenso per il loro trattamento. Se la geolocalizzazione dell'utente fornisse informazionisui suoi spostamenti nell'arco della giornata, sarebbe necessaria una specifica autorizzazione. Ma dato che a questa app interessa unicamente l'indirizzo dell'utente cui inviare, eventualmente, la spesa acquistata on-line, questo tipo di geolocalizzazionenon pone alcun problema.
Questa app, tuttavia, ha interesse a profilare il consumatore perché è interessata ad acquisire informazioni che riguardano le sue abitudini e preferenze alimentari. E' necessario in questo contesto chiedere un consenso preventivo ?Sì[3]. In base a quanto stabilito dall'art. 23 del Codice della privacy: il titolare, vale a dire l'impresa, deve essere in grado di documentare per iscritto un consenso informato, libero e specifico, manifestato dall'interessato per tale finalità. Tale consenso ricomprende, ovviamente, anche il trattamento di dati personali aggregati[4].
In secondo luogo, ci interessa tracciare sessioni e siti web preferiti dell'utente. E' necessario chiedere il suo consenso preventivo? Sì, in base al medesimo art. 23 del Codice.In entrambe le ipotesi di profilazione è anche necessario notificare il

---

[2] I dati raccolti da MyFoody sono, tuttavia, dati personali: «dato personale» è qualunque informazione relativa ad un soggetto, identificato o identificabile, anche indirettamente, mediante il riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale (art. 4, comma 1, lettera b) del Codice Privacy).

[3] E' profilazione quando, oltre a nome, cognome e volumi di spesa, vengono raccolti anche professione, indirizzo mail, numero di cellulare, numero degli scontrini emessi, dettagli dei prodotti e l'esercizio dove erano stati acquistati. Esempio: una nota catena di supermercati ha subito una sanzione amministrativa dell'importo di 54 mila euro per non aver informato correttamente la clientela dell'uso che avrebbe fatto dei dati forniti al momento dell'adesione a un programma di fidelizzazione. Si parlava di "profilazione" e di marketing, ma il modello non consentiva al cliente di esprimere liberamente un consenso separato per i diversi usi dei dati, condizionandoli all'apposizione di un'unica firma. Nel 2010 il Garante ha disposto che per l'accesso ai programmi di fidelizzazione, l'impresa debba dare all'utente la possibilità di rifiutare il consenso al trattamento di dati non necessari e della possibile cessione dei dati così raccolti.

[4] Nell'eventualità in cui il fornitore intenda, invece, utilizzare per la profilazione dati personali aggregati, per i quali non risulti acquisito il consenso degli interessati, sarà necessario che presenti al Garante una richiesta di verifica preliminare, in quanto il trattamento presenta rischi specifici per l'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che il trattamento può determinare (art. 24, comma 1, lett. g) del Codice).

trattamento dei dati personali al Garante (art. 37, comma 1, lettera d, Codice della privacy), attraverso il sito di quest'ultimo (art. 38, Codice della privacy). Un'ulteriore notificazione è necessaria anche quando un tale trattamento cessi[5].Ricordiamo che si è in presenza di profilazione anche quando vengono analizzate le preferenze dichiarate in fase di iscrizione ad un servizio[6].

Piuttosto che con un pop-up, MyFoody intende chiedere all'utente il separato consenso per tali *cookies* durante la fase di registrazione, imprescindibile per effettuare la spesa online[7]. Quindi, vi sarà un *link* informativo ad una pagina dove tutti i *cookies* sono esplicati.

MyFoody acquisisce i dati dell'utente per finalità statistiche e di marketing. E' neces-

---

[5] Di séguito le sanzioni in caso di omessa o incompleta notificazione.
Art. 163 - *Omessa o incompleta notificazione*
1. Chiunque, essendovi tenuto, non provvede tempestivamente alla notificazione ai sensi degli articoli 37 e 38, ovvero indica in essa notizie incomplete, è punito con la sanzione amministrativa del pagamento di una somma da ventimila euro a centoventimila euro.

[6] Sulla profilazione, vedi il regolamento emesso dal Garante nel 2009: "Prescrizioni ai fornitori di servizi di comunicazione elettronica accessibili al pubblico, che svolgono attività di profilazione".

[7] Dal 1° giugno 2012 l'utilizzo di file cookie è possibile solamente con il **preventivo esplicito** consenso degli utenti (D.lgs. 28 maggio 2012 n. 69 e direttiva 2009/136/CE).I titolari dei siti internet devono quindi domandare il consenso agli utenti per installare file cookie nei loro pc e, in caso di mancata risposta o di rifiuto, non possono farlo. Neppure possono utilizzare altri dati idonei a tracciare la navigazione degli utenti.La modifica si colloca nella generale tendenza ad assoggettare sempre più tipi di trattamento dei dati al previo consenso dell'interessato, soprattutto nell'ambito di operazioni di *direct marketing* e pubblicità comportamentali.Alla regola generale fanno eccezione i cookie **strettamente necessari** per:
a) il funzionamento del sito (come ad esempio i cookie che riconoscono il sistema operativo del pc che si connette al sito);
b) consentire l'uso di una specifica funzionalità esplicitamente richiesta dall'utente (ad esempio i cookie per l'autenticazione, per la memorizzazione del "carrello" dei siti e-commerce, per la riproduzione di file multimediali, ecc.).
Pertanto, non rientrano nell'esenzione - e richiedono quindi il preventivo esplicito consenso - i cookie che permettono semplicemente di migliorare il funzionamento del sito, come i cookie che rendono la navigazione più veloce o che mostrano i contenuti di maggiore interesse per l'utente alla luce delle scelte precedenti.
Inoltre, i cookie indicati ai punti a) e b), per godere dell'esenzione, non possono restare nei pc degli utenti oltre il tempo della sessione di navigazione. Questo significa che devono essere eliminati in via automatica con la chiusura del browser. Si può peraltro ritenere che la cancellazione possa essere in alcuni casi ritardata, ad esempio per consentire all'utente di riprendere la consultazione del sito interrotta a causa di problemi di connessione o in caso di chiusura accidentale del browser, come ritenuto anche dal Working Party, che riunisce i rappresentanti dei Garanti della privacy dei paesi UE, in un parere del 7 giugno 2012. La ritardata cancellazione di alcuni cookie, infatti, può permettere la continuazione della compilazione di un modulo, o il recupero del carrello della spesa nei siti di e-commerce, anche dopo la chiusura del browser.
Il consenso preventivo degli utenti può essere ottenuto con un'informativa specifica per i cookie e l'impiego di software di chiaro e semplice utilizzo (ed es. un pop-up con l'indicazione dei tipi di cookie e la richiesta del consenso).
Vedi: http://www.diritto24.ilsole24ore.com/avvocatoAffari/mercatiImpresa/2012/09/privacy-online-e-cookie-necessario-il-consenso-preventivo-dellutente.php (ultimo accesso: 2 giugno 2014). Sui cookies, vedianchel'*Article 29 data protection working partyArticle 29 of Directive 95/46/EC. Itis an independentEuropeanadvisory body on data protection and privacy.*Questo gruppo di lavoro è stato costituito ai sensi dell'art. 29 della Direttiva 95/46/EC. I suoi compiti sono descritti all'art. 30 della Direttiva 95/46/EC e art.15 della Direttiva 2002/58/EC (e-privacy directive).

saria, dunque, un'ulteriore richiesta di consenso all'utente? Sì, qualora i dati venissero comunicati a terzi all'interno dell'UE, sarebbe necessaria un'ulteriore richiesta di consenso all'utente. Il Codice della privacy è ancora più restrittivo quando si parla di comunicazione dei dati a terzi extra-UE (artt. 43 e 44 Codice della Privacy).
Ricordiamo che per le aziende che intendano consentire pagamenti tramite il portale on-line, non è necessaria una richiesta di consenso separato all'utente. Se, invece, il pagamento avvenisse tramite app, con il proprio credito telefonico,vi sarebbero dei requisiti stringenti da seguire, come comunicato dal Garante lo scorso gennaio in materia di *mobile remote payment*[8].
È opportuno, riprendendo in questa sede le riflessione del Prof. Stefano Rodotà, che anche in ambito internautico, adottare venga adottato il "principio di precauzione", sia a livello privatistico, sia istituzionale, per evitare che il rapporto, sempre più importante, tra persona e macchina, venga governato solo dalla logica economica. Se si cerca di ammassare dati su dati da affidare poi ad un algoritmo, le persone sono trasformate in astrazioni. Tutto questo impone di chiedersi se e come la società dell'algoritmo possa essere democratica.

[8] Vedi anche: http://nova.ilsole24ore.com/esperienze/privacy-da-pagamento (ultimo accesso: 31 maggio 2014).

Rivista elettronica di Diritto, Economia, Management

N. 1 - 2017 · pp. 111-115

Il percorso normativo del Fascicolo Sanitario Elettronico e l'esperienza della Regione Sardegna

Marcello Tidore

Sommario: 1. Le principali tappe normative del Fascicolo Sanitario Elettronico fino al recente Decreto del Presidente del Consiglio dei Ministri n. 178 del 29 Settembre 2015 2. Un breve cenno al FSE della Regione Autonoma della Sardegna

Abstract: il Fascicolo Sanitario Elettronico rappresenta una delle più significative testimonianze dell'evoluzione digitale della Sanità. La sua diffusione a livello regionale è stato il primo fondamentale passo, che, però è stato caratterizzato da una forte eterogeneità dovuta all'assenza di una disciplina omogenea di livello legislativo. Oggi, superato questo grande ostacolo, sarà possibile superare i rallentamenti e, nel contempo, creare una circolazione di informazioni sicura e rispettosa dei diritti degli interessati.

1. Le principali tappe normative del Fascicolo Sanitario Elettronico

È stata l'Autorità Garante per la protezione dei dati personali a rilevare l'esigenza una disciplina del Fascicolo Sanitario Elettronico (di seguito FSE) che garantisse i diritti degli interessati. In tal senso, nel mese di marzo dell'anno 2009, fu avviata, dalla suddetta Authority, una consultazione pubblica sulle Linee Guida approvate il 22 gennaio 2009 rivolta a tutti i soggetti e alle categorie interessate e in particolare a all'attenzione "*degli organismi e professionisti sanitari pubblici e privati, dei MMG e dei PLS, degli organismi rappresentativi di operatori sanitari e delle associazioni di pazienti interessati*".

La consultazione si concluse con l'approvazione, in via definitiva, delle "*Linee guida in tema di Fascicolo sanitario elettronico e di dossier sanitario*", che furono pubblicate nella Gazzetta Ufficiale n. 178 del 3 agosto 2009.

Queste primo provvedimento, necessarie a causa della totale assenza di disciplina da parte di fonti Legislative (e Regolamentari), conteneva alcune precisazioni importanti per la salvaguardia del diritto alla riservatezza, confermava la grande utilità del trattamento informatizzato della storia clinica del paziente per il miglioramento dei servizi sanitari e al contempo riteneva il FSE uno strumento di miglioramento delle

Articolo pervenuto il 16 Febbraio 2017, approvato il 20 Marzo 2017

allocazione delle risorse con riduzione di sprechi e di inefficienze.
Successivamente, sulla medesima linea direttrice, il Garante privacy, approvò le Linee guida in tema di referti online (pubblicate il 15 luglio 2009).
Dopo quasi due anni (marzo 2011), finalmente arrivarono le prime Linee guida nazionali sul Fascicolo Sanitario Elettronico da parte del Ministero della Salute, alle quali seguì il Decreto Legge 70 del 13/05/2011 recante le "*Prime disposizioni urgenti per l'economia*" su referti e pagamenti on-line.
Si dovette attendere ancora un altro anno per avere la prima fonte normativa con forza di Legge tutta dedicata al FSE. Si trattava della riforma della Sanità del Ministro della Salute Balduzzi, che con il cosiddetto Decreto Crescita 2.0 (D.L. n. 179 del 18/10/2012, successivamente convertito nella Legge n. 221 del 17/12/2012) introduceva "*Ulteriori misure urgenti per la crescita del Paese*" e colmava la lacuna normativa in materia di FSE temporaneamente colmata dall'Autorità Garante.
Nel 2013, con il "Decreto del Fare" (D.L. n. 69 del 21/06/2013, successivamente convertito nella Legge n. 98 del 9/08/2013) recante "*Disposizioni urgenti per il rilancio dell'economia*", furono introdotte (art. 17) ulteriori misure finalizzate a favorire la realizzazione del FSE.
Il quadro normativo è stato completato soltanto di recente con il D.P.C.M. n. 178 del 29 settembre 2015 "*Regolamento in materia di fascicolo sanitario elettronico*", che è entrato in vigore il 26 novembre del 2015 completato da un disciplinare che contiene i dettagli di tipo tecnico[1].
Detta fonte (art. 12, co. 7) prevede che con uno o più decreti attuativi, acquisito il parere del Garante per la protezione dei dati personali, siano stabiliti: *"i contenuti del FSE e del dossier farmaceutico nonché i limiti di responsabilità e i compiti dei soggetti che ne concorrono all'implementazione, i sistemi di codifica dei dati, le garanzie e le misure di sicurezza da adottare nel trattamento dei dati personali nel rispetto dei diritti dell'assistito, le modalità e i livelli diversificati di accesso al FSE e le modalità di attribuzione di un codice identificativo univoco dell'assistito che non consenta l'identificazione diretta dell'interessato, i criteri per l'interoperabilità del*

[1] Per un quadro completo della disciplina del FSE, le fonti sopraccitate vanno necessariamente coordinate con quelle del seguente elenco:
- il Decreto del Presidente della Repubblica 26 marzo 2008 -"Attuazione dell'articolo 1, comma 810, lettera c), della legge 27 dicembre 2006, n. 296 in materia di regole tecniche e trasmissione dati di natura sanitaria, nell'ambito del Sistema pubblico di connettività". Pubblicato nella Gazzetta Ufficiale del 28 maggio 2008, n. 124;
- il Decreto Legislativo 7 marzo 2005 n.82 "Codice dell'Amministrazione Digitale"; il Decreto Legislativo 196/03 Codice Privacy;
- la Legge 27.12.2006, n. 296, art. 1, comma 810 lettera c), che prevede il collegamento telematico in rete dei medici prescrittori del SSN;
- il DPCM 26.03.2008, in materia di regole tecniche e trasmissione dati di natura sanitaria. In particolare, l'art. 4 che disciplina la trasmissione telematica dei dati delle ricette al Ministero dell'Economia e delle Finanze (MEF);
- il DM 02.02.2009, che stabilisce le modalità di avvio sperimentale dell'applicazione delle disposizioni di cui il detto art. 4. In particolare prevede che la sperimentazione sia definita attraverso accordi specifici tra la Regione, il MEF e il Ministero del lavoro, della salute e delle politiche sociali.

FSE a livello regionale, nazionale ed europeo, nel rispetto delle regole tecniche del Sistema Pubblico di Connettività".

Così, sulla base della predetta disposizione, il Tavolo Tecnico, coordinato dall'Agenzia per l'Italia Digitale e dal Ministero della Salute con i rappresentanti del Ministero dell'Economia e delle Finanze, delle Regioni e delle Province Autonome, nonché dal Consiglio Nazionale delle Ricerche e del CISIS (Centro Interregionale per i Sistemi Informatici, Geografici e Statistici), ha definito lo schema generale del Decreto attuativo, che stabilisce i contenuti obbligatori e facoltativi del FSE.

Nello specifico, in primo luogo, prescrive, in modo uniforme per tutti i fascicoli istituiti da Regioni e Province autonome, che tali contenuti siano costituiti da un nucleo minimo di dati e documenti obbligatori, nonché da dati e documenti integrativi.

In merito alla protezione dei dati personali, in ossequio alla disciplina di settore, si definiscono le regole di manifestazione del consenso dell'interessato e quelle relative al contenuto dell'informativa che gli operatori sanitari sono tenuti a rendere al paziente.

Nello specifico si dispone che l'informativa debba indicare tutti gli elementi richiesti dall'art. 13 del D.lgs. 196/03. Per quanto concerne il consenso, invece, viene operata la distinzione tra consenso all'implementazione e consenso alla consultazione, che sono diversi dal consenso ordinario che viene prestato dall'interessato sottoposto a eventuali prestazioni sanitarie, poiché si basano su un'attività di trattamento dei dati personali di tipo diverso.

Il consenso alla creazione del FSE, infatti, autorizza l'accesso al fascicolo per finalità di cura, di ricerca e di governo; il consenso alla consultazione, invece, si esprime in un momento successivo e la sua eventuale mancanza autorizzerebbe l'uso dei dati soltanto per fini di governo e di ricerca ai sensi dell'art. 12, commi 3-bis e 5, e degli artt. 7 e 8 del Decreto in esame.

Il consenso anche dopo che è stato manifestato può essere successivamente revocato, anche per via telematica e nel caso in cui l'assistito non abbia compiuto la maggiore età o sia sottoposto a tutela, sia i consensi devono essere espressi dal soggetto che esercita la potestà o da colui che lo rappresenta legalmente (in qualità di tutore, amministratore di sostegno o altra legittimazione) mediante l'esibizione di un proprio documento di identità.

Quale massima espressione del diritto di autodeterminazione, nella manifestazione del consenso è riconosciuto il diritto dell'interessato all'oscuramento dei dati e dei documenti sanitari e socio-sanitari che lo riguardano, a tutti i soggetti abilitati all'accesso, e anche che questi ultimi non vengano a conoscenza di tale scelta da parte del paziente (oscuramento dell'oscuramento).

Elemento di particolare novità, rispetto alla disciplina precedente, è rappresentato dal fatto che nel Decreto è presente una netta distinzione tra i titolari del trattamento in base a ciascuna finalità per cui il FSE è stato istituito:

- nel caso di trattamento per finalità di cura, sono qualificati come titolari i soggetti del SSN e dei servizi socio-sanitari regionali che prendono in cura l'assistito;

- per i trattamenti effettuati per scopi di ricerca, sono invece titolari le Regioni e Province Autonome e il Ministero della salute, nei limiti delle rispettive competenze attribuite dalla legge;
- per le finalità di governo, titolari sono le Regioni e Province Autonome, il Ministero della Salute e il Ministero del Lavoro e delle Politiche Sociali.

Una parte del Decreto dettaglia, con rigore, le misure di sicurezza che gli i titolari del trattamento debbono adottare per la protezione dei dati trattati mediante il FSE. In particolare, è disposto, da una parte, che nell'utilizzo di sistemi di memorizzazione o archiviazione dei dati vanno attuati idonei accorgimenti per la protezione dei dati registrati rispetto ai rischi di accesso abusivo, furto o smarrimento parziali o integrali dei supporti di memorizzazione o dei sistemi di elaborazione portatili o fissi. Dall'altra, per la consultazione in sicurezza dei dati, gli accessi al FSE da parte degli operatori del SSN, dovranno essere tracciabili e la consultazione di esso dovrà essere limitata, solo per il tempo strettamente necessario alla erogazione delle cure. Elemento di particolare novità è l'introduzione dell'obbligo di segnalazione al Garante, entro una settimana dal verificarsi dell'evento, nel caso in cui le informazioni trattate nell'ambito del FSE subiscano violazioni tali da comportare la perdita, la distruzione o la diffusione indebita di dati personali. La comunicazione deve descrivere la natura della violazione dei dati personali occorsa e l'indicazione delle categorie e del numero di interessati coinvolti.

Seguendo la struttura del Decreto, nella parte finale si trovano le indicazioni con le quali vengono definiti i criteri per l'interoperabilità del FSE a livello regionale, nazionale ed europeo, nel rispetto delle regole tecniche del Sistema Pubblico di Connettività.

Un breve cenno al FSE della Regione Autonoma della Sardegna

Nella regione Sardegna il FSE è sviluppato nell'ambito di un progetto denominato MEDIR, che prevede un modello omogeneo di Sistema Informativo Sanitario Regionale mediante l'interconnessione in rete del personale medico e l'integrazione dei sistemi informativi esistenti.

L'l'infrastruttura, che ha permesso al realizzazione del FSE, è stata creata per mezzo di un sistema sanitario informatizzato su una rete telematica di collegamento tra i MMG, PLS e altre strutture sanitarie.

Tale rete integrata consente agli operatori (e ai cittadini) di disporre delle informazioni sanitarie relative ai singoli assistiti attraverso il tracciamento degli eventi che hanno interessato la loro storia clinica. Sono consentiti gli accessi alle diverse strutture sanitarie del territorio regionale e in futuro, con le dovute integrazioni, anche a strutture extraregionali. Il sistema permette, inoltre, il costante aggiornamento

delle informazioni contenute nella scheda clinica del MMG e del PLS attraverso la comunicazione tra FSE, il repository del sistema e la cartella del medico di fiducia.
In conclusione, è doveroso un breve riferimento al rigore con il quale è stato valutato l'impatto del FSE Sardegna con la disciplina dettata in materia di protezione dei dati personali. In tal senso, nel rispetto dei dettami del D.lgs. 196/03, i documenti contenuti nel FSE Sardegna sono garantiti da elevati livelli di sicurezza e protezione informatica e telematica. In tal senso, il paziente può accedere al FSE soltanto se è in possesso della propria TS-CNS dotata di microchip, che deve essere preventivamente attivata presso gli sportelli dedicati e che è protetta da un PIN). Si consideri, inoltre, che la raccolta di dati personali sanitari avviene soltanto se l'assistito ha fornito il proprio consenso al medico di base, al pediatra o all'Azienda Sanitaria Locale di appartenenza. Consenso che egli ha la possibilità di revocare in ogni momento presso gli stessi soggetti, senza alcuna conseguenza negativa sulla possibilità di usufruire di prestazioni mediche e assistenza sanitaria.

Rivista elettronica di Diritto, Economia, Management

N. 1 - 2017 · pp. 116-131

La conservazione dei documenti informatici per i professionisti, le aziende e la P.A.

Gianluca Satta - Giuliano Marconi

Abstract: L'articolo illustra le nuove "regole tecniche sui sistemi di conservazione", emanate con d.p.c.m. 3 dicembre 2013 e pubblicate nella G.U del 12 marzo 2014, con le quali sono state definite nuove misure e adempimenti per i soggetti pubblici e privati in materia di gestione e conservazione dei documenti informatici. Tra le novità più significative: il superamento della distinzione fra conservazione di documenti informatici e conservazione sostitutiva di documenti analogici, l'introduzione di un sistema di conservazione in grado di garantire autenticità, integrità, affidabilità, leggibilità e reperibilità dei documenti informatici, la previsione della figura del Responsabile della conservazione e, infine, l'obbligo del Manuale della conservazione.

Parole chiave: sistema di conservazione, documenti informatici, regole tecniche, codice dell'amministrazione digitale, modelli organizzativi, responsabile della conservazione, manuale di conservazione.

1. Introduzione

Con il Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013, pubblicato in Gazzetta Ufficiale il 12 marzo 2014 (suppl. ord. n. 20, serie gen. 59), sono state emanate le regole tecniche, ai sensi dell'art. 71 del Codice dell'Amministrazione Digitale (in seguito CAD), in materia di sistema di conservazione dei documenti informatici. Il decreto si compone anche di cinque allegati in cui sono dettagliati gli aspetti tecnici in merito ai formati digitali, agli standard da utilizzare, alle caratteristiche del pacchetto di archiviazione, ai metadati e, infine, è stato disposto anche un glossario con le definizioni dei principali termini utilizzati.

La nuova disciplina, entrata in vigore l'11 aprile 2014, ha abrogato la precedente

Articolo pervenuto il 16 Febbraio 2017, approvato il 20 Marzo 2017

deliberazione CNIPA n. 11/2004, contenente le "*Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali*".
I sistemi di conservazione già esistenti e strutturati sulla base delle precedenti regole tecniche, pur essendo considerati validi, dovranno essere adeguati alle nuove disposizioni tecniche entro l'11 aprile 2017[1].

1.2 Le novità delle regole tecniche.

La principale novità delle nuove regole sulla conservazione riguarda il superamento della distinzione tra conservazione dei documenti analogici e conservazione dei documenti digitali, presente nella precedente disciplina, oggi abrogata. Le regole tecniche, infatti, prevedono un unico sistema di conservazione, valido ed applicabile a tutti i documenti informatici, in linea con le nuove regole tecniche sul documento informatico.
Tali regole, attualmente non ancora in vigore[2], introducono una nuova concezione di documento informatico attraverso la definizione delle modalità di formazione dello stesso, colmando un vuoto normativo lasciato dal Codice dell'amministrazione digitale. Infatti, secondo la definizione del CAD, il documento informatico è la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti; lo stesso Codice però, pur prevedendo la piena validità ed efficacia dello stesso, a condizione che siano rispettate le norme tecniche regolamentari, nulla dice sulle modalità di formazione del documento informatico.
Ai sensi dell'art. 3 dell'attuale bozza delle regole tecniche, il documento informatico è quello ottenuto direttamente mediante l'uso di appositi software (es. *word processors* o elaboratori di testo), e sono i cosiddetti documenti digitali "nativi". I documenti informatici sono generati anche attraverso l'acquisizione di un documento informatico per via telematica o su supporto informatico (es. attraverso il download da un server cloud o dalla posta elettronica), l'acquisizione della copia per immagine su supporto informatico di un documento analogico (es. il *file* "pdf" ottenuto con la scansione di un documento cartaceo) e, infine, mediante l'acquisizione della copia informatica di un documento analogico (es. il *file* "pdf" avente contenuto identico ad un documento cartaceo).
Il documento informatico, quindi, è non solo quello "nativo", ma anche quello ottenuto dal processo di trasformazione dal formato cartaceo al formato digitale. Per questa ragione, le regole tecniche sulla conservazione prevedono un unico sistema di conservazione che si applica ai documenti informatici, formati secondo le moda-

[1] Trentasei mesi dalla data di entrata in vigore delle regole tecniche di cui al D.P.C.M. 3 dicembre 2013.

[2] La bozza delle regole tecniche sul documento informatico è pubblicata sul sito web dell'Agid (Agenzia per l'Italia Digitale), l'autorità che coordina le azioni in materia di innovazione e promuove le tecnologie ICT a supporto della pubblica amministrazione.

lità sopra descritte. Anche la conservazione non è più detta "sostitutiva" in quanto, oggetto di attenzione del legislatore non è più il documento cartaceo, destinato ad essere sostituito da un equivalente documento digitale, ma solo ed unicamente il documento informatico, ottenuto attraverso le modalità già esaminate.
Rispetto alla precedente disciplina, è stato introdotto anche il concetto di "sistema di conservazione", definito come un sistema che assicura la conservazione, dalla presa in carico sino all'eventuale scarto, dei documenti informatici e dei fascicoli informatici con i metadati associati, garantendo, al contempo, autenticità, integrità, affidabilità, leggibilità e reperibilità.
Figura centrale è il responsabile della conservazione, il "*dominus*" del sistema a cui è affidata la gestione e la definizione delle politiche di conservazione dei documenti informatici, individuato tra i soggetti interni all'ente che ha l'obbligo di conservazione.
Le regole tecniche, infine, sono state elaborate nel rispetto del cd. principio della neutralità tecnologica, spesso adottato nella legislazione in ambito informatico. Per garantire la massima espressione della libertà di autodeterminazione e della libera concorrenza nel mercato, il legislatore individua le caratteristiche generali e fissa gli obiettivi da raggiungere, senza imporre l'adozione di una particolare tecnologia, e lasciando la libertà di scelta al singolo. Il sistema di conservazione dei documenti informatici, infatti, è definito individuando le caratteristiche e gli obiettivi che questo deve assicurare, lasciando al responsabile della conservazione la possibilità di individuare quali strumenti tecnologici utilizzare.

2. Ambito di applicazione del CAD e delle Regole tecniche.

L'ambito soggettivo di applicazione delle norme sulla conservazione dei documenti informatici è definito dal combinato disposto dell'art. 2 delle regole tecniche di cui al D.P.C.M. 3 dicembre 2013 e dell'art. 2, commi 2 e 3 del Codice dell'Amministrazione Digitale.
I destinatari delle norme tecniche sono tutte le amministrazioni dello Stato[3]. Inoltre,

[3] Richiamando espressamente l'art. 1, comma 2, D. Lgs. 30 marzo 2001, n. 165, l'ambito di applicazione del CAD (e delle regole tecniche dettate in sua applicazione) comprende: "*gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le Regioni, le Province, i Comuni, le Comunità montane. e loro consorzi e associazioni, le istituzioni universitarie, gli Istituti autonomi case popolari, le Camere di commercio, industria, artigianato e agricoltura e loro associazioni, tutti gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti del Servizio sanitario nazionale l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN) e le Agenzie di cui al decreto legislativo 30 luglio 1999, n. 300. Fino alla revisione organica della disciplina di settore, le disposizioni di cui al presente decreto continuano ad applicarsi anche al CONI*"

nell'ambito della pubblica amministrazione, per individuare correttamente l'ambito di applicazione della normativa sulla conservazione è necessario fare riferimento anche ai criteri di riparto delle competenze previsto dall'art. 117 della Costituzione. In virtù del richiamo espresso all'art. 3 del D.P.R. 28 dicembre 2000, n. 445 (Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa), le disposizioni di cui al capo II del CAD (dedicato al documento informatico e firme elettroniche, trasferimenti, libri e scritture), unitamente alle regole tecniche in commento, si estendono anche a tutti i cittadini italiani e dell'Unione europea, alle persone giuridiche, alle società di persone, agli enti, alle associazioni e ai comitati aventi sede legale in Italia o in uno dei Paesi dell'Unione europea.
La disciplina sulla conservazione si applica, altresì, ai soggetti esterni a cui è affidata la gestione o la conservazione dei documenti informatici e ai conservatori accreditati ai sensi dell'art. 44-bis del CAD.
Quanto all'ambito oggettivo di applicazione, per individuare i soggetti che hanno l'obbligo di adottare un sistema di conservazione dei documenti informatici si deve fare riferimento ai destinatari delle norme sopra richiamate.
L'art. 20, comma 5 del CAD prevede che gli obblighi di conservazione e di esibizione di documenti, si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se le procedure utilizzate sono conformi alle regole tecniche in materia di sistemi di conservazione di cui al D.P.C.M. 3 dicembre 2013. Pertanto, solamente coloro che hanno l'obbligo di conservare documenti per i quali è prevista la produzione direttamente ed unicamente in formato digitale, senza poter utilizzare il formato cartaceo ai fini della validità legale dello stesso, patiranno l'obbligo di procedere alla conservazione. Devono quindi sussistere due condizioni: l'obbligo di conservazione e l'obbligo di produzione in formato elettronico.
La Pubblica Amministrazione è, senza dubbio, il principale destinatario delle regole sulla conservazione, in quanto tutta la documentazione amministrativa necessita di essere conservata per rispondere ad esigenze di carattere pubblico, per garantire il corretto funzionamento dell'intero apparato burocratico e, infine, per ragioni di interesse storico. Tuttavia in assenza di una norma che definisca, per la pubblica amministrazione, un obbligo generale di produrre i documenti in formato elettronico, bisogna fare riferimento alle singole disposizioni che individuano i settori nei quali, anche indirettamente, è prevista la formazione obbligatoria di documenti informatici[4]. Più in generale, attraverso il ricorso alle tecnologie dell'informazione nei

[4] A titolo di esempio si pensi alle pubblicazioni legali in forma cartacea. A decorrere dal 1° gennaio 2011, con la L. 18 giugno 2009, n. 69, è stato riconosciuto effetto di pubblicazione legale agli atti e ai provvedimenti amministrativi pubblicati sui siti informatici delle amministrazioni e le pubblicazioni in forma cartacea non hanno più effetto di pubblicità legale. Dal 2013, anche le pubblicazioni delle procedure ad evidenza pubblica e i bilanci sono effettuate in formato digitale. Anche la presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti, tra le imprese e le amministrazioni pubbliche deve avvenire esclusivamente utilizzando le tecnologie dell'informazione e della comunicazione. Infine, anche nell'ambito della sanità elettronica le amministrazioni regionali hanno già introdotto nuovi strumenti, quali la cartella sanitaria elettronica, il fascicolo sanitario elettronico, la ricetta elettronica, con l'obiettivo di digitalizzare tutto il sistema sanitario.

procedimenti amministrativi le pubbliche amministrazioni realizzano gli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza e semplificazione, previsti dal Codice dell'Amministrazione Digitale. Tra le misure introdotte, in linea con tali obiettivi, rientra l'obbligo per le amministrazioni di utilizzare mezzi informatici per la formazione dei documenti originali[5], l'introduzione del protocollo informatico e della gestione digitale dei flussi documentali.

Alla luce di queste osservazioni, con il processo di dematerializzazione delle attività e dei procedimenti amministrativi, quasi tutta la produzione documentale delle amministrazioni pubbliche si sviluppa solo ed esclusivamente in formato digitale e, conseguentemente, per la pubblica amministrazione è necessario il ricorso ai sistemi di conservazione al fine di garantire le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità dei documenti informatici.

Sotto il profilo civilistico, per il settore privato delle imprese e dei professionisti, l'art. 2220 del Codice Civile prevede l'obbligo di conservazione per dieci anni dei documenti contabili, delle fatture, delle lettere e dei telegrammi ricevuti e delle copie delle fatture, delle lettere e dei telegrammi spediti[6]. In ambito fiscale, l'art. 22 del D.P.R. 29 settembre 1973, n.600 stabilisce l'obbligo di conservazione delle scritture contabili obbligatorie e la relativa documentazione fino a quando non siano definiti gli accertamenti relativi al corrispondente periodo d'imposta[7].

Per i soggetti privati, quindi, l'unico documento per il quale è previsto l'uso esclusivo del formato digitale per la validità legale dello stesso, e la sua conservazione obbligatoria, è la fattura elettronica emessa in favore della P.A.. Infatti, tutti i privati che effettuano prestazioni in favore della pubblica amministrazione devono emettere, trasmettere, conservare e archiviare la fattura esclusivamente in formato elettronico.

In tutti i casi in cui è riconosciuta la validità legale del documento cartaceo, ovvero quando la normativa non impone una scelta in favore del digitale, la produzione dei documenti esclusivamente in formato elettronico rappresenta un'alternativa, seppur vantaggiosa in termini di praticità ed economicità, ma non un obbligo. Ne consegue che anche il ricorso ai sistemi di conservazione dei documenti informatici è facoltativo quando, per i destinatari delle norme tecniche e del CAD, non sia previsto un obbligo di legge che imponga la produzione di documenti digitali.

---

5 Art. 40 del CAD.

6 Gli imprenditori commerciali devono, inoltre, conservare il libro giornale, il libro degli inventari e le scritture contabili. Le società per azioni devono conservare il libro soci, il libro delle obbligazioni, il libro delle adunanze delle assemblee, del consiglio di amministrazione (o del consiglio di gestione), del collegio sindacale, del comitato esecutivo, dell'assemblea degli obbligazionisti e il libro degli strumenti finanziari. Le società a responsabilità limitata devono conservare il libro soci, il libro delle decisioni dei soci, degli amministratori, il libro del collegio sindacale o del revisore.

7 In materia fiscale, alcuni dei documenti di cui è obbligatoria la conservazione sono: i registri IVA, il registro dei corrispettivi per mancato o irregolare funzionamento del registratore di cassa, il registro unico e quello riepilogativo, il registro delle ricevute fiscali, il registro merci, il registro onorari (per i professionisti). Infine, per i datori di lavoro è previsto l'ulteriore obbligo di tenuta del libro matricola, del libro paga e del registro degli infortuni.

2.1 La conservazione dei documenti nel CAD

La regola generale[8] prevede che tutti i documenti degli archivi, le scritture contabili, la corrispondenza e qualunque atto, dato o documento per i quali è prescritta la conservazione per legge o regolamento, possono (e non devono) essere riprodotti su supporto informatico. Qualora si intenda optare per la conservazione digitale, al fine di mantenere la piena validità legale dei documenti informatici[9], devono essere rispettate le regole tecniche previste nel D.P.C.M. 3 dicembre 2013. Il legislatore, quando non ha previsto un obbligo di produzione dei documenti in formato digitale, ha lasciato al singolo la facoltà di ricorrere a questa soluzione e ne ha dettato le regole da seguire.
Per agevolare la gestione dei documenti informatici, nei casi in cui sia obbligatorio, l'archiviazione degli stessi[10], ferma la loro conservazione permanente con modalità digitali, può essere eseguita anche con modalità cartacea, ma solo per rispondere alle esigenze correnti. Pertanto, l'archiviazione cartacea dei documenti informatici è consentita solamente durante la fase iniziale del ciclo di vita del documento[11], al fine di garantirne l'immediata accessibilità e reperibilità fino alla conclusione della pratica o del procedimento a cui il documento si riferisce.

3. La conservazione e le regole sulla privacy

Le norme previste dal Codice dell'Amministrazione Digitale e le regole sulla conservazione dei documenti informatici devono essere applicate nel rispetto della disciplina rilevante in materia di trattamento dei dati personali.
Per comprendere le ragioni dello stretto rapporto tra le due discipline, è sufficiente richiamare l'attenzione sul concetto di dato personale, da intendersi come qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale. Tutti i documenti oggetto di conservazione, salvo qualche eccezione particolare, contengono dati o informazioni personali. Per trattamento si intende qualunque tipo di operazione svolta sui dati[12], tra cui anche la

---

[8] Art. 43 del CAD.

[9] I documenti possono essere sia nativi-digitali che documenti nativi-analogici memorizzati su supporto digitale.

[10] Sulla base delle definizioni contenute nell'allegato n.1 delle regole tecniche, per "archiviazione" si intende l'attività di inserimento e ordinamento del documento all'interno dell'archivio, "*un complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività*"

[11] Questa fase può essere meglio definita come "archivio corrente"

[12] L'art. 4, comma 1, lett. a) considera trattamento: "*la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il*

conservazione. Conservare un documento implica, quindi, trattare i dati personali in esso contenuti; per questa ragione, come richiesto dal Garante per la protezione dei dati personali nel parere n. 214 del 24 aprile 2013 sullo schema delle regole tecniche sulla conservazione dei documenti informatici, la conservazione deve avvenire nel rispetto delle norme di cui al D. Lgs. 196/2003 (Codice della Privacy).
In particolare, il sistema di conservazione deve essere organizzato in modo tale da assicurare il rispetto delle regole previste dagli articoli da 31 a 36 del Codice della Privacy e dal disciplinare tecnico di cui all'allegato B, sulle misure minime e sulle misure idonee di sicurezza. Le prime sono tassativamente elencate nell'allegato B e comprendono, per i trattamenti effettuati con strumenti elettronici, come nel caso dei sistemi di conservazione, l'adozione di un sistema di autenticazione informatica, di autorizzazione, di misure informatiche atte ad impedire l'intrusione nei sistemi, il salvataggio periodico dei dati e il recupero degli stessi in caso di distruzione. Le misure idonee di sicurezza, invece, sono le stesse misure adottate in relazione alle tecnologie al momento conosciute e alle caratteristiche del trattamento, e sono definite in modo tale da ridurre al minimo i rischi che il sistema di conservazione concretamente comporta[13].
Tali adempimenti in materia di misure di sicurezza si applicano a tutti i trattamenti di dati effettuati al fine di conservare i documenti informatici, e si aggiungono a tutti gli altri adempimenti che ciascun soggetto titolare del trattamento deve eseguire nel rispetto delle norme di cui al D. Lgs. 196/2003.
Per garantire il rispetto e il coordinamento delle regole sopra richiamate, il legislatore ha previsto che il responsabile della conservazione operi di intesa con il responsabile del trattamento[14], e con altre figure responsabili della sicurezza e dei sistemi informativi, tra cui rientrano sicuramente gli amministratori di sistema[15] e, nell'ambito delle pubbliche amministrazioni, i soggetti responsabili dell'ufficio previsto dall'art. 17 del CAD, il responsabile o il coordinatore della gestione documentale.
In linea con quanto espresso dal Garante nel parere sullo schema delle regole, un unico soggetto, laddove possibile, può ricoprire il ruolo di responsabile della conservazione e di responsabile del trattamento, limitatamente ai dati personali contenuti nei documenti oggetto del sistema di conservazione. Non sempre però questo è possibile, per due motivi: da una parte il titolare non è obbligato a nominare un responsabile del trattamento e, dall'altra, la conservazione può essere affidata ad un

raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati"

[13] L'analisi deve tener conto dei rischi di distruzione e perdita dei dati, di accesso non autorizzato e di trattamento eseguito per finalità diverse dalla conservazione.

[14] L'art. 4, comma 1, lett. g) del D. Lgs. 196/2003, definisce il responsabile dl trattamento come: "*la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali*"

[15] L'amministratore di sistema è una figura obbligatoria, sia per i privati che per le pubbliche amministrazioni, introdotta con Provv. Garante Privacy del 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008), con il compito di vigilare sul corretto utilizzo dei sistemi informatici.

soggetto esterno ai sensi dell'art. 5 delle regole tecniche.
Nel primo caso, l'assenza di nomina del responsabile del trattamento non esclude l'obbligo di nominare il responsabile della conservazione il quale, seppur non previsto da alcuna norma, dovrà coordinarsi direttamente con il titolare del trattamento. Ciò si desume dal fatto che il titolare, quale "*dominus*" del trattamento, può decidere se delegare o meno una parte delle sue funzioni ad un responsabile del trattamento. Inoltre, la nomina del responsabile esprime una delega di funzioni e, venendo a mancare tale nomina, le funzioni continuano a restare in capo al soggetto delegante, ovvero il titolare. Non vi è dubbio che, per effetto dell'introduzione della nomina obbligatoria del responsabile della conservazione, il titolare del trattamento dovrà valutare l'opportunità di delegare ad esso anche le funzioni di responsabile del trattamento, limitatamente ai dati trattati nel sistema di conservazione.
Nella seconda ipotesi, quando il responsabile della conservazione affida la gestione della conservazione ad un soggetto esterno (cd. *outsourcing*), il ruolo del responsabile del trattamento e della conservazione non possono più coesistere in capo alla stessa persona. Infatti, da una parte, l'esternalizzazione del processo di conservazione non implica l'attribuzione al soggetto esterno del ruolo di responsabile della conservazione, che rimane sempre interno all'amministrazione o ente (pubblico o privato)[16]. Dall'altra, il soggetto esterno affidatario della conservazione dei documenti informatici, dovrà assumere il ruolo di responsabile esterno del trattamento dei dati. In ogni caso, la nomina ai sensi del codice privacy deve essere eseguita con atto espresso, non potendo essere implicita nella nomina del soggetto responsabile della conservazione, o nell'atto con cui quest'ultimo affida la gestione all'esterno.

4. Il sistema di conservazione

Il sistema di conservazione è quel complesso di procedure e soluzioni tecnologiche necessarie ad assicurare la conservazione a norma dei documenti elettronici nonché la disponibilità dei fascicoli informatici mediante l'adozione di regole, procedure, tecnologie e modelli organizzativi per la gestione di tali processi. Il sistema di conservazione assicura[17], dalla presa in carico dal produttore fino all'eventuale scarto, la conservazione degli oggetti in esso conservati, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità. Gli "oggetti" cui fa riferimento la norma sono i documenti informatici (o, nel caso di una pubblica amministrazione,

[16] L'art. 44, comma 1-*ter*, CAD prevede che: "*il responsabile della conservazione può chiedere la conservazione dei documenti informatici o la certificazione della conformità del relativo processo di conservazione a quanto stabilito dall'articolo 43 e dalle regole tecniche ivi previste, nonché dal comma 1 ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative e tecnologiche*"

[17] Ai sensi del combinato disposto dell'art. 3 del D.P.C.M. 3 dicembre 2013 e dell'art. 44, comma 1, del Codice dell'Amministrazione Digitale.

i documenti amministrativi informatici) nonché i fascicoli informatici - ovvero le aggregazioni documentali informatiche - contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che appartengono al fascicolo o all'aggregazione documentale. Sia nel primo sia nel secondo caso gli anzidetti "oggetti da conservare" dovranno essere accompagnati dai metadati[18] a loro associati.
Il sistema di conservazione deve altresì assicurare il trattamento dell'oggetto conservato per l'intero ciclo di gestione, ovverossia per l'intero arco temporale di esistenza del documento informatico[19], dalla sua formazione alla sua eliminazione o conservazione nel tempo. Soprattutto, il sistema di conservazione deve garantire l'accesso all'oggetto conservato indipendentemente dall'evoluzione del contesto tecnologico. Proprio per garantire questo, il decreto in esame ha individuato i riferimenti per gli standard, le specifiche tecniche e i formati utilizzabili per il sistema di conservazione.

4.1. Ruoli e facoltà dei soggetti coinvolti del procedimento di conservazione

All'interno del sistema di conservazione vi sono diversi soggetti che esercitano le proprie facoltà e svolgono i loro incarichi; tali figure, sono il produttore, l'utente ed il responsabile della conservazione. Il produttore è una persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni tale figura s'identifica con il responsabile della gestione documentale.[20]
L'utente è la persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di suo interesse. Quando l'utente vuole accedere ai documenti conservati, deve richiedere al sistema di conservazione l'accesso - nei limiti previsti dalla legge - ai documenti conservati per acquisire le informazioni di suo interesse. Tali informazioni vengono fornite dal sistema di conservazione mediante la produzione – secondo le modalità previste dal manuale di conservazione - del pacchetto di distribuzione selettiva[21]: quindi l'utente,

---

[18] Ai sensi dell'allegato 1 del D.P.C.M. 3 dicembre 2013 per metadati si intende "*insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione*." Detto insieme è descritto nell'allegato 5 delle regole tecniche.

[19] Oppure, come detto, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico.

[20] Ovvero con il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

[21] L'art. 10 del D.P.C.M. 3 dicembre 2013 prevede che il sistema di conservazione deve permetter ai soggetti autorizzati l'accesso diretto – anche da remoto – al documento informatico conservato, attraverso la produzione di un pacchetto di "distribuzione selettiva". Gli oggetti destinati alla

debitamente autorizzato, effettuerà l'accesso diretto, anche da remoto, al documento informatico conservato di suo interesse.
Il responsabile della conservazione è la figura professionale cardine del sistema di conservazione, egli definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia (anche in relazione al modello organizzativo adottato). Il responsabile della conservazione, sotto la propria responsabilità, può delegare lo svolgimento del processo di conservazione, o di parte di esso, ad uno o più soggetti di specifica competenza ed esperienza in relazione alle attività ad essi delegate. Tale delega è formalizzata, esplicitando chiaramente il contenuto della stessa, ed in particolare le specifiche funzioni e competenze affidate al delegato.

4.2. Gli oggetti della conservazione ed il processo di conservazione

La norma distingue gli oggetti della conservazione in pacchetti di versamento, pacchetti di archiviazione[22] e pacchetti di distribuzione.
Il pacchetto di versamento è lo strumento mediante il quale il produttore invia il pacchetto informativo[23] al sistema di conservazione; quando è finalmente accettato dal sistema di conservazione, il pacchetto di versamento prende il nome di pacchetto di archiviazione. Il pacchetto di distribuzione, invece, è un pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una richiesta di quest'ultimo.
Come detto, il processo di conservazione inizia nel momento in cui il produttore,[24] mediante la formazione del "pacchetto di versamento", riversa nel sistema di conservazione l'oggetto da conservare ed i metadati ad esso associati o, in alternativa, i soli metadati. In seguito il pacchetto di versamento sarà sottoposto a verifica al fine di accertare che i contenuti di questo siano compatibili con quanto previsto dal manuale di conservazione e dall'art. 11 del decreto[25]. Nel caso in cui, a seguito delle verifiche effettuate, si dovessero riscontrare delle anomalie[26] nell'anzidetto pacchetto

conservazione dovranno utilizzare i formati previsti dall'allegato 2.

[22] Per garantire la interoperabilità tra i sistemi di conservazione, la norma impone ai soggetti che svolgeranno l'attività di conservazione dei documenti informatici di adottare, almeno per la gestione dei pacchetti di archiviazione, le specifiche della struttura dati contenute nell'allegato 4 del D.P.C.M. 3 dicembre 2013.

[23] Ovverosia, il "contenitore informatico" che racchiude al suo interno gli oggetti da conservare oppure anche i soli metadati riferiti a quegli oggetti.

[24] Per la P.A. questa figura coincide con il Responsabile della Gestione Documentale (o Responsabile della tenuta del Protocollo informatico; per i privati questo ruolo può essere ricoperto dal responsabile dell'ufficio che si occupa di protocollare e gestire i documenti e le comunicazioni.

[25] I documenti informatici destinati alla conservazione utilizzano i formati previsti nell'allegato 2 del D.P.C.M. 3 dicembre 2013.

[26] La norma non specifica espressamente quali anomalie potrebbe rilevare il responsabile della conservazione al momento del suo controllo, ma, a rigor di logica, queste ultime potrebbero ragionevolmente riguardare il formato del documento informatico da conservare (ad es. la scelta di

di versamento, il Responsabile della Conservazione rifiuterà di eseguire il versamento all'interno nel sistema di conservazione.
Una volta che il responsabile della conservazione avrà verificato che il pacchetto di versamento sia in possesso dei requisiti formali previsti dalla legge questo sarà accettato dal sistema di conservazione; quindi lo stesso sistema genererà il "rapporto di versamento", il riferimento temporale[27]ed una o più impronte[28] calcolate sull'intero pacchetto di versamento (secondo le modalità prescritte dal manuale).
Se previsto dal manuale di conservazione, il responsabile della conservazione apporrà al rapporto di versamento anche la sua firma digitale o elettronica qualificata.
Il passaggio successivo prevede la trasformazione del "pacchetto di versamento" in "pacchetto di archiviazione"[29]; quest'ultimo dovrà contenere il documento da conservare[30], i metadati a questo associati, il rapporto di versamento, l'impronta, la marca temporale ad esso relativi e la struttura descrittiva dell'indice del pacchetto di archiviazione. Tale struttura fa riferimento allo standard SInCRO[31], che è lo standard nazionale riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione. La struttura descrittiva dell'indice deve essere specificamente articolata per mezzo del linguaggio formale XML. A questo punto il documento è conservato nel rispetto delle regole tecniche previste dalla legge. Rimarrà dentro il sistema di conservazione per il tempo previsto dalle norme che regolano la conservazione di quel particolare documento (il ciclo di vita del documento, dalla sua produzione allo scarto, quando questo è possibile, è disciplinato nel manuale di gestione oppure nel manuale di conservazione).
In seguito al suo ingresso al sistema di conservazione, i soggetti legittimati a rivestire il ruolo di "utente" potranno accedere al documento conservato mediante la presentazione di una richiesta alla quale seguirà, se accolta, la preparazione e l'eventuale sottoscrizione[32]del pacchetto di distribuzione "selettiva".

---

un formato inidoneo) o i metadati ad esso associati (ad es. invalidità nel linguaggio XML mediante il quale è stato creato il file di metadati associato al documento da conservare).

[27] Ai sensi dell'allegato 1 del D.P.C.M. 3 dicembre 2013, è l'informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento.

[28] È la sequenza di simboli binari (*bit*) di lunghezza predefinita generata mediante l'applicazione di un'opportuna funzione di *hash* ad una evidenza informatica. L'evidenza informatica è una sequenza di simboli binari (*bit*) che può essere elaborata da una procedura informatica. Solitamente è contenuta in un file tipo txt o XML.

[29] Il pacchetto di archiviazione è il pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento e deve essere preparato, sottoscritto con firma digitale – o firma elettronica qualificata – e gestito sia sulla base delle specifiche tecniche contenute nel decreto (alleg. 4) che delle modalità previste dal manuale di conservazione.

[30] Sempre che il documento da conservare sia stato inserito nel "pacchetto di versamento", infatti, la norma dispone che nel pacchetto di versamento sia inserito l'oggetto da conservare ed i metadati ad esso associati oppure i soli metadati.

[31] Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010).

[32] Se previsto dal manuale di conservazione, la sottoscrizione sarà effettuata mediante firma digitale o elettronica qualificata.

Dopo aver preso visione del pacchetto di distribuzione, l'utente[33] potrà richiedere al medesimo sistema di conservazione la produzione di duplicati informatici – o copie informatiche – dei documenti conservati di suo interesse.
L'anzidetta produzione dovrà comunque rispettare, quanto al formato utilizzato, quanto previsto dalle regole tecniche in materia di formazione del documento informatico.
La fase finale del ciclo di vita del documento coincide con lo scarto; in questo caso, il decreto prevede che, alla scadenza dei termini di conservazione previsti, prima di procedere con lo scarto dovrà darsi informativa al produttore e, nel caso in cui l'archivio (sia pubblico che privato) rivesta un particolare valore storico, il produttore dovrà previamente ricevere l'autorizzazione allo scarto da parte del Ministero dei beni e delle attività culturali e del turismo.
Per garantire il potere di vigilanza conferito all'Agenzia per l'Italia digitale il decreto in oggetto prevede che, fatte salve le previsioni del Codice dei Beni Culturali, i dati – e le relative copie di sicurezza - dovranno essere conservati sul territorio nazionale e l'accesso a questi ultimi dovrà essere garantita presso la sede del produttore il quale dovrà adottare misure di sicurezza conformi a quelle stabilite dal D.P.C.M. 3 dicembre 2013.

4.3. Modelli organizzativi relativi al sistema di conservazione

La conservazione può essere svolta[34] sia internamente che esternamente alla struttura organizzativa del soggetto produttore dei documenti informatici da conservare. Qui emergono le prime differenze tra privati e pubblica amministrazione: per i primi, quando è svolta esternamente, la conservazione dovrà essere eseguita - anche nel caso in cui questa sia solo parzialmente esternalizzata - da soggetti pubblici o privati che offrono idonee garanzie organizzative e tecnologiche, oppure da un conservatore accreditato presso l'Agenzia per l'Italia digitale. La pubblica ammini-

[33] Il D.P.C.M. 3 dicembre 2013 definisce l'utente quale *"persona, ente o sistema"*, senza fornire ulteriori indicazioni per meglio individuare quali soggetti possono rivestire questo ruolo. Appare plausibile che l'anzidetto ruolo possa essere rivestito dal soggetto che ha creato il documento informatico conservato, ma non solo; per quanto riguarda i documenti conservati dalla P.A. tale ruolo potrà essere rivestito da tutti coloro che, ai sensi della L. n. 241/1990, hanno un interesse ad accedere e ad estrarre copia del documento conservato, quindi da tutti i *"soggetti privati, compresi quelli portatori di interessi pubblici o diffusi, che abbiano un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso"*. Secondo un orientamento giurisprudenziale (Consiglio di Stato – Sez. V, Sent. n. 3190/2011), anche la P.A. può esercitare il diritto di accesso disciplinato dalla L. n. 241/1990. Infatti, il principio di leale cooperazione istituzionale, sancito all'art. 22, co. 5 della L. 241/1990, in materia di acquisizione di documenti amministrativi da parte di soggetti pubblici, "non può essere inteso come preclusivo dell'applicazione dell'istituto dell'accesso nei confronti dei soggetti pubblici aspiranti ad una acquisizione documentale". Infine, non si può nemmeno escludere che il ruolo di "utente" possa essere rivestito da un sistema (*rectius*, sistema informatico) come nel caso di una procedura informatizzata di accesso ai documenti conservati.

[34] Ai sensi dell'art. 5 del D.P.C.M. 3 dicembre 2013 e dell'art. 44 del Codice dell'Amministrazione Digitale.

strazione, invece, quando non realizza i processi di conservazione all'interno della propria struttura organizzativa, deve obbligatoriamente rivolgersi ad un conservatore accreditato presso l'Agenzia per l'Italia digitale[35], fatto salvo quanto previsto dal Codice dei Beni Culturali.
L'affidamento ad un soggetto esterno deve essere effettuato mediante contratto (o convenzione di servizio) che preveda l'obbligo del rispetto del manuale di conservazione predisposto dal responsabile della stessa.
Sulla base delle previsioni del D.lgs. n. 196/2003 il soggetto esterno, cui è affidato il processo di conservazione, assume anche il ruolo di responsabile del trattamento dei dati.
Resta ferma la competenza del Ministero dei beni e delle attività culturali e del turismo in materia di tutela dei sistemi di conservazione degli archivi pubblici o degli archivi privati[36]che rivestono interesse storico particolarmente importante[37].

5. Il responsabile della conservazione

Il responsabile della conservazione, pur rivestendo un ruolo di assoluto rilievo all'interno di un'unità organizzativa, di un ufficio o di una pubblica amministrazione non opera da solo ma opera d'intesa con altre figure. I soggetti con i quali deve coordinare il suo lavoro sono il responsabile del trattamento dei dati personali, il responsabile della sicurezza, il responsabile dei sistemi informativi[38], ed infine con il responsabile della gestione documentale[39].
Dal punto di vista generale, il responsabile della conservazione definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare - della quale tiene evidenza - e gestisce il processo di conservazione in modo da garantirne nel tempo la conformità alla normativa vigente; predispone il manuale di conservazione e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.
A livello operativo svolge funzioni sia d'impulso sia di controllo del procedimento di

---

[35] Le modalità con cui si svolge l'accreditamento dei soggetti richiedenti sono disciplinate dalla Circolare n. 65 del 10 aprile 2014 emanata dall'Agenzia per l'Italia digitale.

[36] Quando è intervenuta la "dichiarazione dell'interesse culturale" ai sensi dell'art. 13 del D.lgs. n.42/2004.

[37] L'art.21, lett. d), del D.lgs. n. 42/2004 dispone che *"Sono subordinati ad autorizzazione del Ministero: (…) lo scarto dei documenti degli archivi pubblici e degli archivi privati per i quali sia intervenuta la dichiarazione ai sensi dell'art. 13, nonché lo scarto di materiale bibliografico delle biblioteche pubbliche, con l'eccezione prevista all'art. 10, co. 2, lett. c), e delle biblioteche private per le quali sia intervenuta la dichiarazione ai sensi dell'art. 13"*.

[38] Questa figura, nel caso delle pubbliche amministrazioni centrali, coincide con il responsabile dell'ufficio di cui all'art. 17 del Codice dell'Amministrazione Digitale.

[39] Nelle pubbliche amministrazioni che hanno al loro interno più Aree Organizzative Omogenee, il Responsabile della Conservazione opera d'intesa con il Coordinatore della gestione documentale.

conservazione: riguardo alla prima, genera il rapporto di versamento[40] e il pacchetto di distribuzione che poi sottoscrive, se previsto dal manuale di conservazione, con firma digitale o firma elettronica qualificata. Riguardo alla seconda, allo scopo di garantire la conservazione e l'accesso ai documenti informatici, effettua il monitoraggio circa la corretta funzionalità del sistema di conservazione.
A tale fine si assicura che il sistema di conservazione sia verificato periodicamente – comunque con cadenza non superiore ai cinque anni –, e che gli archivi in esso contenuti siano sempre integri e leggibili. Proprio per questo motivo, la norma gli impone di adottare tutte le misure necessarie al fine di rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, di ripristinarne la corretta funzionalità. Stesso ragionamento fa la norma con riguardo al problema dell'obsolescenza dei formati: il responsabile della conservazione, rilevata l'evoluzione del contesto tecnologico, provvede ad effettuare duplicati (o copie dei documenti informatici conservati) e ad adottare le misure necessarie per la sicurezza fisica e logica del sistema di conservazione.
Il responsabile della conservazione svolge anche una funzione di garanzia e assistenza nei confronti dei soggetti che, per ragioni del loro ufficio, debbano relazionarsi con la struttura del sistema di conservazione: garantisce a questi l'assistenza e le risorse necessarie per l'espletamento delle loro attività.
In particolare, egli assicura, nei casi in cui sia richiesto il suo intervento, la presenza di un pubblico ufficiale[41] e, all'occorrenza, coadiuva gli organismi competenti per l'espletamento delle attività di verifica e di vigilanza.
Provvede, quando gli sia richiesto dagli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati presso l'archivio centrale dello Stato e negli archivi di Stato.
Il responsabile della conservazione[42]può chiedere di certificare la conformità del processo di conservazione. Anche in questo caso la norma detta una disciplina diversa a seconda che il procedimento di certificazione venga richiesto da un soggetto privato o pubblico.
Per i primo, il responsabile della conservazione potrà richiedere la certificazione della conformità del processo di conservazione "*a soggetti, pubblici o privati, che offrano idonee garanzie organizzative e tecnologiche, ovvero a soggetti cui è stato riconosciuto il possesso dei requisiti di cui all'art. 44-bis, co.1, del Codice dell'Amministrazione Digitale, distinti dai conservatori o dai conservatori accreditati*". Le pubbliche amministrazioni, invece, potranno richiedere di certificare la conformità del processo di conservazione unicamente "*a soggetti, pubblici o privati, cui è stato riconosciuto il possesso dei requisiti di cui all'art. 44-bis, co. 1, del Codice dell'Amministrazione Digitale, distinti però, dai conservatori accreditati*". Pertanto, la cer-

[40] Quando quest'operazione non è svolta in modo automatizzato dal sistema di conservazione.

[41] Le modalità con cui viene richiesta la presenza di un pubblico ufficiale ed i casi per i quali è previsto il suo intervento sono riportate nel manuale di conservazione.

[42] Ai sensi dell'art. 44, co. 1-ter del Codice dell'Amministrazione Digitale.

tificazione dei sistemi può essere affidata solamente a soggetti diversi, indipendenti rispetto al conservatore, in grado di garantire terzietà ed imparzialità rispetto al sistema da certificare.

6. Il manuale di conservazione

Il manuale di conservazione è lo strumento che descrive il sistema di conservazione dei documenti informatici nel suo insieme e ne detta le regole fondamentali per il funzionamento.
Come detto in precedenza, il Manuale di Conservazione deve riportare la descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione e di evoluzione delle medesime. Rispetto alla struttura organizzativa, il Manuale di Conservazione deve riportare le funzioni, le responsabilità e gli obblighi dei diversi soggetti che intervengono nel processo di conservazione; in modo particolare, i dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema di conservazione nonché, se durante lo svolgimento del loro mandato, hanno concesso deleghe e, nel caso affermativo, gli ambiti oggetto della delega stessa e le funzioni espletate dai delegati.
Con riferimento agli oggetti sottoposti a conservazione, il manuale deve indicare i formati gestiti dal sistema, i metadati da associare alle diverse tipologie di documenti (e le eventuali eccezioni), la descrizione della modalità di presa in carico dei pacchetti di versamento - comprensiva della predisposizione del relativo rapporto di versamento -, la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione, i tempi entro i quali le diverse tipologie di documenti devono essere scartati ovvero trasferiti in conservazione e le normative in vigore nei luoghi dove sono conservati i documenti.
Quanto detto in precedenza sullo scarto e conservazione vale anche nel caso delle pubbliche amministrazioni solo quando questi dati non siano già riportati nel manuale di gestione.
Il manuale di conservazione disciplina le funzioni svolte dal responsabile della conservazione e le modalità con cui intervenire; il manuale descrive anche le procedure di monitoraggio della funzionalità del sistema di conservazione nonché le verifiche – alle quali il responsabile della conservazione è tenuto – sull'integrità degli archivi, evidenziando le soluzioni da adottare in caso di anomalie. Quando sono rilevati come obsoleti, il manuale della conservazione individua le procedure per la produzione di duplicati o delle copie dei documenti conservati.
Il manuale deve anche riportare le modalità con cui l'utente può accedere ai documenti conservati e quindi come si deve svolgere il processo di esibizione: dalla fase di esportazione dal sistema di conservazione fino alla produzione del "pacchetto di distribuzione" nei confronti del richiedente.

N. 1 - 2017 • pp. 131

PARTE SECONDA

Ambiente, CAD, Sistemi intelligenti, Robotica medica, Qualità della scuola

Rivista elettronica di Diritto, Economia, Management

N. 1 - 2017 · pp. 132-137

La tutela dell'ambiente: esigenze di *governance* e partecipazione democratica

Wanda D'Avanzo

Abstract: I diversi problemi a livello ambientale di cui ancora, troppo spesso, si sente parlare dovrebbero costituire la spinta per una maggiore e più efficace attenzione alle norme che disciplinano e tutelano il diritto di ognuno a vivere in un ambiente migliore. Proprio perché l'ambiente rappresenta l'insieme delle condizioni indispensabili allo svolgimento della vita umana, la sua conservazione risponde ad un interesse diffuso che deve essere tutelato come un diritto precipuo della persona umana nella sua dimensione sociale.
Ciò implica la necessità del raggiungimento di uno standard minimo di qualità ambientale, e l'affermazione di diritti procedurali quale quello ad una buona amministrazione, con particolare riferimento al diritto di partecipazione, che tutelino l'aspettativa e l'esigenza della protezione ambientale.
The different environmental problems should be the impetus for a greater and more effective attention to the rules which govern and protect everyone's right to live in a better environment. Precisely because the environment is the essential condition to human life, its preservation responds to a widespread interest which must be protected as a primary right of the human person in his social dimension. This implies the necessity of achieving a minimum of environmental quality standards, and establishment of procedural rights such as that to good administration, with particular reference to the right of participation, that safeguard the expectations and the demands of environmental protection.

Parole chiave: Ambiente, partecipazione, *governance*, democrazia.

Sommario: 1. Introduzione; 2. La Convenzione di Aarhus in tema di partecipazione; 3. La tutela dell'ambiente tra democrazia partecipativa e democrazia deliberativa; 4. Conclusioni.

1. Introduzione

Le problematiche ambientali sono caratterizzate da diversi fattori: il bisogno di provvedere e prevenire tutti quei fenomeni, i cui effetti negativi sono destinati a manifestarsi nel futuro; la compresenza di molteplici soggetti pubblici, la cui azione è indirizzata e va coordinata; il coinvolgimento di differenti e rilevanti interessi pubblici; l'impiego di risorse finanziarie, pubbliche e private, finalizzato alla tutela e al

Articolo pervenuto il 2 Maggio 2017, approvato il 1 Giugno 2017

risanamento dei danni ambientali.
Per tali ragioni, nel corso degli ultimi decenni, è stato incentivato l'utilizzo di strumenti ordinamentali adatti alle molteplici esigenze di tutela dell'ambiente[1].
I cambiamenti sociali dell'epoca attuale, inoltre, hanno messo in luce la necessità di far evolvere anche le procedure e l'organizzazione poste alla base dei tradizionali sistemi politici, amministrativi e decisionali. E proprio per questo la più recente riflessione teorica e il dibattito istituzionale hanno evidenziato la necessità di sostituire ai meccanismi rigidi della regolamentazione pubblica dei modelli più idonei a garantire una tutela ambientale efficace[2].
Le politiche pubbliche specie in ambito ambientale ai diversi livelli istituzionali mostrano numerosi limiti rispetto alla soluzione di problemi emergenti e di fronte a nuovi bisogni diversificati, provenienti da attori del mondo economico, istituzionale e dalla società civile. Processi di delocalizzazione e internazionalizzazione in ambito economico hanno generato incertezza rispetto alle prospettive future di molte filiere produttive e rispetto all'opportunità di promuovere investimenti e ricerca, ponendo la necessità di rinnovare le modalità gestionali ed organizzative del sistema economico[3].
Dunque, a fronte della crisi generale degli strumenti democratici tradizionali, emerge una tendenza che punta a governare la complessità sociale, economica e istituzionale dando maggiore voce ai cittadini.
La gestione delle politiche ambientali è passata, così, da modelli e strutture di *government* a processi di *governance*: ossia dal rigido modello gerarchico istituzionale alla interazione di iniziative e risorse fondate sul principio della responsabilità condivisa[4].
Ciò vuol dire garantire un'effettiva collaborazione tra attori pubblici e privati ai diversi livelli, dalla formulazione delle politiche alla loro attivazione. Gli attori coinvolti nei processi di *governance* devono avere una sufficiente discrezionalità che consenta loro di allineare le attività alle condizioni richieste dai contesti politico-sociale ed economico ai vari livelli; i nuovi strumenti di tutela ambientale devono lasciare alle autorità competenti e agli *stakeholders* discrezionalità nell'attuazione degli obiettivi fissati[5].
In questa organizzazione che diventa «a rete», la *governance* appunto, il coinvolgimento dei diversi attori a vari livelli diventa partecipazione attiva con strumenti di supporto alle decisioni[6].

---

1 Cangelosi G., *Tutela dell'ambiente e territorialità dell'azione ambientale*, Milano, 2009, 175; ed anche, Dell'Anno P., *Manuale di diritto ambientale*, Padova, 2003, 158 ss.

2 Clarich M., *La tutela dell'ambiente attraverso il mercato*, in *Annuario 2006: analisi economica e diritto amministrativo*, Milano, 2007, 104.

3 AA.VV., *Partecipare e decidere. Insieme è meglio. Una Guida per amministratori e tecnici*, Bologna, 2009, 23.

4 Zortea M., *Integrazione ambientale nei progetti di sviluppo*, Milano, 2013, 37.

5 Alberton M. - Montini M., *Vecchi e nuovi modelli di* governance *nel diritto ambientale: quali limiti e quali prospettive?*, in Id. (a cura di), *La* governance *ambientale europea in transizione*, Milano, 2008, 184.

6 Così, Flori M., *Pianificazione territoriale e urbanistica sostenibile: una rassegna critica introduttiva*,

2. La Convenzione di Aarhus in tema di partecipazione

La *governance* persegue il duplice obiettivo di consentire una gestione coordinata degli strumenti di programmazione e gestione delle politiche propri dei soggetti istituzionali e di favorire, al contempo, un processo di decisione «dal basso» di tutti i soggetti pubblici e privati interessati ai temi dello sviluppo territoriale attraverso lo strumento della concertazione.
E la materia ambientale rappresenta un settore in cui si manifestano con maggiore forza interessi conflittuali e che mobilita la società civile verso processi di democrazia partecipativa.
Proprio per questo, l'argomento ambiente costituisce uno degli interessi preminenti della Comunità europea, che, già nel 1998, ha siglato la Convenzione di Aarhus sull'accesso alla informazione, la partecipazione del pubblico ai processi decisionali e l'accesso alla giustizia in materia ambientale[7].
In tema di partecipazione ai procedimenti ambientali la Convenzione ha proclamato che una tutela dell'ambiente adeguata è essenziale per il benessere dell'uomo e ha riconosciuto espressamente il diritto di ognuno a vivere in un ambiente adatto a garantire la propria salute e il proprio benessere, nonché il dovere, sia individuale che collettivo, di tutelare e valorizzare l'ambiente nell'interesse delle generazioni presenti e future.
La Convenzione ha rappresentato applicazione del decimo principio della Dichiarazione di Rio de Janeiro secondo cui «i problemi ambientali sono meglio gestiti se vi è partecipazione di tutti i cittadini interessati, ai diversi livelli», e ha dato pieno riconoscimento ai diritti umani ambientali e ai diritti ambientali procedurali[8].
Peraltro, la Convenzione ha costituito a lungo il principale riferimento in materia fino all'approvazione della direttiva 2003/35/CE sulla partecipazione del pubblico all'elaborazione di piani e programmi in materia ambientale.
In merito, si è dato ampio spazio alla necessità di sviluppare ed incentivare, sul piano dell'attività amministrativa, l'impiego dei c.d. strumenti negoziali, rappresentati dagli accordi volontari, che risponde all'esigenza di favorire la diretta assunzione di responsabilità da parte di soggetti privati che agiscono nel quadro di un rapporto di collaborazione con gli organi pubblici nel perseguimento dei comuni obiettivi di tutela dell'ambiente.

in Ferlaino F. (a cura di), *Strumenti per la valutazione ambientale della città e del territorio*, Milano, 2010, 35.

[7] De Pascali P., Governance *&* Governance *del territorio: introduzione ad un quadro incerto*, in Id. (a cura di), *Territori della* governance. *Indagini ed esperienze sulla* governance *ambientale nella pianificazione territoriale*, Milano, 2008, 32-33.

[8] Pizzanelli G., *La partecipazione dei privati alle decisioni pubbliche. Politiche ambientali e realizzazione delle grandi opere*, Milano, 2010, 179.

3. La tutela dell'ambiente tra democrazia partecipativa e democrazia deliberativa

Per favorire la *governance*, si rende necessario rendere disponibile e fruibile l'informazione ambientale quale strumento essenziale a favorire comportamenti collaborativi, a condividere le decisioni pubbliche, a controllare i risultati dell'attività amministrativa, in una parola, ad incentivare la partecipazione[9].

Partecipazione che, come riconosciuto dalle norme internazionali, assume, nella materia ambientale, delle connotazioni particolari.

L'ambiente, infatti, per la sua forte carica valoriale, che «sollecita un elevato grado di responsabilità sociale, di dovere dei cittadini e di amministrazione partecipata e condivisa, si presenta come uno spazio giuridico aperto, desoggettivato, in cui si staglia massimamente la funzione, ossia l'attività funzionalizzata all'obiettivo, in luogo di "chi" la svolge. La tensione morale della società civile assume, nel campo elettivo della tutela dell'ambiente, maggiore forza, accrescendo il vincolo di solidarietà e di responsabilità»[10].

La ricerca della *governance* appare il punto chiave della riflessione ambientale. Essa, infatti, richiede una maggiore attenzione al coinvolgimento dell'opinione pubblica, quale soggetto partecipante all'organizzazione e al controllo della cosa pubblica.

E la partecipazione assume, in questo modo, «una forma democratica di accrescimento della legittimazione delle decisioni assunte dal pubblico potere di stampo rappresentativo, secondo una logica inclusiva […]»[11].

Le «decisioni ambientali mostrano sempre più la tendenza all'attenuazione del carattere autoritario del potere pubblico, per preferire metodi consensuali "partecipativi" di produzione delle regole […]». E «la soluzione dei problemi ambientali non dipende più in via esclusiva dalla responsabilità delle istituzioni pubbliche, ma da una nuova etica ambientale di tutti gli attori sociali, con la consapevolezza che solo una decisione condivisa riesce ad essere effettiva»[12].

L'ambiente rappresenta un ambito in cui la specialità della normativa consente un'esperienza di democrazia partecipativa, in cui società ed istituzioni si incontrano entro procedure fondate sui ruoli previsti dei vari attori e aventi spesso un forte elevato di istituzionalizzazione, di innovazione organizzativa. Società e istituzioni sono connesse tra loro entro una stessa operazione, e si produce una oggettiva affermazione

---

[9] Maioli C. - Ortolani C., *Sui profili giuridici della gestione dell'informazione territoriale della Pubblica Amministrazione*, in *www.altalex.com*, 2007.

[10] Feola M., *Ambiente e democrazia. Il ruolo dei cittadini nella* governance *ambientale*, Torino, 2014, 68.

[11] Feola M., *op. cit.*, 72.

[12] Feola M., *op. cit.*, 75. Si vedano anche in ordine al rapporto tra strumenti negoziali, partecipazione e democrazia Vitale A., *Diritto pubblico*, Salerno, 2008; Rossi G. (a cura di), *Diritto dell'ambiente*, Torino, 2011.

della legittimità di entrambe[13].
Democrazia partecipativa il cui scopo è quello di evolversi sempre più in democrazia deliberativa, affinché i cittadini possano contribuire direttamente alle politiche pubbliche ed ai loro processi di formazione e le istituzioni rispondere del loro operato. Una forma di partecipazione che va oltre la mera attività consultiva per realizzare il coinvolgimento pieno delle organizzazioni della società civile nel processo decisionale sulla base di un confronto informato, argomentato e orientato alla ricerca di soluzioni condivise[14].

4. Conclusioni

Se appropriatamente definite, dunque, le esigenze di partecipazione e le tecniche di *governance* mostrano un elevato potenziale, consentendo di mettere insieme un numero rilevante di attori e contribuendo a far crescere il senso di responsabilità e cooperazione, migliorando i flussi di conoscenza esperta verso i regolatori, in un ambito, quale quello ambientale, generalmente caratterizzato da asimmetria informativa[15].
I processi partecipati, ove attuati, potrebbero potenzialmente determinare un miglioramento della qualità ambientale, favorendo l'innovazione tecnologia; incoraggiando un approccio proattivo da parte del settore industriale; supportato gli strumenti regolamentativi in situazioni amministrative complesse[16].
La caratteristica precipua della partecipazione è quella di migliorare le modalità attraverso cui vengono perseguiti gli obiettivi di pubblico interesse, favorendo la definizione concordata tra i diversi attori sociali, economici ed istituzionali degli obiettivi e lo scambio delle informazioni. Questo aspetto presenta delle potenzialità interessanti dal punto di vista della capacità di cogliere e sfruttare, in particolare, le specificità locali dei sistemi territoriali coinvolti, con una migliore aderenza alle problematiche peculiari, e di conseguenza, con l'ottimizzazione dell'azione rispetto ad obiettivi determinati, misurati e adattati alle reali necessità e a determinate condizioni di funzionamento[17].
Sfruttare in pieno questo potenziale potrebbe aiutare ad affrontare i molti problemi

---

[13] Picerno R., *Fondamenti costituzionali della cittadinanza attiva*, in De Martin G.C. - Bolognino D. (a cura di), *Democrazia partecipativa e nuove prospettive della cittadinanza*, Milano, 2010, 17.

[14] Falasca C., *L'ambiente e l'informazione*, Tricase (Le), 2014.

[15] Reho M., *Le misure per la tutela e valorizzazione del paesaggio introdotte dalla nuova PAC. Valutazioni di efficacia in relazione ai fattori di contesto e alle modalità di gestione*, in Marangon F. (a cura di), *Gli interventi paesaggistico-ambientali nelle politiche di sviluppo rurale*, Milano, 2006, 35.

[16] Ballarin Denti A. - Grasso M. - Pareglio S., *Aspetti biologici ed economici nel rapporto tra inquinamento e ambienti agro-forestali*, in Cellerino R. (a cura di), *Economisti ambientali italiani*, *Atti della quarta riunione*, Milano, 1999, 28.

[17] Kühtz S., *Energia e sviluppo sostenibile. Politiche e tecnologie*, Soveria Mannelli, 2005, 57.

ambientali irrisolti.
I diversi problemi a livello ambientale di cui ancora, troppo spesso, si sente parlare dovrebbero costituire la spinta per una maggiore e più efficace attenzione alle norme che disciplinano e tutelano il diritto di ognuno a vivere in un ambiente migliore. Proprio perché l'ambiente rappresenta l'insieme delle condizioni indispensabili allo svolgimento della vita umana, la sua conservazione risponde ad un interesse diffuso che deve essere tutelato come un diritto precipuo della persona umana nella sua dimensione sociale[18].
Ciò implica la necessità del raggiungimento di uno standard minimo di qualità ambientale, e l'affermazione di diritti procedurali quale quello ad una buona amministrazione, con particolare riferimento al diritto di partecipazione, che tutelino l'aspettativa e l'esigenza della protezione ambientale[19].
In tal senso, dovrebbero essere sfruttate le potenzialità del sistema di *governance*, specie a livello locale, il cui scopo è sempre di più quello di democratizzare l'azione di governo, attraverso la diffusione di strumenti di collaborazione.

[18] Leccese E., *Danno all'ambiente e danno alla persona*, Milano, 2011, 54 ed anche Corasaniti A., *La tutela degli interessi diffusi davanti al giudice ordinario*, in *Riv. trim. dir. proc. civ.*, 1978, 180.

[19] Grassi S., *Problemi di diritto costituzionale dell'ambiente*, Milano, 2012, 73.

Rivista elettronica di Diritto, Economia, Management

N. 1 - 2017 · pp. 138-168

L'introduzione del FOIA in Italia. Gli esiti del primo esperimento italiano e il confronto con il '*Freedom of Information Act*' inglese

Francesco Addante

Abstract: Dopo ben quattro anni da quando Matteo Renzi ne parlò la prima volta ufficialmente, il FOIA, acronimo di *Freedom of Act Information*, approda in Italia. Il confronto scientifico giuridico rileva alcune riflessioni tra la prima versione del FOIA italiano, dopo la pubblicazione delle Linee guida definitive sui limiti al *neo* accesso civico "*generalizzato*" di cui alla Determinazione ANAC n. 1309 del 28 Dicembre 2016[1], e il corrispondente inglese, consolidato, ormai, dal 2005. La comparazione descrive, passo passo, tutti quei dettagli delle Linee guida esaminate che possono essere oggetto di miglioramento. Un miglioramento che trova la sua fonte proprio dall'eccellenza dell'esperienza inglese nel tracciare la strada sul come comportarsi in determinate circostanze affinché possa, effettivamente, essere esercitato un concreto diritto all'informazione.

Four years later when Matteo Renzi spoke about it for the first time officially, the FOIA - Freedom of Information Act – arrives in Italy. The legal scientific comparison detects some reflections between the first version of the Italian FOIA, after the publication of the final guidelines about the limits of the new rules of the "generalized" civic access (see ANAC Determination n. 1309 of 28th December 2016) and the English FOIA already consolidated in 2005 . The comparison describes, step by step, all details of the tested guidelines that can be object of improvement. This improvement, that is, how to have a better approach to deal with the own right of information, finds its source in the excellence of the English experience.

Parole chiave: Foia, Trasparenza, Accesso, Regno Unito, Italia, Libertà, Informazione, Civil law

Sommario: 1.Introduzione - 2. Il bilanciamento tra divulgazione generalizzata e la

[1] ANAC Determinazione n. 1309 del 28/12/2016 Linee guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co. 2 del d.lgs. 33/2013 Art. 5- bis, comma 6, del d.lgs. n. 33 del 14/03/2013 recante «*Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*» disponibile all'indirizzo http://www.anticorruzione.it/portal/public/classic/AttivitaAutorita/AttiDellAutorita/_Atto?ca=6666

Articolo pervenuto il 2 Maggio 2017, approvato il 1 Giugno 2017

tutela di altrettanto validi interessi - 3. I margini di miglioramento per un buon FOIA – 3.1. Perplessità in merito al differimento dei termini per la totale efficacia del diritto di accesso ai dati aggiuntivi – 3.2 Definizione di "*accesso generalizzato*"- 3.3. Legittimazione generalizzata - 3.4. Il '*prejudice test*' (Test legale di pregiudizio)- 3.5. Informazioni che devono essere rilasciate - 3.6. Open data - 3.7. Registro delle motivazione oltre che delle richieste di accesso presentate - 3.8. Formato in cui richiedere dati, informazioni e documenti - 3.9. Decertificazione - 3.10. '*NCND*': il non confermare o il non negare di possedere le informazioni richieste - 3.11. Trasparenza Proattiva e Reattiva - 3.12. Le modalità della richiesta - 3.13. Domande Vessatorie e Ripetute - 3.14. La consulenza e ragionevole assistenza da garantire anche rispetto alle istanze dal contenuto generico - 3.15. Unico ufficio per i riscontri alle istanze - 3.16. Massima collaborazione nei confronti del richiedente, sempre e comunque, reattiva e proattiva - 3.17. Raccomandazioni circa la gestione delle richieste, delle informazioni e le procedure di riesame - 3.18. Giustificazione della proroga per questioni particolarmente complesse - 3.19. Il workflow della gestione della richiesta - 3.20. Raccomandazioni in caso di richiesta di riesame - 3.21. Regole sull'informazione ambientale mancanti – 3.22.Sanzioni chiare e rigorose per i casi di illegittimo diniego di accesso, ma solo in UK - 4.Conclusioni – 5. Fonti normative – 6. Sitografia

1. Introduzione

Il '*Freedom of Information Act*' (FOIA) è la '*legge sulla libertà all'informazione*' in virtù della quale il richiedente può accedere a dati e documenti della pubblica amministrazione anche se non sono stati resi pubblici. Si tratta di uno sconvolgimento copernicano dell'accesso a tutti gli atti della P.A., così come proclamato dal Governo che ne ha avuto l'iniziativa e in linea con quanto già accade da decenni in altri Paesi europei (da 250 anni in Svezia[2]) e anglosassoni. Anche in Italia, il FOIA ha visto la luce il *23 giugno 2016*, quando è entrato in vigore il D.Lgs. 97/2016[3] che ha modificato il D.lgs. 33/2013[4] (Decreto Trasparenza) apportandone significative modifiche,

---

[2] PEROSINO, M "*La libertà di stampa è nata in Svezia e oggi compie 250 anni*", 2 Dicembre 2016, raggiungibile all'indirizzo http://www.lastampa.it/2016/12/02/esteri/la-libert-di-stampa-nata-in-svezia-e-oggi-compie-anni-KVkydYsECxk9Mk9MnRdEML/pagina.html

[3] D.lgs 25 maggio 2016, n. 97, "*Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicita' e trasparenza, correttivo della legge 6 novembre 2012, n. 190 e del decreto legislativo 14 marzo 2013, n. 33, ai sensi dell'articolo 7 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche*" (GU Serie Generale n.132 del 8-6-2016), disponibile all'indirizzo http://www.gazzettaufficiale.it/eli/id/2016/06/08/16G00108/sg e http://www.funzionepubblica.gov.it/articolo/ministro/12-02-2016/trasparenza (Avviso su Normattiva del testi integrato e coordinato delle modifiche al D.lgs. 33/2013: 10 giugno 2016, disponibile all'indirizzo http://www.normattiva.it/showNewsDetail?id=637&backTo=archivio&anno=2016)

[4] D.lgs. 33/2013, "*Decreto Trasparenza*", "*Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*", disponibile su http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2013-03-14;33

anche se il totale dispiegamento degli effetti giuridici avrà luogo il 23 dicembre nella previsione della piena operatività della nuova disciplina e il 23 giugno 2017 per la definitiva centralizzazione dei dati detenuti dalle P.A. presso le Banche dati di cui all'allegato B[5] introdotto dal decreto di modifica. La reale novità del "*Freedom Information Act*", in Italia, è **l'estensione dell'originario "accesso civico" anche a "*dati ulteriori***" che quindi è più ampio rispetto a quello che era previsto originariamente dal previgente art. 5 ma con il **limite** del rispetto degli interessi pubblici e privati "giuridicamente rilevanti" (specificati successivamente nel nuovo art. 5-bis). Pertanto, con il FOIA viene sancita l'universale pubblicità, conoscibilità, fruizione, utilizzo e riutilizzo di documenti, informazioni e dati, oggetto di pubblicazione obbligatoria "**e non**". Tuttavia, già con il previgente Decreto Trasparenza, dal 21 aprile 2013, attraverso i '*dati a pubblicazione obbligatoria'* **chiunque** poteva vigilare, attraverso il sito web istituzionale, sulle" finalità e le modalità di utilizzo delle risorse pubbliche" da parte delle pubbliche amministrazioni[6].
Il *28 dicembre 2016*, con Determinazione n. 1309[7] sono state approvate dall'ANAC, **in via, definitiva**, le *linee guida operative* che definiscono le **esclusioni** e i **limiti** al **neo** accesso civico "*generalizzato*" di cui all'art. 5 co.2 del D.lgs. 33/2013[8], relative ai dati, informazioni e documenti "*aggiuntivi*" rispetto a quelli a pubblicazione obbligatoria[9] aggiornati sempre a fine di quest'anno[10]. Quindi, solo dopo qualche giorno di ritardo[11] rispetto alla scadenza fissata dal D.lgs. 97/2016 di modifica, l'Autorità, d'intesa (il 15 dicembre) con il Garante per la protezione dei dati personali, è riuscita, eccezionalmente, ad approvarle ottenendo il 22 dicembre, anche, il parere favorevole della Conferenza unificata.

---

5 Allegato "B" di cui all'art.9-bis del D.lgs. 33/2013 "*Banche Dati*", disponibile all'indirizzo http://www.governo.it/sites/governo.it/files/allegato_2.pdf

6 Art. 1 co. 1 (*Principio generale di trasparenza*) del D.lgs. 33/2013, "*Decreto Trasparenza*"

7 ANAC Determinazione n. 1309 del 28/12/2016 Linee guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co. 2 del d.lgs. 33/2013 Art. 5- bis, comma 6, del d.lgs. n. 33 del 14/03/2013 recante «*Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*»

8 Art. 5 co. 5 (*Accesso civico a dati e documenti*) del D.lgs. 33/2013, "*Decreto Trasparenza*"

9 ANAC Delibera n. 1310 del 28/12/2016 "*Prime linee guida recanti indicazioni sull'attuazione degli obblighi di pubblicità, trasparenza e diffusione di informazioni contenute nel d.lgs. 33/2013 come modificato dal d.lgs. 97/2016*" raggiungibile all'indirizzo http://www.anticorruzione.it/portal/public/classic/AttivitaAutorita/AttiDellAutorita/_Atto?ca=6667

10 ADDANTE, F.," *Trasparenza. Dal 31 gennaio 2017 parte la vigilanza ANAC sui nuovi adempimenti informativi*", 11 Gennaio 2017, raggiungibile all'indirizzo http://www.forumpa.it/riforma-pa/trasparenza-dal-31-gennaio-2017-parte-la-vigilanza-anac-sui-nuovi-adempimenti-informativi

11 ADDANTE, F., "*FOIA. Oggi, 23 dicembre entra, o meglio, sarebbe dovuto entrare in vigore il nuovo diritto all'informazione*", 23 Dicembre 2016, raggiungibile all'indirizzo http://www.forumpa.it/foia-oggi-23-dicembre-entra-o-meglio-sarebbe-dovuto-entrare-in-vigore-il-nuovo-diritto-allinformazione

2. Il bilanciamento tra divulgazione generalizzata e la tutela di altrettanto validi interessi

In tutti gli ordinamenti che hanno adottato il *Freedom of Information Act* "la **conoscibilità** generalizzata degli atti diviene la **regola generale** mentre la **riservatezza e il segreto sono eccezioni**." [12] Ed è quello che ha fatto in Italia il legislatore, il quale "ha posto la trasparenza e l'accessibilità come la **regola** rispetto alla quale i limiti e le esclusioni previste dall'art. 5 bis del d.lgs. 33/2013 rappresentano eccezioni, e come tali sono da interpretarsi restrittivamente". Il legislatore non opera, come nel caso delle eccezioni assolute, una generale e preventiva individuazione di esclusioni all'accesso generalizzato, ma rinvia da una attività valutativa che deve essere effettuata dalle amministrazioni con la tecnica del **bilanciamento**, caso per caso, tra l'interesse pubblico alla **disclosure generalizzata** e la tutela di **altrettanto validi interessi** considerati dall'ordinamento". "L'amministrazione, cioè, è tenuta a verificare, una volta accertata *l'assenza di eccezioni assolute, se l'ostensione degli atti possa determinare un pregiudizio concreto e probabile agli interessi indicati dal legislatore*[13]. Le eccezioni, infatti, esistono proprio per proteggere le informazioni che non devono essere divulgate, ad esempio perché divulgarle sarebbe dannoso per un'altra persona o per l'interesse pubblico. Le deroghe all'accesso possono riferirsi anche a solo ad una parte delle informazioni, e quindi ad alcune sezioni di un documento o potrebbe essere necessario applicare eccezioni di diverso tipo alle diverse sezioni di uno stesso documento. Molti sono i dubbi sull'effettività posta dalle linee guida ANAC sia per le notevoli difficoltà interpretative e applicative derivanti da prescrizioni troppo ampie e, probabilmente, eccedenti i principi indicati dalla legge delega che invece in quest'ultima erano più ridotte e in considerazione dal fatto che strumenti di '*soft law*', quali quelli che andrà, appunto, ad impiegare l'Autorità, per definizione non dettano obblighi, né è stato previsto diversamente nel D.lgs. 97/2016[14]. Se le ipotesi di eccezione alla trasparenza fossero state normativamente formulate in maniera più contenuta e puntuale, non sarebbe forse stata necessaria un'appendice regolatoria funzionale a definirle ulteriormente, moltiplicando le pre-

---

[12] ANAC Schema di "*Linee Guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co. 2 del d.lgs. 33/2013*". Par. 2.1. "Introduzione" di "L'accesso civico generalizzato: caratteristiche e funzioni", scadenza consultazione il 28 novembre 2016 raggiungibile all'indirizzo http://www.anticorruzione.it/portal/rest/jcr/repository/collaboration/Digital%20Assets/anacdocs/Attivita/ConsultazioniOnline/20161111/CO.accesso.civico.11.11.16.pdf

[13] ANAC Schema di "Linee Guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co. 2 del d.lgs. 33/2013" Par. 5.2 "*Limiti (eccezioni relative o qualificate)*"

[14] AZZOLLINI, V. e RAGONE, M, "*Trasparenza: ancora troppi dubbi sull'efficacia del Foia italiano*", 7 Giugno 2016, disponibile all'indirizzo http://stradeonline.it/diritto-e-liberta/2070-trasparenza-ancora-troppi-dubbi-sull-efficacia-del-foia-italiano

scrizioni tra cui orientarsi per l'accesso alla auspicata "casa di cristallo".[15] Anzi, ora, con la proposta di linee guida in esame, fornendo specificazioni ed esemplificazioni volte a dettagliare le eccezioni troppo genericamente formulate, al fine dichiarato di "circoscrivere" gli ambiti che ne sono oggetto, l'Autorità pare addirittura amplificarne l'estensione[16].

Tuttavia nel focalizzare quanto già sancito dal D.lgs. 33/2013, riformato dal D.lgs. 97/2016 (FOIA), vengono definite le:

1. **eccezioni assolute,** cioè le esclusioni all'accesso nei casi in cui una norma di legge, disponga la non ostensibilità di dati, documenti e informazioni per tutelare interessi prioritari e fondamentali, quali le fattispecie indicate nell'**art.5 bis co.3**, ossia, i casi di **segreto di Stato**, e altri casi di divieto di accesso o divulgazione previsti dalla legge, ivi compresi i casi in cui l'accesso è subordinato dalla disciplina vigente al rispetto di specifiche condizioni, modalità o limiti, inclusi quelli di cui all'articolo 24, comma 1[17], della legge n. 241 del 1990 (*procedimenti tributari, atti normativi, amministrativi generali, di pianificazione e di programmazione, informazioni psicoattitudinali nei procedimenti selettivi,ecc*);

2. **eccezioni** relative o **qualificate** (i limiti al di fuori dei casi sopra indicati) che si configurano laddove le amministrazioni dimostrino che la diffusione dei dati documenti e informazioni richiesti possa determinare, con *valutazione di probabilità e non di semplice possibilità*, un pregiudizio concreto agli interessi pubblici e privati di particolare rilievo giuridico[18] elencati ai **commi 1 e 2 dell'art. 5-bis**, ossia:

- al comma 1, gli **interessi pubblici**: *sicurezza e ordine pubblico, sicurezza nazionale, difesa, questioni militari, relazioni internazionali, politica e stabilità finanziaria ed economica dello Stato, indagine reati, svolgimento attività ispettive*
- al comma 2, gli **interessi privati**: *protezione dei dati personali, libertà e segretezza della corrispondenza, interessi economici e commerciali: proprietà intellettuale, diritto d'autore, segreti commerciali*

Il FOIA inglese, allineandosi allo stesso principio, similmente, ma in modo ancora più significativo, ha sancito che la "*divulgazione*" delle informazioni dovrebbe essere la "**regola**" a meno che non ci sia una "***buona ragione*" per non farlo**[19]. Pertanto

---

[15] AZZOLINI, V., "*FOIA italiano: sarà vera trasparenza?*", 25 maggio 2016, raggiungibile all'indirizzo https://www.leoniblog.it/2016/05/25/foia-italiano-sara-vera-trasparenza/

[16] AZZOLLINI, V. "*FOIA all'italiana: fatta la regola, l'Anac trova le (numerose) deroghe*", 24 Novembre 2016, raggiungibile all'indirizzo http://phastidio.net/2016/11/24/foia-allitaliana-fatta-la-regola-lanac-trova-le-numerose-deroghe/

[17] Art. 24 co.1 (*Esclusione dal diritto di accesso*) della Legge 241/1990 e s.m.i. recante "*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*", disponibile su http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1990-08-07;241~art24!vig=

[18] AZZOLLINI, V. e RAGONE, M,, "*Linee Guida Anac sul Foia, tra limiti alla discrezionalità e maggiori margini di arbitrio*", 24 Novembre 2016 raggiungibile all'indirizzo www.forumpa.it/riforma-pa/linee-guida-anac-sul-foia-tra-limiti-alla-discrezionalita-e-maggiori-margini-di-arbitrio

[19] ICO.org.uk, "*Guide to freedom of informationt*", par. "*What are the principles behind the Freedom of Information Act?*" raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-

se "*qualsiasi informazione che deve essere rilasciata in base al FOIA* è rivolta al mondo intero" l'informazione pubblica dovrebbe essere resa sempre disponibile a meno che non ci sia una buona ragione per negarne l'accesso e la legge lo consente. Le eccezioni anglosassoni sono, in linea di massima, quelle che il FOIA italiano ha indicato nella sua disciplina ma rispetto a quest'ultime sono ben più circostanziate e, tranne pochi casi tassativi, non sono così assolute se a prevalere è l'interesse alla divulgazione. Direttive dettagliate di comportamento che guidano compiutamente le P.A. ad effettuare un adeguato bilanciamento e ben circoscrivono i passi da seguire, seppur nella loro libera autonomia di scelta. Valutazione che, proprio in virtù di confini di un percorso ben tracciato, consentono alle Amministrazioni inglesi di **avvicinare il più possibile l'ago della bilancia agli interessi della divulgazione** delle informazioni piuttosto che a quelli contrapposti, consentendo, di fatto, ai fruitori il pieno esercizio dei loro diritti alla 'conoscenza'[20]. Decisioni quelle delle P.A. italiane che, al momento, con la proposta di linee guida in consultazione, sembrano, di contro, dirigersi in senso diametralmente opposto proprio perché *sono assenti quelle specifiche indicazioni* a cui, invece, le direttive inglesi fanno esplicitamente riferimento. Alcune deroghe riguardano un particolare "*tipo*" di informazioni come quelle relative alla "**politica del governo**", altre si basano sul "*danno*" che si verrebbe a creare se la divulgazione fosse tale da pregiudicare un'"**indagine penale**" o pregiudichi gli "**interessi commerciali**" di qualcuno[21]. Le P.A. inglesi sono obbligate a negare l'accesso con assoluta certezza se l'eccezione al riguardo è '**assoluta**' come quella che interessa i "**servizi di sicurezza**". Tuttavia, la maggior parte delle eccezioni non sono assolute ma sono '**qualificate**' (o relative) e richiedono l'applicazione di un "**test di interesse pubblico**" tramite il quale le P.A. devono decidere se, prima di divulgare le informazioni, prevalgono gli interessi pubblici. Per non divulgare informazioni, l'Ente deve *dimostrare* che quelle informazioni, e solo quelle, sia meglio non divulgarle in considerazione di *valutazioni di interesse pubblico*. Di contro, potrebbe, invece, essere necessario divulgare le informazioni anche rispetto ad una deroga (in questo caso non assoluta). Ciò implica che, sempre nell'interesse pubblico, anche le informazioni riservate o esenti possono essere comunque divulgate. In tale circostanza occorre fare attenzione a non consentire l'accesso in violazione di altre leggi rispetto alle disposizioni specifiche previste del FOIA come la divulgazione di informazioni personali in violazione della legge sulla protezione dei dati. Ad esempio, (questo è quello a cui fanno riferimento le linee guida inglesi) la BBC, in riscontro ad una richiesta tesa a conoscere gli elementi di spesa costitutivi del

of-information/what-is-the-foi-act/

[20] ADDANTE, F., "*Foia, ecco come funzionano le eccezioni nel Regno Unito*", 13 Dicembre 2016, raggiungibile all'indirizzo http://www.agendadigitale.eu/egov/foia-ecco-come-funzionano-le-eccezioni-nel-regno-unito_2702.htm

[21] ICO.org.uk, "*Guide to freedom of information*", par. "*When can we refuse a request for information?*" raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/refusing-a-request/

prezzo del canone, ha dovuto scegliere di divulgare le informazioni richieste perché a fronte di un pregiudizio dei suoi interessi commerciali tale rischio non era sufficientemente significativo da essere ritenuto più rilevante della sua responsabilità nei confronti dei cittadini per l'uso di denaro pubblico.[22]

3. I margini di miglioramento per un buon FOIA

Uno sguardo al FOIA del Regno Unito fornisce interessanti spunti di riflessione che quello italiano può importare nei limiti del suo ordinamento. Si riportano, quindi, nel seguito i punti critici[23], sui quali potrebbe essere utile intervenire grazie all'apporto che può provenire dal meglio dell'esperienza inglese, ormai consolidata dal 2005, e nella speranza che la legge sulla libertà all'informazione italiana, possa, effettivamente dirigersi in questo senso dopo la consultazione delle "*linee guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co. 2 del d.lgs. 33/2013*", terminata il 28 novembre 2016 e l'approvazione definitiva del 28 dicembre dello stesso anno. Esse non hanno efficacia vincolante, né dalla loro violazione potrebbero scaturire conseguenze in punto di diritto, tuttavia, non si esclude che la loro inosservanza possa essere considerata in sede di valutazione giurisdizionale.[24]

3.1 Perplessità in merito al differimento dei termini per la totale efficacia del diritto di accesso ai dati aggiuntivi

Pur apprezzando l'utilità di un indice di possibile esistenza di pregiudizi agli interessi rilevanti tutelati, l'ANAC si è appropriata di un autorità normativa che non è sua. Ossia quella di attribuire alle Amministrazioni la facoltà di potersi dotare di Regolamenti con cui procedere alla individuazione delle categorie di documenti formati, o comunque, rientranti nella loro disponibilità, sottratti al neo accesso generalizzato, e soprattutto di prorogare ulteriormente al 23 giugno 2017[25] per tale scopo la data del 23 Dicembre 2016 che invece è stata stabilita da una disposizione di rango seconda-

---

[22] ICO.org.uk, "*Guide to freedom of information*", par. "*When can we refuse a request for information?*" raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/refusing-a-request/

[23] Della versione definitiva si segnalano solo le parti che hanno modificato quella in consultazione

[24] MACKINSON, T., "*Foia, esperti e associazioni all'Anac: "Le sue linee guida affosseranno la legge*", 9 dicembre 2016, raggiungibile all'indirizzo http://www.ilfattoquotidiano.it/2016/12/09/foia-esperti-e-associazioni-allanac-le-sue-linee-guida-affosseranno-la-legge/3248051/

[25] ANAC Schema di "*Linee Guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co. 2 del d.lgs. 33/2013*". Par. 6.2.3 "*Divieti di divulgazione espressamente previsti dal regolamento governativo di cui al co. 6 dell'art. 24 della legge 241/1990 e dai regolamenti delle pubbliche amministrazioni adottati ai sensi del co. 2 del medesimo articolo 24*"

rio in attuazione ad una di rango primario.
Tra le altre proposte accolte nella versione definitiva, si corregge, al par. 9. "*Decorrenza della disciplina..*", il testo preliminare prescrivendo **un'immediata applicazione** e non una '*auspicabile nel più breve tempo possibile'* sebbene poi si mantiene una piccola proroga (presumibilmente con scadenza precedente al 23 giugno 2017 visto il termine temporale eliminato) per l'adozione di una disciplina interna[26] sugli aspetti procedimentali.

3.2 Definizione di '*accesso generalizzato*'

Per quanto attiene alla terminologia, l'accesso definito "*generalizzato*"[27] dalle linee guida in consultazione è generalizzato (per dati aggiuntivi) come quello (per dati a pubblicazione obbligatoria) del previgente D.lgs.33/2013, motivo per cui, sarebbe, invece, opportuno distinguere i due tipi di accesso ed evitare che si crei confusione, utilizzando le seguenti definizioni:

- accesso civico '**Ordinario**' (previgente) anziché 'semplice', e
- accesso civico '**Rafforzato**' (introdotto) anziché 'generalizzato'.

3.3 Legittimazione generalizzata

Anche se è già probabilmente insito nello stesso principio, la FAQ "*Chi può presentare istanza di accesso civico ai sensi dell'art. 5 del d. lgs. n. 33/2013?*"[28] non chiarisce, come ha fatto il FOIA inglese, che la "richiesta di accesso può essere presentata anche da organizzazioni, ad esempio da una testata giornalistica, un comitato, una società, o da una persona per conto di un'altra, come ad esempio un avvocato per conto di un cliente." [29]

3.4 Il '*prejudice test*' (Test legale di pregiudizio)

Ribadendo quanto già affermato dalla norma, le linee guida, in consultazione, ricordano che la P.A., nell'attività di bilanciamento degli interessi contrapposti (divulgazione o diniego), si deve prodigare ad identificare un **pregiudizio** che deve essere

---

[26] ADDANTE, Modello di Istanza per richiedere l'Accesso civico generalizzato in attesa che le P.A. si adeguino alla nuova disciplina, 8, Gennaio 2017, disponibile all'indirizzo http://www.francescoaddante.eu/anticorruzione/istanza_accesso_civico_generalizzato_modello.docx

[27] ANAC Schema di "*Linee Guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co. 2 del d.lgs. 33/2013*". Par. 1 "*Definizioni*"

[28] ANAC Schema di "*Linee Guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co. 2 del d.lgs. 33/2013*". Allegato "*Modalità per esercitare il diritto di accesso civico*", FAQ, p. 27

[29] ICO.org.uk, "*Guide to freedom of information*", par. "*Who can make a freedom of information request?*" raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/

concreto agli interessi considerati e che, quindi, dovrà essere valutato rispetto al *momento* (non è possibile il diniego se è sufficiente il *differimento*) ed al contesto (*natura*[30] del dato) in cui l'informazione viene resa accessibile, consentendo l'accesso parziale "qualora la protezione dell'interesse sotteso alla eccezione sia invece assicurato dal diniego di *disclosure* di una parte soltanto". Valutazioni che dovranno essere svolte secondo un *processo logico* desunto dal modello anglosassone: il "*Prejudice test*" il quale, per assicurare il principio di *concretezza*, stabilisce che deve sussistere un *preciso nesso di causalità* tra l'accesso e il pregiudizio. Tuttavia, le linee guida italiane portano direttamente al "*Prejudice test*" chi deve effettuare la valutazione senza prima aver definito quelle che gli inglesi hanno precisato essere le '*class-based*' e '*prejudice-based'*, oltre che la distinzione tra esse, elementi necessari e propedeutici a risolvere il "test legale" in questione. Inoltre, il "*Prejudice test*" italiano non si riferisce anche a quello che gli inglesi chiamano **NCND**: "il non confermare o il non negare di possedere le informazioni richieste" (pur avendolo accennato in altro contesto). Le *'class-based'* (*exemptions*) si riferiscono alle eccezioni che si applicano solo a una particolare **categoria** o classe di informazioni, come quelle relative alla corrispondenza con la famiglia reale. Le '*prejudice-based'* (*exemptions*) si basano sulla valutazione di un tipo specifico di *danno* **che può essere causato** dalla divulgazione ('*prejudice*'), ad esempio, alla salute e alla sicurezza o i diritti personali di un privato (per una maggiore comprensione la guida riporta: "*Le notizie divulgate in modo irresponsabile dai media possono pregiudicare il risultato di un processo*" [31])

3.5 Informazioni che devono essere rilasciate

Se, come riconosciuto dalla proposta di linee guida, alla luce della riflessione normativa recente e meno recente, occorre riferirsi al dato conoscitivo come tale *indipendentemente dal supporto fisico*[32] sui cui è incorporato e *a prescindere dai vincoli derivanti dalle sue modalità di organizzazione e conservazione*, perché non precisare (tra le FAQ dell'Allegato) che, come ha fatto il FOIA inglese, "trattasi di documenti cartacei (anche le bozze), e-mail, note, informazioni memorizzate sul computer, cassette audio e video, (registrazioni di conversazioni telefoniche e video) micro-fiches, mappe, fotografie, note scritte a mano o qualsiasi altra forma di informazione[33] (se ovviamente ostensibile)"? Naturalmente occorrerebbe (se non lo si è già fatto perché

---

[30] Art. 3 co. 1-ter (*Principio generale di trasparenza*) del D.lgs. 33/2013, "*Decreto Trasparenza*"

[31] ICO.org.uk, "*Guide to freedom of information*", par. "*When can we refuse a request for information?*" raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/

[32] ANAC Schema di "*Linee Guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co. 2 del d.lgs. 33/2013*". Par. 4.2. "*Ambito oggettivo*"

[33] ICO.org.uk, "*Guide to freedom of information*", par. "*When is information covered by the Freedom of Information Act?*" raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/

comunque lo prevedono le norme italiane sulla organizzazione del proprio patrimonio informativo) avviare un processo di registrazione/archiviazione/classificazione dei dati di cui si è in possesso..

3.6 Open data

Così come già acclarato dal documento in consultazione, sarebbe opportuno, in particolare, citare, nelle FAQ dell'allegato di cui alla proposta delle linee guida, la facoltà di poter richiedere anche i dati in formato elettronico (**dataset**) il quale corredato degli opportuni *meta-dati* visto che tutti i "dati e i documenti che le amministrazioni titolari pubblicano, con qualsiasi modalità, senza l'espressa adozione di una licenza", si intendono rilasciati come dati di tipo aperto[34]. A tal riguardo, gli anglosassoni, indicando i requisiti specifici in materia, stabiliscono che è necessario rendere disponibile qualsiasi dataset che può essere richiesto a meno che non è opportuno farlo in forma riutilizzabile e anche se non rientrano informazioni che l'Ente possiede in modo registrato[35]. Inoltre, perché, sempre come suggeriscono gli inglesi, non utilizzare gli open data per registrare, classificare, organizzare e individuare in modo *centralizzato* tutte le richieste di accesso sotto forma di *meta-richieste*[36]? In caso contrario, i registri[37] suggeriti dalle linee guida rimarrebbero confinati all'interno di ogni singola P.A.

3.7 Registro delle motivazione oltre che delle richieste di accesso presentate

In aggiunta al *registro delle richieste di accesso presentate* (per tutte le tipologie di accesso), indicato dalla proposta di linee guida, sarebbe utile stabilire l'adozione di uno ulteriore dei **motivi** delle decisioni assunte da ciascuna delle P.A., in caso di diniego all'accesso, in modo da giustificarle, in maniera più organizzata rispetto a quanto si può rilevare dal singolo atto amministrativo, al TAR (o al Responsabile della trasparenza/Difensore civico). Una sorta di storico da cui rilevare elementi di continuità, correlazione, tempo trascorso tra vecchie e nuove istanze, risposte già fornite, così da avere gli elementi necessari per costituire, nel tempo, delle FAQ (ma-

---

[34] Art. 52 co. 2 (*Accesso telematico e riutilizzo dei dati delle pubbliche*) del D.lgs. 82/2005 s.m.i., "*Codice dell'amministrazione digitale*" (CAD) raggiungibile all'indirizzo http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-03-07;82!vig=

[35] ICO.org.uk, "*Guide to freedom of information*", par. "*What information do we need to publish?* raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/publication-scheme/

[36] ICO.org.uk, "*Guide to freedom of information*", par. "*When is information covered by the Freedom of Information Act?*" raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/

[37] ANAC Schema di "*Linee Guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co. 2 del d.lgs. 33/2013*". Par. 9 "*Disciplina transitoria*"

gari localizzate in modo centralizzato per tutte le P.A. sul sito web dell'ANAC) a cui sia gli utenti che le P.a. possano fare autorevolmente riferimento. Tale suggerimento fu proposto nel corso del recente *OpenGov Forum*[38] ed è già realtà in Inghilterra con la catalogazione dei provvedimenti intrapresi dall'ICO[39].
Recependo tale proposta l'Autorità monitorerà l'applicazione della legge aggiornando, dopo un anno, le Linee Guida in modo da fornire una più precisa individuazione delle esclusioni disposte dalla legge. Un monitoraggio che si realizzerà attraverso un "*c.d. registro degli accessi*" il quale, appunto, non si limiterà solo a contenere l'elenco delle richieste come prevedeva la versione in consultazione, ma lascerà traccia anche del relativo esito. Un repertorio storico dal quale l'aggiornamento prenderà importanti spunti che gli 'consentiranno di *tenere conto delle prassi nel frattempo formatasi con le decisioni delle amministrazioni e di eventuali ricorsi amministrativi o giurisdizionali'*. Inoltre, il registro, che dovrà essere pubblicato e aggiornato almeno ogni sei mesi in Amministrazione Trasparente, '*può essere utile per le p.a. che in questo modo rendono noto su quali documenti, dati o informazioni è stato consentito l'accesso'*.

3.8 Formato in cui richiedere dati, informazioni e documenti

Tra le indicazioni circa il formato in cui richiedere dati, informazioni e documenti, sarebbe opportuno citare, nelle FAQ dell'allegato, quanto il FOIA inglese stabilisce per i propri utenti, chiedendo loro, quindi, di specificare il formato accettabile (anche diverso da quello di origine) in cui si desidera ricevere le informazioni, facendo rilevare il diritto di consultarne più di uno (fotocopia o a stampa, via e-mail o su pen-drive, forma sintetica, ispezione di persona degli archivi, per telefono), spiegando che si è tenuti a rispettare le preferenze, purché siano ragionevoli e riportando i costi di riproduzione ed eventualmente di spedizione e chiedendo preventivamente la disponibilità a pagare[40].

3.9 Decertificazione

È restrittiva la prescrizione indicata in merito al consentire l'accesso ai documenti detenuti e gestiti dalla **sola amministrazione destinataria dell'istanza** e *non anche a quelli che potrebbero avere le altre amministrazioni* se questo è necessario per esaudire correttamente la richiesta e ad esse (le certificanti) l'Ente procedente può

---

[38] *Open Government* 3° Piano di Azione 2016 - 2018, Proposta di ADDANTE F. del 26 agosto 2016 alle 1:38 pm, raggiungibile all'indirizzo http://open.gov.it/consultazione-terzo-nap/foia-attuazione-e-monitoraggio/

[39] ICO, *Information Commissioner Office*. Organi di Guida e Controllo dell'esercizio al diritto all'informazione raggiungibile all'indirizzo https://ico.org.uk/about-the-ico/

[40] ICO.org.uk, "*Guide to freedom of information*", par. "*In what format should we give the requester the information?*" raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/receiving-a-request/

collegarsi (in cooperazione applicativa e avendo stipulato adeguate convenzioni) per fornire informazioni relative "a stati, fatti e qualità documentabili e certificabili dalla pubblica amministrazione"[41] (richieste dal diretto interessato e sempreché siano ostensibili a terzi).

3.10 '*NCND*': il non confermare o il non negare di possedere le informazioni richieste.

Ci si riferisce a quelle ipotesi per le quali" *il confermare o il negare se si detiene qualsiasi informazione*" potrebbe avere per *conseguenza situazioni dannose* a diritti pubblici e privati. Differentemente da quanto documenta il FOIA inglese, la proposta di linee guida, pur suggerendo alle P.A., al par. 5.3. "*La motivazione del diniego all'accesso*", di comunicare, in tale circostanza, le "categorie di interessi pubblici o privati che si intendono tutelare e almeno le fonti normative che prevedono l'esclusione/limitazione, non codifica tale comportamento con il nome di *NCND* o altro riferimento analogo, tantomeno ne riporta esempi concreti che possono fornire indicazioni operative alle Amministrazioni italiane. Inoltre prevede tale tipo di riscontro solo se il richiedente pretenda (quindi con una successiva istanza) una puntale specificazione delle ragioni del diniego[42]. Per gli stessi motivi (anche se già insito nel ragionamento sul NCND italiano) sarebbe stato utile specificare nelle FAQ costituende che le P.A. sono tenute a dare spiegazioni al richiedente anche in riferimento al fatto **che si posseggano o meno le informazioni richieste**[43] e non solo il fornirle, questo anche e *soprattutto nei casi di diniego*.

3.11 Trasparenza Proattiva e Reattiva

Al fine di fornire alle P.A. una situazione di insieme più globale che possa aiutarle a comprendere meglio le modalità di accesso generalizzato dei "*dati aggiuntivi*" sarebbe stato necessario integrare le linee guida in questione specificando (come fanno quelle inglesi) che per le Amministrazioni due sono gli obblighi principali:

1. pubblicare alcune informazioni in modo **proattivo** attraverso lo schema di pubblicazione" (All. A del decreto trasparenza declinato in quello (All. 1[44] della Delibera

---

[41] Dipartimento della Funzione Pubblica "*La decertificazione*" raggiungibile all'indirizzo http://www.funzionepubblica.gov.it/semplificazione/le-azioni-trasversali-di-semplificazione/la-decertificazione

[42] ANAC Schema di "*Linee Guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co. 2 del d.lgs. 33/2013*". Par. 5.3 "*La motivazione del diniego all'accesso*"

[43] ICO.org.uk, "*Guide to freedom of information*", par. "*Why use a 'neither confirm nor deny' response*" raggiungibile all'indirizzo https://ico.org.uk/media/1166/when_to_refuse_to_confirm_or_deny_section_1_foia.pdf

[44] ANAC Delibera n. 1310 del 28/12/2016 Prime linee guida recanti indicazioni sull'attuazione degli obblighi di pubblicità, trasparenza e diffusione di informazioni contenute nel d.lgs. 33/2013 come modificato dal d.lgs. 97/2016 -. All 1) - Elenco degli obblighi di pubblicazione disponibile

n. 1310 del 28 dicembre 2016) che ha sostituito l'All. 1[45] della Delibera CiVit n. 50/2013);

2. rispondere alle richieste di informazioni (trasparenza **reattiva**) (dati aggiuntivi rispetto a quelli a pubblicazione obbligatoria);

invitando le Amministrazioni[46] (così come accade per quelle inglesi) a

- pubblicizzare l'esistenza dello schema di pubblicazione in qualsiasi modo (anche bacheche, volantini o manifesti) normalmente utilizzato per comunicare con il pubblico,
- informare l'istante che ha il diritto a chiedere ulteriori dati, visto che tale schema rappresenta il minimo di quello che occorre divulgare,
- tenendo in considerazione il fatto che gli utenti debbano sempre poter accedere regolarmente alle informazioni, o riceverle prontamente e automaticamente, ogni volta che le chiedono[47] (ribadendo quanto già normato in riferimento alla qualità dei dati), quali, invece, sono quelle escluse dalla pubblicazione.

3.12 Le modalità della richiesta

Non si concorda con le disposizioni della proposta di linee guida che prescrivono quale condizione indispensabile di validità la sottoscrizione[48] da parte del richiedente o comunque l'instaurarsi di misure che consentano una preventiva verifica della sua identità senza alcun accenno a soluzioni alternative il cui unico scopo sia solo quello di presentare le istanze. Ad esempio, "una corrispondenza avvenuta tramite l'indirizzo istituzionale nome.cognome@governo.it non potrebbe essere soggetta a richiesta FOIA" [49]. Per quelli che sono i fini in materia di trasparenza, la modalità telematica non è solo quella che si esplica con i mezzi indicati dal CAD[50], inoltre,

all'indirizzo http://www.anticorruzione.it/portal/rest/jcr/repository/collaboration/Digital%20Assets/anacdocs/Attivita/Atti/determinazioni/2016/1310/Del.1310.2016.All_new.xls

[45] CiVit Delibera n. 50 del 04 luglio 2013, "*Linee guida per l'aggiornamento del Programma triennale per la trasparenza e l'integrità 2014-2016*", All. 1 – Obblighi di pubblicazione errata corrige e integrazioni- formato excel (settembre 2013) raggiungibile all'indirizzo http://www.anticorruzione.it/portal/rest/jcr/repository/collaboration/Digital%20Assets/anacdocs/Attivita/Atti/Delibere/2013/50/Obblighi-di-pubblicazione-ERRATA-CORRIGE-settembre-2013.xls

[46] ICO.org.uk, "*Guide to freedom of information*", par. "*What do we need to tell people about the Freedom of Information Act?*" raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/

[47] ICO.org.uk, "*Guide to freedom of information*", par. "*Why must we publish information, rather than simply responding to requests?*" raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/publication-scheme/

[48] ANAC Schema di "*Linee Guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co. 2 del d.lgs. 33/2013*". Allegato "*Modalità per esercitare il diritto di accesso civico*", FAQ, p. 27

[49] ANGHELE', F., "*FOIA italiano: l'Anac partorisce il topolino*", Riparte il Futuro, 29 novembre 2016 raggiungibile all'indirizzo https://www.riparteilfuturo.it/blog/articoli/foia-anac-linee-guida-eccezioni

[50] "Le istanze presentate per via telematica alle pubbliche amministrazioni e ai gestori dei servizi

anche se fosse vero il contrario, il Dlgs.33/2013 sancisce tale modalità solo in modo facoltativo[51] e non obbligatorio. Il FOIA inglese conferma questo orientamento ritenendo valida l'istanza di accesso civico presentata via email, via web o tramite Facebook o Twitter[52], l'importante è che sia scritta e che ci sia l'indicazione del proprio indirizzo. Quello scozzese o l'EIR, accettano, per la stessa finalità, persino un messaggio registrato in segreteria telefonica[53].

3.13 Domande Vessatorie e Ripetute

La proposta di linee guida sancisce che eventuali richieste di accesso civico devono essere ritenute inammissibili laddove risultino *manifestamente irragionevoli* senza però indicare come valutarne la *irragionevolezza*[54]. In riferimento alle 'richieste massive' di cui alla *FAQ (5)* delle linee guida definitive , pur in presenza di una maggior apertura nel consentire l'accesso ad 'un numero cospicuo di documenti ed informazioni', il principio secondo il quale tali richieste devono essere ritenute *manifestamente irragionevoli* è ancora troppo generico: '*oggettive condizioni suscettibili di pregiudicare in modo serio ed immediato il buon funzionamento dell'amministrazione*'. Il Foia inglese fa riferimento ad un "livello sproporzionato o ingiustificabile di angoscia o irritazione" fornendo a tale scopo degli indicatori[55] (la cui traduzione è stata riportata nella trattazione di dettaglio: Linguaggio offensivo o aggressivo, Gravame per la P.A., Rancori personali, Accuse infondate, Intransigenza, Richieste frequenti o frapposte, Intenzione deliberata di causare disturbo, Approccio indiscriminato, Sforzo sproporzionato, Nessun intento evidente di ottenere informazioni, Richieste futili) molto specifici per individuare se si tratta di una richiesta *vessatoria* e invitando le P.A. ad analizzare *il contesto e la storia, l'identità del richiedente e*

pubblici sono valide se:
a) sottoscritte mediante la firma digitale o la firma elettronica qualificata;
b) l'istante è identificato attraverso il sistema pubblico di identità digitale (SPID), nonché carta di identità elettronica o la carta nazionale dei servizi;
c) sono sottoscritte e presentate unitamente alla copia del documento d'identità;
d) trasmesse dall'istante mediante la propria casella di posta elettronica certificata" Art. 65 (*Istanze e dichiarazioni presentate alle pubbliche amministrazioni per via telematica*) del D.lgs. 82/2005 s.m.i., "*Codice dell'amministrazione digitale*" (CAD).

[51] "L'istanza **può** essere trasmessa per via telematica secondo le modalità previste dal decreto legislativo 7 marzo 2005, n. 82… Art. 5 co. 3, 3° capoverso (*Accesso civico a dati e documenti*) del D.lgs. 33/2013, "*Decreto Trasparenza*".

[52] ICO.org.uk, "*Guide to freedom of information*", par. "*What makes a request valid?* raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/receiving-a-request/

[53] FOIA.IT, Iniziativa per l'adozione di un Freedom of Information Act in Italia, Campagna per la Libertà d'Informazione, "*Breve Guida al Freedom of Information Act (Legge sulla Libertà d'Informazione) e Altri Nuovi Diritti all'Informazione*", par. "*Come posso richiedere informazioni ai sensi della legge?*", p.22, raggiungibile all'indirizzo http://www.foia.it/docs/foia-it_doc010.pdf

[54] ANAC Schema di "*Linee Guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co. 2 del d.lgs. 33/2013*". Par. 4.2. "*Ambito oggettivo*"

[55] ICO.org.uk, "*Guide to freedom of information*", par. "*Dealing with vexatious requests (section 14)*", raggiungibile all'indirizzo https://ico.org.uk/media/1198/dealing-with-vexatious-requests.pdf

il precedente contatto. Deve ovviamente trattarsi di *circostanze legittime*[56] rispetto alle quali sono sancite delle *raccomandazioni* il cui mancato rispetto comporta una violazione di legge a meno che l'Amministrazione non ne giustifichi un adeguato scostamento. Anche per quanto riguarda le richieste ripetute il FOIA inglese fornisce dettagli importanti (riportando esempi specifici di fatti concreti) prevedendo che "normalmente è possibile non fornire un riscontro ad una richiesta se è *identica* o sostanzialmente *simile* a quella che in precedenza è stata soddisfatta per lo stesso richiedente" ma esclude tale ipotesi quando si tratta di un *argomento correlato*, se non vi è una *sovrapposizione completa* o *sostanziale* tra richiesta precedente e successiva/e, e se è trascorso un *ragionevole periodo*[57] (anche questo non è stato stabilito dalla legge ma dipende dalle circostanze, tra cui, ad esempio, la frequenza con cui si apportano *modifiche* alle informazioni). Alla luce di quanto su esposto, sia per le vessatorie che per le ripetute, si rileva l'importanza di un adeguato utilizzo dei *Registri* che devono essere i più possibili descrittivi ed esaustivi proprio per valutare elementi di *continuità* e *correlazione*.

3.14 La consulenza e ragionevole assistenza da garantire anche rispetto alle istanze dal contenuto generico

Viene sancita l'inammissibilità della genericità dell'oggetto tanto da non ritenere valida una richiesta di accesso civico *meramente esplorativa*[58] al contrario di quanto stabilisce la stessa norma[59] (nella versione definitiva dopo le osservazioni dei rappresentanti della società civile e del Consiglio di Stato) e il FOIA inglese. Seppur leggermente rafforzata rispetto alla versione in consultazione, nella definitiva è rimasta **una facoltà** e non invece un obbligo quella di chiedere agli istanti *una precisazione più dettagliata* del contenuto richiesto. Infatti, in tali situazioni, le linee guida anglosassoni ritengono che "***ogni** autentico **tentativo** di descrivere le informazioni* è **sufficiente a far "scattare" il diritto alla conoscenza** anche se la descrizione *non è chiara* (ambigua o con diverse potenziali interpretazioni) o si pensa che sia troppo *ampia o irragionevole*"[60]. Quindi 'non si può rifiutare una richiesta semplicemente perché non sembra essere di molto

---

[56] ICO.org.uk, "*Guide to freedom of information*", par. "*When can we refuse a request as vexatious?*" raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/refusing-a-request/

[57] ICO.org.uk, "*Guide to freedom of information*", par. "*When can we refuse a request because it is repeated?*" raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/refusing-a-request/

[58] ANAC Schema di "*Linee Guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co. 2 del d.lgs. 33/2013*". Par. 4.2. "*Ambito oggettivo*"

[59] L'istanza di accesso civico identifica ~~chiaramente~~ i dati, le informazioni o i documenti richiesti. Art. 5 co. 3, 2° periodo (*Accesso civico a dati e documenti*) del D.lgs. 33/2013, "Decreto Trasparenza". L'aggettivo "*chiaramente*" fu cancellato nella versione definitiva rispetto a quelle preliminare.

[60] ICO.org.uk, "*Guide to freedom of information*", par. "*What makes a request valid?*" raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/receiving-a-request/

valore' e "**qualsiasi lettera** o **e-mail** ad un'autorità pubblica per chiedere accesso è ritenuta **giuridicamente valida** quale richiesta di informazioni protocollata ai sensi del FOIA, così come una **semplice domanda**. Per gli stessi motivi deve essere un obbligo e non una facoltà quella di chiedere, da parte delle Amministrazioni, agli istanti una precisazione più dettagliata del contenuto richiesto. In queste circostanze si esorta le P.A. inglesi a fornire *consulenza* e una *ragionevole assistenza* a chiunque abbia inoltrato o *intenda presentare* una richiesta di accesso alle informazioni con lo stesso trattamento che riceverebbe il cliente di un'azienda privata: parlargli, spiegargli come funziona il FOIA, chiarendo che tipo di informazioni potrebbero essere divulgate, scoprire quello che vuole, e poi contattarlo per verificare di aver capito bene quello che chiede o consigliandolo di riformulare la sua istanza, spiegando, ad esempio, quali possano essere le opzioni a sua disposizione, chiedere se qualcuna di queste potrebbe adeguatamente rispondere alla sua esigenza, descrivergli la natura delle informazioni, o fornire quelle aggiuntive per aiutare a considerarle nel contesto. "In ogni caso, l'utente dovrà ricevere assistenza *se non riesce a capire* quali informazioni siano disponibili, se non è riuscito a presentare una valida richiesta (nel qual caso la P.A. si deve prodigare a istruirlo adeguatamente affinché ci riesca) o se l'Ente non è in grado di comprenderla"[61]. Un comportamento diverso da quanto indicato viene valutato attentamente dall'Autorità di controllo ai fini di eventuali provvedimenti da intraprendere.

3.15 Unico ufficio per i riscontri alle istanze

Guardando al FOIA inglese, le linee guida italiane proposte dalla consultazione avrebbero, forse, dovuto suggerire alle P.A. un adeguamento organizzativo tale da prevedere il riscontro dell'istanza da parte di **chi detiene i dati**[62]**.** Ufficio che potrebbe rivolgersi, nel corso della propria istruttoria, ad uno *giuridico* (ormai divenuto indispensabile per tutti gli adempimenti a cui sono sottoposti le P.A.) *competente (anche) in materia di FOIA, e centralizzato* per tutti gli altri. Punto di riferimento che sarà in grado di supportare le Posizioni Organizzative destinatarie dell'istanza nella ponderazione tra l'interesse pubblico alla disclosure generalizzata e la tutela di altrettanti validi interessi considerati dall'ordinamento, rispetto ad eccezioni assolute e qualificate.

3.16 Massima collaborazione nei confronti del richiedente, sempre e comunque, reattiva e proattiva

Proprio perché hanno il compito di fornire alle P.A. indicazioni operative di comportamento, le linee guida dovrebbero, in particolare nelle FAQ, fare sempre e co-

[61] ICO.org.uk, "*Guide to freedom of information*", par. "*Can a question be a valid request?*" raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/receiving-a-request/

[62] ICO.org.uk, "*Guide to freedom of information*", par. "*Does all the information have to be on a website?*" (post holders) raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/publication-scheme/

munque riferimento ad un principio fondamentale: quello di suggerire, se non persino imporre di *aiutare il richiedente*, soprattutto l'istante in difficoltà, ad esercitare correttamente il proprio di diritto di conoscenza, fornendo una **consulenza e ragionevole assistenza**[63] in ogni circostanza, anche in misura preventiva. Nella FAQ (3) della versione definitiva si stabilisce che tutte le P.A. interessate "sono tenute a prendere in considerazione le richieste di accesso generalizzato a prescindere dalla presenza o meno di una motivazione o giustificazione". Un principio che prima si limitava solo ad indicare l'ammissibilità di una richiesta priva degli stessi presupposti. Tuttavia, le linee guida italiane, così come fanno quelle inglesi, dovrebbero (subito per quello che è possibile importare come esperienza dagli altri ordinamenti, in futuro per ciò che si può imparare dopo) riportare, in modo articolato e il più possibile approfondito, esempi di **casi reali e buone pratiche** che possono aiutare le P.A. a decidere come meglio comportarsi nelle stesse e identiche circostanze. La corretta compilazione dei Registri prima accennati potrebbe fornire un grande aiuto in tal senso.

3.17 Raccomandazioni circa la gestione delle richieste, delle informazioni e le procedure di riesame

Per rendere effettivamente concretizzabile la collaborazione che devono prestare le P.A. è necessario predisporre delle raccomandazioni (all'interno delle stesse linee guida) che condizionando proceduralmente/operativamente e controllando in qualche modo (in maniera non vincolante, ma l'Ente che se ne discosta lo deve adeguatamente motivare) il comportamento delle Amministrazioni, siano in grado di costituire una guida essenziale e fondamento per il raggiungimento di tale scopo. A tal riguardo il FOIA inglese prevede raccomandazioni circa la "gestione delle richieste"[64], delle "informazioni", e in particolare delle procedure di "riesame" (in caso di reclamo o anche revisione interna) per cui vengono indicati i casi in cui attivarla e le operazioni da intraprendere per garantire la buona riuscita della decisione finale.

3.18 Giustificazione della proroga per questioni particolarmente complesse

Nell'**ambito delle stesse scadenze,** previste dalla normativa, non si evidenzia la possibilità, seppur in casi eccezionali, di concedere una **proroga** che dovrebbe es-

---

[63] ICO.org.uk, "*Guide to freedom of information*", par. "*Duty to provide advice and assistance (section 16)*" raggiungibile all'indirizzo https://ico.org.uk/media/1624140/duty-to-provide-advice-and-assistance-foia-section-16.pdf

[64] ICO.org.uk, "*Guide to freedom of information*", par. "*What are our obligations under the Freedom of Information Act?*" raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/

sere necessaria solo se la valutazione dell'esistenza di un interesse pubblico sollevi questioni *particolarmente complesse* e che l'amministrazione deve essere in grado di giustificare. Tantomeno non si è previsto l'obbligo di rendere nota un'adeguata motivazione anche nei casi in cui **non si detengono i dati richiesti**[65], ossia nelle ipotesi **NCND** prima citate, circostanze quest'ultime, comunque, rilevate dalla linee guida in corso d'adozione, nonostante manchi una loro precisa identificazione.

3.19 Il workflow della gestione della richiesta

Dovendo le P.A. italiane districarsi[66], con molte difficoltà e incertezze, tra i *tre diversi tipi di accesso*[67], sarebbe opportuno integrare la versione finale delle linee guida con un diagramma di flusso di gestione della richiesta[68] che sia in grado di fornire una panoramica dettagliata dei passi (singole azioni) che la P.A deve seguire quando deve svolgere l'attività valutativa con la tecnica del bilanciamento, caso per caso, tra l'interesse pubblico alla *disclosure generalizzata* (sia per dati obbligatori che aggiuntivi) e la tutela di altrettanti validi interessi considerati dall'ordinamento. Nel Regno Unito, il diagramma in questione, riporta con dettaglio e certezza, step by step, il *percorso di comportamento* che la P.A. deve rispettare, pur nell'ambito della sua autonoma discrezionalità, a seconda del verificarsi di specifiche circostanze, per valutare e infine determinare se sia possibile, o meno, rilasciare le informazioni richieste. Ogni passaggio è corredato dal riferimento e collegamento alle diverse articolazioni (sezioni) delle linee guida e della relativa normativa.

3.20 Raccomandazioni in caso di richiesta di riesame

L'allegato "Modalità per esercitare il diritto di accesso civico" (FAQ "È possibile in ogni caso ricorrere al giudice? [69]) non riporta, come invece prevede il D.lgs.33/2013 novellato il riferimento al **Difensore Civico**[70] per gli Enti territoriali in caso di ricorso al TAR avverso la sua decisione. Impostazione che è stata rivista nella versione

---

[65] ICO.org.uk, "*Guide to freedom of information*", par. "*Do we have to tell them what information we have?*" raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/receiving-a-request/

[66] ADDANTE, F., "*Foia, ecco gli ostacoli nella fase attuativa*", 5 Settembre 2016, raggiungibile all'indirizzo http://www.agendadigitale.eu/egov/foia-ecco-gli-ostacoli-nella-fase-attuativa_2410.htm

[67] ADDANTE, F., "*Foia, prima e dopo: come cambia il percorso di accesso civico (infografica)*", 3 Ottobre 2016, raggiungibile all'indirizzo http://www.agendadigitale.eu/egov/foia-prima-e-dopo-come-cambia-il-percorso-di-accesso-civico-infografica_2525.htm

[68] ICO.org.uk, "*Guide to freedom of information*", par. "*flowchart of request handling under foia*" raggiungibile all'indirizzo https://ico.org.uk/media/for-organisations/documents/1167/flowchart_of_request_handling_under_foia.pdf

[69] ANAC Schema di "*Linee Guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co. 2 del d.lgs. 33/2013*". Allegato "*Modalità per esercitare il diritto di accesso civico*", FAQ, p. 29

[70] Art. 5 co. 8 (*Accesso civico a dati e documenti*) del D.lgs. 33/2013, "*Decreto Trasparenza*"

definitiva e in cui degna di nota è, invece, l'integrazione di una disposizione importante: in riferimento alla *FAQ (13),* rispetto alla versione in consultazione, **l'obbligo di motivazione** espressa a giustificazione dell'esistenza di un pregiudizio concreto, (che si aggiunge dovrà essere '*adeguata*') in caso di diniego all'accesso **si estende alle eccezioni assolute** e per quelle **qualificate** anche alla tutela **degli interessi pubblici** sanciti dalla norma. Esso viene ampliato **anche per i provvedimenti di accoglimento** specie quando è adottato nonostante l'opposizione del controinteressato. Probabile recepimento del suggerimento che sollecitava l'ANAC ad indicare la necessità di valutare con esattezza **i motivi** per i quali ad una P.A. fosse consentito di rifiutare le istanze. Le linee guida inglesi (che anche se non giuridicamente vincolanti producono comunque il loro effetto) forniscono spunti interessanti, da eventualmente introdurre (nel limiti del possibile e della compatibilità dell'ordinamento) in quelle italiane, per il *comportamento* che potrebbero (*dovrebbero*) *assumere il Responsabile della Trasparenza* e il *Difensore Civico* durante la procedura di riesame. Infatti, una dettagliata procedura stragiudiziale permette, grazie all'autorità della ICO[71], alla collaborazione dei vari attori e ad un attento rilievo dei motivi e del comportamento assunto dalle amministrazioni nelle loro decisioni, di assicurare, nella maggior parte dei casi, il diritto all'informazione in quei casi in cui il diniego o il differimento è illegittimo. Questo ha degli effetti positivi sulle cause giudiziarie che si riducono a quelle strettamente necessarie al quale il richiedente può comunque ricorrere **senza alcuna spesa**. Nell'attività di riesame si prende in considerazione la *portata*, la *qualità* e la *completezza* delle ricerche oltre a *testare* la *forza del ragionamento* e delle *conclusioni*. Viene messa in rilevanza che è **responsabilità** della P.A. *dimostrare* il **perché**[72] dovrebbe essere consentito rifiutare una richiesta di accesso, motivo per cui è nel loro interesse cooperare pienamente all'indagine. Se l'Amministrazione non riesce a seguire le buone pratiche, come stabilito nei codici di pratica, l'ICO può emettere una **raccomandazione pratica**. Non adempiervi comporterà probabilmente **violazione** della legge. Ad esempio, può raccomandare di *introdurre una procedura di revisione interna, o migliorare la formazione del personale*.[73]

3.21 Regole sull'informazione ambientale mancanti

Non si fa alcun accenno al comportamento che dovrebbero assumere le P.A. nel caso fossero interpellate per una richiesta di accesso alle *informazioni ambientali*,

---

[71] *Information Commissioner's Office*, informazioni raggiungibili all'indirizzo https://ico.org.uk/about-the-ico/

[72] ICO.org.uk, "*Guide to freedom of information*", par. "*What happens if we don't have the information?*" raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/receiving-a-request/

[73] ICO.org.uk, "*Guide to freedom of information*", par. "*What about poor practice that doesn't amount to a breach of the Act?* raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/complaints/

"aggiuntive", rispetto a quelle a pubblicazione obbligatoria. Argomento di assoluto rilievo (e per tale importanza disciplinata dagli inglesi come specifica materia a parte[74]) in quanto trattasi di disposizioni che sono state emanate in attuazione di una direttiva EU[75] che garantisce *un più forte diritto di accesso all'informazione* rispetto a quanto non sia previsto dallo stesso FOIA. In previsione di una futura trattazione sarebbe opportuno contemplare, così come stabiliscono quelle inglesi che discendono dalla stessa direttiva, la *libera divulgazione* delle informazioni sulle *emissioni nell'ambiente* che non possono essere più negate per qualsivoglia motivo di *riservatezza commerciale*[76]. Limitatamente all'informazione di carattere amministrativo, in Inghilterra è persino consentito il diritto di accesso alle informazione di carattere ambientale in possesso dei tribunali e delle corti d'appello[77]. Sarebbe pertanto utile una regolamentazione dettagliata per l'accesso in materia ambientale, con riferimento sia ai dati obbligatori che non, sulla falsa riga di quanto prevedono le linee guida inglesi.

3.22 Sanzioni chiare e rigorose per i casi di illegittimo diniego di accesso, ma solo in UK

Nel Regno Unito vale le regola fondamentale secondo cui una P.A. infrange il "Freedom of Information Act" se non riesce a rispondere adeguatamente ad una richiesta di accesso, ad adottare il modello dello schema di pubblicazione, o non pubblica i dati corretti, oppure se **distrugge, occulta, altera o ostacola deliberatamente**[78] le informazioni richieste tanto da impedirne il rilascio. Quest'ultima inottemperanza è un reato penale. Al riguardo, l'attività dell'ICO è innanzitutto quella di **capire i motivi del diniego**[79] (provvedendo in questi casi con ammonizioni, se persiste l'inerzia,

---

[74] ADDANTE, F, "*FOIA, le norme cornice utili alla normativa: l'esempio del Regno Unito*", 6 Gennaio 2017, raggiungibile all'indirizzo http://www.agendadigitale.eu/egov/foia-le-norme-cornice-utili-alla-normativa-l-esempio-del-regno-unito_2785.htm

[75] Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC

[76] FOIA.IT, Iniziativa per l'adozione di un Freedom of Information Act in Italia, Campagna per la Libertà d'Informazione, "*Breve Guida al Freedom of Information Act (Legge sulla Libertà d'Informazione) e Altri Nuovi Diritti all'Informazione*", par. "*Informazioni Ambientali*", p.4, raggiungibile all'indirizzo http://www.foia.it/docs/foia-it_doc010.pdf

[77] FOIA.IT, Iniziativa per l'adozione di un Freedom of Information Act in Italia, Campagna per la Libertà d'Informazione, "*Breve Guida al Freedom of Information Act (Legge sulla Libertà d'Informazione) e Altri Nuovi Diritti all'Informazione*", par. 2 "*Come ottenere le informazioni - Quali enti sono previsti dalla legge?*", p.7, raggiungibile all'indirizzo http://www.foia.it/docs/foia-it_doc010.pdf

[78] ICO.org.uk, "*Guide to freedom of information*", par. "*Are there criminal offences in the Freedom of Information Act?"* raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/complaints/

[79] *E' responsabilità* della P.A. *dimostrare* il **perché** dovrebbe essere consentito *rifiutare una richiesta di accesso*, ed è nel loro interesse cooperare pienamente all'indagine. Da ICO.org.uk, "*Guide to freedom of information*", par. "*What should we do if someone complains to the ICO about how we have handled a request?"* raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/complaints/

a obbligare le amministrazioni all'invio di informazioni e delle ragioni che ne hanno giustificato il mancato assenso) verificando se effettivamente esistono i presupposti e non solo quella di sollecitare la P.A. a fornire un riscontro quando la stessa non ha un buon motivo per non farlo. L'ICO non può sanzionare la P.A. che non riesce a rispettare la legge, né può richiedere di pagare un risarcimento a tutti coloro che violano la legge ma il potere di emettere legalmente un richiamo con decisioni **vincolanti**. La notifica della decisione dichiarerà se la P.A. ha rispettato la legge, e, in caso negativo, cosa dovrebbe fare per soddisfare il diritto all'informazione[80]. Nelle circostanze in cui un'Autorità pubblica persiste nel rifiuto di collaborare, l'ICO ha l'autorità di emettere un *avviso di informazione*. Anche in questo caso si tratta di un avviso *giuridicamente vincolante* che obbliga una P.A. a fornire le informazioni o le ragioni che le sono chieste.[81] Non sono previste sanzioni pecuniarie o detentive per non aver fornito informazioni su richiesta o per la mancata pubblicazione ma le Amministrazioni potrebbero essere ritenute responsabili di **oltraggio alla corte** per non essersi **conformate** ad un *preavviso di decisione*, *diffida* o *informativ*a. Questo potrebbe comportare una **sanzione** o, in teoria, il **carcere** per un alto ufficiale delle Amministrazioni.[82] Completamente differente è la situazione in Italia e nonostante le correzioni apportate, grazie all'intervento dei rappresentanti della Società civile, al pessimo testo,[83] in versione preliminare del FOIA, della previsione di un ricorso stragiudiziale gratuito nei casi di mancata o negativa risposta per evitare la necessità del ricorso al TAR. Infatti, accanto alla possibilità di richiesta di riesame al responsabile della prevenzione e della trasparenza dell'amministrazione (che decide con provvedimento motivato entro 20 giorni) è prevista la possibilità del rimedio stragiudiziale, in particolare nel caso di atti delle Regioni o degli enti locali, costituito dal ricorso al difensore civico competente per ambito territoriale, ove costituito, che si pronuncia entro 30 giorni: laddove non istituito la competenza è attribuita al difensore civico competente per l'ambito territoriale immediatamente superiore[84]. Disposizione, quest'ultima, che potrebbe determinare delle discriminazioni negli strumenti di tutela della trasparenza a svantaggio di cittadini di Comuni o Regioni in

---

[80] ICO.org.uk, "*Guide to freedom of information*", par. "*What happens when someone complains?"* raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/complaints/

[81] ICO.org.uk, "*Guide to freedom of information*", par. "*What should we do if someone complains to the ICO about how we have handled a request?"* raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/complaints/

[82] ICO.org.uk, "*Guide to freedom of information*", par. "*Are there criminal offences in the Freedom of Information Act?"* raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/complaints/

[83] Schema di decreto di modifica del D.lgs. 33/2013, in versione preliminare, pubblicato il 12 e il 13 Febbraio 2016, disponibile all'indirizzo http://www.governo.it/sites/governo.it/files/testo_21 %281%29 %281%29.pdf

[84] FAINI, F. "*Trasparenza della PA, tutto ciò che c'è da sapere sui nostri diritti*", 11 Luglio 2016, disponibile all'indirizzo http://www.agendadigitale.eu/smart-cities-communities/trasparenza-della-pa-tutto-cio-che-c-e-da-sapere-sui-nostri-diritti_2331.htm

cui il difensore civico, non è più obbligatorio, non è stato previsto o, se pur previsto nello Statuto, non è stato eletto[85]. E' da notare, infatti, che tale figura negli anni è andata a scomparire e quindi non è più molto diffusa sul territorio[86], pertanto può non rivelarsi misura efficace in concreto[87]. Inoltre, vengono, assegnate ai responsabili della prevenzione della corruzione degli oneri e delle responsabilità del tutto nuove e molto ingenti, che non sarà facile per queste figure – nate con tutt'altra finalità – fronteggiare[88]. il responsabile suddetto non assicura la terzietà necessaria all'organo di seconda istanza, non solo perché appartiene all'amministrazione che ha adottato alla decisione oggetto di giudizio, ma altresì in quanto potrebbe aver contribuito all'adozione della decisione stessa[89]. Quindi a rischio di incostituzionalità, non sono stati rispettati i principi delega stabiliti dalla legge di Riforma Madia in base ai quali era stata individuata nell'ANAC l'Autorità al quale il cittadino avrebbe dovuto presentare ricorso[90] per l'inerzia della P.A. ad un riscontro di accesso civico e la previsione di chiare e puntuali sanzioni.[91]

4. Conclusioni

Il tentativo di introdurre una legge sulla libertà dell'informazione in Italia, seppur apprezzabile negli intenti, è da ritenere ancora insoddisfacente. Invece, il Foia inglese mostra alle PA come esercitare la propria discrezionalità nell'assicurare ai propri cittadini (e non) il diritto all'accesso[92]. Rispetto a quest'ultimo, in quello italiano

---

[85] STRANO, L., "Foia: *Il decreto nasconde tre tradimenti alla trasparenza PA*", 1 Giugno 2016, disponibile all'indirizzo http://www.agendadigitale.eu/egov/strano-foia-ecco-i-tre-modi-con-cui-il-decreto-tradisce-l-abc-della-trasparenza_2262.htm

[86] RIPARTE IL FUTURO, "*Ecco cosa pensiamo del Freedom of Information Act*", 21 Maggio 2016, disponibile all'indirizzo https://www.riparteilfuturo.it/la-nuova-legge-sul-foia

[87] FAINI, F., "*Fino a che punto possiamo mettere il naso nella PA? Ecco il quadro dopo il Foia*", 3 Giugno 2016, disponibile all'indirizzo http://www.agendadigitale.eu/smart-cities-communities/fino-a-che-punto-possiamo-mettere-il-naso-nella-pa-ecco-il-quadro-dopo-il-foia_2275.htm

[88] BARRERA, G., "*Il «FOIA italiano» è legge: cosa cambia nell'accesso ai documenti*", 20 Giugno 2016, disponibile all'indirizzo http://www.ilmondodegliarchivi.org/editoriali/368-il-foia-italiano-e-legge-cosa-cambia-nell-accesso-ai-documenti

[89] AZZOLLINI, V. e RAGONE, M, "*Trasparenza: ancora troppi dubbi sull'efficacia del Foia italiano*", 7 Giugno 2016, disponibile all'indirizzo http://stradeonline.it/diritto-e-liberta/2070-trasparenza-ancora-troppi-dubbi-sull-efficacia-del-foia-italiano

[90] Il c.1 lett. h dell'art.7 della L.124/2015 (Riforma P.A. Madia) recita all'ultimo periodo: "*..procedure di ricorso all'Autorità nazionale anticorruzione.… nonché' della tutela giurisdizionale ai sensi dell'articolo 116 del codice del processo amministrativo, di cui all'allegato 1 del decreto legislativo 2 luglio 2010, n. 104, e successive modificazioni..*"

[91] Il c.1 lett. h dell'art.7 della L.124/2015 (Riforma P.A. Madia) recita all'ultimo periodo: "*..previsione di sanzioni a carico delle amministrazioni che non ottemperano alle disposizioni normative in materia di accesso..*"

[92] ADDANTE, F., "*Il Foia inglese, un esempio per l'Italia*", 25 Novembre 2016, raggiungibile all'indirizzo http://www.agendadigitale.eu/egov/il-foia-inglese-un-esempio-per-l-italia_2670.htm

manca un modello di comportamento preciso, un organo, come l'ICO, che deputato a svolgere solo compiti strettamente collegati al FOIA e alla privacy, sappia effettivamente condurre i richiedenti e i destinatari delle loro istanze ad una vera divulgazione delle informazioni. Concretezza che si realizza compiutamente con un lavoro di continua ricerca della perfezione attraverso l'emanazione di istruzioni operative e procedurali scaturite da casi concreti e maturati progressivamente nel tempo che cambiano in modo repentino a seconda di come cambiano le esigenze (ne sono una prova le FAQ registrate indicanti l'esito dei riscontri e rese pubbliche da tutti gli Enti con un unico sistema di classificazione), con processi che spingono le Amministrazione a fare del loro meglio con chi chiede l'accesso, essendo le stesse obbligate a fornire tutta la *ragionevole consulenza* possibile, anche solo si trattasse di rispondere ad una domanda, per assistere i richiedenti, in caso di loro difficoltà, al fine di indicargli il modo migliore di presentare l'istanza o aiutarli nella ricerca delle informazioni detenute. Attraverso il tracciamento delle diverse azioni intraprese, specifiche raccomandazioni e dettagli precisi sulle procedure di revisione obbligano, in caso di reclamo, le P.A. a dimostrare, con le dovute giustificazioni, un diverso comportamento assunto rispetto a quello che sono tenute ad avere e le ragioni che le hanno indotte a trattenere le informazioni richieste. Pertanto, prima di decidere il diniego, è necessario che la P.A. si assicuri di avere effettuato adeguatamente tutte le ricerche del caso, che le stesse siano state correttamente indirizzate e che, quindi, *non esistono ragioni convincenti* per arrivare a sostenere di non detenere alcuna delle informazioni registrate. Tutto ciò prima ancora che si arrivi dal Giudice, fase nella quale, non solo il richiedente può fare a meno di un avvocato (come in Italia in questo caso specifico) ma sono totalmente gratuite il contributo unificato e le spese giudiziarie[93]. Le Amministrazioni italiane, almeno per il momento (non si sa quando riusciranno a farlo), sono abituate a prendere le loro decisioni ragionando su un testo normativo che gli dica (quasi) esattamente come comportarsi, atteggiamento tipico di di una cultura '*Civil law*' dove le regole sono scritte e codificate e diversamente da quanto accade nei paesi del '*Common law*' in cui i comportamenti sono dettati da precedenti giurisprudenziali e quindi da un'esperienza in continuo perfezionamento evolutivo che si consolida progressivamente recependo la dinamicità degli sviluppi e delle esigenze variabili della società. Ne è una prova lampante quanto sta accadendo con il nuovo codice degli Appalti[94] che, al momento, anche

---

[93] "*Non è prevista alcuna tassa di ricorso al Tribunale e non occorre essere rappresentati da un avvocato o da un procuratore legale, anche se è consigliabile avere un'assistenza professionale legale. Tuttavia occorre tenere presente che un appello in tribunale può richiedere molto tempo e una preparazione accurata*". Da ICO.org.uk, "*Guide to freedom of information*", par. "*What does it cost to appeal against the ICO's decision?*" raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/complaints/

[94] D.lgs. 18 aprile 2016, n. 50, "*Attuazione delle direttive 2014/23/UE, 2014/24/UE e 2014/25/UE sull'aggiudicazione dei contratti di concessione, sugli appalti pubblici e sulle procedure d'appalto degli enti erogatori nei settori dell'acqua, dell'energia, dei trasporti e dei servizi postali, nonché' per il riordino della disciplina vigente in materia di contratti pubblici relativi a lavori, servizi e forniture*", (Codice degli Appalti e delle Concessioni) raggiungibile all'indirizzo http://www.

perché privo di rilevanti disposizioni attuative, alcune delle quali scadute da tempo, fa molta fatica a far comprendere alle Amministrazioni che poco è scritto e molto viene lasciato alla loro libera discrezionalità. Motivo per cui occorre muoversi secondo una ottima capacità di scelta che alla fine del processo di maturazione del Codice dovrebbe vedere in campo solo quelle che saranno in grado di rimanere sul mercato, le migliori in qualità, le più qualificate. A queste si appoggeranno tutte le altre per espletare le proprie funzioni di affidamento anche in conclusione dei processi di aggregazione degli acquisti. Ma l'ostacolo fondamentale è sempre lo stesso, le decisioni devono essere prese sapendo ben interpretare gli strumenti di "*soft law*", districandosi tra linee guida vincolanti, non vincolanti o semplici raccomandazioni. Un nuovo trend che, non trovando alcuna collocazione nella gerarchia delle fonti del diritto italiano e per il quale, ancora una volta, viene chiamata ad essere protagonista un'Autorità indipendente, appunto l'ANAC già al limite nello sforzo di risolvere tutti i problemi dell'Italia, per disporre in sostituzione di chi dovrebbe invece farlo in modo confacente al diritto, sta portando scompiglio e confusione tra gli addetti ai lavori i quali non hanno ancora capito o devono ancora abituarsi al fatto che, con il nuovo sistema, sono obbligate '*motivare adeguatamente*' lo scostamento della loro scelta rispetto a quella segnata e ritenuta ideale dalle linee guida per il buon andamento dell'azione amministrativa. Lo scopo è anche quello, proprio in sintonia con la filosofia del 'Common law', di dotare l'ANAC di uno strumento flessibile che, sensibile alle istanze e alle esigenze raccolte tramite la consultazione pubblica da parte di tutti quei soggetti che poi saranno interessati dalle stesse disposizioni che si formeranno con la versione definitiva, possa avvicinarsi il più possibile al meglio che si possa fare. Ma questo non può essere realizzato se a monte non vi sono disposizioni primarie da parte degli organi istituzionali preposti che fissino dei paletti precisi e chiari e si stabilisca chi fa cosa, tantomeno si può demandare all'ANAC il compito di individuare le soluzioni adeguate perché al livello superiore non sono stati capaci di sbrogliare la matassa. E' quello che ha provato a fare l'Autorità con la proposta di linee guida esaminate cercando di fornire istruzioni operative rispetto alle indicazioni chiare della Legge delega ma che poi sono cadute nell'oblio con il decreto attuativo. Pertanto, nonostante gli innumerevoli sforzi compiuti, le P.A. avranno, al momento, ancora difficoltà a comportarsi per compiere il giusto bilanciamento degli interessi e adempiere alle finalità del FOIA circa il "diritto di conoscenza" nella più totale incertezza normativa che spingerà le Amministrazioni italiane, anche quelle più virtuose, a decidere di negare l'accesso piuttosto che rischiare di essere sanzionate perché, ad esempio per ragioni di privacy maggiormente rilevanti individuabili tra pesi e contrappesi, potevano evitare di divulgare le informazioni richieste. Può, infatti, reputarsi che i pubblici dipendenti saranno più propensi al rigetto delle richieste della trasparenza, per il quale resterebbero comunque impuniti, che all'accoglimento delle stesse, a seguito del quale potrebbero incorrere in

normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2016-04-18;50!vig=

pene previste da discipline diverse, segnatamente in materia di privacy, a tutela di interessi giuridicamente tutelati[95]. Certo, questo è solo un primo tentativo di introdurre il FOIA in Italia e la sperimentazione al 28 dicembre 2016 potrebbe portare a dei miglioramenti ma rispetto a quello che gli inglesi hanno fatto per avere un vera 'Legge sulla libertà dell'informazione', occorre lavorare ancora tantissimo[96]. In Italia, dopo la caduta del Governo Renzi, la situazione attuale è di grande instabilità, pertanto ci si domanda se ci saranno in futuro, si spera nell'immediato, le condizioni affinché l'attuale Governo in carica o quello successivo, prima o dopo le nuove elezioni, avrà l'intenzione, ma soprattutto la capacità di proseguire il lavoro incompiuto e soprattutto di accogliere il meglio che possa provenire dall'esperienza di altre nazioni, appunto come quella del Regno Unito. Ma per fare tutto ciò occorre prima di tutto un reale '*cambiamento radicale di cultura*' improntato al Common Law e di sicuro questo non avverrà in tempi brevi. La speranza è che, fra un anno, al termine del monitoraggio, si possa effettivamente individuare quanto occorra con i dovuti approfondimenti e dopo aver raccolto i primi frutti della sperimentazione. Il buon esito dell'operazione dipenderà sia dall'impegno delle P.A. nello sviluppare una valutazione attenta e ragionata, caso per caso, che dall'intervento di una cittadinanza attiva interessata a migliorare le criticità e non invece chiusa in una muta rassegnazione nel credere che tanto non si risolverà mai nulla.

5. Fonti Normative (in ordine cronologico)

Legge 241/1990 e s.m.i. recante "*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*", disponibile su http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1990-08-07;241

Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC

D.lgs. 7 marzo 2005, n. 82, "*Codice dell'Amministrazione Digitale*", (CAD) con in particolare modifiche ed integrazioni del D.lgs 4 aprile 2006, n. 159 e del D.L. 30 dicembre 2010, n. 235 disponibile su www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-03-07;82

D.lgs. 33/2013, "*Decreto Trasparenza*", "*Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte del-*

[95] AZZOLINI, V., "*FOIA italiano: sarà vera trasparenza?*", 25 Maggio 2016, raggiungibile all'indirizzo https://www.leoniblog.it/2016/05/25/foia-italiano-sara-vera-trasparenza/

[96] ADDANTE, F., "*Ottimi i miglioramenti dell'ANAC, ma occorre fare ancora tanto per un vero FOIA?*", 11 Gennaio 2017, raggiungibile all'indirizzo Ottimi i miglioramenti dell'ANAC, ma occorre fare ancora tanto per un vero FOIA

le pubbliche amministrazioni", disponibile su http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2013-03-14;33

A.N.AC., (ex CiVit) Delibera n. 50/2013 "*Linee guida per l'aggiornamento del Programma triennale per la trasparenza e l'integrità 2014-2016*" disponibile su http://www.anticorruzione.it/portal/public/classic/AttivitaAutorita/AttiDellAutorita/_Atto?id=06b340010a7780425ec5237d6ee89951. Allegato 1 disponibile su http://www.anticorruzione.it/portal/rest/jcr/repository/collaboration/Digital Assets/anacdocs/MenuServizio/FAQ/Trasparenza/Obblighi-di-pubblicazione-ERRATA-CORRIGE-settembre-2013.xls

Legge 7 agosto 2015, n. 124, "Deleghe al Governo in materia di riorganizzazione delle amministrazioni pubbliche" (Riforma PA Madia) disponibile su http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2015-08-07;124!vig=

Schema del D.lgs. di modifica del Decreto Trasparenza e della Legge Anticorruzione, approvato, in via preliminare, dal Consiglio dei Ministri n. 101 del 21 Gennaio 2016:"*Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza, correttivo della legge 6 novembre 2012, n. 190, e del decreto legislativo 14 marzo 2013, n. 33, a norma dell'articolo 7 della legge 7 agosto 2015, n. 124*" disponibile su

http://www.funzionepubblica.gov.it/articolo/ministro/12-02-2016/trasparenza (Testo in PDF, pubblicato sul Governo.it, il 12 Febbraio,: http://www.francescoaddante.eu/anticorruzione/testo_21.pdf, pubblicato sul Governo.it, sostituito da quello pubblicato il 13 Febbraio,: http://www.governo.it/sites/governo.it/files/testo_21 %281%29 %281%29.pdf)

Schema di decreto di modifica del D.lgs. 33/2013, in versione preliminare, pubblicato il 12 e il 13 Febbraio 2016, disponibile all'indirizzo http://www.governo.it/sites/governo.it/files/testo_21 %281%29 %281%29.pdf

D.lgs. 18 aprile 2016, n. 50, "Attuazione delle direttive 2014/23/UE, 2014/24/UE e 2014/25/UE sull'aggiudicazione dei contratti di concessione, sugli appalti pubblici e sulle procedure d'appalto degli enti erogatori nei settori dell'acqua, dell'energia, dei trasporti e dei servizi postali, nonché' per il riordino della disciplina vigente in materia di contratti pubblici relativi a lavori, servizi e forniture", (Codice degli Appalti e delle Concessioni) raggiungibile all'indirizzo http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2016-04-18;50!vig=

D.lgs 25 maggio 2016, n. 97, "*Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicita' e trasparenza, correttivo della legge 6 novembre 2012, n. 190 e del decreto legislativo 14 marzo 2013, n. 33, ai sensi dell'articolo 7 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche*" (GU Serie Generale n.132 del 8-6-2016), disponibile all'indirizzo http://www.gazzettaufficiale.it/eli/id/2016/06/08/16G00108/sg e http://www.funzionepubblica.gov.it/articolo/ministro/12-02-2016/trasparenza (Av-

viso su Normattiva del testi integrato e coordinato delle modifiche al D.lgs. 33/2013: 10 giugno 2016, disponibile all'indirizzo http://www.normattiva.it/showNewsDetail?id=637&backTo=archivio&anno=2016)

(Allegato "B" di cui all'art.9-bis del D.lgs. 33/2013 "*Banche Dati*", disponibile all'indirizzo http://www.governo.it/sites/governo.it/files/allegato_2.pdf)

ANAC Schema di "*Linee Guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co. 2 del d.lgs. 33/2013*". Scadenza consultazione il 28 novembre 2016 raggiungibile all'indirizzo http://www.anticorruzione.it/portal/rest/jcr/repository/collaboration/Digital%20Assets/anacdocs/Attivita/ConsultazioniOnline/20161111/CO.accesso.civico.11.11.16.pdf

ANAC Determinazione n. 1309 del 28/12/2016 Linee guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co. 2 del d.lgs. 33/2013 Art. 5- bis, comma 6, del d.lgs. n. 33 del 14/03/2013 recante «*Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*» disponibile all'indirizzo http://www.anticorruzione.it/portal/public/classic/AttivitaAutorita/AttiDellAutorita/_Atto?ca=6666

ANAC Delibera n. 1310 del 28/12/2016 "*Prime linee guida recanti indicazioni sull'attuazione degli obblighi di pubblicità, trasparenza e diffusione di informazioni contenute nel d.lgs. 33/2013 come modificato dal d.lgs. 97/2016*" raggiungibile all'indirizzo http://www.anticorruzione.it/portal/public/classic/AttivitaAutorita/AttiDellAutorita/_Atto?ca=6667

FOIA. Le Linee guida del Regno Unito

ICO.org.uk, "*Guide to freedom of information*", par. "*What are the principles behind the Freedom of Information Act*?" raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/

ICO.org.uk, "*Guide to freedom of information*", par. "*When can we refuse a request for information?*" raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/refusing-a-request/

ICO.org.uk, "*Guide to freedom of information*", par. "*Who can make a freedom of information request?*" raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/

ICO.org.uk, "*Guide to freedom of information*", par. "*When is information covered by the Freedom of Information Act?"* raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/

ICO.org.uk, "*Guide to freedom of information*", par. "*What information do we need to publish?"* raggiungibile all'indirizzo https://ico.org.uk/

for-organisations/guide-to-freedom-of-information/publication-scheme/
ICO, *Information Commissioner Office*. Organo di Guida e Controllo dell'esercizio al diritto all'informazione, raggiungibile all'indirizzo https://ico.org.uk/about-the-ico/

ICO.org.uk, "*Guide to freedom of information*", par. "*In what format should we give the requester the information?"* raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/receiving-a-request/

ICO.org.uk, "*Guide to freedom of information*", par. "*Why use a 'neither confirm nor deny' response*" raggiungibile all'indirizzo https://ico.org.uk/media/1166/when_to_

refuse_to_confirm_or_deny_section_1_foia.pdf

ICO.org.uk, "*Guide to freedom of information*", par. "*What do we need to tell people about the Freedom of Information Act?"* raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/

ICO.org.uk, "*Guide to freedom of information*", par. "*Why must we publish information, rather than simply responding to requests?*" raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/publication-scheme/

ICO.org.uk, "*Guide to freedom of information*", par. "*What makes a request valid?",* raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/receiving-a-request/

ICO.org.uk, "*Guide to freedom of information*", par. "*Dealing with vexatious requests (section 14)",* raggiungibile all'indirizzo https://ico.org.uk/media/1198/dealing-with-vexatious-requests.pdf

ICO.org.uk, "*Guide to freedom of information*", par. "*When can we refuse a request as vexatious?*", raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/refusing-a-request/

ICO.org.uk, "*Guide to freedom of information*", par. "*When can we refuse a request because it is repeated?",* raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/refusing-a-request/

ICO.org.uk, "*Guide to freedom of information*", par. "*Can a question be a valid request?*", raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/receiving-a-request/

ICO.org.uk, "*Guide to freedom of information*", par. "Does *all the information have to be on a website?",* (post holders) raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/publication-scheme/

ICO.org.uk, "*Guide to freedom of information*", par. "*Duty to provide advice and assistance"* (section 16)" raggiungibile all'indirizzo https://ico.org.uk/media/1624140/duty-to-provide-advice-and-assistance-foia-section-16.pdf

ICO.org.uk, "*Guide to freedom of information*", par. "*What are our obligations under the Freedom of Information Act?*", raggiungibile all'indirizzo https://ico.org.uk/for-

organisations/guide-to-freedom-of-information/what-is-the-foi-act/

ICO.org.uk, "*Guide to freedom of information*", par. "*Do we have to tell them what information we have?",* raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/receiving-a-request/

ICO.org.uk, "*Guide to freedom of information*", par. "*flowchart of request handling under Foia*", raggiungibile all'indirizzo https://ico.org.uk/media/for-organisations/documents/1167/flowchart_of_request_handling_under_foia.pdf

ICO.org.uk, "*Guide to freedom of information*", par. "*What happens if we don't have the information?",* raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/receiving-a-request/

ICO.org.uk, "*Guide to freedom of information*", par. "*What about poor practice that doesn't amount to a breach of the Act?",* raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/complaints/

ICO.org.uk, "*Guide to freedom of information*", par. "*Are there criminal offences in the Freedom of Information Act?",* raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/complaints/

ICO.org.uk, "*Guide to freedom of information*", par. "*What should we do if someone complains to the ICO about how we have handled a request?*", raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/complaints/

ICO.org.uk, "*Guide to freedom of information*", par. "*What happens when someone complains?*", raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/complaints/

ICO.org.uk, "*Guide to freedom of information*", par. "*What should we do if someone complains to the ICO about how we have handled a request?*", raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/complaints/

ICO.org.uk, "*Guide to freedom of information*", par. "*Are there criminal offences in the Freedom of Information Act?",* raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/complaints/

ICO.org.uk, "*Guide to freedom of information*", par. "*What does it cost to appeal against the ICO's decision?",* raggiungibile all'indirizzo https://ico.org.uk/for-organisations/guide-to-freedom-of-information/complaints/

6.Sitografia (in ordine alfabetico)

ADDANTE, F., "*Foia, ecco gli ostacoli nella fase attuativa*", 5 Settembre 2016, raggiungibile all'indirizzo http://www.agendadigitale.eu/egov/foia-ecco-gli-ostacoli-nella-fase-attuativa_2410.htm

ADDANTE, F., "*Foia, prima e dopo: come cambia il percorso di accesso civico (in-*

fografica)", 3 Ottobre 2016, raggiungibile all'indirizzo http://www.agendadigitale.eu/egov/foia-prima-e-dopo-come-cambia-il-percorso-di-accesso-civico-infografica_2525.htm

ADDANTE, F., "*Il Foia inglese, un esempio per l'Italia*", 25 Novembre 2016, raggiungibile all'indirizzo http://www.agendadigitale.eu/egov/il-foia-inglese-un-esempio-per-l-italia_2670.htm

ADDANTE, F., "*Foia, ecco come funzionano le eccezioni nel Regno Unito*", 13 Dicembre 2016, raggiungibile all'indirizzo http://www.agendadigitale.eu/egov/foia-ecco-come-funzionano-le-eccezioni-nel-regno-unito_2702.htm

ADDANTE, F, "*FOIA, le norme cornice utili alla normativa: l'esempio del Regno Unito*", 6 Gennaio 2017, raggiungibile all'indirizzo http://www.agendadigitale.eu/egov/foia-le-norme-cornice-utili-alla-normativa-l-esempio-del-regno-unito_2785.htm

ADDANTE, F., "*FOIA. Oggi, 23 dicembre entra, o meglio, sarebbe dovuto entrare in vigore il nuovo diritto all'informazione*", 23 Dicembre 2016, raggiungibile all'indirizzo http://www.forumpa.it/foia-oggi-23-dicembre-entra-o-meglio-sarebbe-dovuto-entrare-in-vigore-il-nuovo-diritto-allinformazione

ADDANTE, "*Modello di Istanza per richiedere l'Accesso civico generalizzato in attesa che le P.A. si adeguino alla nuova disciplina*", 8, Gennaio 2017, disponibile all'indirizzo http://www.francescoaddante.eu/anticorruzione/istanza_accesso_civico_generalizzato_modello.docx

ADDANTE, F., "*Ottimi i miglioramenti dell'ANAC, ma occorre fare ancora tanto per un vero FOIA?*", 11 Gennaio 2017, raggiungibile all'indirizzo Ottimi i miglioramenti dell'ANAC, ma occorre fare ancora tanto per un vero FOIA

ADDANTE, F.," *Trasparenza. Dal 31 gennaio 2017 parte la vigilanza ANAC sui nuovi adempimenti informativi*", 11 Gennaio 2017, raggiungibile all'indirizzo http://www.forumpa.it/riforma-pa/trasparenza-dal-31-gennaio-2017-parte-la-vigilanza-anac-sui-nuovi-adempimenti-informativi

ANGHELE', F., "*FOIA italiano: l'Anac partorisce il topolino*", Riparte il Futuro, 29 novembre 2016 raggiungibile all'indirizzo https://www.riparteilfuturo.it/blog/articoli/foia-anac-linee-guida-eccezioni

AZZOLINI, V., "*FOIA italiano: sarà vera trasparenza*?", 25 maggio 2016, raggiungibile all'indirizzo https://www.leoniblog.it/2016/05/25/foia-italiano-sara-vera-trasparenza/

AZZOLLINI, V. e RAGONE, M, "*Trasparenza: ancora troppi dubbi sull'efficacia del Foia italiano*", 7 Giugno 2016, disponibile all'indirizzo http://stradeonline.it/diritto-e-liberta/2070-trasparenza-ancora-troppi-dubbi-sull-efficacia-del-foia-italiano

AZZOLLINI, V. "*FOIA all'italiana: fatta la regola, l'Anac trova le (numerose) deroghe*", 24 Novembre 2016, raggiungibile all'indirizzo http://phastidio.net/2016/11/24/foia-allitaliana-fatta-la-regola-lanac-trova-le-numerose-deroghe/

AZZOLLINI, V. e RAGONE, M,, "*Linee Guida Anac sul Foia, tra limiti alla discrezionalità e maggiori margini di arbitrio*", 24 Novembre 2016 raggiungibile all'indirizzo www.forumpa.it/riforma-pa/linee-guida-anac-sul-foia-tra-limiti-alla-discrezionalita-e-maggiori-margini-di-arbitrio

BARRERA, G., "*Il «FOIA italiano» è legge: cosa cambia nell'accesso ai documenti*", 20 Giugno 2016, disponibile all'indirizzo http://www.ilmondodegliarchivi.org/editoriali/368-il-foia-italiano-e-legge-cosa-cambia-nell-accesso-ai-documenti

Dipartimento della Funzione Pubblica "La *decertificazione*" raggiungibile all'indirizzo http://www.funzionepubblica.gov.it/semplificazione/le-azioni-trasversali-di-semplificazione/la-decertificazione

FAINI, F., "*Fino a che punto possiamo mettere il naso nella PA? Ecco il quadro dopo il Foia"*, 3 Giugno 2016, disponibile all'indirizzo http://www.agendadigitale.eu/smart-cities-communities/fino-a-che-punto-possiamo-mettere-il-naso-nella-pa-ecco-il-quadro-dopo-il-foia_2275.htm

FAINI, F. "*Trasparenza della PA, tutto ciò che c'è da sapere sui nostri diritt*i", 11 Luglio 2016, disponibile all'indirizzo http://www.agendadigitale.eu/smart-cities-communities/trasparenza-della-pa-tutto-cio-che-c-e-da-sapere-sui-nostri-diritti_2331.htm

FOIA.IT, Iniziativa per l'adozione di un Freedom of Information Act in Italia, Campagna per la Libertà d'Informazione, "*Breve Guida al Freedom of Information Act (Legge sulla Libertà d'Informazione) e Altri Nuovi Diritti all'Informazione*", raggiungibile all'indirizzo http://www.foia.it/docs/foia-it_doc010.pdf

MACKINSON, T., "*Foia, esperti e associazioni all'Anac: "Le sue linee guida affosseranno la legge*", 9 dicembre 2016, raggiungibile all'indirizzo http://www.ilfattoquotidiano.it/2016/12/09/foia-esperti-e-associazioni-allanac-le-sue-linee-guida-affosseranno-la-legge/3248051/

Open Government 3° Piano di Azione 2016 - *2018*, Proposta di ADDANTE F. del 26 agosto 2016 alle 1:38 pm, raggiungibile all'indirizzo http://open.gov.it/consultazione-terzo-nap/foia-attuazione-e-monitoraggio/

PEROSINO,M "*La libertà di stampa è nata in Svezia e oggi compie 250 anni*", 2 Dicembre 2016, raggiungibile all'indirizzo http://www.lastampa.it/2016/12/02/esteri/la-libert-di-stampa-nata-in-svezia-e-oggi-compie-anni-KVkydYsECxk9Mk9MnRdEML/pagina.html

RIPARTE IL FUTURO, "*Ecco cosa pensiamo del Freedom of Information Act*", 21 Maggio 2016, disponibile all'indirizzo https://www.riparteilfuturo.it/la-nuova-legge-sul-foia

STRANO, L., "*Foia: Il decreto nasconde tre tradimenti alla trasparenza PA*", 1 Giugno 2016, disponibile all'indirizzo http://www.agendadigitale.eu/egov/strano-foia-ecco-i-tre-modi-con-cui-il-decreto-tradisce-l-abc-della-trasparenza_2262.htm

N. 1 - 2017 · pp. 169-198

La Scuola della Qualità

Paola De Lumè – Pasquale Sarnacchiaro

Abstract: Da sempre il tema della qualità e dell'efficienza delle istituzioni scolastiche occupa un ruolo cruciale nel dibattito culturale e politico del nostro paese e la recente emanazione della L. 107/2015 non fa che alimentare il fermento che si è creato intorno a questo dibattito. Promulgata in data 13 luglio 2015 e battezzata come "Buona Scuola", la legge n. 107 ha puntato sin da subito alla messa in atto di un processo di riforma, snellimento e superamento di tutte quelle pratiche e consuetudini che ancora oggi continuano a caratterizzare la scuola italiana. Tra i punti principali della riforma, un piano straordinario di assunzioni e lo stanziamento di risorse stabili per la formazione e la valorizzazione del personale docente; inoltre, un'offerta formativa più ricca e flessibile per gli studenti ed un piano di investimenti per la creazione di ambienti digitali innovativi. La riforma del 2015 pone dunque molta enfasi sul raggiungimento da parte delle scuole di *standard* qualitativi adeguati e porta in primo piano non solo la valutazione in quanto indicatore fondamentale dello "stato di salute" degli istituti scolastici ma anche il ruolo del Dirigente Scolastico in quanto *leader* educativo chiamato a mettere in atto il progetto d'istituto. Ad oltre un anno dalla promulgazione della L. 107/2015, tuttavia, molto di quanto pianificato non è andato esattamente nella direzione sperata e diversi aspetti rimangono ancora da chiarire circa la sua reale ricaduta sul sistema scolastico italiano. Tra criticità e casi di successo, appare comunque evidente come la riforma costituisca oggi un'importante tappa nella storia della scuola italiana e possa essere pensata come una base da cui partire per poter ambire ad una scuola di qualità.

Abstract: The issue of the quality and efficiency of government-funded schools has always been present in the Italian cultural and political discourse and the recent reform of the Italian school education system seems to further foster this debate. The Italian Government approved the new law called *La buona scuola* in July 2015 (Law 107/2015). The reform's main aim is to show ways how to remove old policies, practices and obstacles to the good functioning of the Italian school system. The main pillars of the reform concern teacher recruitment, provisions to support teacher training and evaluation, improving of digital skills, and changes in the school curriculum by introducing and/or strengthening some subjects. The overall framework of the reform underlines the Government's commitment to ensuring high quality standards, with the emphasis especially on school assessment as an indicator of the successes and failures of schools and on the role of Headteachers in school improvement. The reform is now approaching its second year and it is clear that the Italian education system is still affected by long-standing problems. Nevertheless, we have to admit that the school reform has made some progresses in improving the

Articolo pervenuto il 2 Maggio 2017, approvato il 1 Giugno 2017

education system over the last few years and it may be considered as a starting point for developing schools based on quality principles.

Parole Chiave: Buona Scuola – Qualità – Valutazione – Merito – Indicatori

1. Efficacia, efficienza e qualità

Nell'ottobre del 2003 il Ministro Letizia Moratti firmava le cosiddette *Linee guida per una scuola di qualità*[1] con le quali venivano recepiti i principali orientamenti a cui si ispiravano le normative dell'epoca sia a livello nazionale sia a livello comunitario. "*La maggior parte dei paesi post-moderni* – scriveva il Ministro – *nel definire i fattori d'investimento e gli obiettivi strategici delle rispettive politiche economiche, ha individuato nell'efficacia e nell'efficienza dei propri sistemi educativi e nella valorizzazione delle risorse umane gli elementi fondamentali per garantire livelli di formazione di alto e qualificato profilo, assicurare competitività e sviluppo al sistema produttivo e promuovere l'educazione alla cittadinanza, nonché la crescita democratica delle proprie comunità*[2]".

A distanza di oltre dieci anni dalla pubblicazione delle cosiddette *Linee guida Moratti*, il tema del miglioramento della qualità e dell'efficienza delle istituzioni scolastiche torna ad occupare – con rinnovato vigore – un ruolo di primo piano nel dibattito politico italiano che la recente emanazione della L. 107/2015[3] ha contribuito ad alimentare. Tra gli aspetti su cui viene posta particolare enfasi nel dibattito attualmente in corso emergono con particolare forza aspetti quali l'autonomia delle istituzioni scolastiche finalizzata al raggiungimento di *standard* qualitativi elevati, la produttività del sistema scolastico – da intendere in termini di efficacia e di efficienza – e, non da ultimo, il ruolo del Dirigente Scolastico in questa fase cruciale di rinnovamento.

---

[1] Disponibile su *http://archivio.pubblica.istruzione.it/argomenti/qualita/testi/lineeguidadefinitive.htm*

[2] Nota ministeriale MIUR Per una scuola di qualità. Linee guida, 2003 (prot. 2794 del 7/11/2003)

[3] L. 13 luglio 2015, n. 107

Una delle parole chiave che caratterizza maggiormente questa fase è la parola "qualità", un termine che nel tempo ha acquistato sempre nuova forza e che viene oggi utilizzato – e molto spesso abusato – nei contesti più disparati con connotazioni e sfumature di significato differenti se non addirittura in contraddizione tra loro. Le parole di Robert M. Pirsig riportate di seguito provano a spiegare la contraddizione di fondo che c'è nella parola qualità: "*La qualità … sappiamo cos'è eppure non lo sappiamo. Questo è contraddittorio. Alcune cose sono meglio di altre cioè hanno più qualità. Ma quando provi a dire in che cosa consiste la qualità astraendo dalle cose che la posseggono, paff, le parole ti sfuggono di mano. Ma se nessuno sa cos'è, ai fini pratici non esiste per niente. Invece esiste eccome. Su cos'altro sono basati i voti, se no? Perché mai la gente pagherebbe una fortuna per certe cose, e ne getterebbe altre nella spazzatura? Ovviamente alcune sono meglio di altre… ma in cosa consiste il «meglio»?*[4]".

Nel 2000, tenendo ben presente l'obiettivo di raggiungere *standard* di qualità in grado di costruire un'economia basata sulla conoscenza e di promuovere la modernizzazione del modello sociale europeo, il Consiglio Europeo si riuniva a Lisbona[5] con lo scopo di definire i seguenti obiettivi strategici da adottare entro il 2010:

- ✓ aumentare la qualità e l'efficacia dei sistemi di istruzione e formazione nell'Unione europea;
- ✓ facilitare l'accesso di tutti ai sistemi di istruzione e formazione;
- ✓ aprire al mondo esterno i sistemi di istruzione e formazione.

Sulla scia di quanto definito dalla strategia di Lisbona, la più recente strategia "UE 2020[6]" punta al superamento di sfide sempre più impegnative e al raggiungimento di traguardi sempre più importanti attraverso un migliore utilizzo degli strumenti e delle risorse disponibili e grazie ad una più intensa collaborazione tra l'Unione Europea e gli Stati membri in materia di istruzione e di formazione professionale.

Nel 1999, con il D.P.R. 275/1999[7] - art. 8, capo III (Curricolo nell'autonomia) – veniva esplicitata l'importanza della definizione di *standard* di qualità del servizio scolastico, fissando anche metodi e scadenze per rilevazioni periodiche volte alla verifica del raggiungimento degli stessi. A tale scopo veniva infatti istituito il Centro europeo dell'educazione[8], un organismo autonomo preposto alla verifica, al supporto

---

[4] Pirsig, R., M., *Lo Zen e l'arte della manutenzione della motocicletta* (*Zen and the Art of Motorcycle Maintenance*, 1974), trad. di Delfina Vezzoli, Adelphi, Milano 1990

[5] Presidenza del Consiglio Europeo, Conclusioni della Presidenza, Consiglio Europeo di Lisbona 23/24 Marzo 2000

[6] Commissione delle Comunità europee Europa 2020 una strategia per una crescita intelligente, sostenibile e inclusiva, Comunicazione della Commissione Com(2010) 2020

[7] DPR N. 275/99 Regolamento dell'autonomia delle Istituzioni scolastiche

[8] Istituito con DPR n. 419 del 31.05.1974; riformato a norma dell'articolo 21, comma 10 della legge 15 marzo 1997, n. 59. Con il decreto legislativo del 20 luglio 1999, il 258/99, in applicazione della legge n. 59 del 15/3/99 (art. 11), non appena sarà pronto il regolamento esecutivo, il Cede assumerà il nome e le funzioni di "Istituto nazionale per la valutazione del sistema dell'istruzione"

ed al monitoraggio del servizio sostenendo le istituzioni scolastiche nell'efficace raggiungimento degli obiettivi prefissati. In tal senso, l'autonomia diventava un potente strumento a supporto delle istituzioni scolastiche di cui avvalersi per innalzare i livelli di integrazione e per promuovere una maggiore partecipazione delle famiglie – e più in generale dell'intera società – al processo di formazione dei bambini e dei ragazzi.

La definizione di *standard* qualitativi costituisce pertanto una tappa imprescindibile per poter offrire un servizio sempre più rispondente alle reali esigenze della società, vale a dire un servizio valido in termini di efficacia, efficienza e produttività. Quando si parla di produttività con riferimento al sistema scolastico si rimanda a due aspetti fondamentali vale a dire l'efficacia e l'efficienza. Così come la parola "qualità" è arrivata ad occupare nel tempo un ruolo sempre più centrale nel dibattito attuale, anche i termini appena citati rivestono un'importanza fondamentale nel momento in cui si vanno a definire i parametri attraverso cui misurare questa "qualità": laddove con il termine "efficacia" si indica il rapporto tra i risultati raggiunti in relazione agli obiettivi prefissati, con la parola "efficienza" si tiene conto invece del rapporto tra i risultati raggiunti e i costi sostenuti per il loro raggiungimento.

Efficacia = Ps/O
l'efficacia è data dal risultato [ovvero dal prodotto (P) o dal servizio (S)] ottenuto da una certa attività in relazione all'obiettivo (O) previsto per quell'attività.

Efficienza = E x R / R'
l'efficienza è data dall'efficacia per le risorse assegnate diviso le risorse effettivamente utilizzate.

Una volta definito il significato delle parole efficacia ed efficienza diventa più semplice cogliere il senso di un termine ampiamente utilizzato in ambito aziendale ma che oggi assume notevole importanza anche nell'ambito del sistema educativo. Il termine in questione è la parola "produttività" il cui significato può essere meglio illustrato ricorrendo alla seguente formula:

Produttività = Ps/R'

Indicando con Ps i risultati ottenuti (prodotto o servizio) e con R' le risorse spese per ottenerlo, si ottiene l'indice di produttività che può essere definito anche con la formula:

Produttività = E' x O/R

ovvero la produttività può essere intesa anche come il prodotto dell'efficienza per la produttività teorica (data dal rapporto tra obiettivi e risultati).
Traducendo le formule appena illustrate in termini di produttività nell'ambito del sistema scolastico, si può concludere che un'istituzione scolastica può dirsi realmente produttiva quando chi opera al suo interno è in grado di pianificare interventi mirati che si prefiggano degli obiettivi raggiungibili e nei quali vengano utilizzate in maniera efficiente tutte le risorse necessarie per poterli raggiungere. A

tal proposito, diventa fondamentale il ruolo del Dirigente Scolastico che, in qualità di rappresentante legale dell'ente che amministra (così come indicato dall'art. 25, II comma del D.Lgs. 165/2001[9]), è tenuto ad organizzare le attività del proprio istituto attenendosi a criteri di efficienza e di efficacia formativa.
A fronte delle riforme che nel corso del tempo hanno provato a disegnare una scuola di qualità – efficace ed efficiente – si è assistito in realtà ad una considerevole razionalizzazione della spesa pubblica per l'istruzione, chiedendo alla scuola di raggiungere risultati e traguardi sempre più importanti attraverso un'ottimizzazione della gestione delle risorse disponibili, anche quando queste ultime non risultano adeguate alle reali esigenze degli istituti. Con le leggi promulgate a partire dai primi anni novanta (Cfr., ad esempio, l'art. 1 della L. 241 del 7 agosto 1990[10]), l'interesse del legislatore si è spostato infatti sempre di più verso una politica di rinnovamento della pubblica amministrazione e, in particolare, verso la scuola, nucleo cardine della società da cui far partire questo processo di rinnovamento. Sempre maggiore enfasi è stata pertanto posta su prodotti e obiettivi da raggiungere per garantire la qualità del servizio offerto. La necessità di misurare questi obiettivi, tuttavia, ha innescato un processo di "managerializzazione" della scuola che, oggigiorno, viene spesso valutata per i risultati raggiunti senza tener in debito conto le procedure e le strategie adottate per raggiungerli.
Per poter valutare concretamente l'operato di un'istituzione scolastica in termini di efficienza, efficacia e produttività, è necessario tener conto di alcuni aspetti fondamentali che costituiscono una fonte preziosa di informazioni circa l'azione e le pratiche didattico-educative messe in atto.

2. Valutazione e autovalutazione d'istituto: una finestra sul sistema scolastico

Quando si parla di valutazione, si fa generalmente riferimento agli esiti derivanti dal confronto tra gli obiettivi programmati dallo *staff* docente e la situazione di fatto dell'apprendimento degli studenti. La valutazione è un indicatore molto importante dello "stato di salute" di un'istituzione scolastica: se circolare, aperta, unitaria e non separatoria, la valutazione consente non solo di ottenere importanti informazioni circa il cosiddetto "profitto scolastico" ma, allo stesso tempo, funge anche da termometro di quanto accade quotidianamente in classe, misurando il benessere degli alunni e la rispondenza tra quanto proposto e quanto realmente atteso da alunni e famiglie.

Al fine di misurare in maniera più sistematica i livelli di apprendimento degli alunni e, allo stesso tempo, di monitorare la qualità dell'offerta proposta dai diversi istituti scolastici su scala nazionale, sono nati in Europa sistemi di valutazione basati

[9] D.Lgs. n. 165/201, art. 25, II comma

[10] Legge n. 241 del 7 agosto 1990, art. 1, principio della buona amministrazione

sull'utilizzo di prove nazionali standardizzate. È quanto è accaduto anche in Italia dove, raccogliendo l'eredità del Centro Europeo dell'Educazione (CEDE), l'Ente di ricerca INVALSI (Istituto Nazionale per la Valutazione del Sistema educativo di Istruzione e di formazione) si è imposto con l'obiettivo e la funzione di proporre e somministrare a livello nazionale *test* standardizzati ed esami organizzati a livello centrale. Sulla base di quanto predisposto nell'art. 3 della Legge n. 53 del 2003, l'INVALSI ha competenza amministrativa a effettuare "*verifiche periodiche e sistematiche sulle conoscenze e abilità degli studenti e sulla qualità complessiva dell'offerta formativa delle istituzioni scolastiche e formative*[11]". Identificandosi come l'ente preposto ad una valutazione di sistema in grado di verificare il servizio scolastico nella sua globalità, l'INVALSI è nato quindi allo scopo di lavorare per il miglioramento continuo e una sempre maggiore armonizzazione della qualità del sistema di istruzione tramite la redazione di protocolli di valutazione e la somministrazione di prove di verifica standardizzate. Tra le sue prerogative rientra infatti anche quella di orientare le politiche educative nazionali proponendo un modello di valutazione basato su quattro elementi fondamentali ovvero: il contesto, l'*input*, i processi e i prodotti (elementi noti con l'acronimo CIPP). Congiuntamente ai processi di valutazione interna ed esterna, l'autovalutazione costituisce uno strumento di importanza estrema in quanto consente a chiunque operi all'interno di un'istituzione scolastica di cogliere i punti forti e i punti deboli dell'offerta formativa proposta e, di conseguenza, di intervenire in maniera adeguata allo scopo di migliorare le proprie capacità in relazione agli obiettivi prefissati. I processi di autoanalisi e di autovalutazione rappresentano dei momenti fondamentali di apertura verso l'esterno: attraverso una presa di coscienza della situazione reale in cui versa ciascuna istituzione scolastica, diventa molto più facile pianificare e successivamente attuare delle politiche educative mirate e rispondenti alle reali esigenze dell'utenza.

2.1. Il Sistema Nazionale di Valutazione (SNV) e la cultura della valutazione finalizzata al miglioramento

Il Sistema Nazionale di Valutazione (SNV)[12] nasce con l'intento di orientare le politiche educative verso una crescita culturale, economica e sociale dell'Italia, favorendo allo stesso tempo il pieno realizzarsi dell'autonomia delle istituzioni scolastiche. Un ruolo determinante ai fini del raggiungimento di questi obiettivi viene svolto dai diversi istituti di cui si compone il SNV, vale a dire l'Istituto nazionale per la valutazione del sistema di istruzione e formazione (INVALSI), l'Istituto nazionale di documentazione, innovazione e ricerca educativa (INDIRE) e il cosiddetto Contingente ispettivo. Ad essi devono poi essere aggiunti la Conferenza per il coordinamento funzionale del

[11] Art. 3 Legge n. 53 del 2003; Art. 3 D.Lgs. 286/2004

[12] Il Sistema nazionale di valutazione del sistema educativo di istruzione e formazione nasce con il D.L. n. 225 del 2010, Legge di conversione n. 10 del 2011

SNV ed i Nuclei di valutazione esterna che, con il loro apporto, contribuiscono al lineare svolgimento delle attività di valutazione. Avvalendosi di questi importanti organi – e sentito il parere della Conferenza unificata previo concerto con il Ministro del lavoro e delle politiche sociali – il Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR) emana periodicamente (circa ogni tre anni) le priorità strategiche della valutazione del sistema educativo d'istruzione. Si punta quindi alla realizzazione di un sistema di valutazione che sia allo stesso tempo organico e integrato, che riassuma in sé tutte le caratteristiche di un sistema di qualità in cui nessuna delle componenti della valutazione venga trascurata. Un sistema che, partendo dalla valutazione degli apprendimenti[13], sia poi in grado di valutare l'operato delle istituzioni scolastiche[14] nel loro complesso tenendo in doveroso conto i risultati raggiunti da chi opera all'interno della scuola, ovvero i docenti ed il Dirigente Scolastico, valutandone la professionalità[15].

2.1.1. Le fasi della valutazione

Tra gli obiettivi strategici della valutazione di sistema rientra prioritariamente quello di promuovere a livello nazionale una cultura della valutazione che miri ad una maggiore valorizzazione del ruolo degli istituti scolastici nel processo di autovalutazione e al conseguente miglioramento della qualità dell'offerta formativa[16]. Affinché questo obiettivo possa concretizzarsi, si è reso necessario definire in maniera chiara e articolata le fasi attraverso cui effettuare la valutazione di sistema. L'art. 6 del DPR 80 del 28 marzo 2013 illustra le quattro fasi relative al procedimento di valutazione delle istituzioni scolastiche e indica i tempi di attuazione e gli attori coinvolti nella valutazione.

a) Autovalutazione: la prima fase riguarda l'autovalutazione delle istituzioni scolastiche. Tutte le scuole, sia statali sia paritarie, sono state chiamate a compilare il cosiddetto Rapporto di Autovalutazione (RAV[17]), ovvero un piano di analisi e di valutazione interna a più dimensioni condotto sulla base di una serie di indicatori e di dati comparati forniti dal MIUR. Oltre ad offrire una rappresentazione della realtà di ciascuna scuola in quanto ne coglie le specificità e fornisce informazioni circa il suo funzionamento, il RAV è uno strumento determinante per poter capire la direzione in cui la scuola deve muoversi e verso cui orientare il proprio piano di

---

[13] Art. 1 comma 181 lettera i, legge 107/2015: adeguamento della normativa in materia di valutazione e certificazione delle competenze degli studenti, nonché degli esami di Stato

[14] DPR 80/2013, Regolamento sul sistema nazionale di valutazione in materia di istruzione e formazione; DIRETTIVA del 18 settembre 2014, n. 11, Priorità strategiche del Sistema Nazionale di Valutazione per gli anni scolastici 2014/2015, 2015/2016 e 2016/2017

[15] Art. 1 commi 126/130 e commi 86, 93, 94, legge 107/2015

[16] DPR 80/2013, art. 2, comma 1: "Ai fini del miglioramento della qualità dell'offerta formativa e degli apprendimenti, il SNV valuta l'efficienza e l'efficacia del sistema educativo di istruzione e formazione"

[17] Art. 6 del DPR n.80 del 2013

intervento. La pubblicazione dei RAV sulla sezione "Valutazione" del portale "Scuola in chiaro[18]" permette inoltre di accedere alla documentazione prodotta dal Nucleo Interno di Valutazione (NIV) di ciascun istituto scolastico e, ad oggi, ha restituito dati significativi circa l'operato del 95% delle scuole italiane coinvolte[19].
Tra gli obiettivi di miglioramento identificati, sono emersi in particolare:

RAV	
AREA ESITI	**AREA PROCESSI**
miglioramento risultati studenti	miglioramento curricolo e progettazione didattica
miglioramento risultati prove Invalsi	miglioramento ambienti di apprendimento
miglioramento competenze chiave e di cittadinanza	sviluppo e valorizzazione risorse umane
miglioramento risultati a distanza	migliore orientamento/integrazione scolastica
	maggiore integrazione con territorio e famiglie
	migliore organizzazione della scuola

Il Rapporto di Autovalutazione si articola in 5 sezioni:
- **Contesto e risorse:** in questa sezione le scuole hanno la possibilità di esaminare il contesto di appartenenza attraverso un'analisi della popolazione scolastica, del territorio e del capitale sociale, delle risorse economiche e materiali e delle risorse professionali.
- **Esiti:** traguardi raggiunti dagli studenti (analisi dei risultati scolastici e dei risultati nelle prove standardizzate, delle competenze chiave e di cittadinanza e dei risultati a distanza).
- **Processi:** esame di tutti i processi e delle pratiche educative messi in atto dalla scuola, attraverso l'analisi di: curricolo, progettazione e valutazione; ambiente di apprendimento; inclusione e differenziazione; continuità e orientamento o pratiche gestionali e organizzative; orientamento strategico e organizzazione della scuola; sviluppo e valorizzazione delle risorse umane; integrazione con il territorio e rapporti con le famiglie.
- **Processo di autovalutazione:** riflessione sul processo di autovalutazione in corso e sull'eventuale integrazione con pratiche auto-valutative pregresse nella scuola.
- **Individuazione di priorità e traguardi:** ai fini della redazione di un piano di miglioramento, vengono identificati i traguardi e gli obiettivi di processo da raggiungere per poter migliorare gli esiti.

b) Valutazione Esterna: con la seconda fase, si passa invece alla cosiddetta

[18] *http://cercalatuascuola.istruzione.it/cercalatuascuola/*

[19] Dai dati emersi attraverso una prima analisi dei RAV prodotti risulta, ad esempio, che il 20% delle scuole ha presentato informazioni non conformi ai criteri di coerenza e di attendibilità attesi, mentre il 52,9% delle scuole ha fornito dati aggiuntivi. (disponibile su *http://www.istruzione.it/snv/allegati/SNV_RAV_Numeri_DEFINITIVA.pdf*)

"valutazione esterna", ovvero la valutazione delle scuole per il prossimo triennio (fino ad un massimo del 10% delle scuole fra statali e paritarie per ciascun anno scolastico) da parte dei Nuclei di Valutazione Esterna, attivata a partire dall'anno scolastico 2015/2016 (Cfr. Direttiva 11/2014[20]).

c) Azioni di miglioramento: sempre a partire dall'anno scolastico 2015/2016, prendono inoltre avvio le azioni di miglioramento identificate attraverso il RAV. Il cosiddetto piano di miglioramento (noto anche come **PdiM**) è coordinato dal Dirigente Scolastico che ne è responsabile e che, coadiuvato dal Nucleo di Valutazione e Miglioramento, promuove tutte le azioni necessarie per coinvolgere l'intera comunità scolastica nel processo di miglioramento ed innovazione della scuola, rendendola partecipe degli obiettivi e delle azioni di intervento prefigurate. Parallelamente all'apertura verso l'esterno, il Dirigente deve anche saper confrontarsi con chi opera all'interno dell'istituzione scolastica e deve essere in grado di identificare le risorse materiali e le professionalità in essa presenti per raggiungere gli obiettivi individuati attraverso il PdiM.

d) Rendicontazione sociale[21]: nell'ottica della trasparenza e della disseminazione dei risultati ottenuti attraverso l'analisi e l'autovalutazione di ciascun istituto scolastico, a partire dall'anno scolastico 2016/2017 si rende necessaria l'attivazione da parte delle scuole di iniziative informative pubbliche ai fini della rendicontazione sociale e del maggiore coinvolgimento della comunità di appartenenza ai fini del miglioramento del servizio. L'esame delle diverse fasi in cui si articola l'attuale sistema di valutazione ci consente di cogliere l'enorme portata del processo valutativo e la sua ricaduta in termini di miglioramento della qualità del servizio offerto dalle istituzioni scolastiche. Concetto ribadito dalla Direttiva n. 11 del 18 settembre 2014 nella quale si afferma che "*la valutazione è finalizzata al miglioramento della qualità dell'offerta formativa e degli apprendimenti*[22]".

3. La valorizzazione del merito: il Comitato di valutazione dei docenti

Quello che un tempo era conosciuto come "*Comitato per la valutazione del servizio dei docenti*", è rubricato oggi sotto la voce *Comitato per la valutazione dei docenti*. Ai sensi del comma 129 dell'art. 1 della Legge 107/2015[23] viene identificato presso ciascuna istituzione scolastica ed educativa un Comitato per la valutazione dei docenti

[20] DIRETTIVA del 18 settembre 2014, n. 11, Priorità strategiche del Sistema Nazionale di Valutazione per gli anni scolastici 2014/2015, 2015/2016 e 2016/2017

[21] DPR del 28 marzo 2013, art. 6, comma 1, lettera *d*

[22] Direttiva del 18 settembre 2014, n. 11, "*Priorità strategiche del Sistema Nazionale di Valutazione per gli anni scolastici 2014/2015, 2015/2016 e 2016/2017*"

[23] Art. 11 del D.Lgs. 297 del 1994, novellato dal comma 129 dell'art.1 della Legge n.107 del 13 luglio 2015 (c.d. "legge buona scuola")

presieduto dal Dirigente Scolastico, con mandato triennale e senza alcun onere per la finanza pubblica. Il Comitato è composto da tre docenti interni all'istituto, da due rappresentanti dei genitori (per la scuola dell'infanzia e per il primo ciclo di istruzione) oppure da un rappresentante degli studenti e da un rappresentante dei genitori (per il secondo ciclo di istruzione), e da un componente esterno individuato dall'Ufficio Scolastico Regionale (USR). Fra i compiti specifici dei membri del Comitato rientra innanzitutto quello di lavorare sull'individuazione di criteri validi e trasparenti ai fini della valutazione e della valorizzazione del merito dei docenti impiegati presso ciascun istituto scolastico. Una volta stabiliti i criteri necessari per poter essere valutati in maniera trasparente e condivisa dall'intera comunità scolastica, il Dirigente Scolastico provvederà ad assegnare un *bonus* che andrà a premiare l'impegno e i meriti professionali del personale dell'istituto.

La professionalità del corpo docente impiegato presso un'istituzione scolastica è determinante per assicurare la qualità del servizio da essa offerto. Per tale motivo, numerosi sono stati nel tempo i tentativi di definire criteri e strategie utili per valutarne in maniera adeguate competenze e abilità. Dopo il concorso per *merito distinto e note di qualifica* del 1958 e il cosiddetto "concorsone" del 2000, nel 2003 l'attenzione si è concentrata sulla valutazione delle *performance* dei singoli insegnanti con la proposta dell'ARAN[24] ai sindacati di tener conto del rapporto esistente tra *performance* delle scuole, risultati degli allievi e carriera docente. A distanza di pochi anni, nel 2008, la proposta di legge Aprea recante "*Norme per l'autogoverno delle istituzioni scolastiche e la libertà di scelta educativa delle famiglie, nonché per la riforma dello stato giuridico dei docenti*" individuava poi un percorso basato su tre distinti livelli professionali (docente iniziale, docente ordinario e docente esperto) e su una progressione economica basata sull'anzianità.

Infine, con la Legge n. 107 del 2015 si è cominciato a delineare un percorso di valorizzazione del merito del personale docente (Cfr. artt. 126-130 L. 107/2015) con l'istituzione a decorrere dall'anno 2016 di un apposito fondo destinato a premiare l'operato del personale docente di ruolo delle istituzioni scolastiche sulla base dei criteri individuati dal Comitato di valutazione dei docenti. Tra i parametri di riferimento per la valutazione dei docenti rientrano:

- ✓ la qualità dell'insegnamento;
- ✓ il contributo apportato ai fini del miglioramento dell'istituzione scolastica;
- ✓ il contributo al successo formativo degli studenti;
- ✓ le responsabilità assunte nel coordinamento organizzativo, didattico e di formazione del personale;
- ✓ i risultati ottenuti dal potenziamento delle competenze degli studenti;
- ✓ i risultati ottenuti dall'innovazione didattica e metodologica;
- ✓ i risultati ottenuti tramite la collaborazione alla ricerca didattica, alla produzione di documentazione ed alla diffusione di buone pratiche didattiche.

[24] Agenzia per la Rappresentanza Negoziale delle Pubbliche Amministrazioni

3.1. La valutazione della Dirigenza scolastica

Così come si è reso necessario valutare – per poi eventualmente premiare – l'operato di tutti quei docenti che quotidianamente contribuiscono a rendere la scuola un ambiente altamente formativo e arricchente per ogni alunno, allo stesso modo sono stati pensati diversi sistemi e strumenti per poter valutare il lavoro di chi presiede e gestisce gli istituti scolastici, vale a dire il Dirigente.

Nel tempo è emersa con sempre maggiore vigore la necessità di poter valutare la professionalità dei dirigenti allo scopo di garantire l'adeguatezza degli interventi messi in atto rispetto ai bisogni specifici e reali della loro utenza e della comunità territoriale.
Già nel 1999 con l'art. 41 del CCNI si rendeva manifesta per i Capi d'istituto l'intenzione di sostituire i "*rapporti informativi annuali formulati dal provveditore agli studi con un atto di apprezzamento della qualità dei processi attivati da parte di un nucleo di valutazione regionale*"[25]. Tra gli elementi fondamentali da prendere in esame ai fini della valutazione dei Capi d'istituto, nel citato articolo rientravano il contesto socio-economico in cui è calata la realtà scolastica presieduta da ciascun soggetto esaminato e i risultati dei processi messi in atto al fine di raggiungere gli obiettivi prefissati nel piano dell'offerta formativa. In questo modo, il Capo d'istituto veniva valutato per le competenze inerenti la capacità di direzione e organizzazione dell'istituzione scolastica, la capacità di intrattenere relazioni positive e proficue all'interno ed all'esterno della scuola presieduta, l'abilità nel creare percorsi innovativi di crescita e sviluppo, e la capacità di valorizzare al meglio le risorse umane disponibili e di saper gestire in maniera ottimale le risorse finanziarie e strumentali a disposizione[26].
Le stesse aree di competenza dei Capi d'istituto sono state poi integrate nel cosiddetto modello SI.VA.DI.S 2005/2006[27], con il quale è stata posta particolare enfasi sulla capacità dei presidi di promuovere la qualità dei processi formativi attraverso la progettazione e l'innovazione dei processi di apprendimento individuali e collettivi. Al 2006 risale invece l'intervento del Ministro Fioroni che, tramite la Legge finanziaria n. 296, assegnava all'istituto INVALSI prerogative specifiche in merito alla definizione di "*procedure da seguire per la valutazione dei dirigenti scolatici*", alla formulazione di "*proposte per la formazione dei componenti del team di valutazione*" e alla realizzazione del "*monitoraggio sullo sviluppo e sugli esiti del sistema di valutazione*"[28].
A due anni di distanza, nel 2008, l'INVALSI era pronto a presentare all'allora Ministro

[25] Art. 20 del CCNL del comparto scuola e art. 41 CCNI scuola del 31 agosto 1999

[26] Art. 41 CCNI scuola del 31 agosto 1999

[27] Sistema di valutazione dei dirigenti Scolastici: sperimentazione gruppo di lavoro IRRE Toscana, 2005-2006

[28] Art. 1, comma 613 L. 296/2006

dell'istruzione Gelmini il sistema di valutazione denominato "*La valutazione dei Dirigenti scolastici*[29]", che prevedeva la definizione – di concerto con il Direttore dell'Ufficio Scolastico Regionale – di obiettivi quantitativi che i dirigenti avrebbero dovuto raggiungere nel percorso triennale di valutazione.
Del 2012 è poi la sperimentazione "*Valutazione e Sviluppo Scuola – VALeS*", un'iniziativa sperimentale derivante dall'esperienza del progetto VSQ[30] e nata per individuare criteri, strumenti e metodologie validi per la valutazione degli istituti scolastici e dell'azione della dirigenza scolastica[31].
La figura del Dirigente Scolastico ha acquistato nel tempo un'importanza sempre maggiore in ragione del ruolo cruciale che riveste nella gestione e nella conduzione di una scuola che sia in grado di formare le giovani generazioni fornendo loro tutti gli strumenti necessari per abitare il proprio tempo in maniera consapevole e con la giusta dose di resilienza. Per tale ragione, come illustrato nei paragrafi precedenti, numerosi sono stati nel tempo i tentativi messi in atto dal Ministero dell'istruzione e da enti e nuclei appositamente costituiti allo scopo di esaminare e valutare l'operato dei Dirigenti Scolastici. La valutazione dei Dirigenti Scolastici, effettuata ai sensi dell'articolo 25, comma 1, del D.Lgs. 30 marzo 2001, n. 165, deve essere dunque intesa come un importante ausilio e uno strumento efficace per coadiuvare ed orientare la loro azione e per sviluppare ulteriormente la loro professionalità. La più recente legislazione in materia prende infatti in esame alcuni aspetti fondamentali ai fini di una valutazione ottimale dei dirigenti. In base all'art. 1, c. 93, della L. 107/2015, l'accento viene posto su specifiche dimensioni professionali da tenere in debita considerazione quando si procede nella valutazione, vale a dire:

- *"competenze gestionali ed organizzative finalizzate al raggiungimento dei risultati, correttezza, trasparenza, efficienza ed efficacia dell'azione dirigenziale, in relazione agli obiettivi assegnati nell'incarico triennale;*
- *valorizzazione dell'impegno e dei meriti professionali del personale dell'istituto, sotto il profilo individuale e negli ambiti collegiali;*
- *apprezzamento del proprio operato all'interno della comunità professionale e sociale;*
- *contributo al miglioramento del successo formativo e scolastico degli studenti e dei processi organizzativi e didattici, nell'ambito dei sistemi di autovalutazione, valutazione e rendicontazione sociale;*
- *direzione unitaria della scuola, promozione della partecipazione e della collaborazione tra le diverse componenti della comunità scolastica, dei rapporti con il contesto sociale e nella rete di scuole.*[32]"

Sempre dalla L. 107/2015 si evince poi che "*per dare piena attuazione all'autonomia*

[29] Disponibile su http://www.invalsi.it/download/Rapporto_IParte.pdf e su http://www.invalsi.it/download/Rapporto_IIParte.pdf

[30] Valutazione per lo Sviluppo della qualità delle scuole (VSQ)

[31] Circolare VALeS del 3 febbraio 2012, n. 16

[32] Art. 1, c. 93, della L. 107/2015

scolastica e alla riorganizzazione del sistema di istruzione, il Dirigente Scolastico […] garantisce un'efficace ed efficiente gestione delle risorse umane, finanziarie, tecnologiche e materiali, nonché gli elementi comuni del sistema scolastico pubblico, assicurandone il buon andamento"[33].

4. Il Dirigente Scolastico e la qualità dei processi formativi

Elemento imprescindibile di un sistema di istruzione e di formazione di qualità è l'abilità di coloro che sono a capo degli istituti scolastici di pianificare percorsi e procedure in grado di soddisfare i bisogni e le aspettative dei fruitori del servizio (alunni, genitori, territorio). In tal senso, il Dirigente Scolastico riveste un ruolo di estrema importanza nel perseguimento di obiettivi concreti e tangibili, così come specificato nell'art. 25 del D.Lgs. 165/2001[34] in cui viene spiegato il passaggio dal ruolo direttivo al ruolo dirigenziale[35] e si parla dei dirigenti in termini di "referenti unici" sia per l'esercizio delle funzioni pubbliche che vengono loro assegnate sia ai fini del perseguimento della flessibilità, della diversificazione, dell'efficienza e dell'efficacia del servizio scolastico sopra menzionate. Il Dirigente assume dunque un ruolo strategico nei processi di autovalutazione d'istituto e nell'attuazione delle misure migliorative pensate per la realtà in cui opera coadiuvato nel suo lavoro dagli altri componenti della comunità scolastica (Collegio dei docenti, Consiglio d'Istituto e genitori) – con chiare funzioni di gestione finanziaria, organizzativa e di coordinamento e, di conseguenza, con maggiori responsabilità. Il Dirigente è dunque un *manager* che deve distinguersi per la propria abilità nel creare all'interno del proprio istituto un clima di serenità e cooperazione in grado di motivare tutto il personale a prendere parte attiva nel processo di miglioramento auspicato a livello ministeriale e non solo. Per queste sue prerogative e peculiarità, la figura del Dirigente risponde a quanto proposto già nel 1998 da Lorenzo Fischer e Marco Masuelli nella loro ricerca intitolata "*I dirigenti e l'autonomia delle scuole*[36]". Il Dirigente Scolastico, per Fischer e Masuelli, deve essere allo stesso tempo: a) un *leader* culturale che concordemente con il *team* docente e con gli *stakeholders* sviluppa un progetto culturale che farà da sfondo ad ogni iniziativa intrapresa per innalzare i livelli di qualità della scuola); b) un *leader* strategico abile nel mediare e negoziare sia con gli organi collegiali all'interno del proprio istituto sia con gli enti esterni; c) un *leader*

[33] Art .1, comma 78, Legge 107 del 13 luglio 2015

[34] Derivante dai precedenti D.L. n. 59/97 art. 21 e n. 59/98

[35] Il D.Lgs 59/1998 disciplina la qualifica dirigenziale dei capi di istituto delle istituzioni scolastiche autonome, a norma dell'articolo 21, comma 16, della legge 15.03.97, n.59

[36] Fischer, L., Masuelli, M., I dirigenti e l'autonomia delle scuole. Una ricerca sui capi d'istituto di fronte alla riforma, Ed. Franco Angeli, Milano, 1998

educativo che si adopera per promuovere al meglio una comunità di apprendimento e, infine, d) un *leader* ricettivo che sa cogliere i segnali provenienti dall'interno e dall'esterno e che si dà da fare per soddisfare i bisogni della propria utenza.
Come verrà illustrato nel paragrafo che segue, il bagaglio di competenze del Dirigente trova specifica attuazione nella definizione del piano triennale dell'offerta formativa – noto anche come PTOF – di recente introduzione.

4.1. La scuola che cambia e il PTOF: il piano dell'offerta formativa alla luce della L. 107/2015

Con la Legge 107/2015 alla tradizionale dicitura "Piano dell'Offerta Formativa (POF)" va ad aggiungersi una nuova connotazione, ovvero la valenza triennale dello stesso. L'ex art. 1, comma 14 della L. 107/2015[37], in particolare, esplicita la natura di questo nuovo piano e lo descrive come il documento fondamentale costitutivo dell'identità culturale e progettuale delle istituzioni scolastiche in quanto ne spiega la progettazione curricolare, educativa e didattica adottata nell'ambito della propria autonomia. Il Piano triennale è elaborato dal Dirigente Scolastico, sentito il Collegio dei Docenti, il Consiglio d'Istituto e i cosiddetti *stakeholders*, ovvero i principali attori economici, sociali e culturali del territorio con cui la scuola interagisce nella sua quotidianità.
In connessione con il piano di miglioramento[38] (PdiM) elaborato da ogni istituto, il piano triennale identifica il fabbisogno relativo ai posti del personale amministrativo, tecnico e ausiliario e il fabbisogno di infrastrutture e di attrezzature materiali, proiettando verso il futuro i traguardi che le scuole intendono raggiungere al termine del triennio attingendo a tutte le risorse professionali e finanziarie a loro disposizione.
Ciò che caratterizza il PTOF sono la sua natura dinamica e la sua coerenza rispetto all'impianto formativo di ciascun istituto per poter sostenere concretamente le azioni individuate come prioritarie dalla comunità scolastica[39]. Il piano triennale dell'offerta formativa è un documento estremamente importante per poter comunicare con l'utenza in maniera chiara, immediata e soprattutto trasparente: chi legge il PTOF è consapevole degli obiettivi che un istituto si prefigge e dei traguardi che esso intende raggiungere nel medio-lungo periodo attingendo alle risorse realmente disponibili ed adeguando costantemente la propria offerta alle esigenze emerse in fase di autoanalisi e di autovalutazione d'istituto.

[37] Ex art. 1, comma 14, Legge 13 luglio 2015, n. 107

[38] DPR 28 marzo 2013, n. 80

[39] Con riferimento a quanto emerso dal RAV, ai dati messi a disposizione dal MIUR, ai traguardi definiti dalle Indicazioni nazionali o dalle Linee guida.

5. *Best practices*: le buone pratiche del mondo della scuola

L'espressione "buone pratiche[40]" è utilizzata nella letteratura per indicare e descrivere i risultati di un progetto o di un'iniziativa in comparazione con i risultati attesi, tenendo conto dei suoi punti di forza e di debolezza e dei processi messi in atto per poterlo implementare in maniera efficace ed ottimale.
Nel mondo della scuola, quando si parla di "buone pratiche", ci si riferisce in particolare a tutte quelle iniziative, soluzioni operative e approcci metodologici che si sono saputi connotare come positivi per l'efficacia degli esiti che hanno permesso di raggiungere e per il loro carattere di innovatività e qualità. In quanto "comunità di pratiche", la scuola dà quotidianamente forma organizzativa alle proprie idee progettuali e, laddove queste ultime si contraddistinguono per la loro portata innovativa e per la loro applicabilità in altri contesti, si può parlare di *best practices* in quanto esse costituiscono un utile ed efficace riferimento per trarre spunti e soluzioni nuove da adattare alla diverse realtà in cui vengono applicate. Affinché la scuola possa diventare una scuola basata su buone pratiche e possa offrire modelli di riferimento a livello nazionale e non solo, la legislazione più recente ha individuato alcune priorità fondamentali da perseguire per offrire a tutti un servizio di qualità (priorità politica 1 e 4), garantendo a tutti gli studenti "*luoghi di apprendimento sicuri e un percorso scolastico che possa incidere positivamente nella realizzazione del loro progetto di vita e sul loro futuro, permettendo a tutti i meritevoli, ancorché privi di mezzi, di raggiungere i più alti gradi dello studio secondo il dettato della nostra Costituzione*"[41]. Risulta fondamentale in questo senso il contributo del Dirigente Scolastico nel saper individuare obiettivi significativi per la comunità e nell'assicurare la qualità dei processi formativi[42]. Sempre nell'Atto di indirizzo del Ministero dell'Istruzione, dell'Università e della Ricerca, prot. n.2 del 4 febbraio 2015 vengono poi elencate altre priorità altrettanto significative, ovvero:

[40] Bjørn Stigson offre la seguente spiegazione dell'espressione inglese *best practices: "A best practice is a technique or methodology that, through experience and research, has proven to reliably lead to a desired result. A commitment to using the best practices in any field is a commitment to using all the knowledge and technology at one's disposal to ensure success*".

[41] Atto d'indirizzo MIUR del 4 febbraio 2015, prot. 2 concernente le politiche del Ministero per l'anno 2015

[42] Art. 25 D.Lgs. 59/1998

Priorità politica 4 e 7	Contrastare la dispersione scolastica e favorire politiche per l'inclusione di tutti i bambini e ragazzi e aumentare il numero di studenti della scuola secondaria
Priorità politica 5 e 6	Valorizzare la professione docente e del personale scolastico tutto
Priorità politica 6	Rafforzare le competenze e l'insegnamento di discipline che sono patrimonio storico, culturale e artistico del nostro paese e accelerare sulle nuove alfabetizzazioni
Priorità politica 7	Sviluppare l'apprendimento permanente per la crescita e il potenziamento dei sistemi integrati di istruzione, formazione e lavoro, favorendo esperienze significative di alternanza tra scuola e lavoro, lavorando in sinergia con il tessuto imprenditoriale e regionale
Priorità politica 9	Lavorare ad una scuola "aperta", che sviluppi progetti e programmi dedicati, vicini alla disabilità e al contatto con il territorio e le sue problematiche per contrastare la dispersione scolastica
Priorità politica 10	Sviluppare la digitalizzazione per aumentare l'efficienza e migliorare la scuola con nuove modalità di insegnamento e apprendimento, promuovendo la dematerializzazione, la digitalizzazione e la trasparenza

Fonte: *Atto d'indirizzo MIUR del 4 febbraio 2015, prot. 2*

A distanza di oltre dieci anni dal lancio del cosiddetto "*Progetto qualità*" da parte del Ministro Gelmini[43], si torna dunque a puntare sulla definizione di regolamenti e direttive che forniscano indicazioni utili per il regolamento ed il coordinamento dei processi formativi e degli esiti di qualità. Tra i punti principali trattati nel documento sul "*Progetto qualità*" rientravano infatti sia la necessità di fornire un'adeguata formazione ai docenti sia il bisogno di partire dalla motivazione degli studenti per poter pianificare percorsi di qualità consoni alle loro reali esigenze formative. In questo modo diventavano dunque possibili e auspicabili traguardi quali la diffusione delle sopramenzionate "buone pratiche" ed il miglioramento *in itinere* di quelle già messe in atto. In questo documento veniva quindi a delinearsi l'idea di certificazione della qualità sulla falsariga dei criteri valutativi esplicitati nelle "Regole ISO 9001" del 2000[44].

5.1. La certificazione della qualità: approcci alla cultura della qualità e della valutazione

Nei precedenti paragrafi si è cercato di dare una definizione del termine "qualità" partendo da altri due concetti ad esso strettamente connessi, ovvero il concetto di "efficacia" e quello di "efficienza". In termini aziendali, quando si parla di strategia della qualità si fa riferimento ad una visione globale della qualità i cui elementi fondanti sono l'attenzione ad ogni dettaglio e la ricerca del miglioramento continuo

[43] Nota prot. N. 2741 del 7 Novembre 2003

[44] ISO 9000 identifica una serie di norme e linee guida sviluppate dall'ISO, che propongono un sistema di gestione per la qualità, pensato per gestire i processi aziendali affinché siano indirizzati al miglioramento della efficacia e dell'efficienza della organizzazione oltre che alla soddisfazione del cliente.

e dinamico (ovvero un processo iterativo che dovrebbe andare avanti all'infinito, ripartendo nella ricerca di un ulteriore possibile miglioramento). Nel momento in cui vengono interiorizzati questi principi si può cominciare a parlare di "progetto di qualità".

Nel tempo si è assistito ad una graduale evoluzione dei metodi e degli approcci finalizzati a misurare la qualità dell'offerta formativa e, più in generale, dei servizi offerti dalle scuole. Come ben illustrato dal professor Mario Castoldi dell'Università di Torino, numerosi sono stati gli approcci ideati ai fini della valutazione delle *performance* di chi opera all'interno della scuola.
In tabella vengono sintetizzati alcuni tra gli approcci più significativi:

APPROCCIO	Caratteristiche
Soddisfazione del cliente	• Analisi bisogni formativi e giudizi espressi dagli utenti; • soddisfazione dell'utente quale base da cui partire per valutare prodotti e/o servizi.
Diagnosi organizzativa	• Analisi aspettative dell'utente ed analisi sistemica dell'organizzazione scolastica; • enfasi su contesto ambientale, risorse disponibili, processi attivati e risultati raggiunti.
Autoanalisi d'istituto	• Valutazione quale occasione di auto-apprendimento; • coinvolgimento diretto degli operatori nell'azione valutativa; • focalizzazione del processo di auto-revisione sulle priorità individuate.
Indicatori educativi	• Definizione di un sistema organizzato di dispositivi di allarme allo scopo di accertare lo stato di salute delle scuole e a segnalare eventuali disfunzioni.
Controllo degli esiti formativi	• Focus sui risultati ottenuti anziché sui processi; • efficacia di un sistema educativo data dalla sua capacità di perseguire i propri obiettivi formativi attraverso un sistema rigoroso di accertamento che consenta di valutare la qualità complessiva del servizio scolastico.

Fonte: *Castoldi, M., Autoanalisi di istituto, in Cerini G., Spinosi M. (a cura di), Voci della scuola, Tecnodid, Napoli, 2003*

Certificare la qualità significa "*documentare ogni fase del processo aziendale, dalla produzione alla gestione dei materiali, dal controllo della produzione alla gestione dei documenti*". Con la pubblicazione della nuova versione della Norma ISO 9001 (che regola i sistemi di gestione della qualità delle organizzazioni), molte aziende si sono adoperate per ottenere una certificazione della conformità delle modalità di gestione della produzione e della qualità. È quanto si è tentato di fare nel documento citato nel paragrafo precedente, vale a dire il documento "*Progetto qualità*" del 2003 nel quale si prefigurava una valutazione della qualità realizzata dalle scuole in grado di creare una "positiva competizione" tra le stesse. Questa sana competizione, stando alle parole riportate nel documento, faciliterebbe "*la spontanea sottoposizione delle scuole 'all'accreditamento' e quindi ad una crescita controllata di qualità*[45]". Solo attraverso una partecipazione consapevole e attiva degli istituti scolastici al processo

[45] Nota prot. N. 2741 del 7 Novembre 2003

di valutazione diventa possibile attuare piani e strategie volte al miglioramento del servizio educativo offerto[46].

Accanto alla certificazione ISO 9000, esistono altri modelli di valutazione esterna basati sull'attivazione di processi di autoanalisi e autovalutazione. Tra questi esamineremo brevemente il modello Efqm (*European Framework for Quality Management*) e il CAF (*Common Assessment Framework*).

European Framework for Quality Management (Efqm)

Il modello EFQM per l'Eccellenza permette alle organizzazioni e ai suoi *manager* di comprendere le relazioni causa-effetto tra ciò che la loro organizzazione fa e i risultati che ottiene. Si tratta di un modello flessibile e non prescrittivo che può essere applicato a qualsiasi tipo di organizzazione e, in quanto tale, è stato spesso indicato come un modello valido anche per il mondo della scuola. Uno dei suoi punti di forza è che esso consente a chi opera all'interno di un'organizzazione (leggasi scuola) di condividere conoscenze e competenze e di lavorare ai fini di un miglioramento continuo. Affinché ciò accada, risulta determinante la figura del *leader* a capo dell'organizzazione: solo grazie ad una direzione strategica e ad una forte *leadership* infatti, si può pensare ad un successo duraturo.
I criteri su cui si basa il modello EFQM sono in tutto nove e si dividono in due gruppi: cinque criteri costituiscono i cosiddetti "fattori abilitanti" mentre i restanti quattro vengono raggruppati sotto la voce "risultati". Mentre i **a)** fattori abilitanti descrivono l'operato di un'organizzazione ed i metodi e le strategie impiegate per raggiungere determinati risultati, i quattro criteri denominati **b)** "risultati" riguardano per l'appunto i risultati, ovvero i traguardi raggiunti dall'organizzazione.

Common Assessment Framework (CAF)

Il CAF o Griglia Comune di Autovalutazione è uno strumento di *Total Quality Management*[1] ispirato dal modello di eccellenza EFQM della *European Foundation for Quality Management* (EFQM) e dal modello Speyer della *German University of Administrative Sciences*. L'idea alla base del modello CAF è che solamente attraverso una *leadership* strategica un'organizzazione possa migliorare di continuo le proprie *performance* e raggiungere quindi risultati eccellenti. Tramite una griglia di valutazione, il CAF agevola il lavoro delle organizzazioni del settore pubblico in quanto consente loro di comprendere al meglio il processo di autovalutazione (seguendo il percorso noto come *Plan-Do-Check-Act*) per poter intraprendere adeguate azioni di miglioramento.

5.1.1. La situazione italiana e il quadro europeo

Un breve richiamo alla situazione delle scuole in Europa ci consentirà di capire un po' meglio la posizione della scuola italiana – in termini di valutazione e di qualità – rispetto agli altri Stati membri dell'Unione Europea.
Valutazioni internazionali come ad esempio i *test* OCSE-PISA[47] rendono possibile

[46] Circolare n. 47 del 21 ottobre 2014

[47] Indagine internazionale denominata *Programme for International Student Assessment* (PISA) promossa dall'OCSE per poter valutare su base triennale il livello di istruzione degli adolescenti dei principali paesi industrializzati.

confrontare la qualità dei risultati e delle competenze in uscita tra diversi sistemi educativi. Non bisogna dimenticare tuttavia le peculiarità dei diversi sistemi educativi in quanto fondamentali per poter meglio comprendere i motivi che portano a collocare a livelli diversi i Paesi coinvolti nella valutazione. Quando si parla di valutazione bisogna distinguere fra valutazione interna e valutazione esterna. Per quel che riguarda la prima forma di valutazione, ad eccezione del Lussemburgo e della Bulgaria, essa è presente in tutti i restanti Paesi europei, sia essa obbligatoria o solo raccomandata.
Passando invece alla valutazione esterna, sulla base dei dati trasmessi periodicamente dalla rete Eurydice[48], risulta che mentre nella maggior parte dei Paesi europei essa viene effettuata da un corpo ispettivo indipendente dall'amministrazione centrale, in altri Stati invece essa è obbligatoria e sistematica e viene svolta da due autorità educative ben distinte (come nel caso di Danimarca, Svezia, Regno Unito, Islanda, Repubblica Ceca, Estonia, Lituania, Polonia e Slovacchia). Tra i Paesi appena citati, il Regno Unito è meritevole di considerazioni particolari in quanto sebbene si possa riscontrare un'impronta fondamentalmente privatistica e manageriale nella gestione delle scuole, esiste anche un ben definito ispettorato a livello nazionale, l'OFSTED[49], a cui spetta la responsabilità della valutazione. Nel Regno Unito la valutazione degli insegnanti avviene su base annuale ed è affidata al capo d'istituto coadiuvato da un consulente esterno e da alcuni membri dell'organo di gestione della scuola, il cosiddetto *School Governing Body* (SGB). In altri Paesi, come la Finlandia e la Norvegia, la valutazione esterna viene applicata a discrezione delle municipalità in quanto essa non è definita da una legge. Infine, nel caso di Paesi come l'Italia, la Finlandia, la Norvegia, l'Ungheria, la Grecia, il Lussemburgo, la Bulgaria e Malta – in cui la valutazione esterna non è molto diffusa – esiste un sistema di valutazione che abbraccia diversi aspetti come la valutazione del sistema educativo in generale oppure la valutazione delle autorità locali o degli insegnanti su base individuale.

5.2. Modelli e proposte progettuali per misurare la qualità e premiare il merito

Dopo aver esaminato alcune tra le certificazioni maggiormente utilizzate ai fini della misurazione della qualità delle *performance* e dei risultati raggiunti dagli istituti scolastici, sarà utile passare brevemente in rassegna le azioni ed i modelli proposti a livello ministeriale per incentivare le buone prassi e premiare le scuole che si sono contraddistinte per la qualità del servizio offerto.
Già nel 1999, con il regolamento recante norme in materia di autonomia delle istituzioni

[48] Rete istituzionale che raccoglie, aggiorna, analizza e diffonde informazioni sulle politiche, la struttura e l'organizzazione dei sistemi educativi europei.

[49] *Office for Standards in Education, Children's Services and Skills*

scolastiche[50], alla voce "Verifiche e modelli di certificazione" dell'art. 10 Capo III, si affermava la necessità da parte del Ministero della Pubblica Istruzione di fissare metodi e scadenze per rilevazioni periodiche finalizzate alla verifica del raggiungimento degli obiettivi di apprendimento e degli *standard* di qualità del servizio. Sulla scia di quanto affermato in questo documento – che occupa un ruolo centrale nella vita del sistema scolastico italiano – molte altre iniziative si sono susseguite nel tempo. Nella relazione[51] del Consiglio Europeo del 14 febbraio 2001, ad esempio, venivano individuati gli obiettivi futuri e concreti dei sistemi di istruzione e di formazione e, tra le finalità strategiche identificate per poter innalzare la qualità dei sistemi educativi e di istruzione, rientravano il miglioramento dei livelli di istruzione e formazione professionale degli insegnanti e dei formatori e l'incremento dell'alfabetizzazione in quanto elemento fondamentale per poter sviluppare le successive capacità di apprendimento e le opportunità di impiego in conclusione del percorso scolastico. Particolare enfasi veniva poi posta sul fatto di attuare un piano di investimenti finalizzato ad un utilizzo attento e consapevole delle cosiddette TIC, ovvero delle Tecnologie dell'Informazione e della Comunicazione[52]. All'anno scolastico 2010/2011 risale poi il progetto sperimentale di *Valutazione per lo Sviluppo della Qualità delle scuole* (anche noto come VSQ), nato allo scopo di introdurre sistemi di misurazione delle *performance* delle scuole per poterne individuare punti di forza ma anche criticità su cui lavorare, per identificare le eccellenze e per pianificare azioni di supporto e di miglioramento in linea con le esperienze di successo esperite a livello internazionale[53]. Del 2012 è poi la sperimentazione "*Valutazione e Sviluppo Scuola - VALeS*", un'iniziativa sperimentale derivante appunto dall'esperienza del progetto VSQ[54] e nata per individuare criteri, strumenti e metodologie validi per la valutazione degli istituti scolastici e dell'azione della dirigenza scolastica[55]. Sempre nel 2012 è stato inoltre avviato il "*Piano Nazionale qualità e Merito (PQM)*", un progetto nato per assicurare ad ogni classe, in ogni parte del Paese, un insegnamento e un apprendimento di qualità e per promuovere un sistema di "*valutazione responsabile e funzionale*", teso al miglioramento del sistema educativo ed alla valorizzazione dell'autonomia scolastica e pensato per proporre delle azioni mirate a supporto della qualità dell'insegnamento, per promuovere una cultura di responsabilizzazione delle scuole e per attivare azioni di miglioramento finalizzate a superare le criticità emerse nel sistema scolastico italiano.

---

[50] Art. 21, della legge 15 marzo 1999, n. 59

[51] Relazione del Consiglio (Istruzione) per il Consiglio Europeo sugli obiettivi futuri e concreti dei sistemi di istruzione e di formazione, Bruxelles, 14 febbraio 2001

[52] A partire dal 2008, stato poi avviato da parte del MIUR un processo di digitalizzazione della scuola con il Piano Nazionale Scuola Digitale (PNSD) finalizzato a favorire e supportare il cambiamento e l'innovazione del sistema Scuola.

[53] Cfr. D.Lgs. Del 27 ottobre 2009, n. 150

[54] Valutazione per lo Sviluppo della qualità delle scuole (VSQ)

[55] Circolare VALeS del 3 febbraio 2012, n. 16

Di più recente emanazione, il DPR 80/2013 ha stabilito poi che le istituzioni scolastiche devono essere in grado di pianificare e di attuare degli "*interventi migliorativi anche con il supporto dell'INDIRE o attraverso la collaborazione con Università, Enti di ricerca, associazioni professionali e culturali*". A tale scopo, è stato anche previsto un finanziamento da parte del MIUR per incentivare i progetti inerenti i piani di miglioramento delle scuole.[56]"

6. La qualità alla luce delle novità introdotte dalla riforma

Da sempre il tema della qualità e dell'efficienza delle istituzioni scolastiche occupa un ruolo cruciale nel dibattito culturale e politico del nostro paese e la recente emanazione della L. 107/2015 non fa che alimentare il fermento che si è creato intorno a questo dibattito. Promulgata in data 13 luglio 2015, recante "*Riforma del sistema nazionale di istruzione e formazione e delega per il riordino delle disposizioni legislative vigenti*", la legge n. 107 - battezzata anche come "Buona Scuola" - ha puntato sin da subito alla messa in atto di un processo di riforma, snellimento e superamento di tutte quelle pratiche e di quelle cattive consuetudini che ancora oggi continuano a caratterizzare la scuola italiana. Tra i punti principali della riforma, un piano straordinario di assunzioni per oltre 100.000 insegnanti e lo stanziamento di risorse stabili per la formazione e la valorizzazione del personale docente; inoltre, un'offerta formativa più ricca e flessibile per gli studenti ed un piano di investimenti per la creazione di ambienti digitali innovativi incentrati sulla laboratorialità. Ad oltre un anno dalla promulgazione della L. 107/2015, tuttavia, molto di quanto preventivato non è andato esattamente nella direzione sperata e, per avere un quadro più chiaro della situazione post-riforma, sarà utile analizzare punto dopo punto i cambiamenti e le novità da essa introdotte.

Tra i principali obiettivi della riforma, enorme rilevanza è stata attribuita all'attuazione di un piano di assunzioni di nuovi insegnanti tramite concorso per poter eliminare in via definitiva le Graduatorie ad Esaurimento (cosiddette GaE) e per porre fine all'annoso problema del precariato. A causa dei tempi di espletamento piuttosto lunghi dell'ultimo concorso bandito, tuttavia, la situazione che si riscontra oggi è ben diversa da quella auspicata dal legislatore. Tanti docenti dovranno infatti continuare ad attendere per l'assunzione in ruolo sebbene molte cattedre risultino ad oggi ancora vacanti.

Accanto ad un piano di assunzioni finalizzato alla copertura delle cattedre vacanti, la cosiddetta "Buona Scuola" ha previsto anche l'inserimento nelle scuole di ogni ordine e grado di docenti specializzati per il potenziamento della didattica e per

[56] DM 435/2015, art. 25, comma 2, lettera a

l'arricchimento dell'offerta formativa delle scuole. Nonostante il chiaro intento del legislatore di dotare le scuole di un organico dell'autonomia funzionale alle reali esigenze delle scuole e in grado di attuare il progetto educativo d'istituto delineato nel Piano dell'Offerta Formativa (che ora diventa triennale e viene indicato con l'acronimo PTOF), in numerosissimi casi questo obiettivo è stato disatteso. Inseriti nelle scuole allo scopo di potenziare discipline quali a) la musica e l'educazione motoria nella scuola primaria, b) le lingue straniere nella scuola secondaria di primo grado, c) Diritto ed Economia nella scuola secondaria di secondo grado, troppo spesso i docenti dell'organico di potenziamento si sono ritrovati in realtà a svolgere funzioni completamente differenti da quelle previste e, in particolare, a ricoprire il ruolo di supplenti. Ideata nell'ottica di un superamento definitivo del sistema di supplenze su cui si basa il funzionamento della macchina scolastica italiana, a distanza di più di un anno dalla sua applicazione si può quindi concludere che la riforma ha fallito nel suo tentativo di scardinare questo sistema in quanto il ricorso alle supplenze continua ad essere una prassi ancora molto diffusa nel nostro Paese. A questo sistema di assunzioni la legge 107 del 2015 ha inoltre affiancato un meccanismo definito "chiamata diretta" finalizzato al reclutamento dei docenti direttamente da parte dei Dirigenti Scolastici sulla base di un attento vaglio delle candidature e dei *curricula vitae et studiorum* pervenuti nelle scuole. Scopo di tale iniziativa è quello di garantire il superamento del vecchio modello basato sul reclutamento per anzianità di servizio e di agevolare il passaggio ad un nuovo sistema di reclutamento per competenze. Alla luce di quanto emerso nei primi mesi di applicazione, tuttavia, risulta piuttosto evidente che questa iniziativa non ha dato i frutti sperati e sono stati numerosissimi i casi di richiesta di conciliazione da parte dei docenti trasferiti in regioni diverse da quella di provenienza (e, in particolare, da Sud verso il Nord Italia).

Parallelamente ad un piano di assunzioni basato sulle competenze dei docenti e sulla capacità del Dirigente Scolastico di selezionare i profili più adeguati per le esigenze specifiche di ciascun istituto, la riforma ha previsto anche la possibilità di premiare chi, all'interno della scuola, si distingue per meriti e capacità professionali. Altro punto interessante della "Buona scuola" è dunque l'istituzione di un fondo destinato alla valorizzazione del personale docente in relazione al merito ed al contributo apportato da ciascuno ai fini del miglioramento dell'offerta formativa e al pieno raggiungimento degli obiettivi della scuola di appartenenza. A tale scopo la riforma ha previsto la costituzione di appositi Nuclei di valutazione presieduti dal Dirigente Scolastico e chiamati a stabilire dei criteri specifici per poter valutare al meglio l'operato di ciascun docente ai fini dell'attribuzione del *bonus* premiale. Relativamente all'a.s. 2015/2016, anno di prima attribuzione del cosiddetto *bonus* premiale ai docenti da parte dei Dirigenti Scolastici degli istituti di ogni ordine e grado, è emersa una situazione tutt'altro che semplice e lineare. Nonostante l'impegno dei Comitati di valutazione nel creare criteri trasparenti sulla base dei quali attribuire il *bonus*, molti dubbi sono emersi circa la corretta assegnazione dello stesso. In numerosi casi, infatti, le scuole hanno optato per una distribuzione "a

pioggia" del fondo destinato al *bonus* premiale anziché creare delle fasce di merito legate all'effettivo contributo apportato da ciascun docente ai fini del miglioramento dell'istituto e dell'offerta formativa dello stesso. Conseguenza di una simile scelta è stata, ovviamente, la polemica legata al fatto che docenti quotidianamente impegnati nel processo di rinnovamento e miglioramento della propria scuola sono stati posti sullo stesso piano di coloro che, pur svolgendo egregiamente il proprio lavoro di docenti impegnati nell'attività didattica e curricolare, non hanno tuttavia contributo ad ampliare l'offerta attraverso percorsi di ricerca-azione, sperimentazione ed innovazione didattica.
Congiuntamente all'attribuzione del *bonus* premiale, inoltre, la riforma ha previsto lo stanziamento di un fondo destinato ai docenti. Già dall'anno scolastico 2015/2016 infatti molti insegnanti hanno cominciato a beneficiare di un contributo o *voucher* del valore di 500 euro all'anno destinato alla formazione ed all'aggiornamento professionale. Tra le pecche di questo incentivo, tuttavia, il fatto che lo stanziamento di questi fondi sia stato previsto esclusivamente a favore dei docenti di ruolo escludendo dal beneficio tutti gli insegnanti con contratto a tempo determinato nonostante l'impegno profuso da questi ultimi per il corretto funzionamento dell'istituto presso cui prestano servizio sia lo stesso dei loro colleghi con contratto a tempo indeterminato e, soprattutto, nonostante il fatto che la formazione e l'aggiornamento dovrebbero essere garantiti a tutti i docenti in eguale misura indipendentemente dalla tipologia del contratto stipulato con la scuola.
Sempre nell'ambito della formazione e dell'aggiornamento rientra poi lo stanziamento di fondi per la formazione in servizio obbligatoria per i docenti in coerenza con il PTOF redatto da ciascuna scuola e con il cosiddetto Piano nazionale per la scuola digitale (PNSD) che prevede l'ampliamento dell'offerta formativa d'istituto e la formazione continua dei docenti e, in generale, di tutto il personale scolastico. Lanciato lo scorso anno in tutte le scuole, il Piano prevede il finanziamento di iniziative finalizzate alla promozione dell'innovazione nelle scuole. Tra queste iniziative, la copertura tramite rete wi-fi, la realizzazione dei cosiddetti *atelier* o laboratori creativi dotati di stampanti 3D e di tecnologie avanzate nei vari cicli di istruzione e la creazione di ambienti digitali e di spazi alternativi per l'apprendimento. Numerosissimi sono stati i corsi attivati per la formazione dei docenti, del personale amministrativo e tecnico e degli stessi Dirigenti Scolastici. Sono state inoltre nominate diverse figure responsabili per l'attuazione del Piano Nazionale Scuola Digitale e, tra questi, gli Animatori Digitali ed il cosiddetto *Team* dell'innovazione.
Laddove il PNSD ha raggiunto risultati importanti promuovendo l'innovazione e la cultura del digitale nelle scuole, un po' meno fortunata è stata l'esperienza dell'alternanza scuola-lavoro. Nata con l'intento di avvicinare il mondo della scuola e dell'istruzione a quello delle professioni, non sempre questa iniziativa ha dato i risultati sperati. Accanto a situazioni positive che hanno avuto un grande impatto sul percorso di formazione degli alunni della scuola secondaria di secondo grado, sono state riscontrate non poche anomalie segnalate da diversi istituti per i quali non è stato possibile attuare in maniera adeguata percorsi di alternanza scuola-lavoro a

causa della penuria di proposte valide per gli studenti oppure per la mancanza sul territorio di realtà in grado di accogliere gli studenti e di formarli adeguatamente.
Passando infine ad un altro dei punti nodali della Legge 107/2015, non si può trascurare di analizzare i risultati derivanti dall'attuazione di un piano di investimenti pensato per la manutenzione, ristrutturazione e messa in sicurezza delle scuole italiane nonché per l'adeguamento antisismico e la costruzione di edifici scolastici innovativi dal punto di vista architettonico, impiantistico e tecnologico. Nonostante i casi di successo e di piena attuazione della riforma, molto spesso, a remare contro queste iniziative sono intervenuti diversi fattori di disturbo ed episodi poco edificanti; tra questi, tutti quei casi segnalati in diverse scuole del territorio nazionale relativamente al crollo di solai o di interi edifici resi antisismici ma, come smentito dai fatti del 2012, crollati a seguito dei terremoti verificatisi nell'Italia centrale. Ancora molto rimane da fare in tema di edilizia scolastica e di ridefinizione degli *standard* da seguire per la messa in sicurezza degli edifici presenti sul territorio nazionale; ciononostante, seppur con i suoi ambiziosi obiettivi, la riforma del 2015 non deve essere vista solo come una goccia in mezzo al mare ma come un'occasione da sfruttare al meglio affinché l'idea di scuola buona ed innovativa non rimanga solamente sulla carta ma porti nel breve periodo ai risultati sperati.
Da questo breve *excursus* e da un bilancio del primo periodo di applicazione della legge 107 del 2015 si evince come, sotto diversi punti di vista, gli obiettivi ed i "buoni propositi" della *Buona scuola* siano stati spesso disattesi. È tuttavia riduttivo e forse anche troppo presto poter pensare di fare un bilancio chiaro ed esaustivo di quelli che sono gli effetti della riforma e dei suoi *pro* e *contro*. Per tale ragione, questa breve analisi di alcuni tra gli aspetti peculiari della legge 107/2015 si propone come una prima fotografia della situazione *post-riforma*, provando a raccogliere i primi dati relativamente alla sua ricaduta sul sistema scolastico italiano e al suo impatto su tutti gli attori coinvolti in questo processo.
Alla luce di quanto emerso nei paragrafi precedenti, sarà dunque utile riallacciarsi al tema da cui ha preso avvio il presente lavoro, ovvero il tema della qualità nella scuola e della valorizzazione del merito, per provare a coglierne appieno la portata in funzione di quanto evidenziato.
Nel 2008, nel suo libro *Meritocrazia: Quattro proposte concrete per valorizzare il talento e rendere il nostro paese più ricco e più giusto*[57], il saggista Roger Abravanel descriveva un percorso meritocratico pensato per la scuola italiana e basato su concetti chiave quali la valutazione e la misurazione oggettiva del merito. L'autore sosteneva che, per poter migliorare, la scuola italiana dovrebbe proporsi come un sistema basato su una misurazione oggettiva del merito - e quindi sulla valutazione dello stesso - dalla quale andrebbe a scaturire una "sana" competizione in grado a sua volta di generare merito e, di conseguenza, a migliorare il sistema. Leggendo tra i paragrafi del fascicolo "La Buona Scuola", si riscontra un evidente richiamo

[57] Abravanel R., *Meritocrazia: Quattro proposte concrete per valorizzare il talento e rendere il nostro paese più ricco e più giusto*, Milano, Garzanti, 2008

del legislatore a quanto proposto da Abravanel nel testo citato. Anche per la L. 107/2015, quindi, la valutazione occupa un ruolo di primo piano in quanto punto di partenza per rilevare gli elementi di forza e di debolezza del sistema educativo e per intervenire in maniera adeguata per poterlo migliorare. Se è vero che dalla competizione possono spesso scaturire esperienze positive volte al miglioramento ed alla valorizzazione dei meriti personali, è anche vero che altrettanto spesso dalla competizione possono nascere situazioni di conflitto e di emarginazione. Il modello che ha caratterizzato nel tempo e che caratterizza ancora oggi il sistema scolastico italiano è quello basato su una cultura del confronto e della cooperazione piuttosto che su una cultura del conflitto e della competizione. Alcune delle novità introdotte dalla L. 107/2015, in effetti, sembrerebbero privilegiare un modello meritocratico come quello delineato nelle pagine del libro di Abravanel, un modello valido ma che, in alcuni casi, ha creato situazioni di malcontento tra coloro che operano nel mondo della scuola. Tra le proposte più dibattute rientrano, ad esempio, la cosiddetta "chiamata diretta" dei docenti da parte dei Dirigenti Scolastici che suscita non pochi dubbi per via dell'ampia discrezionalità lasciata al Capo d'istituto; altro aspetto dibattuto, inoltre, il riconoscimento del merito dei docenti e la conseguente attribuzione del *bonus* premiale sulla base di criteri non sempre ben specificati oppure pensati per "accontentare" tutti e non escludere nessuno.

Il merito non è un qualcosa da riconoscere in modo arbitrario né da attribuire in maniera indiscriminata. Tutti i docenti sono chiamati a svolgere il proprio lavoro al meglio delle loro capacità e possibilità allo scopo non solo di ottenere il massimo da ciascuno studente ma anche per rendere migliore e più stimolante l'ambiente in cui lavorano. Il merito professionale è qualcosa che esula dagli incentivi o dalle promesse di riconoscimento ufficiale dell'operato di ciascuno; una scuola può definirsi davvero "buona" se, indipendentemente dal premio finale, chi vi opera all'interno è motivato a crescere professionalmente e lavora affinché tutti abbiano questa opportunità. A maggior ragione se, al termine di un anno scolastico di intenso lavoro, gli incentivi per i dipendenti della scuola vengono distribuiti "a pioggia" e non sempre sulla base degli effettivi risultati raggiunti da ciascuno.

Quando si parla di qualità con riferimento al mondo della scuola diventa necessario individuare degli *standard* che consentano di misurare in maniera efficace i risultati raggiunti. Con il termine risultati ci si riferisce non solo agli esiti formativi, alle prestazioni ed alle competenze acquisite dagli alunni, ma anche a tutto il sistema educativo ed al contesto in cui avviene l'apprendimento. Si deve cioè tener conto della qualità dei processi di insegnamento, delle metodologie e delle strategie messe in atto per consentire il successo formativo di tutti gli alunni e non si deve trascurare poi l'ambiente di apprendimento e il macro-contesto in cui essi si formano. Il ruolo dell'insegnante in questo senso è determinante: l'insegnante deve saper motivare i propri allievi e infondere il piacere dell'apprendere, deve incentivare i momenti di confronto e di condivisione tra alunni ma anche tra colleghi ed esperti del settore. L'attenzione di ogni singolo individuo verso anche il minimo dettaglio e la continua ricerca del miglioramento devono essere alla base del processo di cambiamento

e rinnovamento della scuola: solo in questo modo si può cominciare a parlare di scuola di qualità.
Innescare un processo di miglioramento nel sistema scolastico italiano è quanto mai indispensabile nella fase storico-sociale che stiamo vivendo e si può ambire a ciò solo innalzando la qualità dell'insegnamento e valorizzando adeguatamente il merito sul piano professionale.

BIBLIOGRAFIA

- Abravanel R., *Meritocrazia: Quattro proposte concrete per valorizzare il talento e rendere il nostro paese più ricco e più giusto*, Milano, Garzanti, 2008
- Allulli G., *Le misure della qualità*, Seam, Roma, 2000
- Allulli G., "*La Raccomandazione europea per la garanzia di qualità dell'istruzione e della formazione professionale*", in Professionalità n. 106, ed. La scuola, Brescia, 2009
- Commissione Europea (1995), *White paper on Education and Training – Teaching and Learning towards the Learning Society* COM(95) 590
- Commissione delle Comunità europee (2009), *Progress towards the Lisbon Objectives in Education and Training Indicators and Benchmarks* 2009. SEC(2009) 1616
- Commissione delle Comunità europee Europa 2020 una strategia per una crescita intelligente, sostenibile e inclusiva, Comunicazione della Commissione Com(2010) 2020
- Fassari L., *Managerializzazione della scuola ed organizzazione curricolare: spunti di riflessione per un dibattito incrociato*, in Benadusi L., Serpieri R., (a cura di), *Organizzare la scuola dell'autonomia*, Carocci, Roma, 2000
- Fischer L., Masuelli M., *I dirigenti e l'autonomia delle scuole. Una ricerca sui capi d'istituto di fronte alla riforma*, Ed. Franco Angeli, Milano, 1998
- Franceschini G., *Apprendere, insegnare, dirigere nella scuola riformata. Aspetti metodologici e profili professionali*, Edizioni ETS, Pisa, 2000
- Isfol, a cura di Allulli G. e Tramontano I., *I modelli di qualità nel sistema di formazione professionale italiano*, Rubettino, 2007
- OECD (2005) *Teachers matter: attracting, developing and retaining effective teachers, Education and Training Policy*, OECD Publishing Paris
- OECD, Education at a glance, OECD Indicators, OECD Publishing Paris anni vari
- Presidenza del Consiglio Europeo, Conclusioni della Presidenza, Consiglio Europeo di Lisbona 23/24 Marzo 2000
- Rondanini L., Capaldo N., *Manuale per dirigenti scolastici. Gestire e organizzare la scuola*, Centro Studi Erickson, 2013
- Rychen D.S., Salganik L.H., *Agire le competenze chiave. Scenari e strategie per il benessere consapevole*, Franco Angeli, 2007
- Stufflebeam D. et al., Educational evaluation and decision making, Itasca, IL: F. E. Peacock, 1971

- Visser W., Matten D., Pohl M., Tolhurst N., *The A to Z of Corporate Social Responsibility: A Complete Reference Guide to Concepts, Codes and Organisations*, John Wiley&Sons Ltd, 2007, p. 44
- Watzlawick P., Wekland J.H., Fisch R., *Change. Sulla formazione e la soluzione di problemi*, Astrolabio Ubaldini Edizioni, Roma, 1974
- Xodo C., Angeli F., *Il Dirigente Scolastico. Una professionalità pedagogica tra management e leadership*, Franco Angeli, Milano, 2010

RIFERIMENTI NORMATIVI

- Decreto Legislativo 16 aprile 1994, n. 297, "*Testo Unico delle disposizioni legislative in materia di istruzione*"
- Decreto Legislativo 6 marzo 1998, n. 59, "*Disciplina della qualifica dirigenziale dei capi di istituto delle istituzioni scolastiche autonome, a norma dell'art. 21, c.16, della legge 15 marzo 1997, n. 59*"
- D.P.R. 8 marzo 1999, n. 275, "*Regolamento recante norme in materia di Autonomia delle istituzioni scolastiche ai sensi dell'art.21, della legge 15 marzo 1999, n. 59*"
- D.P.R. 18 giugno 1998, n. 233, "*Regolamento recante norme per il dimensionamento ottimale delle istituzioni scolastiche e per la determinazione degli organici funzionali dei singoli istituti, a norma dell'art. 21 Legge n. 59 del 16.07.97*"
- Decreto Interministeriale 1 febbraio 2001, n. 44. "*Regolamento concernente le Istruzioni generali gestione amministrativo-contabile delle istituzioni scolastiche"*
- Decreto Legislativo 30 marzo 2001, n. 165, "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche"
- Legge 28 marzo 2003, n. 53, "*Delega al Governo per la definizione delle norme generali sull'istruzione e dei livelli essenziali delle prestazioni in materia di istruzione e formazione professionale*"
- Decreto Legislativo 19 novembre 2004, n. 286, "*Istituzione del Servizio nazionale di valutazione del sistema educativo di istruzione e di formazione, nonché riordino dell'omonimo istituto, a norma degli articoli 1 e 3 della legge 28 marzo 2003, n. 53*"
- Legge 27 dicembre 2006, n. 296, "*Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge finanziaria 2007)*"
- Direttiva n. 75 del 15 settembre 2008 (Ministro Gelmini)
- Legge 4 marzo 2009, n. 15, "*Delega al Governo finalizzata all'ottimizzazione della produttività del lavoro pubblico e alla efficienza e trasparenza delle pubbliche amministrazioni nonché disposizioni integrative delle funzioni attribuite al Consiglio nazionale dell'economia e del lavoro e alla Corte dei conti*"
- Decreto Legislativo 27 ottobre 2009, n. 150, "*Attuazione della legge 4 marzo 2009, n. 15, in materia di ottimizzazione della produttività del lavoro pubblico e di efficienza e trasparenza delle pubbliche amministrazioni*"
- Decreto Legislativo n. 213 del 31 dicembre 2009, "*Riordino degli enti di ricerca*

in attuazione dell'articolo 1 della legge 27 settembre 2007 n. 165"

- D.L. n. 225 del 2010, Legge di conversione n. 10 del 2011, "*Conversione in legge, con modificazioni, del decreto-legge 29 dicembre 2010, n. 225, recante proroga di termini previsti da disposizioni legislative e di interventi urgenti in materia tributaria e di sostegno alle imprese e alle famiglie*"
- DPR del 28 marzo 2013, n. 80, "*Regolamento sul sistema nazionale di valutazione in materia di istruzione e formazione*"
- Direttiva del 18 settembre 2014, n. 11, "*Priorità strategiche del Sistema Nazionale di Valutazione per gli anni scolastici 2014/2015, 2015/2016 e 2016/2017*"
- Circolare n. 47 del 21/10/2014, "*Priorità strategiche della valutazione del Sistema educativo di istruzione e formazione. Trasmissione della Direttiva n. Il 18.09.2014"*
- Atto d'indirizzo del MIUR del 4 febbraio 2015, prot. 2
- DM 16 giugno 2015, n. 435, "*Criteri e parametri per l'assegnazione diretta alle istituzioni scolastiche nonché per la determinazione delle misure nazionali relative la missione Istruzione Scolastica, a valere sul Fondo per il funzionamento delle istituzioni scolastiche*"
- Legge 13 luglio 2015, n. 170, "*Riforma del sistema nazionale di istruzione e formazione e delega per il riordino delle disposizioni legislative vigenti*"

Rivista elettronica di Diritto, Economia, Management

N. 1 - 2017 · pp. 197-218

Riforma del Codice dell'Amministrazione Digitale (CAD), Identità digitale, E-payment pubblico: la matrice europea di una nuova stagione dell'*e-Government*

Santo Gaetano

Abstract: Tra le aree di intervento definite dell'Agenda Digitale europea, quella che ha trovato più spazio nell'Agenda Digitale Italiana è sicuramente la "*ICT-enabled Benefts for EU society",* che ha l'obiettivo di rendere fruibili per i cittadini tutti i benefici derivanti dall'utilizzo delle tecnologie ICT. Al fine di colmare il gap del nostro Paese rispetto al resto dell'Europa in materia di digitalizzazione, il legislatore italiano, con l'entrata in vigore del D.lgs. n. 179/2016, ha riformato il Codice dell'Amministrazione digitale prevedendo alcuni interventi che costituiscono attuazione dell'Agenda europea. Tra questi i più importanti sono: la costruzione di un'Anagrafe nazionale della popolazione residente (ANPR); la realizzazione e diffusione del Sistema Pubblico di gestione dell'Identità Digitale (SPID); la previsione dell'obbligo per tutte le amministrazioni di accettare i pagamenti attraverso sistemi di pagamento elettronico ivi inclusi, per i micro-pagamenti, quelli basati sull'uso del credito telefonico (cfr. art. 5 del CAD come modificato dal d.lgs. 179/2016); la promozione della diffusione del domicilio digitale delle persone fisiche, al fine di facilitare le comunicazioni con le pubbliche amministrazioni (art. 3 bis CAD, come modificato dal d.lgs. 179/2016); la diffusione della connettività internet negli uffici e luoghi pubblici (art. 8 bis del CAD, introdotto dal d.lgs. n. 179/2016). Quest'ultima misura appare strumentale alla effettività dei diritti digitali del cittadino, tuttavia ne rappresenta il nodo critico: infatti solo assicurando l'effettivo accesso alla rete a tutti gli utenti, in forma gratuita, l'attuazione dell'*e-Government* potrà dirsi compiuta.

Parole chiave: Agenda digitale, *e-Governmen*t, Codice dell'amministrazione digitale, Digitalizzazione della pubblica amministrazione, Identità digitale, *e-Payment* pubblico.

Articolo pervenuto il 2 Maggio 2017, approvato il 1 Giugno 2017

come *diritto* di cittadinanza digitale. – 5. La Direttiva PSD2 ed il Regolamento UE n. 751/2015 quali normative evolutive per l'*e-Payment* pubblico. - 6. La diffusione della connettività alla rete internet: profili critici conclusivi.

1. L'*e-Government* quale strumento di modernizzazione e di riforma dell'amministrazione: profili introduttivi.

Il concetto di *e-Government* viene oggi declinato come l'interazione digitale tra amministrazione e privati ed, in particolar modo, come offerta di servizi *on-line* a cittadini e imprese[1].

Il fenomeno ha suscitato un crescente interesse nei vari Paesi a tal punto da essere analizzato dalle Nazioni Unite, le quali, nel Rapporto annuale sull'*e-Government* quale strumento di sviluppo sostenibile del 2016, sottolineano un sensibile aumento dei Paesi che usano strumenti informatici nella pubblica amministrazione per offrire servizi *online* ai cittadini, in virtù della relazione tra progresso tecnologico e sviluppo economico degli Stati [2]. Ciò in quanto i servizi di *e-Government* possono ridurre i costi e permettere ad amministrazioni pubbliche, cittadini ed imprese di risparmiare tempo.

È evidente come l'offerta di servizi informatici da parte delle amministrazioni pubbliche possa comportare effetti positivi sotto diversi aspetti.

Innanzitutto è resa più efficiente l'attività dell'amministrazione, sia interna che nella relazione con il pubblico; infatti, sotto il profilo del c.d. *back office*, il ricorso alle ICT permette all'amministrazione di giungere alle proprio decisioni in modo più rapido a tutto beneficio dei costi, grazie ad una ricerca più spedita di documenti, dati e persino atti di atre amministrazioni. Inoltre, sotto il profilo del c.d. *front* office, il privato, cittadino o impresa, può partecipare più agevolmente ai procedimenti grazie ad una rinnovata possibilità di recepimento di dati ed informazioni anche *online* [3]. Con

---

[1] M.L.MADDALENA, *La digitalizzazione della vita dell'amministrazione e del processo*, Relazione tenuta nell'ambito del Convegno "*L'Italia che cambia: dalla riforma dei contratti pubblici alla riforma della p.a.*", Varenna, 22-24 settembre 2016, su *giustizia-amministrativa.it* del 4 ottobre 2016.

[2] Si legge alla pag. 36 della Comunicazione della Commissione europea sull'Agenda digitale europea del 19.5. 2010 COM(2010)245, che il notevole dinamismo e l'innovazione propri del settore e l'influenza che le ICT esercitano sulla trasformazione delle modalità di funzionamento degli altri settori, comportano la generazione del 5% del PIL europeo e rappresentano un valore di mercato di 660 miliardi di euro l'anno, ma contribuiscono alla crescita complessiva della produttività in misura notevolmente maggiore (il 20% deriva direttamente dal settore delle ICT e il 30% dagli investimenti nelle ICT). http://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A52010DC0245

[3] M.L.MADDALENA, *op.cit,* pag.3; nonché V.F. COSTANTINO, *L'uso della telematica nella pubblica amministrazione,* in *L'azione amministrativa. Saggi sul procedimento amministrativo,* AA.VV., Giappichelli, 2016, pag. 246 e ss.

l'ulteriore effetto di stimolare la popolazione ad incrementare le proprie competenze informatiche in modo da sostenere la domanda di servizi interattivi, riducendo così quel divario digitale (*digatal divide*), che, come vedremo, costituisce uno dei maggiori freni alla diffusione delle tecnologie nel mondo produttivo e nella società [4].
Si comprende quindi come ormai l'utilizzo delle tecnologie sia diventato il più importante strumento di riforma e modernizzazione della pubblica amministrazione, in vista di una triplice finalità: innanzitutto, promuove la semplificazione e la riorganizzazione dei procedimenti nonché un maggior coordinamento delle competenze. Infatti l'*e-Government* "mira a semplificare i rapporti tra amministrazione e cittadini; richiede pertanto una re-ingegnerizzazione dei processi che, da un lato, elimini i passaggi inutili tra gli utenti e le amministrazioni – riportando su queste ultime l'onere della raccolta delle informazioni in possesso del settore pubblico – e, dall'altro, riduca le duplicazioni di attività e di controlli attraverso un accentramento dei servizi di supporto comuni a varie amministrazioni (*procurement*, gestione dei sistemi informativi, ecc)" [5].
In secondo luogo, la diffusione delle ICT rileva ai fini della realizzazione del c.d. *Open Government* [6], fondato sull'idea che il potere pubblico debba essere esercitato in modo trasparente nei confronti dei cittadini, favorendo forme di "democrazia collaborativa" e garantendo maggiori controlli sulla pubblica amministrazione [7].
Infine, le recenti innovazioni tecnologiche hanno reso possibile una maggiore interazione tra potere pubblico e cittadini. Infatti lo sviluppo attuale della rete internet (c.d. *Web 2.0*) permette la predisposizioni di siti istituzionali interattivi e con una reale possibilità di confronto in tempo reale con gli utenti, mediante forum di discussione e commenti, il che comporta enormi possibilità di interazioni tra gli utenti e, quindi, tra cittadini e Pubblica Amministrazione; laddove, invece, il precedente modello (c.d. *Web 1.0*) permetteva l'utilizzo dei siti delle amministrazioni in modalità

---

[4] La mancanza di competenze digitali in ampie fasce della popolazione è infatti uno dei principali problemi riscontrati nella diffusione delle ICT, in relazione al quale la Commissione europea, nella già citata Comunicazione del 2010 sull'Agenda digitale europea, richiede agli Stati membri importanti sforzi di alfabetizzazione informatica dei cittadini; ed è proprio in questa direzione che si muove anche la *Strategia per la crescita digitale 2014-2020*, approvata dal Consiglio dei ministri il 3 marzo 2015.

[5] ARPAIA, FERRO, GIUZIO, IVALDI, MONACELLI, *L'e-Government in Italia: situazione attuale, problemi e prospettive,* Banca d'Italia, Questioni di Economia e Finanza (*Occasional papers*) pag. 7.

[6] Si tratta di un modello di origine statunitense, esportato a livello internazionale nel 2011 attraverso l'iniziativa multilaterale dell'*Open Government Partnership* (OGP), che vede il coinvolgimento di 65 governi che si impegnano a realizzare alcune iniziative, sintetizzate in un Piano d'azione, cui l'Italia ha aderito, presentando un proprio *Action Plan* nel 2012 e un Secondo Piano d'azione Nazionale nel 2014. Così M.L.MADDALENA, *op.cit,* pag.4.

[7] F.COSTANTINO, voce: *Open Government,* in *Digesto discipline pubblicistiche,* UTET, Aggiornamento 2015, in cui i principi fondanti dell'amministrazione aperta sono: trasparenza (per promuovere l'*accountability* dell'amministrazione attraverso la pubblicazione delle informazioni sull'attività di governo); partecipazione (che consente a chiunque di fornire idee e conoscenze per il miglioramento delle politiche pubbliche); collaborazione (che rafforza l'efficacia dell'azione amministrativa attraverso la cooperazione tra tutti i livelli di governo centrale e locale e le istituzioni private, secondo un modello che nella terminologia nostrana potrebbe essere ricondotto alla sussidiarietà orizzontale).

unicamente informativa ed unidirezionale.
In questo quadro, si ritiene ormai superato quel modello del *New public management* (NPM) nel quale le tecnologie sono unicamente al servizio di una maggiore efficienza ell'apparato amministrativo, senza modificare i processi sottostanti e con scarse ricadute sulle modalità di interrelazione con l'utenza, e che debba passarsi al modello del *Digital Era Government* [8] (DGE).
L'importanza del ricorso alle tecnologie digitali al fine di promuovere un'amministrazione più efficiente, aperta, innovativa, responsabile e partecipata dai cittadini, giustifica il crescente interesse verso lo sviluppo e la diffusione delle ICT nell'amministrazione pubblica anche degli organismi internazionali[9]; e infatti una forte spinta verso la digitalizzazione dell'amministrazione viene proprio dall'Unione Europea attraverso la creazione dell'Agenda digitale per l'Europa.

2. L'Agenda digitale europea e l'attuazione nazionale delle politiche europee sulla digitalizzazione dell'amministrazione.

Nel 2010 l'Unione europea ha varato il programma "Europa 2020": si tratta della strategia decennale per la crescita e l'occupazione, finalizzata alla creazione di condizioni favorevoli ad una crescita intelligente e sostenibile, all'interno della quale viene concepita l'Agenda digitale per l'Europa, quale strumento fondamentale per la diffusione della banda larga e la promozione della competitività dell'UE [10].
L'Agenda digitale europea mira a stabilire il ruolo chiave dell'uso delle ICT affinchè

---

[8] Così M.L.MADDALENA, *op.cit,* pag.5.

[9] Anche l'OCSE, nel luglio 2014, ha adottato una raccomandazione sulle strategie del Governo digitale, http://www.oecd.org/gov/digital-government/recommendation-on-digital-government-strategies.htm ; e nel suo Rapporto "*Digital Government strategies for transforming public services in the welfare areas* " viene in particolare disegnato un percorso che va dal NPM, incentrato unicamente sulla riduzione dei costi e l'efficienza della amministrazione, all'e-Government, nel quale l'uso del'ICT comincia ad essere rivolto agli utenti, mediante l'uso di internet, stimolandosi strumenti di partecipazione procedimentale e di collaborazione nella prestazione dei servizi, fino al Digital Government, nel quale gli utenti divengono – tramite internet – parti attive della modernizzazione del settore pubblico, indicando le loro preferenze, i loro bisogni e contribuendo così a disegnare – in modo realmente partecipato e collaborativo – la programmazione pubblica e il contenuto e le modalità di prestazione dei servizi pubblici, http://www.oecd.org/gov/digital-government/Digital-Government-Strategies-Welfare-Service.pdf .
Si tratta di modelli ispirati ai Paesi del Nord Europa o di Common law e difficilmente esportabili in toto nei nostri confini, ma la cui valenza suggestiva è comunque di grande interesse anche per la realtà italiana, così M.L.MADDALENA, *op.cit.*

[10] L.ROMANI, *La strategia "Europa 2020": obiettivi e criticità, con particolare riferimento all'agenda digitale europea e all'interoperabilità dei sistemi informativi delle amministrazioni pubbliche europee,* in *Riv. amm. Rep. it.,* 2010, 573 ss.

l'Europa possa raggiungere gli obiettivi di sviluppo che si è prefissata per il 2020. Ed, a tal fine, impernia le proprie azioni principali sulla necessità di affrontare gli aspetti: della frammentazione dei mercati digitali; della mancanza di interoperatività; dell'aumento della criminalità informatica con conseguente rischio di un calo della fiducia nelle reti; della mancanza di investimenti nelle reti; dell'impegno insufficiente nella ricerca e nell'innovazione; della mancanza di alfabetizzazione digitale e di competenze informatiche; delle opportunità mancate nella risposta ai problemi della società.

Inoltre, essa si propone di creare un mercato unico digitale basato su Internet ad alta e altissima velocità e su applicazioni interoperabili, al fine di promuovere in Europa condizioni di crescita e sviluppo occupazionale [11].

In questo quadro, particolare attenzione viene riservata ai servizi di *e-Government,* che rappresenterebbero il volano dello sviluppo economico e strumento di promozione di una democrazia maggiormente partecipata dai cittadini.

Al fine di attuare concretamente le indicazioni dell'Agenda digitale europea, miranti allo sviluppo delle tecnologie, dell'innovazione e dell'economia digitale, l'Italia, attraverso l'art. 47, comma 1, del D.L. n. 5/2012, convertito in legge 4 aprile 2012, n. 35, si è dotata dell' "Agenda digitale italiana" (ADI), quale insieme di azioni e norme dirette a: favorire lo sviluppo di domanda e offerta di servizi digitali innovativi; potenziare l'offerta di connettività a larga banda; incentivare cittadini e imprese all'utilizzo di servizi digitali; promuovere la crescita di capacità industriali adeguate, a sostenere lo sviluppo di prodotti e servizi innovativi.

Tramite l'Agenda, avente valenza programmatica, il Governo persegue l'obiettivo prioritario di modernizzare i rapporti tra Pubblica Amministrazione, cittadini ed imprese e, attraverso il Decreto Legge, 18/10/2012 n.179, convertito dalla l.17 dicembre 2012, n.221 (c.d. Decreto crescita 2.0), ha previsto i principali interventi nei seguenti settori:

1. Identità digitale e servizi innovativi per i cittadini: carta di identità e tessera sanitaria elettronica; anagrafe unificata, archivio delle strade, domicilio digitale e posta elettronica certificata obbligatoria per le imprese;

2. Amministrazione digitale e dati aperti: dati e informazioni in formato aperto e accessibile compresi quelli della Pubblica Amministrazione, sistemi digitali per l'acquisto di beni e servizi, trasmissione obbligatoria dei documenti via Internet;

3. Agenda digitale per l'istruzione e la cultura digitale: certificati e fascicoli elettroni-

[11] Il 6 maggio 2015 la Commissione ha adottato la strategia per il mercato unico digitale, che si fonda su tre pilastri: 1) miglioramento dell'accesso dei consumatori e delle imprese ai beni e servizi digitali in tutta Europa; 2) creazione di un contesto favorevole e parità di condizioni per consentire alle reti digitali e ai servizi innovativi di svilupparsi; 3) massimizzazione del potenziale di crescita dell'economia digitale. Si ritiene, infatti, che la diffusione dell'uso di tecnologie digitali possa contribuire in misura di 415 miliardi di euro all'anno all'economia europea, creare nuovi posti di lavoro e migliorare i servizi pubblici e dunque dare un importante contributo al superamento della crisi economica in corso.

ci nelle università, testi scolastici digitali;

4. Misure per la sanità digitale: fascicoli sanitari elettronici, prescrizioni mediche digitali;

5. Forte impulso per la banda larga e ultralarga;

6. Fatturazione elettronica ed *e-payment*;

7. Giustizia digitale[12].

Ma il Governo compie un passo ulteriore verso l'attuazione nazionale delle politiche europee sulla digitalizzazione dell'amministrazione e, in data 3 marzo 2015, ha adottato due documenti programmatici, volti il primo a dettare linee guida per consentire all'Italia di superare il divario tecnologico con gli altri Pesi europei nella diffusione della connettività (*Strategia per la banda ultralarga*) e l'altro per promuovere la diffusione di competenze digitali (*Strategia per la crescita digitale 2014-2020*). Quest'ultimo, in particolare, muove dalla considerazione che il lato più debole nello sforzo di digitalizzazione del Paese sia soprattutto quello della domanda di *e-Government* da parte dei cittadini e delle imprese. Pertanto, esso promuove e pianifica l'informatizzazione della PA – e quindi l'offerta di *e-Government* – con l'obiettivo di accrescerne l'efficienza, ma anche di esercitare un ruolo di traino per l'alfabetizzazione informatica del Paese [13].
Il programma governativo per la Strategia per la crescita digitale 2014-2020, in linea con le politiche prevalenti a livello internazionale, prevede:

1) Azioni sulle infrastrutture. Il programma punta su un potenziamento delle reti (passaggio alla banda ultra larga) e dell'integrazione tra le infrastrutture esistenti; il documento programma un aggiornamento delle regole tecniche del SPC (Sistema pubblico di connettività), che con i propri standard deve costituire l'elemento di integrazione dei sistemi informativi delle pubbliche amministrazioni, favorendone l'interoperabilità. Stabilisce in questo ambito anche un percorso di sfruttamento della tecnologia *cloud computing*, per convergere, a regime, verso un sistema di condivisione delle infrastrutture IT attraverso una graduale migrazione dei sistemi.
L'intervento sulle infrastrutture deve inoltre favorire la diffusione di internet tra i cittadini attraverso la progressiva disponibilità di punti WIFI negli edifici e uffici pubblici (ad es. scuole, ospedali, uffici comunali, zone turistiche, ecc.).

2) Progetti riguardanti le piattaforme abilitanti. Il programma individua i progetti trasversali del cosiddetto "nodo dei pagamenti pubblici" (PagoPA), della fatturazione elettronica, degli open data, oltre a progetti mirati che interessano le principali amministrazioni fornitrici di servizi pubblici (sanità, scuola, giustizia, turismo, agricoltura). Le pubbliche amministrazioni sono tenute ad aderire al sistema dei Pagamenti

---

[12] M.L.MADDALENA, *op.cit.* pag. 13, che richiama *Pubblica amministrazione digitale: come farla davvero EY*, Glocus, maggio 2015, http://www.ey.com/Publication/vwLUAssets/Pubblica_amministrazione_digitale/$FILE/EY-Glocus.pdf

[13] *op.cit.* pag. 15

elettronici, mentre i gestori di pubblici servizi possono partecipare su base volontaria (art. 15, comma 5-bis, D.L. 18 ottobre 2012, n. 179). Il sistema di pagamenti elettronici (pagoPA) consente a cittadini e imprese di effettuare qualsiasi pagamento verso le pubbliche amministrazioni e i gestori di servizi di pubblica utilità in modalità elettronica. Il sistema permette alle PA di: velocizzare la riscossione degli incassi, ottenendone l'esito in tempo reale e potendo effettuare la relativa riconciliazione in modo certo e automatico; ridurre i costi e ottimizzare i tempi di sviluppo delle nuove applicazioni online; eliminare la necessità di stipulare specifici accordi con i prestatori di servizi di riscossione.

3) Adozione di cosiddetti "programmi di accelerazione". Si tratta di programmi finalizzati a diffondere la cultura digitale e ad accrescere le competenze del Paese. Tra questi:

- la costruzione di un'Anagrafe nazionale della popolazione residente (ANPR), che prenderà il posto delle oltre 8.000 anagrafi dei comuni italiani, costituendo un riferimento unico per la Pubblica Amministrazione, le società partecipate e i gestori di servizi pubblici. Con l'ANPR si realizza un'unica banca dati con le informazioni anagrafiche della popolazione residente;
- la realizzazione del Sistema Pubblico di gestione dell'Identità Digitale (*SPID*), è il sistema che permette a cittadini e imprese di accedere con un'unica identità digitale ai servizi online della PA e dei privati aderenti, consentendo: scambio di comunicazioni con conservazione dello storico; accesso a tutti i servizi online; ricezione di avvisi di scadenze; ricezione/effettuazione di pagamenti con conservazione dello storico; archiviazione di propri documenti; interazione con l'anagrafe digitale; formulazione di valutazioni e feedback alle amministrazioni, ecc..
- *Open Data*: sono dati pubblici che devono essere pubblicati in maniera che sia facile il riutilizzo. A tal fine sono fondamentali aspetti quali: licenze, standardizzazione, qualità, accessibilità anche attraverso applicazioni automatizzate. Ogni amministrazione è tenuta a rilasciare Open data per contribuire alla valorizzazione del patrimonio informativo pubblico, in linea con le politiche internazionali e nazionali sugli Open data.

Queste le linee di intervento tracciate nel programma governativo, delle quali una prima traduzione normativa è contenuta nella recente legge di riforma della pubblica amministrazione (l. n.124/2015), la cosiddetta "Legge Madia"; la quale, tra gli obiettivi di fondo, si pone anche la riforma del Codice dell'amministrazione digitale in vista di un suo coordinamento con il Regolamento UE 23 luglio 2014, n. 910, cosiddetto Regolamento *eIDAS* (*Electronic, IDentification Authentication and Signature*).

3. Il Regolamento UE n. 910/2014 eIDAS e il D.lgs. 26 agosto 2016, n. 179: il Codice dell'amministrazione digitale guarda all'Europa.

Il 28 agosto 2014 è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea (Official Journal of the European Union, L. 257) il Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio dell'Unione Europea "in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE".
Il Regolamento, conosciuto anche con l'acronimo *eIDAS* (*Electronic, IDentification Authentication and Signature*), ed entrato in vigore il 17 settembre 2014 ma con applicazione nelle sue parti operative a far data dal 1 luglio 2016, ha l'obiettivo di fornire una base normativa comune per l'Unione Europea in materia di servizi fiduciari e mezzi di identificazione elettronica degli stati membri.
Il regolamento, dunque, fissa le condizioni generali a cui gli Stati membri devono attenersi per il riconoscimento dei mezzi di identificazione elettronica delle persone fisiche e giuridiche; oltre che le regole relative alla transazioni elettroniche e istituisce un quadro normativo relativo alle firme elettroniche, sigilli elettronici, validazioni temporali elettroniche, documenti elettronici, servizi elettronici di recapito certificato e servizi relativi all'autenticazione di siti web.
Con tali premesse, l'attuazione del regolamento in tutti gli stati membri permetterà la creazione di un mercato unico digitale in cui le regole del gioco saranno uguali per tutti.
Tutto questo dovrebbe comportare indiscutibili vantaggi sia in termini di semplificazione per le P.A., che in termini di trasformazione digitale delle imprese e di sviluppo di servizi innovativi e sicuri. Le imprese saranno agevolate nell'estendere la loro attività oltre le frontiere e ad interagire con le autorità pubbliche di altri paesi, grazie agli obblighi di accettazione reciproca da parte degli stati membri nella fruizione dei servizi fiduciari qualificati. I cittadini potranno fruire di servizi *online* anche nei rapporti con le amministrazioni e autorità di altri stati membri, nel campo fiscale, sanitario e dell'istruzione.
Il Regolamento parte dalla considerazione che si rende necessario instaurare un clima di fiducia negli ambienti *online*, per favorire lo sviluppo economico e sociale. Allo stato attuale infatti l'assenza di certezza giuridica nell'ambito del digitale crea un sentimento di scoraggiamento nei consumatori, nelle imprese e nelle autorità pubbliche che non sono portati ad effettuare transazioni per via elettronica e ad usare o adottare servizi in rete. In quest'ottica il regolamento mira a rafforzare la fiducia nell'utilizzo degli strumenti elettronici nel mercato interno dei singoli stati che nell'Unione Europea.
Al fine di raggiungere questo obiettivo il Regolamento punta alla piena realizzazione dell'interoperabilità tra gli stati membri dei sistemi essenziali quali l'identificazione

elettronica, documenti elettronici, firme e servizi di recapito elettronici.
L'interoperabilità fa sì che le barriere elettroniche, ad oggi esistenti tra gli stati membri, vengano meno e i cittadini possano fruire dei servizi non più nel ristretto ambito nazionale ma nel più ampio contesto del mercato europeo, beneficiando dei suoi vantaggi. Tuttavia, il regolamento non intende intervenire nella scelta dei sistemi elettronici a cui affidare la gestione dell'identità digitale, che resta una scelta discrezionale dei singoli stati, ma si preoccupa di garantire che i sistemi di identificazione siano riconosciuti in tutti gli stati membri e che l'identificazione avvenga in modo sicuro.
Perciò, al fine di garantire l'interoperabilità e il riconoscimento dei sistemi identificativi, è stato previsto un regime di notificazione tra gli stati membri dei sistemi identificativi per i servizi *online*. Da qui la necessità ravvisata nelle considerazioni che accompagnano il Regolamento, di istituire un quadro giuridico comune per l'impiego dei servizi fiduciari e dei prestatori di tali servizi.
Evidente come le regole dell'*eIDAS* abbiano impattato sulla normativa italiana primaria e tecnica, in particolar modo sul Codice dell'amministrazione digitale, in merito a vari argomenti. Si comincia con le definizioni, per poi proseguire con i certificatori qualificati e non, le tipologie delle sottoscrizioni informatiche e dei certificati qualificati (che diventano tre: firma elettronica, sigillo elettronico e autenticazione web).
In questi settori poi cambiano le regole per l'accreditamento dei certificatori con la scomparsa del termine accreditamento e la nascita del termine "qualifica" e l'ampliamento della figura del prestatore di servizi di certificazione a quella di "prestatore di servizi fiduciari". Quindi il certificatore accreditato per la firma qualificata diventa un prestatore di servizi fiduciari qualificato per la sottoscrizione elettronica.
Altri servizi fiduciari sono possibili. Tra questi, a puro titolo descrittivo, da citare i servizi di recapito certificato (una sorta di Posta Elettronica Certificata) e quelli di conservazione delle sottoscrizioni (questo servizio ha lo scopo di assicurare la verifica delle sottoscrizioni elettroniche per un lungo periodo di tempo, mentre nell'ordinamento italiano la conservazione digitale è relativa all'intero documento).
Lo spettro di novità che introduce il Regolamento *eIDAS* è ampio; inoltre la natura regolamentare europea di *eIDAS* ne fa una norma di rango superiore a quello nazionale. Ciò ha imposto al Legislatore nazionale il coordinamento tra il Regolamento stesso e il Codice dell'amministrazione digitale.
Ed infatti la legge di riforma della pubblica amministrazione (l. n. 124/2015), la cosiddetta "Legge Madia", con l'art. 1 ha delegato il Governo ad emanare entro dodici mesi norme di modifica del Codice dell'Amministrazione Digitale volte a: "garantire ai cittadini e alle imprese il diritto di accedere a tutti i dati, i documenti e i servizi di loro interesse in modalità digitale" e "la semplificazione nell'accesso ai servizi alla persona, riducendo la necessità dell'accesso fisico agli uffici pubblici".
La delega, tra i principi e criteri direttivi cui deve attenersi il legislatore delegato, individua in particolare quello di "adeguare l'ordinamento alla disciplina europea in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroni-

che (regolamento *eIDAS*)" [14]. A tal fine, il Governo è stato delegato ad attuare una nuova riforma del Codice dell'amministrazione digitale, di cui al d.lgs. Decreto Legislativo 7 marzo 2005, n. 82 (di seguito CAD), il quale aveva già subito negli ultimi dieci anni vari interventi di modifica [15].

In attuazione della delega è stato adottato il d.lgs. 26 agosto 2016, n. 179, pubblicato in G.U. il 13 settembre 2016, ed entrato in vigore il giorno successivo. Esso ha apportato ulteriori rilevanti modifiche al CAD, che hanno inciso sulla maggior parte degli articoli del codice, abrogandone una trentina e rinviando in gran parte all'adozione di norme tecniche, realizzando una imponente opera di semplificazione e razionalizzazione della disciplina.

Si è così inteso superare le criticità emerse nella effettiva attuazione delle precedenti

---

[14] Di seguito sono riportati sinteticamente i criteri direttivi: a) la definizione di livelli minimi di qualità, sicurezza, accessibilità e tempestività dei servizi in modalità digitale, con sanzioni per le amministrazioni inadempienti; b) la ridefinizione e semplificazione dei procedimenti amministrativi, in relazione alle esigenze di celerità, certezza dei tempi e trasparenza nei confronti dei cittadini e delle imprese, mediante una disciplina basata sulla loro digitalizzazione e per la piena realizzazione del principio «innanzitutto digitale» (digital first), nonché dell'organizzazione e delle procedure interne a ciascuna amministrazione; c) garantire, in linea con gli obiettivi dell'Agenda digitale europea, la disponibilità di connettività a banda larga e ultralarga e l'accesso alla rete internet presso gli uffici pubblici; l'accesso e il riuso gratuiti di tutte le informazioni prodotte e detenute dalle amministrazioni pubbliche in formato aperto, l'alfabetizzazione digitale, la partecipazione con modalità telematiche ai processi decisionali delle istituzioni pubbliche, la piena disponibilità dei sistemi di pagamento elettronico nonché la riduzione del divario digitale; d) ridefinire il Sistema pubblico di connettività favorendo l'adesione al Sistema da parte dei privati e garantendo la sicurezza e la resilienza dei sistemi; e) definire i criteri di digitalizzazione del processo di misurazione e valutazione della performance per permettere un coordinamento a livello nazionale; f) coordinare e razionalizzare le vigenti disposizioni di legge in materia di strumenti di identificazione e la relativa normativa di attuazione in materia di SPID; g) favorire l'elezione di un domicilio digitale da parte di cittadini e imprese ai fini dell'interazione con le amministrazioni; h) promuovere un miglior accesso on-line ai servizi per la maternità e la genitorialità; i) razionalizzare gli strumenti di coordinamento e collaborazione delle amministrazioni pubbliche al fine di conseguire obiettivi di ottimizzazione della spesa nei processi di digitalizzazione, favorendo l'uso di software open source; l)razionalizzare i meccanismi e delle strutture di Governance in materia di digitalizzazione; m) semplificare le modalità di adozione delle regole tecniche e lo stesso CAD in modo che contenga esclusivamente princìpi di carattere generale; o) garantire la coerenza giuridica, logica e sistematica della normativa e adeguare, aggiornare e semplificare il linguaggio normativo; p) adeguare l'ordinamento alla disciplina europea in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche (regolamento *eIDAS*); q) prevedere che i pagamenti digitali ed elettronici costituiscano il mezzo principale per i pagamenti dovuti nei confronti della pubblica amministrazione e degli esercenti servizi di pubblica utilità; r) indicare esplicitamente le norme abrogate.

[15] Va infatti ricordato che già il decreto legislativo 30 dicembre 2010, n. 235 (in attuazione di delega recata dalla legge n. 69 del 2009) ha operato una complessiva rivisitazione del codice, al fine di ampliare il novero delle amministrazioni impegnate nella digitalizzazione e conferire maggiore vincolatività ad alcune disposizioni, circa ad esempio le comunicazioni sia all'interno delle amministrazioni nella gestione dei procedimenti amministrativi sia tra queste e i cittadini (a tal fine rivedendo, tra l'altro, le disposizioni in materia di firma digitale, documento informatico, servizi di pagamento). Successivamente, il codice è stato oggetto di ulteriori modifiche ad opera di vari provvedimenti intersettoriali, tra i quali si segnalano, per l'ampiezza delle modifiche apportate, i decreti-legge n. 201 del 2011 (articolo 29-bis) e n. 5 (articoli 6-ter, 47-quinquies e 47-sexies) e n. 179 del 2012 (articoli. 2, 4, 5, 6,9, 9-bis e 15), aventi ad oggetto l'utilizzo di programmi informatici open source, l'introduzione del cd. domicilio digitale, la possibilità di effettuare pagamenti con modalità informatiche, ecc.

riforme e affrontare i nodi delle inefficienze e lentezze del processo di digitalizzazione della amministrazione (e della società) italiana, al fine di rendere effettive e cogenti le misure e gli interventi già da tempo progettati e avviati e vincere le resistenze delle amministrazioni [16].

Venendo adesso agli aspetti sostanziali che la "rivoluzione" *eIDAS* ha introdotto nel nostro ordinamento, si nota come gli ambiti comuni di intervento del Regolamento e del CAD riguardano principalmente tre aree: *SPID*, firme elettroniche e marche temporali. Ciò al fine di garantire maggior validità ed efficacia ai documenti informatici anche privi di firma elettronica ed allo stesso tempo di rafforzare l'efficacia delle firme elettroniche diverse da quella digitale [17].

L'art. 1 comma 1 lett. n-*ter*, nel definire il domicilio digitale come l'indirizzo di posta elettronica certificata o altro servizio elettronico di recapito certificato, rimanda al regolamento *eIDAS* al fine di individuare gli altri servizi elettronici, diversi dalla posta certificata idonei ad essere utilizzati come domicilio digitale.

Le tecniche e i protocolli su cui si basa il Sistema Pubblico per la gestione dell'Identità Digitale sono stati già oggetto di sperimentazione a livello europeo, perciò l'AGid dovrà quanto prima provvedere a comunicare alla Commissione Europea il sistema *SPID*, affinché tale mezzo di identificazione elettronica sia riconosciuto a livello europeo dagli stati membri.

L'ammissione alla notifica del sistema *SPID*, ai sensi dell'art. 9 del regolamento, è possibile solo se il sistema implementato rispetti i requisiti fissati dall'art. 7. In particolare, lo *SPID* deve essere rilasciato dallo stato membro notificante ovvero per conto dello stato membro, deve essere utilizzato da almeno un organismo di diritto pubblico per l'erogazione di un servizio che richieda l'identificazione dell'utente. Inoltre l'attribuzione dell'identità elettronica alle persone fisiche e giuridiche nonché le modalità di autenticazione devono avvenire nel rispetto degli standard fissati nell'atto di esecuzione previsto dall'art. 8 par. 3 del Regolamento.

Altro importante rinvio al regolamento *eIDAS*, è contenuto all'art. 1 comma 1-*bis*. Si tratta di un rinvio integrale all'art. 3 del regolamento, rubricato "Definizioni", e all'interno del quale sono contenute, tra le altre, le definizioni di firma elettronica, sigillo elettronico e validazione temporale elettronica.

Il regolamento *eIDAS* individua e disciplina tre diversi tipi di firme elettroniche: la firma elettronica, la firma elettronica qualificata (FEQ) e la firma elettronica avanzata (FEA).

---

[16] M.L.MADDALENA, *op.cit.* pag. 18, che richiama F. COSTANTINO, *L'uso della telematica nella pubblica amministrazione,* in *L'azione amministrativa. Saggi sul procedimento amministrativo,*AA. VV, Giappichelli, 2016, pag. 24, secondo la quale la principale problematica che si è da sempre riscontrata in relazione a tutta la legislazione in materia informatica è la sua scarsa precettività, dovuta sia alla esistenza di oggettivi profili problematici di natura tecnica o economica, sia alla scarsa efficacia degli strumenti di controllo e sanzione, anche tenuto conto della pluralità dei soggetti pubblici coinvolti e delle inevitabili difficoltà di coordinamento.

[17] Si veda sul punto la relazione illustrativa allo schema di decreto http://www.governo.it/sites/governo.it/files/2_Rel_illustrativa_dlgs_modifica_CAD.pdf

La "firma elettronica" è definita, al n. 10 dell'art. 3, come l'insieme di dati in forma elettronica connessi, tramite associazione logica, ad altri dati elettronici utilizzati dal firmatario per firmare. Definisce a questo punto la "firma elettronica avanzata" come un firma connessa unicamente al firmatario, che sia in grado di identificarlo, e che egli può utilizzare i modo esclusivo, garantendo un elevato grado di sicurezza. Tale firma è inoltre collegata, direttamente nella sua formulazione, ai dati contenuto nel documento informatico su cui è apposta, in modo da consentire l'identificazione di ogni modifica che il documento informatico sottoscritto subisce.
La "firma elettronica qualificata" è invece una tipologia di firma elettronica avanzata, creata da dispositivi dedicati (*hardware* o *software*) che utilizzano certificati qualificati per firme elettroniche. Il certificato non è altro che un attestato, sempre in formato elettronico, rilasciato da un prestatore di servizi fiduciari, che, secondo quanto previsto dall'Allegato I del regolamento, possiede le seguenti caratteristiche: i dati univoci d'identificazione del prestatore di servizi e l'indicazione dello Stato membro in cui è stabilito; il nome della persona fisica o i dati identificativi della persona giuridica; i dati di convalida della firma elettronica che devono corrispondere ai dati di creazione della firma; l'indicazione del periodo di validità del certificato, con l'indicazione ella data di inizio e fine; codice di identità del certificato; la firma del elettronica avanzata o il sigillo elettronico del prestatore di servizi qualificato che rilascia il certificato; il luogo in cui il certificato della firma elettronica o del sigillo elettronico del prestatore di servizi qualificato è disponibile gratuitamente; il luogo in cui si trovano i servizi cui il titolare della firma può rivolgersi per avere informazioni sulla validità del certificato qualificato, indicando espressamente l'ipotesi in cui tali servizi siano allocati su un dispositivo per la creazione di una firma elettronica qualificata, che altro non è che un software o un hardware utilizzato per creare la firma elettronica.
Rispetto alla firma elettronica semplice ed a quella avanzata, la FEQ si basa su un certificato che, in considerazione delle sue caratteristiche, garantisce un maggiore livello di identificabilità del firmatario e di sicurezza.
In materia di firma elettronica, il nuovo Codice dell'Amministrazione Digitale, da un lato, recepisce per rinvio espresso le definizioni di firma digitale contenute nell'art. 3 del Regolamento *eIDAS*, e quindi le relative distinzioni; dall'altro, con l'art. 24, introduce la definizione di firma digitale. Tale definizione, tutta italiana, nel suo contenuto mutua diversi aspetti propri della firma elettronica avanzata e qualificata, come definite nel regolamento *eIDAS* attuando di fatto il principio di neutralità tecnologica, auspicato dallo stesso regolamento nel considerando 27.
Nel nuovo C.A.D. convivono, quindi, le diverse definizioni di firma elettronica del regolamento e la definizione di firma digitale.
Il regolamento *eIDAS*, parla poi di "validazione temporale elettronica" come di uno strumento che permette di collegare il documento elettronico ad un'ora e una data certa in modo che si possa provare la data e l'ora in cui i documenti sono stati creati e quindi esistevano.
Anche per la validazione temporale elettronica, il Regolamento ha previsto una

forma “qualificata” che garantisce un livello di sicurezza maggiore, poiché assicura che dopo l’apposizione della validazione non siano intervenute modifiche sul documento.
Il nuovo C.A.D., all’art. 20 comma 3, disciplina la validazione temporale del documento informatico, attribuendogli l’efficacia dell’opponibilità a terzi se apposta sul documento in conformità con le regole tecniche sulla validazione temporale.
Firme elettroniche qualificate e marche temporali qualificate devono essere rilasciate da prestatori di servizi fiduciari qualificati (*Trust Service Providers – TSP*).
Tali soggetti sono accreditati presso organismi di accreditamento riconosciuti dagli stati membri (in Italia Accredia) e in possesso di una valutazione di conformità (*Conformity Assessment Report*), in assenza della quale tali servizi non possono essere considerati qualificati.
Altra importante novità del Regolamento è il “sigillo elettronico” che, a differenza della firma elettronica, risponde all’esigenza di garantire l’integrità e l’origine dei dati cui è collegato. Il sigillo elettronico è una combinazione di dati in forma elettronica connessi con con i dati elettronici del documento di cui si vuole garantire l’origine o l’integrità.
Anche per il sigillo elettronico il regolamento distingue tra il sigillo elettronico, sigillo elettronico qualificato e avanzato. Il sigillo elettronico “qualificato”, come la FEQ, è caratterizzato dal collegamento ad un certificato elettronico qualificato e dal fatto che viene creato da un software o un hardware dedicato. Come per quello la firma elettronica qualificata, anche il certificato elettronico del sigillo qualificato deve avere i requisiti di cui all’Allegato I del Regolamento. Il sigillo elettronico “avanzato” invece si caratterizza per la maggiore identificabilità del soggetto che lo appone, rispetto a quello semplice, e perché, essendo connesso univocamente con tale soggetto, ne permette l’identificazione. È creato con dati che sono unicamente nella disponibilità del creatore del sigillo e permette di individuare le modifiche che il documento informatico su cui è apposto subisce.

4. *(segue)* l’identità digitale come *diritto* di cittadinanza digitale.

La prima stesura del Codice dell’Amministrazione Digitale, D.lgs. 7 marzo 2005 n. 82, evidenziava già l’intenzione del legislatore di creare una vera e propria Carta dei diritti e dei doveri della digitalizzazione dell’amministrazione, grazie alla quale cittadini e imprese divenivano titolari del diritto all’uso delle tecnologie nei loro rapporti con l’amministrazione, laddove queste ultime erano soggette ad un dovere di digitalizzazione nei rapporti interni e con gli utenti. Tuttavia il processo di digitalizzazione della pubblica amministrazione non è mai arrivato alla piena realizzazione, probabilmente anche a causa della mancanza di obblighi stringenti all’interno della

legge che spingessero l'avanzamento della rivoluzione digitale.
Le successive modifiche al codice hanno sempre tenuto presente gli obiettivi chiave del processo di digitalizzazione, nel tentativo di rendere effettiva la disciplina del CAD, fino ad arrivare all'ultima modifica, voluta dalla riforma Madia e attuata dal d.lgs. n. 179/2016, attraverso la quale il nuovo codice dell'amministrazione digitale riceve gli *input* per l'attuazione della rivoluzione digitale, attraverso obiettivi e principi chiave volti a garantire un livello minimo di sicurezza, fruibilità, qualità e accessibilità dei servizi online erogati dalle P.A.
Obiettivi questi più raggiungibili, laddove, all'art. 14, è previsto un sistema di premi e sanzioni per le Amministrazioni, specie in termini di responsabilità dirigenziale; nonché l'applicazione del principio della competenza statale nella determinazione degli standard di qualità dei servizi che riguardano i diritti civili e sociali, estendendo gli obblighi di digitalizzazione anche alle amministrazioni regionali. Tra questi, il diritto di accesso digitale dei cittadini e delle imprese a dati, documenti e servizi di loro interesse e la semplificazione dell'accesso ai servizi della persona, attraverso l'utilizzo delle nuove tecnologie, sono quelli che direttamente attengono alla semplificazione del rapporto tra cittadini e PA.
L'attuazione di tali principi è stata, ancora una volta, demandata al nuovo Codice dell'Amministrazione Digitale, ma con un'importantissima novità: l'identità digitale come *diritto* di cittadinanza digitale. L'art. 3 del CAD, rubricato "Diritto all'uso delle tecnologie", infatti sancisce il diritto di tutti a fruire delle soluzioni e degli strumenti, messi a disposizione dal Codice, nei rapporti con le Pubbliche Amministrazioni e con le società a controllo pubblico, prevedendo che cittadini ed imprese vantino un vero e proprio diritto ad un'identità digitale attraverso cui essere identificati, e grazie alla quale accedere ed utilizzare i servizi erogati dalle PA (art. 3, comma 1 *quinquies* del CAD, introdotto dal d.lgs. 179/2016).
L'aver elevato al rango di diritto l'uso delle tecnologie, fa si che esso possa trovare tutela giurisdizionale dinanzi al giudice amministrativo, come previsto dall'art. 3 comma 1-*ter*, e rappresenta un passo avanti nella direzione di una reale e totale attuazione del Codice dell'Amministrazione Digitale in vista della creazione di nuovi servizi digitali, erogati dalle amministrazioni, tesi ad attuare compiutamente lo sviluppo dell'*e-Government*.
Nell'ottica, dunque, di rendere effettiva la realizzazione della c.d. "cittadinanza digitale", e di rendere disponibile per tutti un'identità digitale, l'art. 1 della legge Madia, alla lettera *f*, rileva la necessità di armonizzare le disposizioni in materia di strumenti d'identificazione, comunicazione e autenticazione attraverso lo *SPID* (Sistema Pubblico d'Identità Digitale). Si tratta di un sistema aperto che permette agli utenti di accedere, con un'unica identità digitale (un unico PIN e di un unico punto telematico di accesso "Italia Login"), ai servizi *online* della PA e dei privati aderenti, previo accreditamento da parte dell'AGID; e che dovrà gradualmente sostituire gli strumenti della carta nazionale di servizi e della carta di identità elettronica, i quali per la verità non hanno avuto grande diffusione. Lo SPID è già interoperativo con altri sistemi d'identità digitale europei, dato che aderisce allo standard UE *eIDAS* e

al momento attuale è già attivo e funzionante in numerose amministrazioni (Agenzia dell'entrante, INPS, ecc.) [18].

Il nuovo art. 64 del CAD, nel disciplinare lo *SPID*, affida la definizione delle sue caratteristiche ad un nuovo Decreto del Presidente del Consiglio dei Ministri, ancora da emanarsi, lasciando in capo all'Agenzia per l'Italia Digitale il compito di programmarne e curarne l'implementazione.

I soggetti partecipanti allo *SPID* sono innanzitutto i gestori dell'identità digitale, le Amministrazioni fornitrici di servizi, gli utenti e l'AgID. I soggetti prestatori di servizi fiduciari qualificati, di posta elettronica certificata e dell'identità digitale devono conformarsi alle previsioni del regolamento *eIDAS* e devono altresì avere i requisiti fissati dal CAD riguardo alla forma giuridica e al capitale sociale (art. 29).

Gli utenti sono dotati di un'identità digitale che, secondo la definizione dell'art. 1 del CAD, è la rappresentazione informatica del rapporto di corrispondenza tra un utente e i suoi dati identificativi, verificata alla luce di quanto previsto dalle regole tecniche. Grazie all'identità digitale è possibile l'accesso virtuale dell'utente ai servizi della PA, ed è reale la possibilità di porre in essere validamente un atto giuridico all'interno di un sistema informatico. Affinché ciò avvenga correttamente è necessario che il sistema informatico presenti le caratteristiche fissate dalle regole tecniche e che il procedimento, con cui l'atto viene posto in essere, permetta di garantire in modo inequivoco l'acquisizione della volontà dell'utente.

A proposito di accessibilità dei servizi in rete, l'art. 65 del CAD, in materia di istanze e dichiarazioni presentate per via telematica alle Pubbliche Amministrazioni, espressamente prevede la possibilità di presentarle online, sancendone la validità quando l'istante o il dichiarante è identificato attraverso lo *SPID*.

Il legislatore delegato, in attuazione dell'Agenda digitale europea, ha previsto ulteriori ed importanti interventi, in realtà già progettati da tempo e in parte anche attuati, volti: alla promozione della diffusione del domicilio digitale delle persone fisiche (che rimane tuttavia facoltativo), al fine di facilitare le comunicazioni con le pubbliche amministrazioni (art. 3-*bis* CAD, come modificato dal d.lgs. 179/2016), al quale si connette la speculare previsione del "diritto di inviare comunicazioni e documenti alle pubbliche amministrazioni e di riceverne dalle stesse tramite un domicilio digitale" (art. 3, comma 1 *quinquies*, CAD introdotto dal d.lgs. 179/2016); nonché alla costruzione di un'Anagrafe nazionale della popolazione residente (ANPR), che prenderà il posto delle oltre 8.000 anagrafi dei comuni italiani, costituendo un'unica banca dati con le informazioni anagrafiche della popolazione residente.

---

[18] L'introduzione del Sistema Pubblico d'Identità Digitale risale al decreto legge 21 giugno 2013 n. 69, convertito con modificazioni dalla legge 9 agosto 2013 n. 69. In particolare, l'art. 17 ter, modificando l'art. 64 del CAD, introduceva uno strumento per la diffusione dei servizi in rete e l'accesso alla PA digitale da parte di cittadini ed imprese. Le caratteristiche dello *SPID*, al momento della sua introduzione nel CAD erano definite dal D.P.C.M. 24 ottobre 2014, recante "*Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi ed elle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese*".

Già l'art. 1 comma 1 lettera *g*), della legge contenente le deleghe al governo per la riorganizzazione della pubblica amministrazione, nell'ottica di semplificare l'accesso ai servizi della persona e garantire il diritto di accesso dei cittadini e delle imprese ai dati e ai documenti di loro interesse, indica come principio cui deve tendere la riforma del CAD, quello di favorire l'elezione di un domicilio digitale, di cui si possa garantire l'utilizzo anche in caso di mancanza di strutture digitali idonee o in presenza di uno scarso grado di alfabetizzazione digitale e altre barriere all'accesso.
In attuazione di tali principi della legge delega il nuovo Codice dell'Amministrazione Digitale prevede che ciascun cittadino abbia un domicilio digitale presso il quale ricevere le comunicazioni da parte della Pubblica Amministrazione e dei gestori o esercenti pubblici servizi. L'art. 3-*bis*, prevede che il domicilio digitale sia messo a disposizione degli iscritti all'Anagrafe della popolazione residente (ANPR), anche per tutti gli iscritti all'ANPR che non ne hanno fatto richiesta, nell'ottica di diffonderne l'utilizzo su larga scala.
Il registro viene aggiornato in seguito alla comunicazione, fatta da ciascun cittadino al comune di residenza, del proprio domicilio digitale che, a questo punto, costituisce il mezzo esclusivo di comunicazione con le pubbliche amministrazioni, anche per le comunicazioni effettuate ai sensi dell'art. 21-*bis* della legge n. 241/1990, relative a provvedimenti limitativi della sfera giuridica dei privati.
Le Pubbliche Amministrazioni potranno tuttavia continuare ad utilizzare i mezzi ordinari della posta e della raccomandata per inviare le comunicazioni, anche quando esse siano redatte in originale come documenti informatici sottoscritti con firma digitale o elettronica. Di tali documenti, che saranno conservati negli archivi digitali, verrà spedita eventualmente una copia analogica dell'originale digitale. La spedizione della copia analogica a mezzo posta non pregiudica l'osservanza degli obblighi di conservazione e di esibizione previsti dalla legislazione vigente. Il comma 4-*ter* dell'art. 3-*bis*, precisa infatti che essi si considerano rispettati quando la copia analogica del documento informatico riporta una dicitura che specifichi che l'originale informatico da cui è tratta la copia analogica è conservato presso la PA in rispetto delle regole tecniche di cui all'art. 71. Il valore della copia analogica del documento informatico formata secondo le modalità appena enunciate è riconosciuta sempre tranne quando si tratti di documenti che costituiscono certificazioni rilasciate dall'amministrazione che devono essere utilizzate nei rapporti tra privati.
Tuttavia, per la compiuta attuazione delle regole sul domicilio digitale è necessario che venga istituita ed implementata l'Anagrafe Nazionale della Popolazione Residente. L'ANPR, istituita presso il Ministero dell'Interno, è stata concepita come un organismo che subentra all'anagrafe della popolazione residente (APR) e l'anagrafe degli italiani residenti all'estero (AIRE) tenute dai comuni, e in essa confluisce l'archivio informatizzato dei registri dello stato civile. Nonostante ciò determini un accentramento delle informazioni in capo all'ANPR, esse restano comunque nella disponibilità dei comuni per lo svolgimento delle funzioni di competenza del Sindaco e sono accessibili alle Pubbliche Amministrazioni e agli organismi che gestiscono pubblici servizi.

Inoltre, concorre ad assicurare un determinato grado di certezza nell'utilizzo del domicilio digitale e della PEC, la previsione di un unico registro degli indirizzi di posta elettronica certificata, l'indice INI-PEC (Indice nazionale degli indirizzi di posta elettronica certificata di professionisti e imprese), istituito presso il Ministero dello Sviluppo Economico, che costituisce l'unico mezzo di comunicazione tra professionisti e imprese e con le pubbliche amministrazioni [19].
Analogamente è previsto, dall'art. 6-*ter* del CAD, un pubblico elenco di fiducia, denominato "Indice degli indirizzi della pubblica amministrazione e dei gestori di pubblici servizi", nel quale sono indicati gli indirizzi di posta elettronica certificata da utilizzare per le comunicazioni, lo scambio di informazioni e per l'invio di documenti alla P.A.
L'indice è realizzato e gestito dall'AgID e le amministrazioni si preoccupano di aggiornarne le informazioni con cadenza almeno semestrale, secondo le modalità previste dall'AgID. Per le pubbliche amministrazioni, tuttavia, continua a sopravvivere l'Elenco di indirizzi PEC delle P.A., presso il Ministero della Giustizia, ai sensi dell'art. 16 comma 12 del d.l. n. 179/2012.
La coesistenza dei due registri è dovuta al fatto che con il d.l. 179/2016 non si è provveduto all'abrogazione di quest'ultimo registro. Pertanto, i registri contenenti gli indirizzi PEC delle P.A., saranno due, pur avendo entrambi lo stesso valore ai fini della notifica e della comunicazione degli atti in materia civile penale, amministrativa e stragiudiziale. Di questi, solo quello istituito con il nuovo CAD è pubblico, a differenza di quello istituito presso il Ministero della Giustizia che è accessibile esclusivamente dagli uffici giudiziari, uffici notificazioni, esecuzioni e protesti e dagli avvocati.

5. La Direttiva 2015/2366 UE (PSD2) ed il Regolamento UE n. 751/2015 quali normative evolutive per l'*e-Payment* pubblico.

Le continue innovazioni del mercato europeo sul fronte della diffusione delle carte di credito e debito, nonché degli altri strumenti di pagamento elettronici su piattaforme digitali e mobili, hanno evidenziato una carenza di disciplina di livello europeo nel settore dei pagamenti ed una conseguente esigenza di una regolazione unitaria in materia, tale da armonizzare la disomogenità disciplinare tra i singoli stati membri.
Proprio al fine di colmare tale lacuna normativa viene adottata la direttiva 2015/2366/

[19] L' INI-PEC è pubblico e accessibile dal web senza necessità, per gli utenti, di autenticarsi. È realizzato a partire dagli indirizzi pec già indicati nei registri delle imprese o in possesso degli ordini e dei collegi professionali ed è completato con le informazioni circa le identità digitali di imprese e professionisti.

(UE) sui servizi di pagamento nel mercato interno (cd. PSD2) Direttiva PSD2, entrata in vigore il 13 gennaio 2016 e da recepire dagli stati membri entro il 13 gennaio 2018. La direttiva mira a promuovere lo sviluppo di un mercato interno dei pagamenti al dettaglio efficiente, sicuro e competitivo rafforzando la tutela degli utenti dei servizi di pagamento, sostenendo l'innovazione e aumentando il livello di sicurezza dei servizi di pagamento elettronici. Lo scopo che si prefigge è quello di introdurre condizioni di parità e chiarezza giuridica tra gli stati membri, sia nei rapporti con gli operatori del mercato che con gli utenti-consumatori, al fine di apporre un contributo significativo allo sviluppo del mercato europeo.
La direttiva PSD2, che si inserisce nel solco già tracciato dalla prima direttiva UE in materia di pagamenti (cd. PCD[20]), estende il suo ambito di applicazione a tutte le operazioni di pagamento interne all'Unione Europea, incluse quelle verso paesi terzi quando almeno uno dei prestatori di servizi di pagamento coinvolti ha sede dell'Unione. L'obiettivo è quello di permettere ai consumatori, che già utilizzano sistemi di "*banking online*", di utilizzare tale modalità e dispositivi per effettuare qualsiasi tipo di pagamento.
Altro aspetto interessato dalla direttiva PSD2 riguarda la riduzione del c.d."*Surcharge*", ossia dei costi ulteriori a carico degli utenti dei servizi di pagamento, derivanti dalle transazioni effettuate attraverso carte di credito, debito o prepagate.
A tal riguardo la direttiva mira ad un'armonizzazione con il Regolamento UE n. 751/2015, c.d. *MIF*, che individua i massimali uniformi delle commissioni interbancarie sulle transazioni di pagamento, fissando delle percentuali standard, denominate *MIF* (Multilateral Intercharge Fees), da applicarsi in tutto il territorio dell'UE [21]. A

---

[20] La direttiva europea sui servizi di pagamento (Direttiva 2007/64/Ce), anche nota come Psd - Payment services directive, si prefiggeva lo scopo di definire un quadro giuridico comunitario moderno e coerente per i servizi di pagamento elettronici. Più in dettaglio, la Psd risponde ai seguenti obiettivi: regolamentare l'accesso al mercato per favorire la concorrenza nella prestazione dei servizi; garantire maggiore tutela degli utenti e maggiore trasparenza;standardizzare i diritti e gli obblighi nella prestazione e nell'utilizzo dei servizi di pagamento per porre le basi giuridiche per la realizzazione dell'Area unica dei pagamenti in euro (Sepa); stimolare l'utilizzo di strumenti elettronici e innovativi di pagamento per ridurre il costo di inefficienti strumenti quali quelli cartacei e il contante. La Psd è stata recepita nell'ordinamento nazionale con il D.lgs n.11 del 27 gennaio 2010, entrato in vigore il 1° marzo 2010.

[21] Il Regolamento (UE) 2015/751 del 29 aprile 2015, è stato pubblicato sull'Official Journal (la Gazzetta Ufficiale dell'Unione Europea) il 19 maggio 2015. Il nuovo testo entrato in vigore il ventesimo giorno successivo alla pubblicazione (ossia a decorrere dall'8 giugno 2015) stabilisce requisiti tecnici e commerciali uniformi per le operazioni di pagamento basate su carta eseguite nell'Unione Europea, quando sia il prestatore di servizi di pagamento del pagatore (ossia l'Issuer che ha emesso la carta con cui l'acquirente consumatore effettua il pagamento) sia il prestatore di servizi di pagamento del beneficiario (ossia l'Acquirer che ha convenzionato l'esercente per accettare le carte) sono situati nell'Unione. Con "operazioni di pagamento basate su carta" si intende qualsiasi transazione a valere su carta (ossia basata sull'infrastruttura e le regole commerciali di uno schema di carte di pagamento), effettuata sia in presenza del titolare (come è il caso tradizionale di una transazione che si compie presso un esercizio commerciale fisico, tramite POS) si in absentia, per esempio in un contesto e-Commerce o m-Commerce, prescindendo dalla tecnologia di supporto o adozione. In tal senso, rientrano nell'ambito di applicazione anche quei pagamenti che sono eseguiti mediante l'impiego di Mobile Wallet e Digital Wallet, a patto che il risultato sia un'operazione di pagamento

tal riguardo, la ridefnizione dei massimali relativi alle commissioni, che gli esercenti devono pagare alla loro banca, ha comportanto che all'interno della direttiva vengano vietate le maggiorazioni, sui pagamenti elettronici, a carico dell'utente, per tutte le carte dei circuiti soggetti alle commissioni interbancarie multilaterali regolamentate. In tal modo, da un lato, i costi delle transazioni elettroniche vengono ridotti e resi uniformi in tutto il territorio dell'UE; dall'altro, essi non possono essere addebitati in capo al soggetto che paga, favorendo così la diffusione dell'e-payment.
Evidente che sarebbe necessario prevedere che i costi di ciascuna transazione siano a carico dell'Amministrazione e non dell'utente, al fine di favorire la diffusione dell'*e-payment* anche nei confronti della Pubblica Amministrazione [22].
Proprio la direttiva europea PSD2 sui servizi di pagamento è stata la principale ispiratrice di una evoluzione in seno alla Pubblica Amministrazione che guardava all'e-payment solo come una possibilità.
A tal riguardo, in un'ottica di semplificazione e trasparenza dei pagamenti alle P.A

tramite la carta in essi registrata. Il Regolamento si applica altresì ai pagamenti effettuati con carte contact-less e a tutte le transazioni di Mobile Payment che prevedano l'impiego di una carta (Mobile Proximity Payment e Mobile Remote Payment).
In merito agli interventi, il dispositivo prevede, tra gli altri, l'applicazione di un tetto (il c.d. "Cap") alle commissioni di Interchange (le MIF) per i pagamenti con carte di credito e debito fissando nel massimo una soglia dello 0,3% per ogni transazione effettuata con carta di credito e una soglia dello 0,2% sulle transazioni abilitate tramite carte di debito. Per le operazioni nazionali tramite carta di credito, gli Stati membri possono stabilire un massimale per operazione sulle Interchange Fee anche inferiore allo 0,3%. Per le operazioni domestiche con le carte di debito (in Italia, per esempio, per le carte PagoBancomat), i singoli Stati membri possono altresì definire un massimale per operazione sulle commissioni a percentuale inferiore e possono imporre un importo massimo fisso di commissione, quale limite all'importo della commissione risultante dalla percentuale applicabile, oppure, permettere di praticare una commissione fissa di 5 centesimi, eventualmente anche in combinazione con quella variabile, purché il limite rimanga lo 0,2% e a patto che il volume di commissioni annuali così generato, non superi lo 0,2% del totale delle transazioni nazionali eseguite tramite carte di debito, all'interno di ciascuno schema. Inoltre, fino al 9 dicembre 2020, gli Stati membri possono applicare il tetto dello 0,2% calcolato come media annuale ponderata di tutte le transazioni effettuate con le carte di debito nazionali.
I limiti suddetti, non si applicano: alle operazioni tramite carte aziendali (p.e. quelle carte che vengono adottate da un'azienda per consentire ai propri dipendenti in trasferta di pagare i servizi necessari al compimento della missione stessa); ai prelievi di contante presso gli sportelli automatici (ATM); alle operazioni di pagamento con carte appartenenti a schemi "a tre parti" (trattasi di un modello che presuppone l'esistenza nei confronti dello schema di un solo soggetto nel quale collassano entrambe le funzioni di Acquirer e Issuer).
L'esenzione prevista per le carte che appartengono agli schemi "a tre parti", non si applica in tutti quei casi in cui lo schema concede ad altri prestatori di servizi di pagamento la licenza di emissione o di convenzionamento di strumenti di pagamento basati su carta, o entrambi, o emette strumenti di pagamento basati su carta con un partner di carta multimarchio in co-branding o tramite un agente; in tali circostanze, si applicano i limiti di cui sopra.
Tuttavia, fino al 9 dicembre 2018, per quanto concerne le operazioni di pagamento nazionali, un tale schema di carte di pagamento "a tre parti" può essere esentato dagli obblighi di applicazione del Cap, a condizione che le operazioni di pagamento basate su carta effettuate in uno Stato membro nell'ambito di uno schema siffatto, non superino annualmente il 3% del valore di tutte le operazioni di pagamento basate su carta effettuate nello stesso Stato membro.

[22] C. GIURDANELLA, G. CAMPO, E. GUARNACCIA, *Cittadinanza, procedimenti, e-payment: le nuove frontiere della PA digitale*, CeSDA editore, Catania 2017, pag. 84 ss.

nonché di risparmio nella spesa pubblica, è intervenuto il D.lgs. n.179/2016 modificativo dell'art. 5 del Codice dell'Amministrazione Digitale, in forza del quale i pagamenti elettronici nei confronti delle pubbliche amministrazioni *dovranno* aprirsi totalmente all'*e-payment* [23].

Il nuovo testo, a differenza della precedente formulazione che guardava all'*e-payment* solo come una possibilità [24], pone in capo alle pubbliche amministrazioni un vero e proprio obbligo di accettare i pagamenti elettronici [25].

E' lo stesso art. 5, al comma 2, ad assicurare l'operatività di tale sistema attraverso l'utilizzo di una piattaforma tecnologica dedicata all'*e-payment*, messa a disposizione dall'AgID che permette la connessione e l'interoperabilità tra P.A. e prestatori di servizi di pagamento abilitato, nonché il suo utilizzo da parte degli utenti per effettuare i pagamenti per mezzo dell'autenticazione degli utenti tramite SPID [26].

Ma la riforma del CAD in materia di pagamenti elettronici riguarda anche un ulteriore aspetto rilevante: ossia l'apertura della P.A. a ricevere i pagamenti che provengono da circuiti internazionali. Fin adesso infatti gli unici pagamenti elettronici accettati dalle Pubbliche Amministrazioni erano quelli provenienti dalle carte del circuito domestico (tipo P.O.S.), laddove invece venivano escluse tutte le carte appartenenti ai circuiti internazionali. Il D.lgs.n. 179/2016 ha aperto la possibilità affinchè tutti i circuiti di pagamento siano abilitati per i pagamenti nei confronti delle Pubbliche Amministrazioni.

6. La diffusione della connettività alla rete internet: profili critici conclusivi.

Altro nodo centrale della riforma riguarda l'esigenza di superare il *digital divide*, ossia il divario nella popolazione tra coloro che conoscono ed usano efficacemente gli strumenti informatici e coloro che ne sono tagliati fuori; per questi ultimi dovrebbero comunque essere assicurati negli uffici pubblici forme di assistenza per la fruizione dei servizi *online*.

---

[23] Art. 5, comma 1, CAD: "*I soggetti di cui all'articolo 2, comma 2,* (ossia le pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, nonché alle società a controllo pubblico, escluse le società quotate) *sono obbligati ad accettare, tramite la piattaforma di cui al comma 2, i pagamenti spettanti a qualsiasi titolo attraverso sistemi di pagamento elettronico, ivi inclusi, per i micro-pagamenti, quelli basati sull'uso del credito telefonico. Resta ferma la possibilità di accettare anche altre forme di pagamento elettronico, senza discriminazione in relazione allo schema di pagamento abilitato per ciascuna tipologia di strumento di pagamento elettronico come definita ai sensi dell'articolo 2, punti 33), 34) e 35) del regolamento UE 2015/751 del Parlamento europeo e del Consiglio del 29 aprile 2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta*."

[24] Art.5, comma1, nella versione precedente alla modifica intervenuta con il D.lgs.n. 179/2016, così prevedeva: "*i soggetti di cui all'articolo 2, co.2, e* […] *i gestori di pubblici servizi nei rapporti con l'utenza sono tenuti a far data dal 1° giugno 2013 ad accettare i pagamenti ad essi spettanti, a qualsiasi titolo dovuti, anche con l'uso delle tecnologie dell'informazione e della comunicazione…"*

[25] Sono inclusi tra gli strumenti di pagamento elettronici anche: il bonifico; l'ObeP (Online Banking ePayment) ossia un sistema di pagamento sviluppato dagli istituti bancari per permettere di effettuare pagamenti via Internet; sistemi basati sull'utilizzo del credito telefonico, per i micro-pagamenti di importo non superiori a 50 euro e comunque non superiori a 300 euro.

[26] M.BELLINI, *Pagamenti digitali, la svolta dei pagamenti arriva da Spid e dai servizi mobili*, su ForumPa.it del 16/6/2016.

Gli art. 8 e 8–*bis* del CAD prevedono il coinvolgimento dello Stato, di tutte le pubbliche amministrazioni tra cui Regioni, Province, Comuni, Università, Camere di Commercio, enti pubblici non economici, enti del Servizio Sanitario Nazionale nella promozione e gestione di iniziative volte alla c.d. alfabetizzazione informatica, soprattutto tra le categorie a rischio di esclusione, al fine di favorire la diffusione della cultura digitale [27].

L'art. 8-*bis* chiude il cerchio dell'alfabetizzazione informatica, fornendo gli strumenti affinché ciò avvenga: prevede infatti che le pubbliche amministrazioni, in linea con quanto previsto dall'Agenda digitale europea, rendano la rete internet fruibile ai cittadini, nella misura della porzione di banda non utilizzata, presso gli uffici pubblici e i luoghi pubblici, con particolare riguardo alle scuole, al settore sanitario e ai luoghi di interesse turistico attraverso il sistema di identificazione *SPID*, senza che tale previsione comporti un maggior onere di finanza pubblica dal momento che l'iniziativa trova già copertura in fondi di investimento privati e dell'Unione Europee in attuazione del Piano Banda Ultralarga.

La diffusione della connettività internet negli uffici e luoghi pubblici appare quindi la misura più importante degli ultimi interventi di riforma, poiché essa è propulsiva e strumentale alla effettività dei diritti digitali del cittadino. Tuttavia ne rappresenta il nodo critico: infatti solo assicurando l'effettivo accesso alla rete a tutti gli utenti, in forma gratuita, l'attuazione dell'*e-Government* potrà dirsi compiuta.

Dunque va sicuramente salutata con favore la previsione di cui all'art. 8-*bis* del nuovo CAD che prevede la messa a disposizione della connettività alla rete internet presso gli uffici pubblici e in altri luoghi pubblici. Tuttavia va sottolineato in senso critico che non si tratta di una disposizione avente contenuto cogente, dal momento che si afferma soltanto che le Pubblica amministrazione e gli altri soggetti cui si applica il CAD "favoriscono" la disponibilità di connettività alla rete. Inoltre, al comma 2, lo stesso art. 8-*bis* CAD subordina la messa a disposizione della connessione per gli utenti alla disponibilità di banda larga per l'accesso alla rete internet.

In conclusione, le straordinarie potenzialità della digitalizzazione dell'amministrazione, le quali sono funzionali ad un processo inclusivo dei soggetti privati (cittadini e imprese) e ad una loro sempre più stretta partecipazione alla vita della pubblica amministrazione da protagonisti, spingono verso una nuova stagione di matrice europea del *Digital Government*. Pregevoli in tal senso sono stati gli sforzi del Legislatore tesi ad assecondare tale spinta propulsiva riformando l'impianto normativo principe delle politiche di digitalizzazione nostrane. Tuttavia insolute rimangono an-

[27] L'esigenza di alfabetizzazione informatica è comprovata dai dati statistici registrati nel nostro paese che mostrano come l'Italia occupi in questo settore una posizione piuttosto bassa in classifica. Solo il 21% delle famiglie ha accesso alla connessione internet veloce, solo il 59% degli utenti usa internet abitualmente e addirittura il 31% della popolazione non lo ha mai usato. I dati relativi all'utilizzo dell'e-commerce e dei servizi online non sono migliori. Se fino ad ora l'informatizzazione delle Amministrazioni Locali si è attestata ad un livello piuttosto basso e non in linea con gli obiettivi dell'Agenda Digitale Europea ed Italiana, con il nuovo Codice dell'Amministrazione Digitale si vuole dare una spinta a questo processo che sembra essersi arenato.

cora diverse questioni che potrebbero neutralizzare i vantaggi in termini di efficienza, rapidità, economicità dei processi di digitalizzazione dell'agire amministrativo; nonché inattuare le innegabili potenzialità legate alla diffusione e pubblicazione dei dati delle amministrazioni in termini di trasparenza, partecipazione e di volano per lo sviluppo economico.

Particolarmente delicato rimane il problema della sicurezza. Non solo per i rischi di blocco di funzionalità dei sistemi informatici (*crash down*), che potrebbero pregiudicare la continuità dell'attività istituzionale della pubblica amministrazione laddove non vi fossero efficaci piani di rispristino dell'operatività dei sistemi (*disaster recovey*); ma per l'inevitabile dipendenza - che si viene a realizzare - della pubblica amministrazione da soggetti terzi (spesso multinazionali), proprietari e gestori delle tecnologie informatiche, e lo stoccaggio dei dati, soprattutto in caso di uso di tecnologie di *clouds computing*.

Irrisolta ancora è la questione della diffusione dei dati della pubblica amministrazione (c.d. *Open data*) che pone ulteriori interrogativi in relazione al rischio di una asimmetria di posizioni tra privati (non tenuti a pubblicizzare i propri dati) e pubbliche amministrazioni, con possibili ripercussioni sulla tutela dell'interesse pubblico a fronte dell'interesse di grandi gruppi economici privati. Anche sotto questo profilo potrebbero ravvisarsi rischi per la sicurezza e la privacy posto che i dati della pubblica amministrazione, una volta resi accessibili all'esterno incondizionatamente (anche al di fuori dei confini nazionali), potrebbero essere oggetto di analisi e di elaborazioni da parte di soggetti terzi per finalità non controllabili dalla pubblica amministrazione.

Ed infine non dissolti rimangono i già richiamati nodi del divario digitale e delle difficoltà di connessione alla rete internet tuttora presenti che si tradurrebbero in una "esclusione" di intere fasce della popolazione dai servizi pubblici erogati *online*, qualora non venissero adeguatamente colmati.

Rivista elettronica di Diritto, Economia, Management

N. 1 - 2017 · pp. 219-226

La Robotica in sanità. Autonomia, responsabilità e opportunità.

Giovanni Maglio

Abstract: la crescente disponibilità di robot e lo sviluppo dell'Intelligenza Artificiale possono essere strumenti di grande impiego in sanità, ma occorre fare attenzione ai potenziali rischi ed alle conseguenti responsabilità che ne derivano e che gli odierni strumenti giuridici non sono ancora in grado di affrontare in maniera adeguata.
The increasing availability of robots and the development of Artificial Intelligence can be a powerful tool in healthcare, but we should pay attention to the potential risks and the resulting responsibilities that arise from it, and that today's legal instruments are not yet able to deal with it appropriate.

1. Introduzione.

L'attenzione crescente riservata dalle Istituzioni pubbliche alla, ormai, ampia ed inarrestabile diffusione dei robot, si pone nel solco di una quasi ancestrale spinta dell'uomo a regolamentare i rapporti giuridici non solo all'interno della specie umana, ma soprattutto nei confronti di tutto ciò che umano non è e che ha profondi riflessi sulle sfere giuridiche proprie degli umani, dagli esseri vegetali agli animali.
La robotica, da questo punto di vista, va ad arricchire tale elenco, aggiungendo, peraltro, la possibilità di diventare una sorta di "creatore" di altre forme di quella che, per certi aspetti, potrebbe anche considerarsi "forma di vita".
Inizialmente, la produzione di macchine chiamate robot, dalla parola ceca "*robota*"[1] (lavorare duro, lavorare forte) è stata quasi esclusivamente associata alla mera esecuzione di compiti fisici e meccanici ripetitivi, che potevano essere svolti senza particolare difficoltà oppure in ambiti ad elevato tasso di pericolosità o di precisione, quasi sempre sotto la guida di un operatore (c.d. robot industriali[2]).
Il salto di qualità che ha reso la robotica sempre più performante è, invece,

[1] Introdotta dallo scrittore ceco Karel Čapek, il quale usò per la prima volta il termine nel 1920 nel suo dramma teatrale "*I robot universali di Rossum*", come riferimento al lavoro forzato.

[2] Per ulteriori approfondimenti, si v. la definizione e classificazione dell'International Federation of Robotics, reperibile all'indirizzo internet https://ifr.org/img/office/Industrial_Robots_2016_Chapter_1_2.pdf, consultato marzo 2017.

Articolo pervenuto il 2 Maggio 2017, approvato il 1 Giugno 2017

soprattutto merito di quella che viene chiamata Intelligenza Artificiale, e che sta ormai diventando un requisito pressoché inscindibile, nel senso che ogni macchina oggi considerata robot è dotata di I.A., in una delle sue varie classificazioni[3].

2. Autonomia robotica, responsabilità e la Risoluzione del Parlamento Europeo 16.2.2017

Oggigiorno, del resto, non si può fare a meno di considerare inscindibile il connubio tra robotica ed intelligenza artificiale, se si vuole porre la base giuridica per il riconoscimento della autonomia[4] dei robot, della loro eventuale personalità robotica e, soprattutto, della responsabilità derivante dal loro uso o dai loro comportamenti.
Più un robot sarà intelligente, *rectius* dotato di una intelligenza artificiale più sofisticata, infatti, più crescerà la sua capacità di autodeterminarsi[5], in una scala ideale (che si potrebbe chiamare "scala di autonomia robotica"), fino ad arrivare al punto di attribuire una sorta di "soggettività giuridica" dello stesso se non, addirittura, di "capacità giuridica", anche ai fini di una possibile imputabilità del robot.
Alla curva di crescita dell'intelligenza artificiale robotica corrisponderà, poi, una diversa ripartizione delle responsabilità in capo ai vari soggetti coinvolti: progettista, produttore, operatore, utilizzatore-proprietario, robot, terzi (compresi altri robot).
Ovviamente, tale scala di autonomia robotica non potrà prescindere dalle caratteristiche costruttive e di funzionamento del robot, specie in relazione alle connessioni per lo scambio di dati, ai sensori e alle forme utilizzate.
Come pure non può, comunque, essere trascurato che la responsabilità dei diversi soggetti può variare anche in base al tipo di abilità e capacità di cui è dotato il robot o dell'impiego per il quale lo stesso robot è impiegato per compiti che è chiamato ad adempiere, non solo in relazione all'ambiente di riferimento (sede stradale, abitazione privata, struttura sanitaria ecc.), ma anche in base al contesto di utilizzo (persone coinvolte, minori, anziani, persone con ridotte capacità sensoriali

---

[3] Si può definire l'«intelligenza artificiale», in genere abbreviata in I.A. (oppure anche "A.I.", acronimo dell'inglese Artificial Intelligence), come l'«insieme di studi e tecniche che tendono alla realizzazione di macchine, specialmente calcolatori elettronici, in grado di risolvere problemi e di riprodurre attività proprie dell'intelligenza umana» (T. De Mauro, Grande dizionario italiano dell'uso, Torino 2000). Nelle varie definizioni, più o meno condivise tra gli studiosi, poi, in genere si distingue tra I.A. Debole e I.A. Forte. Oggi, nell'ambito della I.A. si sono sviluppate diverse branche, come, ad esempio senza pretesa di esaustività, il machine learning, il cognitive computing, il deep learning e le reti neurali.

[4] Nella definizione contenuta nella Risoluzione del Parlamento Europeo del 16.02.2017, lett. AA: l'autonomia di un robot può essere definita come la capacità di prendere decisioni e metterle in atto nel mondo esterno, indipendentemente da un controllo o un'influenza esterna; tale autonomia è di natura puramente tecnologica e il suo livello dipende dal grado di complessità con cui è stata progettata l'interazione di un robot con l'ambiente.

[5] Attraverso forme di c.d. autoapprendimento intelligente, basato anche sulla realtà circostante.

o di mobilità ecc.).
Ed è proprio nell'ambito sanitario che si stanno riscontrando le prime applicazione operative di robot, ossia macchine intelligenti dotate di sensori e programmate per l'assistenza ai pazienti[67].
Del resto, l'ambito della sanità è quello che meglio si presta allo sviluppo di soluzioni innovative che consentano di ottenere un sensibile miglioramento non solo dal punto di vista terapeutico e diagnostico, ma anche da quello organizzativo e gestionale, potendo conseguire un elevatissimo livello di efficienza ed efficacia che comporta, a livello aggregato, un significativo risparmio in termini di costi per le spese dell'intero sistema sanitario.
Come spesso succede, però, la normativa fatica a seguire il rapido progresso dell'evoluzione tecnologica, anche se da più parti si manifestano esigenze di colmare lacune che necessitano di prescrizioni normative specifiche e pertinenti al tema.
In questa direzione, uno dei primi significativi tentativi è rappresentato dalla Risoluzione del Parlamento Europeo, del 16 febbraio 2017[8] recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica.
Con tale Risoluzione, il Parlamento, tra l'altro, prende atto che gli sviluppi nel campo della robotica e dell'intelligenza artificiale possono e dovrebbero essere pensati in modo tale da preservare la dignità, l'autonomia e l'autodeterminazione degli individui, soprattutto nei campi dell'assistenza e della compagnia e nel contesto delle apparecchiature mediche atte alla "riparazione" o al "miglioramento" degli esseri umani.

---

6 Tra le poche sperimentazioni in ambito sanitario, si può indicare l'esempio di M.A.R.I.O., il robot assistente che, nelle intenzioni del progetto di ricerca, si prenderà cura degli anziani con demenza senile. M.A.R.I.O. è l' acronimo di "*Managing active and healthy aging with use of caring service robots* - Sistema di gestione dell'invecchiamento attivo e in salute mediante l'uso di robot assistivo", e rientra in un progetto di ricerca finanziato con 4 milioni di euro dal programma Horizon 2020 dell'Unione Europea, partito nel febbraio del 2015, coinvolgente 10 enti europei tra cui anche l'Ospedale di San Giovanni Rotondo e che nel settembre 2016 è stato consegnato alla struttura. Il robot, quando sarà completata la fase di sviluppo, assisterà gli anziani dal punto di vista mnemonico e sociale. Ed anche se non fornirà assistenza fisica, aiuterà gli anziani a non sentirsi soli: potrà telefonare, leggere le notizie, fungere da portiere, ricordare gli orari dei pasti o delle pillole. In una prima fase potrà interagire grazie ad un tablet posto sulla parte anteriore, successivamente si attiverà con la voce e risponderà persino ai comandi vocali.
Per maggiori informazioni sul progetto v. l'indirizzo internet http://www.operapadrepio.it/it/ricerca-scientifica/news-ricerca-scientifica/news/4198-il-robot-m-a-r-i-o-%C3%A8-arrivato-in-casa-sollievo-si-prender%C3%A0-cura-degli-anziani-affetti-da-alzheimer-con-demenza-senile-lieve.html, consultato nel marzo 2017.

7 Altro progetto di rilevanza europea è BIOMOT, il quale ha contribuito a far avanzare questo settore emergente, dimostrando che i modelli computazionali personalizzati del corpo umano possono effettivamente essere utilizzati per controllare esoscheletri indossabili. Il progetto ha individuato modi di raggiungere una maggiore flessibilità e prestazioni autonome, che potrebbe contribuire all'uso di robot indossabili per l'assistenza alla mobilità e come strumenti di riabilitazione. Per maggiori informazioni consultare gli indirizzi internet http://www.biomotproject.eu/ e http://cordis.europa.eu/news/rcn/126487_en.html, entrambi consultati nel mese di marzo 2017.

8 Reperibile all'indirizzo internet http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//IT, consultato nel mese di marzo 2017.

Tra i diversi inviti contenuti nella Risoluzione, si chiede alla Commissione di proporre definizioni europee comuni di sistemi ciberfisici, di sistemi autonomi, di robot autonomi intelligenti e delle loro sottocategorie, prendendo in considerazione le seguenti caratteristiche di un robot intelligente:
– l'ottenimento di autonomia grazie a sensori e/o mediante lo scambio di dati con il suo ambiente (interconnettività) e lo scambio e l'analisi di tali dati;
– l'autoapprendimento dall'esperienza e attraverso l'interazione (criterio facoltativo);
– almeno un supporto fisico minore;
– l'adattamento del proprio comportamento e delle proprie azioni all'ambiente;
– l'assenza di vita in termini biologici.
La Risoluzione, poi, indica tre ambiti specifici, nel settore sanitario, cui prestare particolare attenzione:
A) Robot impiegati per l'assistenza;
B) Robot medici;
C) interventi riparativi e migliorativi del corpo umano.
Per quanto riguarda il primo, la Risoluzione sottolinea che la ricerca e lo sviluppo di robot per l'assistenza agli anziani sono diventati, nel tempo, più diffusi ed economici, permettendo così di produrre dispositivi dotati di maggiori funzionalità e più facilmente accettati dai consumatori, evidenziando l'ampia gamma di applicazioni di tali tecnologie utilizzate per la prevenzione, l'assistenza, il monitoraggio, lo stimolo e l'accompagnamento degli anziani, come pure delle persone affette da demenza, disturbi cognitivi o perdita della memoria.
Inoltre, sottolinea che il contatto umano è uno degli aspetti fondamentali delle cure umane, ritenendo che la sostituzione del fattore umano con i robot potrebbe, da una parte, disumanizzare le pratiche di accudimento, ma riconoscendo, d'altra parte, che i robot potrebbero svolgere compiti di assistenza automatizzati e agevolare il lavoro degli assistenti sanitari, migliorando, nel contempo, le cure fornite dal personale sanitario e rendendo il percorso di riabilitazione più mirato, consentendo così al personale medico e agli assistenti di dedicare più tempo alla diagnosi e a una migliore pianificazione delle opzioni terapeutiche.
Tuttavia, la Risoluzione sottolinea che gli assistenti in carne e ossa continueranno a essere necessari e a svolgere un ruolo importante e non completamente sostituibile nella loro interazione sociale.
Per quanto riguarda il secondo ambito, viene sottolineata l'importanza di un'adeguata istruzione, formazione e preparazione per il personale sanitario, quali i medici e gli assistenti sanitari, al fine di garantire il grado più elevato possibile di competenza professionale nonchè per salvaguardare e proteggere la salute dei pazienti, evidenziando la necessità di definire i requisiti professionali minimi che un chirurgo deve possedere per poter far funzionare ed essere autorizzato a usare i robot chirurgici.
Il Parlamento UE considera fondamentale rispettare il principio dell'autonomia supervisionata dei robot, in base al quale la programmazione iniziale di cura e la scelta finale sull'esecuzione spetteranno sempre a un chirurgo umano, sottolineando la

particolare importanza della formazione onde consentire agli utenti di familiarizzarsi con i requisiti tecnologici del settore.
Inoltre, viene richiamata l'attenzione sulla tendenza crescente all'autodiagnosi mediante l'uso di un robot mobile e, di conseguenza, sulla necessità che i medici siano formati per gestire i casi di autodiagnosi, ritenendo che l'utilizzo delle tecnologie in questione non debba sminuire o ledere il rapporto medico-paziente, bensì fornire allo stesso medico un'assistenza nella diagnosi e/o nella cura del paziente allo scopo di ridurre il rischio di errore umano e di aumentare la qualità della vita e la speranza di vita.
È convinzione del Parlamento europeo che, in campo medico, i robot continueranno a compiere progressi nello svolgimento di operazioni chirurgiche ad alta precisione e nell'esecuzione di procedure ripetitive e reputa che tali robot dispongano del potenziale per migliorare i risultati della riabilitazione e fornire un sostegno logistico altamente efficace negli ospedali, osservando che i robot medici possono anche ridurre i costi sanitari, consentendo al personale medico di spostare la propria attenzione dal trattamento alla prevenzione e rendendo disponibili maggiori risorse finanziarie per un migliore adeguamento alla diversità delle esigenze dei pazienti, la formazione continua del personale sanitario e la ricerca.
Per quanto riguarda il terzo ambito, quello che desta maggiori problematiche anche di natura etica, la Risoluzione citata osserva che sono stati compiuti enormi progressi dalla robotica e che l'ulteriore potenziale di quest'ultima nel campo della riparazione e della sostituzione degli organi danneggiati e delle funzioni umane, ma anche le complesse questioni sollevate in particolare dalle possibilità di interventi migliorativi del corpo umano, dal momento che i robot medici e specialmente i sistemi cyberfisici (CPS)[9] possono modificare il nostro concetto di corpo umano in salute, dato che possono essere portati direttamente sul corpo umano o essere impiantati nel corpo umano.
In particolare, sottolinea l'importanza di istituire con urgenza, negli ospedali e in altri istituti sanitari, comitati di roboetica con personale adeguato che abbiano il compito di esaminare e aiutare a risolvere problemi etici complessi e insoliti riguardanti la cura e il trattamento di pazienti.
Del resto, nel campo delle applicazioni mediche essenziali, quali le protesi robotiche, deve essere garantito l'accesso continuo e sostenibile alle manutenzioni, alle migliorie e, in particolare, agli aggiornamenti dei software che ovviano a malfunzionamenti e vulnerabilità, raccomandando la creazione di enti di fiducia indipendenti che dispongano dei mezzi necessari per fornire servizi alle persone che utilizzano avanzati dispositivi medici salvavita, ad esempio in termini di manutenzione, riparazioni e migliorie, inclusi gli aggiornamenti software, soprattutto in caso di interruzione di tali servizi di manutenzione da parte del fornitore originale; suggerisce l'introduzione dell'obbligo per i produttori di fornire a tali enti di fiducia indipendenti istruzioni

[9] Ossia un sistema informatico in grado di interagire in modo continuo con il sistema fisico in cui opera.

di progettazione esaustive, incluso il codice sorgente, come accade per il deposito legale di una pubblicazione presso la biblioteca nazionale.
E ciò, anche in considerazione del fatto che non vanno trascurati i rischi correlati alla possibilità di hacking, disattivazione o cancellazione della memoria dei CPS integrati nel corpo umano, dato che possono mettere in pericolo la salute o, in casi estremi, anche la vita umana[10].
Logica conseguenza è la fondamentale ed imprescindibile attenzione alla sicurezza, intesa nel suo complesso e, quindi, anche come trattamento dei dati personali[11] e delle infrastrutture critiche[12], tanto da attribuire carattere prioritario alla protezione di tali sistemi.
Un principio fondamentale, ai fini della redazione o dell'affinamento di specifici testi normativi, quindi, in tema di responsabilità robotica, potrà essere quello della ripartizione dell'onere della prova, con eventuale inversione dello stesso a carico del soggetto che maggiormente potrà essere ritenuto responsabile, in relazione alle caratteristiche costruttive e funzionali del robot (quindi, in funzione della sua "autonomia") oppure il criterio della gestione del rischio, anche sotto forma di apposite soluzioni assicurative, che tengano in considerazione le peculiarità della materia.
Una brevissima riflessione, al riguardo, va fatta sulla possibilità di "tracciare" l'autonomia di tali macchine intelligenti, attraverso appositi file di *log* del sistema di controllo dei robot, che, in un ipotetico contenzioso, possano fungere da prova per ricostruire l'evento e facilitare l'attribuzione dell'eventuale responsabilità, come una sorta di scatola nera, già di ampia diffusione in altri settori tecnologici.
Ad ogni modo, un aspetto fondamentale della responsabilità dei robot da non trascurare è quello del patrimonio[13], tradizionalmente utilizzato come forma di tutela per il ristoro dei danni subiti dalle vittime.
Appare difficile, infatti, allo stato concepire un robot dotato di autonomia patrimoniale, sulla base della quale farlo rispondere, pecuniariamente, degli eventuali danni cagionati a terzi[14]. Anche se teoricamente possibile, attuare una completa separazione

---

[10] Si pensi al recentissimo episodio di attacco informatico globale, noto sotto il nome di "*Wannacry*", che, in particolare, ha duramente colpito le infrastrutture informatiche del sistema sanitario inglese (NHS).

[11] Ormai con riferimento al Reg. UE 2016/679 del Parlamento Europeo e del Consiglio del 27.04.2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), entrato in vigore il 24.05.2016 e pienamente operativo dal 25.05.2018. A tal proposito, pare lecito chiedersi se un robot particolarmente autonomo può essere considerato titolare di trattamento di dati personali, essere nominato responsabile del trattamento di un titolare oppure semplicemente incaricato del trattamento.

[12] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 06.07.2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

[13] Il riferimento è all'art. 2740 cod. civ. italiano: *Il debitore risponde dell'adempimento delle obbligazioni con tutti i suoi beni presenti e futuri. Le limitazioni della responsabilità non sono ammesse se non nei casi stabiliti dalla legge*.

[14] Al riguardo, si vedano gli interessanti spunti di riflessione sollevati da M. Scialdone (reperibili all'indirizzo internet https://ildirittodeirobot.wordpress.com/2017/02/27/il-ritorno-della-schiavitu-nellera-dei-robot-una-tesi-suggestiva/, consultato il 28.02.2017, il quale ritiene "*Suggestiva la*

patrimoniale del robot, sia pure dotato della più ampia autonomia, sembra ancora avveniristico.
Altro aspetto fondamentale è quello della responsabilità del robot per i danni che lo stesso dovesse cagionare a sé stesso o al proprio utilizzatore-proprietario. In questi casi, occorrerà capire come sia stato concretamente cagionato il danno e, quindi, se attribuirlo ad un uso improprio del robot (anche sotto forma di mancato aggiornamento del sistema e/o delle misure di sicurezza) ovvero ad un suo malfunzionamento riconducibile a difetti e vizi di costruzione/programmazione, facendo eventualmente ricorso all'applicazione delle tradizionali norme in materia di risarcimento del danno.
Una posizione proposta in dottrina[15], è quella di ritenere applicabile la responsabilità prevista nell'ordinamento giuridico italiano dall'art. 2052 c.c. per gli animali, considerando i robot alla stregua di animali domestici.
Ulteriore campo di riflessione, nella ipotesi di ritenere i robot veri e propri soggetti di diritto, potrebbe essere quella basata sulle fattispecie previste dagli artt. 2047 c. c. (Danno cagionato dall'incapace), 2048 c. c. (Responsabilità dei genitori, dei tutori, dei precettori) o 2049 c.c. (Responsabilità dei padroni e dei committenti).
Tuttavia, allo stato dell'arte, in assenza di altre apposite auspicabili normative, la scelta più opportuna potrebbe essere quella di applicare la disciplina dell'art. 2050 c.c. sull'esercizio di attività pericolose oppure del 2051 c.c. sulla responsabilità da cose in custodia, normative che hanno il particolare pregio di imporre stringenti oneri probatori a carico del soggetto ritenuto responsabile.
Infine, non va trascurato il possibile scenario di accesso abusivo al sistema di controllo da remoto del robot, che potrà, quindi, essere "hackerato", ai fini della determinazione della "intenzionalità" o meno della condotta. In questo caso, si potrebbe applicare il principio sancito dal tradizionale broccardo latino "*coactus tamen voluit*"[16]?

tesi avanzata sul Financial Times [https://www.ft.com/content/99d60326-f85d-11e6-bd4e-68d53499ed71] dal Prof. Luciano Floridi secondo cui la risposta andrebbe trovata nel diritto romano laddove era il dominus responsabile per i danni cagionati dalle condotte dei propri schiavi. Una tesi che, tuttavia, finisce per confermare la natura del robot quale oggetto e non soggetto del diritto: nell'antica Roma, infatti, gli schiavi potevano avere un patrimonio separato, il c.d. peculium, nei limiti del quale rispondevano, ma la soggettività era comunque fittizia poiché il patrimonio continuava ad essere posseduto dal dominus e lo schiavo era pur sempre una res.". Molto suggestivi, ma allo stato troppo avveniristico, sarebbe il pensare di infliggere punizioni o sanzioni che provochino al robot sofferenze, come avviene nelle tradizionali fattispecie umane (ad es. restrizione della libertà) e che potrebbero consistere nella disattivazione (temporanea o definitiva) di circuiti o sistemi di funzionamento che impediscano allo stesso di funzionare.

[15] M. Scialdone, "*Il diritto dei robot: la regolamentazione giuridica dei comportamenti non umani*", reperibile all'indirizzo internet *http://www.dimt.it/index.php/it/notizie/14621-83il-diritto-dei-robot-la-regolamentazione-giuridica-dei-comportamenti-non-umani*, consultato il 27.02.2017.

[16] Ovviamente, sul presupposto di poter attribuire al robot in questione una autonoma capacità di autodeterminarsi. La Risoluzione citata ritiene, come indicato nella superiore nota 4, che l'autonomia di un robot può essere definita come la capacità di prendere decisioni e metterle in atto nel mondo esterno, indipendentemente da un controllo o un'influenza esterna.

3. Conclusioni

Come si vede gli interrogativi e le problematiche giuridiche che si presentano sono diverse e di non facile soluzione, anche in considerazione del fatto che, nella rigorosa (quanto utopistica) attuazione delle c.d. leggi della robotica di Asimov[17], non si dovrebbero mai verificare ipotesi in cui il robot arrivi a cagionare danni tali da comportare una responsabilità ed il conseguente risarcimento. In fondo, ma molto utopisticamente, il vero progresso ed il principale scopo dello stesso settore della robotica dovrebbe essere proprio quello di creare macchine talmente perfette che evitino, in radice, la possibilità di incidenti o danni di qualsivoglia entità.
La strada intrapresa dall'U.E., con la citata risoluzione del 16.02.2017, si pone nel solco della creazione di un quadro giuridico, almeno europeo, che eviti la frammentazione normativa, sovente causa di ulteriori problemi e di una più lenta diffusione del progresso, ma che, comunque, dovrebbe tenere in considerazione il respiro universale delle questioni giuridiche (ed etiche) sottese riguardanti l'umanità nel suo complesso.

[17] Le leggi di Asimov sulla robotica sono: (1) Un robot non può recar danno a un essere umano nè può permettere che, a causa del proprio mancato intervento, un essere umano riceva danno. (2) Un robot deve obbedire agli ordini impartiti dagli esseri umani, purchè tali ordini non contravvengano alla Prima Legge. (3) Un robot deve proteggere la propria esistenza, purchè questa autodifesa non contrasti con la Prima o con la Seconda Legge. (cfr. Isaac Asimov, Circolo vizioso, 1942) e, a mo' di norma di "chiusura", (0) Un robot non può recare danno all'umanità, nè può permettere che, a causa del proprio mancato intervento, l'umanità riceva danno.

Rivista elettronica di Diritto, Economia, Management

N. 1 - 2017 · pp. 227-249

Opacità dei sistemi intelligenti e sicurezza informatica: un difficile equilibrio fra regolazione e tecno-regolazione

Gianluigi Fioriglio1

Abstract: I sistemi intelligenti pongono numerose problematiche informatico-giuridiche in vari ambiti, destinate ad aumentare di numero e di intensità con l'avvento della Internet of Things. In particolare, alla tutela della sicurezza informatica si accompagnano sfide giuridiche e dilemmi etici dovuti alla diffusione di sistemi intelligenti e interconnessi che interagiscono non solo reciprocamente ma anche con agenti umani in ambienti informatici e non.

In primo luogo saranno svolte alcune notazioni sui sistemi intelligenti, prendendone in esame il concetto, gli stati cognitivi e la prevedibilità (o la imprevedibilità) delle loro azioni. Ci si soffermerà poi sulle questioni informatico-giuridiche che sorgono, e che possono sorgere, a causa della loro interconnessione nella società contemporanea. Saranno quindi delineati i potenziali limiti del diritto nella regolamentazione della sicurezza dei sistemi intelligenti.

In secondo luogo, sarà presa in esame la questione della opacità dei predetti sistemi nella prospettiva del diritto, che tocca la più ampia tematica della opacità delle norme, così come è stata definita dalla dottrina giusfilosofica. Si proporrà quindi una nozione di opacità variabile che possa applicarsi all'ambito dei sistemi intelligenti.

In terzo luogo, sarà argomentata la necessità di un adeguato intervento del diritto, anche per evitare la prevalenza del potere tecnologico su quello statuale, così da raggiungere un delicato equilibrio fra regolazione e tecno-regolazione.

Parole chiave: sistemi intelligenti, regolazione, tecno-regolazione, sicurezza informatica, agenti software.

[1] Sapienza Università di Roma, Dipartimento di Scienze politiche. Email: *gianluigi.fioriglio@uniroma1.it*.

Articolo pervenuto il 2 Maggio 2017, approvato il 1 Giugno 2017

1. Premessa

Indipendentemente dalla loro percepibilità astratta ed effettiva, i sistemi intelligenti, sovente interconnessi, sono già oggi adoperati per la fornitura di prodotti e servizi di uso comune. L'intelligenza artificiale[2] ha quindi un ruolo molto importante nella società contemporanea e la pervade, grazie all'incessante operato di numerosi agenti intelligenti che svolgono autonomamente diverse funzioni nell'ambito di sistemi più o meno complessi. Con ogni probabilità, però, il suddetto ruolo diverrà assolutamente cruciale negli anni a venire e nei più diversi settori: a mero titolo esemplificativo, basti pensare alla Internet of Things, alle automobili a guida autonoma, agli assistenti virtuali negli smartphone, ai chatbot nei servizi di assistenza ai clienti e per finalità di lotta politica, e così via.

Ai numerosi benefici si accompagnano altrettanti rischi, che toccano anche profili etici e giuridici e che costituiscono sfide ancor più complesse e delicate per il diritto rispetto a quelle ormai «tradizionalmente» poste dalla tecnologia.

In particolare, una sfida alquanto delicata è rappresentata dalla garanzia della sicurezza informatica, la cui attualità è ben lungi dal poter essere messa in discussione. L'interconnessione dei sistemi è una forza ma anche una debolezza: a titolo esemplificativo, servizi resi per via telematica possono essere attaccati con varie modalità finalizzate a creare una sorta di esercito digitale composto da moltissimi dispositivi di uso comune (come le videocamere di sorveglianza) che sono collegati a Internet ma che presentano falle di sicurezza che consentono a un utilizzatore di assumerne il controllo in modo automatizzato e, in ipotesi, di cancellare anche le proprie tracce.

Dal canto suo, il diritto è in difficoltà per la concomitanza di vari fattori: la fornitura e l'utilizzo di prodotti e servizi interconnessi su scala globale, il loro elevatissimo numero, l'estremo tecnicismo della tematica in molteplici settori che tocca quindi diverse branche del diritto, la rapida obsolescenza soprattutto dei prodotti non più supportati ma comunque utilizzati.

Sullo sfondo si pongono due questioni di carattere generale, che possono ritenersi paradigmatiche: l'opacità dei sistemi intelligenti e il ruolo del diritto, sinora subalterno a una tecnologia che non solo non riesce a raggiungere nel suo rapido incedere né a comprendere nella sua essenza ma che è oltretutto il prodotto di poteri economici che sono diventati tali proprio grazie alla tecnologia medesima.

Queste considerazioni rendono sin d'ora palese l'approccio informatico-giuridico di questo scritto e ne suggeriscono l'obiettivo: argomentare una «terza via» che consenta di raggiungere un difficile equilibrio fra regolazione e tecno-regolazione. Si proporrà quindi una nozione di opacità variabile applicabile all'ambito dei sistemi intelligenti.

Pertanto, in primo luogo saranno svolte alcune notazioni sui sistemi intelligenti,

[2] Per un quadro d'insieme sulla intelligenza artificiale cfr. G. Sartor, *L'informatica giuridica e le tecnologie dell'informazione. Corso d'informatica giuridica*, Giappichelli, Torino, 2016, p. 279 ss.

prendendone in esame il concetto, gli stati cognitivi e la prevedibilità (o la imprevedibilità) delle azioni. Ci si soffermerà poi sulle questioni informatico-giuridiche che sorgono, e che possono sorgere, a causa della loro interconnessione nella società contemporanea. Saranno quindi delineati i potenziali limiti del diritto nella regolamentazione della sicurezza dei sistemi intelligenti.
In secondo luogo, sarà presa in esame la questione della opacità dei predetti sistemi nella prospettiva del diritto, che a ben guardare tocca la più ampia tematica della opacità delle norme, così come è stata definita dalla dottrina giusfilosofica.
In terzo luogo, sarà argomentata la necessità di un adeguato intervento del diritto, anche per evitare la prevalenza del potere tecnologico su quello statuale, così da raggiungere un delicato equilibrio fra regolazione e tecno-regolazione.

2. I sistemi intelligenti fra informatica, filosofia e diritto

Il percorso teorico sopra delineato richiede di trattare preliminarmente alcuni aspetti essenziali: il concetto di agente intelligente, la rilevanza o l'irrilevanza dei suoi stati cognitivi nonché la prevedibilità o l'imprevedibilità delle sue azioni. Evidente, quindi, la connessione fra gli aspetti informatici, filosofici e giuridici.
Partendo dai primi, un sistema intelligente può essere monolitico o multi-agente prendendo come riferimento un criterio meramente quantitativo: nel primo opera un solo agente e nel secondo due o più. Inoltre, un sistema può essere complesso e prevederne quindi una molteplicità, inclusi quelli umani che intervengono parallelamente a quelli software in determinati casi o ambiti, fermo restando che la finalità principale dell'utilizzo di un sistema intelligente è proprio quella di evitare l'intervento umano o comunque di limitarlo il più possibile. Vi è dunque un problema di complessità dovuto alla molteplicità di apporti paralleli e stratificati, contemporanei e non, a sistemi estremamente articolati e in ambienti in continua modificazione. Oltretutto, la base di conoscenza di ciascun agente non è fissa e immutabile, ma può cambiare anche sensibilmente grazie ad avanzate tecniche di apprendimento automatico.
È pertanto cruciale il concetto di agente, che è una entità che percepisce il suo ambiente attraverso sensori e agisce in esso mediante attuatori[3]. Possono aversi varie definizioni di agente, ma può qui riprendersi quella «debole» fornita da Wooldridge e Jennings per cui un agente deve avere le seguenti proprietà: (i) autonomia (possibilità di operare senza il diretto intervento umano ed esercizio di un certo grado di controllo sulle proprie azioni e sul suo stadio interno), (ii) abilità sociale (capacità di

[3] S. Russell, P. Norvig, *Artificial Intelligence. A Modern Approach*, 3rd Edition, Prentice Hall, Uppers Saddle River (NJ), 2010, p. 34.

comunicare con altri agenti e con esseri umani), (iii) reattività (percezione dell'ambiente e capacità di reagire in un ragionevole periodo di tempo), (iv) proattività (capacità di agire per il raggiungimento di un risultato e di prendere l'iniziativa)[4].
In linea generale, può altresì distinguersi fra quegli agenti che hanno componenti prettamente «materiali» (come gli automi)[5] e quelli che invece sono composti esclusivamente da software (come, per l'appunto, gli agenti software); invero, anche i secondi hanno bisogno di componenti materiali per poter operare (basti pensare a un comune personal computer), ma sono privi di parti percepibili: sono quindi immateriali. Senza software, comunque, anche gli automi non potrebbero funzionare.
Pertanto, negli agenti software le percezioni e le azioni sono totalmente digitali, ma proprio le azioni sono assolutamente reali e produttive di effetti giuridici: basti pensare al caso dei contratti conclusi via Internet, in cui una parte ben può essere un agente software senza che chi contratta ne abbia percezione. Il riferimento alla materialità permette di cogliere quindi la cifra della differenza fra agenti software e robot, fra chi o cosa non può, o ha difficoltà a, celare la propria intelligenza e la propria autonomia e fra chi o cosa può addirittura nascondere la propria «esistenza» e il proprio operato. La stessa opacità si connota in modo differente, atteso che se il codice è imperscrutabile, così può esserlo chi o cosa lo esegue.
Gli agenti software sono dunque emblematici: innanzi tutto, sono fondamentali per gli stessi automi. Inoltre, esemplificano al contempo la pervasività e l'inafferrabilità delle tecnologie; quest'ultima ne agevola l'opacità e complessivamente si crea un terreno fecondo per la loro tecno-regolazione autoreferenziale.
Proprio la loro autonomia implica primariamente la necessità di interrogarsi sulle dimensioni filosofiche dell'informatica giuridica, poiché tra essi si stabiliscono relazioni semi-giuridiche[6] e il loro agire ha conseguenze di particolare delicatezza per l'intera Società dell'informazione[7]. Può tuttavia conferirsi soggettività giuridica agli agenti? Anche in caso di risposta negativa, ove sia sostenibile la sussistenza di stati cognitivi in capo ad essi, sono quest'ultimi rilevanti o irrilevanti? Sono parimenti rilevanti o irrilevanti la prevedibilità o l'imprevedibilit**à delle loro condotte?**

---

[4] M. Wooldridge, N.R. Jennings, *Intelligent agents: theory and practice*, in *The Knowledge Engineering Review*, 10, 2, 1995, p. 116.

[5] Sugli aspetti informatico-giuridici della robotica cfr., fra gli altri, U. Pagallo, *The Laws of Robots. Crimes, Contracts, and Torts*, Springer, Dordrecht, 2013; sui suoi profili etici e sociali cfr. P. Lin – K. Abney – G.A. Bekey (edited by), *Robot Ethics. The Ethical and Social Implications of Robotics*, MIT Press, Cambridge and London, 2014; sull'autonomia cfr. G. Sartor – A. Omicini, *The Autonomy of Technological Systems and Responsibilities for their Use*, in N. Bhuta – S. Beck – R. Geiss – C. Kress – H.Y. Liu (edited by), *Autonomous Weapons Systems: Law, Ethics, Policy*, Cambridge University Press, Cambridge, 2016, pp. 39-74.

[6] C. Faralli, *La filosofia del diritto contemporanea*, Laterza, Roma-Bari, 2012, p. 81.

[7] Ciò avviene "perché il tramite della comprensione tra l'uomo e la macchina è un significato oggettivato, una struttura formale: *una forma, non una volontà,* una particolare informazione, ed in questa forma *adeontica* **è necessario chiedersi che cosa vi sia di giuridico, oppure che cosa diventi un diritto distaccato dalla volontà diretta all'altrui comportamento"** (F. Romeo, *Il dato digitale e la natura delle cose*, in A. Ballarini (a cura di), *Diritto interessi ermeneutica*, Giappichelli, Torino, 2012, pp. 102-103).

Innanzi tutto, qualsiasi prospettiva si adotti e qualsiasi risposta si voglia fornire in relazione alla prima domanda, è comunque necessario comprendere quando ci si trova dinanzi ad un sistema intelligente al fine di delineare una risposta del diritto alle problematiche che derivano da ciascuno di essi e che si accompagnano ai potenziali benefici.
In questo senso, la base teorica è fornita dall'informatica: così, un sistema rientrante nella predetta definizione, o in altra che dovesse ritenersi preferibile, sarà essenziale per capire l'ambito di operatività delle relative norme e aiutare altresì a comprendere quale paradigma utilizzare. Lo stesso può dirsi per il diritto positivo, così da giungere a norme che siano effettivamente generali ed astratte e che, come i prodotti tecnologici, non siano sottoposte a una obsolescenza sin troppo rapida.
Fra le varie nozioni, quella sopra citata di Wooldridge e Jennings pare essere adatta a tali scopi: è infatti generale, ma allo stesso tempo chiara e specifica nei suoi elementi essenziali che colgono proprio le principali peculiarità di questi agenti e, loro tramite, dei sistemi in cui essi sono adoperati. Appare inoltre comprensibile anche per chi non è dotato di particolari competenze informatiche, anche se poi la sua applicazione ai casi concreti richiederà normalmente l'apporto di un tecnico dotato proprio di tali competenze specialistiche. Ma anche un esperto potrebbe essere costretto a fermarsi dinanzi all'opacità dei codici informatici, come di seguito argomentato: di qui la necessità di una opacità parziale e condizionata.
Questi aspetti permettono di mostrare come, di primo acchito, ciò che accade nell'ambito dei sistemi intelligenti non è ontologicamente paragonabile a ciò che accade nella mente umana: non è una inafferrabilità metafisica, bensì artificiale e prodotta dal connubio fra tecnica e diritto. In sostanza, allo stato non sembra né opportuno né sostenibile attribuire una vera e propria soggettività giuridica agli agenti software e ai robot, cui dovrebbe seguire altresì il riconoscimento di diritti di varia tipologia. È tuttavia opportuno tenere viva la discussione su questa tematica, poiché permette di costruire progressivamente i fondamenti teorici che consentono di strutturare quegli strumenti concettuali necessari per affrontare adeguatamente le sfide che la società tecnologica costantemente pone, quanto meno dal punto di vista etico[8].
Del resto, come evidenzia Paolo Moro, gli automi oggi non sono in grado di riprodurre o formalizzare quello specifico procedimento mentale, ossia l'intuizione intellettuale, che identifica la capacità del pensiero umano di cogliere una cosa; in altri termini, di vederla come qualcosa di intero pur prescindendo da un procedimento logico di tipo dimostrativo. Questa abilità è ben nota sin dalla filosofia classica, come

[8] In materia è imprescindibile il riferimento all'opera di Luciano Floridi e alla sua filosofia dell'informazione. Fra i suoi scritti, cfr. *Infosfera. Etica e filosofia nell'età dell'informazione*, tr. it., Giappichelli, Torino, 2009; *The Ethics of Information*, Oxford University Press, Oxford, 2013; *The Philosophy of Information*, Oxford University Press, Oxford, 2011. Per un quadro generale, cfr. Id. (edited by), *The Cambridge Handbook of Information and Computer Ethics*, Cambridge University Press, New York, 2010, nonché Id. (edited by), *The Routledge Handbook of Philosophy of Information*, Routledge, London and New York, 2016.

dimostra quanto affermato da Aristotele nella *Metafisica*[9], ma è frutto di un'attività non discorsiva bensì intuitiva ed essendo priva di procedimento logico non è formalizzabile e quindi non pare essere riproducibile da un elaboratore elettronico. A quest'ultimo, inoltre, manca la comprensione del ragionamento meccanico che svolge. Emerge, qui, tutta la distanza fra sintassi e semantica. In ultima istanza, vi è il problema dell'attuale impossibilità, per il robot, di riprodurre l'attività della coscienza che rappresenta criticamente se stessa: l'attività dell'autentica filosofia è proprio caratterizzata da essa, che si pone alla radice di qualsiasi pensiero[10]. Del resto, "la coscienza è un qualche cosa che è qualitativamente diverso dal cervello e che si colloca fuori dal corpo. Non è dunque solo un problema di quantità di calcolo ma un problema di qualità di processo"[11].

L'impossibilità di attribuire personalità giuridica agli agenti intelligenti non implica necessariamente quella di individuare in loro delle capacità cognitive che in ultima analisi possono portare alla considerazione di elementi soggettivi attribuiti in via immediata agli stessi e in via mediata al loro utilizzatore o a chi ne ha un controllo esclusivo o comunque determinante nella effettuazione di una determinata condotta. La questione è delicata e di difficile teorizzazione oltre che praticabilità anche ma non esclusivamente in virtù della opacità dei codici informatici. È tuttavia rilevante, poiché le conseguenze giuridiche di una condotta derivano spesso dalla sussistenza dell'elemento soggettivo del dolo o della colpa.

Francesco Romeo evidenzia giustamente che sovente si negano capacità cognitive ai robot o agli agenti software facendo ricorso ad un criterio che appare più rigoroso rispetto a quello adoperato per valutare quelle umane. Tuttavia, la scienza non ha ancora compreso pienamente in base a quali regole gli individui reagiscono agli stimoli, inclusi quelli linguistici; al contrario, le regole secondo cui i programmi rispondono a chi interagisce con loro possono ritenersi conosciute o conoscibili. Ciò nonostante, la maggior parte delle opinioni negative si basa proprio su questa differenza e presunzione. In questa prospettiva, l'imprevedibilità della risposta dell'essere umano o la considerazione di una sua libertà priva di condizionamenti sono

---

[9] Aristotele, *Metafisica*, XII, 9, 1075a.

[10] P. Moro, *Libertà del* robot*? Sull'etica delle macchine intelligenti*, in R. Brighi – S. Zullo, *Filosofia del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e pratica*, Aracne, Roma, 2015, pp. 530-532.

[11] G. Taddei Elmi, *Informatica giuridica. Presupposti, storia, disciplina, insegnamento, esiti*, in Id. (a cura di), *Informatica giuridica*, Simone, Napoli, 2016, p. 38. Pertanto, "le macchine anche molto evolute e molto intelligenti sembrano non superare la dicotomia cosa-persona e la soglia minima di soggettività. Restano, oggi, al livello del valore" (ivi, p. 39). Riferendosi agli automi iperintelligenti, poi, Antonio Tarantino rileva che essi costituiscono la mera espressione (quasi un prolungamento tecnologico) della "sostanza individuale sussistente di natura razionale", anche qualora sia riconosciuta la loro importanza per il progresso scientifico ed umano e indipendentemente dalla capacità di simulare e di riprodurre processi cognitivi, tanto da poterli comunque considerare come costituenti valori socio-economici da tutelare (A. Tarantino, *Elementi di informatica giuridica*, Giuffrè, Milano, 1998, p. 52).

dubbie e quindi è necessaria una più forte opera di riflessione su questo profilo[12]. Una simile impostazione «restrittiva» trova la sua ragion d'essere nella delicatezza della problematica, anche per le conseguenze a cascata che si avrebbero su ciascun ordinamento giuridico: basti pensare alla già citata del riconoscimento della titolarità di una serie di diritti in capo ad essi.
Probabilmente, più che un'attribuzione di diritti agli agenti intelligenti è opportuna un'attribuzione di maggiori obblighi ai loro fornitori.
Tuttavia, i dubbi ben espressi da Romeo forniscono degli utili spunti per argomentare una riferibilità degli atti degli agenti anche al loro utilizzatore qualora essi realizzino effettivamente la sua volontà, andando quindi al di fuori dell'ambito delle ipotesi civilistiche di responsabilità oggettiva e investendo così una problematica che trascende il mero riferimento al diritto positivo.
Essa evidenzia la circostanza per cui la società tecnologica sarà caratterizzata da una esplosione di soggettività che non sono tali e che eppure plasmano la società stessa eseguendo autonomamente una molteplicità di algoritmi e prendendo decisioni in applicazione di direttive comunque previste dall'uomo. In altri termini, agiscono come soggetti e non come oggetti o come cose, ma rientrano nella categoria dei secondi e non dei primi.
Si può pertanto guardare alle fattispecie in cui un sistema intelligente ha un ruolo considerevole non tanto e non solo nella prospettiva civilistica dell'attribuzione a un determinato soggetto delle conseguenze giuridicamente rilevanti dell'azione di un software (o di un automa che esegue il software medesimo), ma si può ipotizzare una lettura più dettagliata che, a un diverso livello teorico-giuridico, permetta di distinguere meglio fra le varie fattispecie. In tal senso, l'indagine sull'elemento soggettivo avrà un duplice beneficio: da un lato, si porrà quale parziale antidoto alla opacità e, dall'altro, permetterà di attribuire conseguenze giuridiche diverse a seconda che la condotta originaria sia stata improntata a dolo o colpa.
Ciò richiede però di soffermarsi sulla prevedibilità o imprevedibilità della condotta degli agenti intelligenti, dal momento che una tesi «forte» della imprevedibilità potrebbe rendere insostenibile una qualsiasi opzione che non implichi un regime di responsabilità oggettiva. Del resto, potrebbe sostenersi che anche un datore di lavoro risponda degli illeciti commessi dai propri dipendenti indipendentemente dalla valutazione dell'elemento soggettivo; questi, però, hanno il libero arbitrio: lo stesso non può dirsi per gli agenti intelligenti.
Con precipuo riferimento a quest'ultimi può distinguersi fra imprevedibilità teorica e pratica. La prima discende dalla considerazione che la combinazione della complessità degli agenti software e degli ambienti rende molto difficile, se non impossibile, una previsione accurata del loro comportamento. La seconda è dovuta al fatto che dedicare le proprie energie all'esatta previsione del comportamento dell'agente sarebbe in contraddizione con il fine di delegare ad esso i compiti cognitivi connessi

[12] F. Romeo, *Il dato digitale e la natura delle cose*, in A. Ballarini (a cura di), *Diritto interessi ermeneutica*, Giappichelli, Torino, 2012, p. 96.

all'attività svolta[13].
L'imprevedibilità può quindi essere utilizzata da fornitori di prodotti e servizi «intelligenti» quale circostanza per esimersi da responsabilità. Sul punto, è interessante notare che i sistemi attuali e soprattutto futuri possono essere caratterizzati da modalità sempre più evolute di apprendimento automatico, per cui il sistema stesso potrebbe modificare la propria condotta dinanzi a fattispecie analoghe o addirittura uguali proprio grazie all'esperienza accumulata. Bisogna però considerare che un sistema risponde pur sempre a delle regole stabilite da chi ne ha il controllo: a differenza dell'essere umano, non ha il libero arbitrio. Quand'anche se ne implementi un simulacro grazie a sofisticati algoritmi, rimarrà tale e le scelte saranno comunque riferibili a chi ne ha strutturato la logica.
Pertanto, l'imprevedibilità non può comunque essere considerata una scusante per il produttore o comunque per il soggetto che ha un controllo esclusivo su ciascun agente, in quanto i primi non possono non prefigurarsela.

3. Sicurezza e interconnessione dei prodotti e dei servizi intelligenti: problemi e soluzioni in prospettiva informatico-giuridica

Le questioni sin qui evidenziate assumono una rilevanza non solo teorica ma anche pratica che oggi non è forse del tutto immaginabile poiché non è possibile prevedere l'evoluzione delle caratteristiche dei sistemi intelligenti, il loro numero e le loro azioni ed interazioni sia reciproche sia con gli agenti umani. Oltre alla variabilità delle condotte altrui (indipendentemente da quelle tenute dagli agenti medesimi in esecuzione di algoritmi di apprendimento automatico e quindi dipendenti anche da variabili ambientali), si deve del resto ricordare che essi operano in ambienti, informatici e non, in continuo divenire. Complessivamente, si ha una società che, a sua volta, è plasmata da tutti questi soggetti (umani) ed oggetti (artificiali): i secondi, però, operano in domini specifici con una intensità e con una autonomia talvolta maggiore rispetto ai primi.
La commistione di aspetti informatici e non, materiali e immateriali, virtuali e reali, umani e artificiali, rende evidente la complessità di un quadro in cui è necessaria una seria ed attenta opera di riflessione sui fondamenti teorici della sicurezza informatica dei sistemi intelligenti in una prospettiva che ponga la tecnologia quale tecnica, i cui fini non possono divenire generali: quest'ultimi, pur nella loro mutevolezza, sono stabiliti da ciascuna comunità nel rispetto dei principi e dei valori che le

[13] G. Sartor, *Gli agenti software e la disciplina giuridica degli strumenti cognitivi*, in *Il diritto dell'informazione e dell'informatica*, 2003, 1, p. 62.

danno vita e che oggi, nelle democrazie, tendono a rinvenirsi primariamente nelle loro costituzioni.
In ragione di ciò, la riflessione informatico-giuridica ha il difficile compito di stabilire i limiti del percorso che l'intelligenza artificiale dovrà seguire nella sua inarrestabile opera di pervasione della società, in modo da evitare ulteriori aumenti incontrollati delle tecno-regolazioni, sia qualitativi sia quantitativi, che tendono a porsi non tanto al di sopra ma quanto al di fuori del diritto stesso[14]. Senza pretese di formale creazione di nuovi ambiti costituzionali, esse si pongono però al di fuori delle protezioni delle tutele minime garantite nei vari Stati: come spiegarsi altrimenti quella opacità dei codici informatici che li rende inconoscibili come fossero entità metafisiche o, nella migliore delle ipotesi, segreti di stato? È forse possibile giungere a una opacità che costituisca una mediazione fra le esigenze della collettività e quelle dei poteri tecno-economici?
La suddetta riflessione è necessaria poiché l'interconnessione di prodotti e servizi intelligenti è gradualmente in crescita e pone le basi per una vera e propria rivoluzione che si realizzerà compiutamente quando le tecnologie saranno più mature e disponibili su una scala ancora più larga nei vari settori di riferimento.
Del resto, specifici aspetti dell'evoluzione tecnologica (fra cui le possibilità di delocalizzazione del *cloud computing*, l'evoluzione della robotica industriale, l'accesso costante al web, l'analisi dei *Big Data*) suggeriscono che si possa giungere a una nuova tipologia di *enhancement* tecnologico quale potenziamento delle capacità

[14] Questa è, a ben guardare, una specificazione del più ampio ambito della tecnoscienza. Essa si arroga il compito di indagare sulle varianti delle possibilità e tende a rendere normativo lo stesso possibile, giungendo altresì alla programmabilità dell'uomo sul piano biopsichico in contrasto con le caratteristiche intenzionali e progettuali dell'essere umano, ridotto a soggetto che realizza una progettualità e una intenzionalità di altri (T. Serra, *L'uomo programmato*, Giappichelli, Torino, 2003, pp. 59-62). L'estrema complessità di una società tecnologica in cui operano degli oggetti che hanno determinate caratteristiche dei soggetti portano quello stesso uomo che li ha creati ad esserne potenzialmente vittima e a un ambiente che non è a sua misura ma che si evolve sulla loro base. Anche in questo senso può così essere letta la critica di Morozov all'internet-centrismo e, soprattutto, al soluzionismo tecnologico per cui le scelte commerciali vengono presentate come risposte ai problemi della società: eppure le risposte sono fornite ancor prima che le relative domande siano formulate (cfr. E. Morozov, *The Net Delusion. The Dark Side of Internet Freedom*, Public Affairs, New York, 2011, e Id., *To Save Everything, Click Here. The Folly of Technological Solutionism*, Public Affairs, New York, 2013). Si ha quindi una regolazione della società ad opera del potere economico che usa quello tecnologico per rafforzarsi, mentre il diritto non ha o non vuole usare gli strumenti. Tuttavia, "politica diritto economia, pur nella loro irriducibile particolarità, sono tra loro collegati dal referente comune che è l'uomo, e ciascuno di essi, da quello economico a quello giuridico a quello politico, fondamentalmente, proprio per restare anche sistema di libertà e non essere solo sistemi di poteri, deve tener conto del referente uomo, che peraltro li ha messi in atto e che deve essere rispettato nella sua capacità di giudizio, anzi educato ad avere e difendere questa capacità di giudizio. Ogni sistema informativo-normativo non deve indicare nel dettaglio ciò che si deve o che non si deve fare, diventando una precettistica, ma deve piuttosto presentare situazioni complesse, in cui informazione e regolamentazione vadano insieme e nelle quali spetti poi al singolo operare una scelta o prendere una decisione. Politica, diritto ed economia, lungi dal risolversi in sistemi di comando, vanno intesi come modelli o schemi di comportamento" (T. Serra, *L'uomo programmato*, op. cit., pp. 64-65).

di un individuo mediante una tecnologia portabile e diffusa[15], che tuttavia è anche tanto pervasiva da rendere l'individuo medesimo del tutto dipendente da essa, con una prevalenza dell'ambito artificiale su quello naturale.
Basti pensare al fatto che già oggi chiunque ne usufruisce compiendo attività oramai routinarie come l'utilizzo di un motore di ricerca web, poiché ciascun motore opera grazie a una molteplicità di agenti che eseguono algoritmi estremamente complessi muovendosi in modo autonomo ed automatizzato nella elaborazione di miliardi di informazioni i cui indici sono così resi disponibili in tempo praticamente reale a ciascun utente[16].
La prospettiva del prossimo futuro appare ancor più delicata e tutt'altro che remota, ove si consideri che attualmente il mercato offre non solo elettrodomestici connessi alla Rete e controllabili anche da remoto, ma addirittura automobili a guida autonoma, come le automobili Tesla, dotate del c.d. "Pilota Automatico" ("Autopilot").
La loro diffusione non è particolarmente rilevante se si paragona il numero di automobili al parco auto circolante o gli elettrodomestici intelligenti a quelli tradizionali. Tuttavia, nel futuro questo numero è destinato ad aumentare sensibilmente, soprattutto grazie ai benefici che se ne possono ottenere e alla progressiva riduzione dei costi che si accompagna all'evoluzione tecnica, ma ciò pone delicati problemi in ordine alla sicurezza di qualsiasi dispositivo connesso a Internet e mostra tutta l'inadeguatezza degli ordinamenti giuridici dinanzi all'avanzamento di tecnologie sviluppate, vendute e utilizzate da privati su un piano generalmente globale.
La riflessione sul punto è tuttavia imprescindibile, dal momento che in prospettiva, si può addirittura giungere a un "uomo-macchina", che "ha barattato la morte di Dio con una tecnologia che lo ha reso onnipotente, potenzialmente libero dalla caducità e dalla fragilità degli organismi biologici. L'uomo-macchina oltrepassa i confini della condizione biologica e naviga in una dimensione digitalica, è un *software* in continuo aggiornamento che ricrea in modo indefinito una propria non-natura. Nel robot umanoide la differenza uomo-macchina collassa in un'unica unità indifferenziata"[17], in cui il proprio il software non può che avere un ruolo cruciale.
L'esperienza, però, insegna che i dispositivi attuali e futuri presentano e presenteranno inevitabilmente falle di sicurezza e limitazioni, magari sconosciute al momento in cui vengono commercializzati o comunque diffusi. Difatti, non v'è dubbio che i servizi intelligenti saranno interconnessi e quindi accessibili anche a potenziali malintenzionati, soprattutto in un'ottica in cui si passa sempre più dal concetto di prodotto a quello di servizio, da *Software as a Product* a *Software as a Service*, e dal controllo dell'utilizzatore a quello del produttore (anche con conseguenze nefaste).

---

[15] A. Santosuosso, *Diritto, scienza, nuove tecnologie*, Cedam, Padova, 2016, p. 346.

[16] Su tale questione sia consentito rinviare a G. Fioriglio, *La "dittatura" dell'algoritmo: motori di ricerca web e neutralità della indicizzazione. Profili informatico-giuridici"*, in *Bocconi Legal Papers*, 2015, 5, pp. 113-139.

[17] P. Becchi, *Homo sapiens, homo cyber, postorganico. Derive o approdi?*, in *Materiali per una storia della cultura giuridica*, 2015, 2, p. 589.

Questa circostanza è paradigmatica nel c.d. *cloud computing*[18], che esemplifica altresì il passaggio dalla proprietà di un prodotto (dunque dalla vendita) alla concessione, a titolo gratuito od oneroso, del prodotto medesimo (dunque alla licenza d'uso, in termini informatici, alla locazione o al comodato).
Questo passaggio non è indolore anche in relazione al dominio sul bene: dopo la vendita di un bene materiale, il venditore ne perde il controllo; ma un prodotto interconnesso può essere legittimamente o illegittimamente controllato dal produttore o dal venditore anche da remoto e l'ambito del suo dominio è ovviamente più ampio qualora il bene non sia stato venduto ma sia solo concesso in uso. In tal modo, si pongono ovvi problemi di privacy, in quanto si ha un controllo continuativo dell'utente, e si tende alla centralizzazione di un ambito del potere informatico che può essere alquanto pericolosa.
Come ben rileva Yochai Benkler, discutendo dei punti di controllo della Rete e quindi con una prospettiva più ampia rispetto al mero *cloud computing*, non bisogna comunque guardare a tale centralizzazione e al suo opposto in termini valoriali, ma bisogna affrontarla senza preconcetti e considerare che già la mera architettura della Rete medesima permette di plasmare il potere[19]. Se ciò è vero per il ciberspazio, che è comunque un sistema di comunicazione, lo è ancor di più per i sistemi intelligenti, in cui le informazioni sono oggetto di trattamenti che uniscono l'elevata capacità computazionale propria degli elaboratori elettronici a talune peculiarità, seppur limitate, dell'intelligenza umana. Queste architetture sono però il frutto di studi e ricerche compiuti generalmente in ambito privato, per concretizzarsi sostanzialmente in programmi che guidano il funzionamento degli agenti software e dei robot: la loro inconoscibilità deriva, quindi, dalla tutela accordata dalle varie normative in materia di proprietà intellettuale e industriale.
Bisogna a questo punto evidenziare due elementi dal punto di vista teorico.
In primo luogo, la condotta degli agenti intelligenti viene svolta in esecuzione di algoritmi sempre più complessi e questi possono essere in grado di prendere decisioni non previste né prevedibili dai loro produttori, in particolare grazie ai meccanismi di autoapprendimento e alla molteplicità di variabili che possono orientarne la condotta medesima. Inoltre possono prendere decisioni che mettono a repentaglio la vita altrui: ad esempio, chi dovrà potenzialmente soccombere fra uno o più pedoni e uno o più passeggeri di un autoveicolo a guida autonoma?[20]

---

[18] Per un quadro generale, cfr. M.N. Campagnoli, *Il* cloud computing: *vantaggi e problematicità*, in *Rivista di filosofia del diritto*, 2016, 1, pp. 109-126.

[19] "To imagine either that all centralized power is good and all decentralized power is criminal and mob-like, or that all decentralized power is participatory and expressive and all centralized power is extractive and authoritarian is wildly ahistorical" (Y. Benkler, *Degrees of Freedom, Dimensions of Power*, in *Daedalus*, 2016, 1, pp. 19-20).

[20] Questa tematica fa emergere, tra l'altro, la difficoltà di separare l'ambito morale da quello giuridico. Rende inoltre palesi le spinte egoistiche di determinati soggetti e il potenziale contrasto fra morale e diritto: secondo un recente studio empirico, molti approvano la scelta di produrre veicoli a guida autonoma che in determinati casi sacrifichino gli occupanti per salvare dei terzi, ma non approvano che una simile scelta sia imposta per legge e in simili casi sarebbero meno propensi all'acquisto di

A differenza di quanto accade oggi dinanzi a scelte tanto difficili, che toccano anche un piano etico oltre che giuridico, la scelta non sarebbe compiuta in modo istintivo all'atto dell'evento tragico: sarebbe predeterminata e quindi svolta su una base razionale anziché emozionale; sulla base della ragione e non dell'istinto, di un utilitarismo che pone anche problemi di uguaglianza sostanziale (non tutti sarebbero uguali in via immediata dinanzi all'algoritmo e in via mediata a chi ne ha predeterminato volontariamente le regole).
Ma vi è di più. Questa scelta è compiuta a priori non dal conducente del bene, nel caso di un autoveicolo (in assenza di un controllo esclusivo), bensì su scala collettiva dal produttore di ciascuno di essi. Qui emerge tutta la drammaticità della problematica e la preponderanza del potere privato su quello pubblico, poiché in esecuzione di algoritmi complessi e sconosciuti sarà una macchina a eseguire la decisione stabilita a monte, nei suoi parametri e nei suoi criteri, dal produttore del bene di cui trattasi. E qui riemergono le considerazioni sopra svolte in relazione alla valutazione degli stati cognitivi dell'agente intelligente, che in questo sono predeterminati dal suo produttore e in relazione ai quali potrebbe ipotizzarsi una responsabilità aggravata; questa si aggiunge a quella oggettiva ove sia accertato che l'azione dell'agente sia valutabile in termini di dolo o di colpa.
La suddetta scala collettiva, inoltre, rende palese che eventuali falle di sicurezza potrebbero essere sfruttate per finalità terroristiche e quindi assumere il controllo di una molteplicità di autoveicoli: ipotesi, questa, tutt'altro che fantascientifica. Il caso degli autoveicoli è emblematico, ma non bisogna sottovalutare che anche altre prodotti (come i droni) potrebbero essere utilizzati con le medesime finalità, e gli esempi potrebbero continuare con altre categorie di prodotti.
Come se non bastasse, l'opacità del codice costituirà uno scudo a difesa di qualsiasi decisione posta in essere: e ciò, si badi, non solo in una prospettiva giuridica, ma anche etica da utilizzarsi strumentalmente per finalità commerciali, poiché non ci si può dimenticare che tali attività sono legittimamente svolte nel rispetto della libertà di impresa. La stessa opacità potrà fungere inoltre da schermo dietro cui celare eventuali vizi o difetti del software, che potrebbero essere nascosti o taciuti.
Proprio questa libertà deve trovare dei limiti adeguati nel diritto: di qui la proposta di «terza via» che sarà di seguito avanzata e che trova già una prima giustificazione nel predetto argomento quando determinati prodotti o servizi, per la loro natura, presentano rischi palesi per la incolumità pubblica. È bene precisare che l'immaterialità del prodotto o del servizio non fa venir meno tali rischi: un esempio paradigmatico può rinvenirsi nei software utilizzati per le operazioni di controllo del traffico (automobilistico, navale o aereo) e alla difficoltà di stabilire delle metodologie adeguate[21].

un simile veicolo (cfr. J.F. Bonnefon – A. Shariff – I. Rahwan, *The social dilemma of autonomous vehicles*, in *Science*, 2016, 24, pp. 1573-1576).

[21] Cfr., anche per i riferimenti bibliografici, G. Contissa, *Responsabilità e automazione. Una metodologia per la valutazione del rischio giuridico basata sull'argomentazione*, in R. Brighi – S. Zullo, *Filosofia*

In secondo luogo, bisogna considerare che, così come nella quotidianità ciascun individuo può essere potenzialmente vittima di crimini quali rapine, truffe e raggiri, così l'interconnessione di tali sistemi li porta a essere vittime di attacchi informatici, con conseguenze ovviamente variabili a seconda del fine che si prefigge l'attaccante. Basti pensare al controllo da remoto di un autoveicolo per compiere un atto di terrorismo, come si è detto, o di una molteplicità di modem per effettuare attacchi informatici su larga scala per rendere inaccessibile un servizio on line. Questi esempi mostrano che anche ciò che sembra innocuo può essere molto pericoloso dal punto di vista informatico e che detta pericolosità può derivare da un utilizzo simultaneo di una molteplicità di simili prodotti, utilizzo reso possibile proprio grazie alla peculiarità delle tecnologie informatiche.

Emergono, pertanto, problematiche giuridiche e dilemmi etici che costituiscono casi veramente difficili che il diritto, per le più varie motivazioni, sembra quasi rifiutarsi di regolamentare. Eppure, la tecnologia, mediante questi sistemi, effettuerà sempre più spesso le veci dell'uomo con modalità tali che la renderanno sempre più inafferrabile anche grazie a quello schermo costituito dall'opacità del codice: bisogna quindi essere particolarmente cauti e rafforzare il ruolo del diritto.

Esso è infatti fondamentale per predisporre regole effettive ed efficaci finalizzate a garantire la sicurezza sia dei loro utilizzatori sia dei terzi in una società che dipende in modo progressivamente crescente proprio da dispositivi e servizi «intelligenti» che devono prendere continuamente delle vere e proprie decisioni che incidono su individui e gruppi, come si è visto. In conseguenza di ciò, la sicurezza di tali sistemi è tanto più imprescindibile quanto più delicate possono essere le conseguenze di eventuali violazioni, soprattutto quando possono compromettere il corretto funzionamento di ciascun procedimento decisionale o quando possono comportare l'illegittima acquisizione di dati personali.

Proprio il diritto è però in difficoltà nel regolamentare fattispecie estremamente tecniche e in continuo divenire; in aggiunta, è proprio esso a farsi dominare dalla tecnica quando l'opacità degli algoritmi, oltre che dei sistemi stessi, è non solo legittimata ma addirittura protetta in massimo grado dalle leggi vigenti; ciò accade anche negli Stati costituzionali, in cui il bilanciamento con i diritti fondamentali viene raramente effettuato quando sono in gioco i diritti di proprietà intellettuale e industriale.

I fornitori di prodotti e servizi ad alto contenuto tecnologico possono infatti godere di un regime di sostanziale esenzione da responsabilità stante la difficoltà di provare eventuali difetti e malfunzionamenti di ciascun sistema, incluse eventuali falle di sicurezza, sia per la sua complessità sia per la segretezza che circonda gli algoritmi eseguiti dal sistema medesimo.

Diviene così quasi impossibile conoscere effettivamente i flussi informativi che li attraversano e le elaborazioni che vengono compiute. Lo stesso vale per la possibilità di accedere a quei sistemi complessi gestiti su scala globale da parte dei maggiori

del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e pratica, Aracne, Roma, 2015, pp. 417-430.

fornitori di servizi, i quali così riescono ad eludere sostanzialmente le normative nazionali sotto questo profilo.
È quindi necessario prendere in considerazione due aspetti: la regolamentazione della sicurezza del sistema e le ricadute in tema di responsabilità.
Entrambi possono essere introdotti facendo riferimento a una semplice schematizzazione: se un illecito è dovuto al sistema (ad esempio, per una sua anomalia), il produttore ne sarà responsabile; se l'utilizzatore ha modificato il sistema o l'azione che ha provocato l'illecito e le sue conseguenze è riferibile all'utilizzatore medesimo, ne sarà responsabile; se il tutto è dovuto a un terzo, ne sarà responsabile.
Il problema è che una simile schematizzazione, che incontrerebbe presumibilmente i favori dei produttori di ciascun sistema e quindi delle lobbies di ciascun settore, si scontra con la complessità della realtà e dell'ambiente in cui ciascun sistema si trova ad operare, per cui diviene difficile, se non talvolta impossibile, individuare la reale causa del problema o stabilire effettivamente quali siano le varie concause oltre che il loro impatto effettivo qualora esse siano singolarmente considerate.
Ciò che conta, però, è che l'attuale quadro normativo, a livello generale, è quello di tutelare in massimo grado il software quale segreto industriale, e lo stesso può dirsi per l'approccio del diritto.
Emerge, ancora una volta, il problema dell'opacità del software e prima ancora degli algoritmi che quel software esegue. Questa difesa ad oltranza deve tuttavia essere attenuata in molteplici settori e la progressiva interconnessione dei sistemi ne impone comunque un generale ripensamento poiché, come si è detto, la falla di un determinato prodotto o servizio può essere utilizzata per attaccarne altri.
Le problematiche che sorgono, però, hanno carattere sia globale sia locale e non ci si può affidare unicamente alla buona fede dei produttori dei beni e dei fornitori dei servizi.
Sul punto non v'è forse bisogno di fare riferimento a raffinate teorie giuridiche essendo sufficiente ricorrere alla comune esperienza per argomentare che l'obbligo della buona fede deve ovviamente sussistere, in linea di principio, ma che la sua sussistenza formale non esime da quella sostanziale. Bisogna al contempo prefigurarne la possibile violazione sia per i rilevanti interessi economici coinvolti sia perché in questi casi possono essere compromessi diritti fondamentali come il diritto alla vita. Emblematico, in tal senso, è il celebre caso Volkswagen sulla manipolazione delle emissioni inquinanti di diversi autoveicoli con specifiche motorizzazioni prodotti dalla stessa: questo gravissimo illecito, compiuto con dolo, è stato scoperto per un caso fortuito ed è rimasto celato sino ad allora grazie all'opacità del software.
Si deve quindi far sì che la sicurezza e l'affidamento dei terzi siano garantiti strutturalmente: specifiche regole devono essere integrate all'interno di tali sistemi per consentire una sorta di verifica esterna svolta a posteriori e attenuarne l'estrema opacità.
Vi è di più. Come rileva Ugo Pagallo traendo spunto dall'applicazione della distin-

zione fra funzione promozionale e repressiva del diritto di Bobbio[22] all'ambito del design (che inerisce all'intento "di plasmare la forma di prodotti e processi, così come la struttura di spazi e luoghi, al fine di ottenere una serie di risultati predeterminati, o di prestazioni desiderate"), questo è idoneo a plasmare prodotti e processi della Società dell'informazione. In effetti, attraverso il design possono perseguirsi tre finalità: modificazione del comportamento degli individui (funzione promozionale), impedimento della verificazione di un presunto evento dannoso (funzione repressiva), riduzione dell'impatto degli eventi dannosi (funzione mediana)[23]. Queste tre funzioni possono dunque essere svolte mediante l'imposizione di regole che devono essere previste in ciascun sistema e che non possono essere aggirate.

In ogni caso, indipendentemente dalla predetta buona fede e dalla proposta all'uopo avanzata, l'interconnessione dei vari sistemi introduce due questioni specifiche su cui riflettere non solo in ottica informatica: come fissare e far rispettare determinati standard di sicurezza? Quale responsabilità ipotizzare?

Questi profili sono indubbiamente problematici. Partendo dalla questione circa gli obblighi di sicurezza, si pongono a loro volta altre domande: chi può fissarli, nella società globale? Come far sì che essi siano rispettati? Per quanto tempo un prodotto dovrebbe rimanere sicuro? Come responsabilizzare non solo i produttori ma anche gli utenti?

In relazione al primo profilo, può osservarsi che essi, come parzialmente accade già oggi, dovrebbe essere fissati il più possibile a livello internazionale, grazie a standard di sicurezza il cui rispetto dovrebbe essere una *condicio sine qua non* per la commercializzazione dei prodotti in ciascuno Stato, cui non può che essere riservata l'azione di verifica.

Il problema, però, risiede non tanto e non solo in questo: piuttosto, bisogna volgere lo sguardo verso l'imposizione di un obbligo di supporto, per ciascun prodotto, per un congruo periodo di tempo. Di certo non si può pretendere che un produttore supporti all'infinito i beni che immette sul mercato, ma può certamente pretendersi che la garanzia della loro sicurezza informatica del prodotto medesimo venga fornita per un periodo di tempo che sia proporzionato alla tipologia del bene.

L'obsolescenza programmata non è, infatti, unicamente quella relativa alle funzionalità e all'aspetto estetico di un prodotto: può essere relativa anche al fatto che diviene tanto insicuro da non dover più essere utilizzato decorso un certo periodo di tempo ove siano presenti falle di sicurezza che lo rendano pericolo sia per l'utilizzatore sia per terzi.

Un simile obbligo dovrebbe essere imposto *ex lege*, per fare in modo che venga rispettato, e potrebbe affiancarsi alle normative che già prevedono determinate ga-

---

[22] N. Bobbio, *Dalla struttura alla funzione. Nuovi studi di teoria del diritto*, Edizioni di Comunità, Milano, 1977.

[23] U. Pagallo, *Il diritto nell'età dell'informazione. Il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti*, Giappichelli, Torino, 2014, p. 130 ss.

ranzie (basti pensare alla garanzia per difetti di conformità). Ovviamente, come si è detto, sarebbe necessario fissare periodi temporali diversi a seconda della tipologia di prodotto. Ciò però è molto difficile, poiché la società globalizzata si caratterizza proprio per il predominio dell'economia sulla politica[24].

Tuttavia, in assenza di interventi legislativi, i produttori e i prestatori di servizi della Società dell'informazione potranno pur sempre contare sulla opacità degli algoritmi garanti dalla legge stessa, con ovvie ricadute in tema di responsabilità che potranno portarli a godere di una posizione ancor più privilegiata. La segretezza del codice è infatti cruciale in quanto può portarli ad esimersi da responsabilità grazie alla circostanza per cui l'utente e il danneggiato avranno serie difficoltà nel provare anomalie o problemi dovuti al software.

Diventi infatti sempre più difficoltoso riuscire a imputare correttamente la responsabilità. Inoltre, aumenta ancora il divario fra la forza del produttore o prestatori di servizi, da un lato, e dell'utente-consumatore, dall'altro (sia che abbia concluso un contratto con il primo, anche in via mediata, sia che si trovi in una posizione di terzietà, come nel caso del pedone ferito od ucciso da un veicolo a guida autonoma).

Innanzi tutto, chi risponde della condotta di un agente intelligente?

Sul punto si possono prendere le mosse da quanto affermato da Sartor, secondo cui **è argomentabile l'**applicazione analogica delle norme sulla responsabilità vicaria, combinandole con quelle attinenti alla responsabilità di proprietari e custodi, e sulla sostituzione nell'attività giuridica, ossia mandato e rappresentanza[25]. In questo senso si può riprendere la tesi di Renato Borruso per cui, nonostante il computer possa valutare le circostanze del caso concreto e decidere in base ad esse, la volontà di tali decisioni deve comunque essere riferita all'uomo poiché questi l'ha preordinata attraverso il programma: in esso va ravvisata la proiezione nel futuro del pensiero e della volontà dell'uomo e conseguentemente la capacità (comunque entro limiti predeterminati) di intendere e di volere[26].

Non pare, pertanto, che vi siano dubbi circa la riferibilità degli effetti negativi della condotta di un agente intelligente al suo produttore qualora questi ne abbia il controllo esclusivo. Ma il quadro sarà generalmente più complesso, poiché a seconda dei casi potranno assumere rilievo varie figure: ad esempio, il produttore o prestatore, il venditore, l'utilizzatore, i terzi (non solo i danneggiati, ma anche terzi produttori e utenti i cui dispositivi o software potrebbero essere causa o concausa di danni oltre che le rispettive compagnie assicurative).

È ragionevole aspettarsi che ciascun produttore cercherà, per quanto possibile,

---

[24] La discussione in materia è molto ampia; per un'agile discussione di un tema tanto complicato cfr. M.R. Ferrarese, *Prima lezione di diritto globale*, Laterza, Roma-Bari, 2012.

[25] G. Sartor, *Gli agenti software e la disciplina giuridica degli strumenti cognitivi*, op. cit., p. 62. Nello stesso senso appaiono M.A. Biasiotti– F. Romano – M.T. Sagri, *La responsabilità degli agenti software per danni prodotti a terzi*, in *Informatica e diritto*, 2002, 2, p. 159.

[26] R. Borruso, *Computer e diritto*, tomo II, Giuffrè, Milano, 1988, pp. 253-255 (Borruso aveva già anticipato tale tesi nel suo *Civiltà del computer*, Ipsoa, Milano, 1978).

di esimersi da responsabilità e sicuramente sarà agevolato dalla forte protezione della segretezza del codice assicurata, in linea generale, dai vari Stati.
La crescente pervasività delle tecnologie intelligenti fa tuttavia comprendere come l'analisi complessiva delle predette questioni vada ben oltre l'ambito civilistico del risarcimento del danno e concerna un aspetto fondamentale della società contemporanea in quanto relativo all'utilizzo di agenti intelligenti in una molteplicità di ambiti e con effetti potenzialmente disastrosi su larga scala. Per rimanere nell'ambito dei veicoli a guida autonoma, cosa succederebbe in caso di malfunzionamenti o di atti di cracking dei sistemi finalizzati a prenderne il controllo o comunque a cagionare sinistri?

4. Opacità delle norme e dei sistemi

La società contemporanea **è caratter**izzata da notevoli asimmetrie e fra esse assume rilievo quella fra la segretezza dei codici informatici e la trasparenza di tutti coloro che, in via mediata o immediata, li utilizzano o sono comunque coinvolti in virtù di esso. Com'è noto, ciascuna persona è sempre più profilata e innumerevoli informazioni che la riguardano sono raccolte ed elaborate da una molteplicità di soggetti, per lo più, ma non esclusivamente, per finalità commerciali[27]. Oggi sussiste la certezza di essere controllati senza tuttavia poterne anticipare le conseguenze anche a lungo termine in virtù del progresso tecnologico che prevedibilmente consentirà trattamenti incrociati di dati sempre più sofisticati anche all'insaputa dei soggetti le cui informazioni vengono trattate[28]. Difatti, anche se oggi non sono disponibili strumenti tanto sofisticati da consentire un perfetto trattamento della enorme e sempre crescente mole di dati personali accumulata, bisogna pur considerare che l'evoluzione della tecnologia suggerisce che in un futuro non troppo remoto sarà possibile effettuare trattamenti incrociati di dati in modo più efficiente, che potrebbero così rendere vane le operazioni di anonimizzazione parziale potenzialmente effettuate sino ad oggi.
La prospettiva futura è quella di una estremizzazione ancora più forte: la trasparenza delle persone aumenterà nella Internet of Things, grazie a strumenti sempre più sofisticati ed autonomi; la segretezza del codice è tuttora garantita dal diritto e

[27] Come rileva Amato Mangiameli, "non è il *brave new world* elettronico *tout court* a creare un nuovo potere sull'individuo e a consentire disincantate gestioni della soggettività, ma è l'accumulo pressoché illimitato di informazioni, la combinazione velocissima dei dati (biometrici e non) tra loro, ed ancora la precisa identificazione del dato in memorie sterminate ed indefettibili" (A.C. Amato Mangiameli, *Informatica giuridica*, Giappichelli, Torino, 2015, pp. 314-315).

[28] Ci si trova ormai dinanzi a una nuova forma di *arcana imperii* che appare quasi paradossale: le tecnologie dell'informazione e della comunicazione rendono la società più trasparente poiché consentono controlli diffusi su qualsiasi potere, ma gli algoritmi che fondano a loro volta il potere dei soggetti che forniscono i relativi servizi tecnologici è assolutamente segreto (S. Rodotà, *Il diritto di avere diritti*, Laterza, Roma-Bari, 2012, p. 402).

presumibilmente continuerà ad esserlo nel futuro, a meno che non si adotti una via che contemperi una regolazione costituzionalmente orientata e la tecno-regolazione già in essere.
Bisogna quindi tendere a una maggiore trasparenza proprio nell'ottica della Internet of Things, in cui sarà altresì necessario stabilire un regime di responsabilità che tenga conto dei molteplici interessi coinvolti nonché di questioni connesse alla «vita» di dispositivi che possono potenzialmente diventare insicuri e addirittura pericolosi per via dell'evoluzione della tecnica.
Ciò richiede, fra l'altro, una diversa responsabilizzazione sia dei produttori e dei prestatori dei servizi sia degli stessi utenti.
Dal punto di vista oggettivo, bisogna chiedersi se il diritto possa imporre un'obbligazione di *disclosure* al prestatore del servizio, in un regime di segretezza del codice, e, in caso positivo, quale prestazione si possa o ci si debba attendere e se detta obbligazione sia desumibile da principi e norme già vigenti oppure se sia necessario l'intervento dei vari legislatori (atteso che simili questioni sono idonee a riverberarsi nella società globale, poiché, fatte salve alcune eccezioni, tali servizi sono normalmente resi su scala mondiale seppur con localizzazioni e altri accorgimenti).
La trasparenza, però, può essere illusoria, poiché il codice di questi agenti sarà necessariamente molto complesso e oltretutto potrebbe essere costantemente modificato. Non è sufficiente neanche esplicitare i criteri che guidano ciascun algoritmo, poiché bisogna comunque verificarne l'implementazione concreta in ciascun programma e in un determinato momento.
La trasparenza è, inoltre, un'arma a doppio taglio, perché il codice potrebbe essere studiato per porre in essere attacchi informatici o comunque utilizzato dai concorrenti per finalità commerciali.
È quindi evidente che l'equilibrio fra le opposte esigenze è molto difficile da raggiungere, anche se le prospettive di una diffusione estremamente forte dei sistemi intelligenti nella vita quotidiana rende non più procrastinabile la ricerca di vie che tutelino maggiormente i diritti delle persone rispetto a quelli dei fornitori di prodotti e servizi. I sistemi che fanno uso di tecniche di intelligenza artificiale sono infatti integrati in prodotti e servizi di uso comune, come smartphone e motori di ricerca, caratterizzati da una connessione permanente o periodica con server remoti che acquisiscono dati e che possono effettuare le elaborazioni applicando il paradigma del *cloud computing*.
È tuttavia ben noto che in simili casi ci troviamo dinanzi a una Internet delle scatole nere[29], che caratterizza una società in cui i flussi informativi viaggiano sovente all'insaputa dei loro utilizzatori. Si ha una opacità assoluta, poiché non è dato sapere quali e quante informazioni siano effettivamente acquisite ed elaborate. Inoltre, gli stessi algoritmi che riguardano le applicazioni dell'intelligenza artificiale appaiono

[29] Sul punto cfr. F. Pasquale, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Harvard University Press, Cambridge and London, 2015.

opachi[30] ed eventuali violazioni di sicurezza potrebbero non essere comunicate dai detentori delle predette informazioni ai relativi interessati, i quali magari sarebbero comunque ignari della quantità di dati in possesso dei primi. Si crea, ovviamente, un circolo vizioso con la complicità dei legislatori che, anziché ridurre tale opacità, la legittimano e depotenziano il diritto al controllo dei propri dati personali.
Le conseguenze sono però ben più gravi se si considerano unitariamente la prevedibile crescita quantitativa e qualitativa dei sistemi intelligenti e l'attitudine tecno-regolativa di un diritto che sembra quasi avere timore di approcciare una tematica in un ambito che pare non essergli proprio ma che lo è in quanto caratterizzante quella stessa società che il diritto è chiamato a regolare. Non è tuttavia un timore, bensì una conseguenza di una società globalizzata in cui il potere si esplica in un reticolo in cui i nodi principali sono strutturati dal potere economico che, in simili casi, deriva la sua forza dalla tecnologia.
Eppure "siamo entrati nella terza rivoluzione tecnologica, la *software revolution:* non possiamo fermarla, ma abbiamo il dovere di controllarla"[31].
È necessario un mutamento di prospettiva. L'opacità, così come si è finora realizzata, pone infatti questioni estremamente delicate, soprattutto nell'ottica della sicurezza non solo informatica. Si può quindi pensare a una opacità relativa, più o meno intensa a seconda degli interessi in potenziale conflitto così da evitare impostazioni estremistiche, tese verso una trasparenza o una segretezza assolute.
Utili spunti possono qui trarsi da quanto argomentato da Damiano Canale in relazione alle c.d. norme opache, ossia quelle norme che vengono applicate dal giudice facendo riferimento a ciò che viene detto dagli esperti ma senza poterle realmente comprendere. In simili ipotesi, l'opacità non **è tuttavia dovuta al** tecnicismo in sé, bensì all'asimmetria cognitiva fra i legislatori e i giudici, da un lato, e gli esperti, dall'altro, poiché quando il linguaggio tecnico non-giuridico è comprensibile dai primi, il diritto non è opaco ed essi operano nell'ambito dei propri ruoli. Qualora ciò non avvenga, essi non possono compiere una serie di attività intellettuali, di scelte pratiche e di ragionamenti[32].
Ebbene, i sistemi intelligenti oggi sono opachi perché non comprensibili non solo ai giuristi, ma già ai loro utilizzatori. Può solo discutersi di ciò che accade in seguito al loro utilizzo, ma operando in ambienti complessi in cui avvengono infinite interazioni diviene estremamente difficile, e talvolta impossibile, comprendere se in essi

---

[30] Difatti, "nonostante le ottime intenzioni degli scienziati, ogni algoritmo che riguarda le applicazioni dell'intelligenza artificiale è frutto di una programmazione assiomatica e rimane opaco, sebbene influisca sull'obiettività dell'informazione e sulla riservatezza, condizionando argomentazioni ed emozioni che si propagano in rete: algoritmi che pretendono di interpretare testi, argomenti, ma anche emozioni, restano ipotesi sottratte alla discussione e formulate da chi detiene il potere di elaborarle ed amministrarle" (P. Moro, *Libertà del* robot*? Sull'etica delle macchine intelligenti*, *op. cit.*, p. 539).

[31] P. Becchi, *Homo sapiens, homo cyber, postorganico. Derive o approdi?*, op. cit., p. 590.

[32] D. Canale, *Norme opache. Il ruolo degli esperti nel ragionamento giuridico*, in *Rivista di filosofia del diritto*, 2015, numero speciale, p. 94 ss.

vi siano anomalie o se essi compiano azioni riferibili ai propri produttori od utilizzatori anche per ciò che concerne l'elemento soggettivo; in ipotesi, tali informazioni potrebbero essere ricavate dallo studio dei rispettivi codici.
Bisogna quindi chiedersi se sia realmente necessario combattere la predetta opacità e, in caso di risposta positiva, come sia possibile.
In primo luogo, ciò è necessario per due ordini di ragioni: la prima è relativa al fatto che un ambito della società sarebbe lasciato a una tecno-regolazione autoreferenziale, per cui alla giuridicità dell'ordinamento si sostituirebbe quella dell'informatica ("code is law", per usare la celebre espressione di Lessig)[33]; la seconda discende dalla circostanza per cui determinati sistemi intelligenti sono in grado di compiere azioni aventi rilevanza giuridica nella società in modo autonomo e dunque al di fuori del controllo del loro produttore, proprietario o utilizzatore.
Più specificatamente, in relazione alla prima bisogna considerare che le azioni di ciascun agente in ciascun sistema sono percepibili all'esterno solo una volta che sono compiute e quindi il suo ragionamento è ricostruibile solo a posteriori. Tuttavia, ricostruire ciò che succede all'interno di tali sistemi è essenziale ove si verifichino degli illeciti o comunque per comprendere se ne siano compiuti. È vero che ciascun produttore o fornitore può comunque esporre gli elementi a tal fine essenziali in modo tale che siano comprensibili a chi di dovere (ad esempio, l'utilizzatore o il giudice) nonostante l'asimmetria cognitiva che sussiste nei confronti di queste tipologie di soggetti. L'opacità estrema, però, impedisce di acquisirne la prova, perché è un ambito sottratto al controllo del potere giudiziario: e ciò sostanzialmente pur se non formalmente. Anche ove ciò dovesse essere necessario, difficilmente un giudice imporrà di effettuare una verifica del codice utilizzato da uno dei poteri informatici dominanti nella prestazione dei propri servizi, in quanto esso è un segreto industriale utilizzato nella fornitura di servizi a milioni o addirittura a miliardi di utenti da parte di un soggetto avente una rilevanza economica (e quindi politica nella società globalizzata) superiore a quella di molti Stati. Così, l'economia prevale sul diritto e un ambito è di fatto inconoscibile per quest'ultimo, sottratto allo sguardo dei poteri pubblici e, soprattutto, sottratto alla legge.
Oltretutto, se l'ambiente in cui vengono intessute le relazioni umane è già plasmato dall'attuale rivoluzione fondata sulle tecnologie dell'informazione e della comunicazione[34], lo sarà maggiormente in presenza di tecnologie ancor più pervasive ed avanzate; pertanto non ci si può esimere dal regolarle compiutamente e da valutare giuridicamente le loro azioni.
La seconda ragione si connette alla prima, poiché nella società opereranno sempre più numerosi agenti intelligenti in modo autonomo rispetto al soggetto che ne è, o che ne sarà, responsabile: detta autonomia è però fattuale e non giuridica, per cui le loro azioni saranno pur sempre riferibili ad un determinato soggetto, quanto meno

[33] L. Lessig, *Code. Version 2.0*, Basic Books, New York, 2006, *passim*.

[34] U. Pagallo, *Il diritto nell'età dell'informazione*, op. cit., p. 24.

in teoria. L'opacità potrà costituire uno schermo per nascondere eventuali anomalie del software e, dinanzi ad un sistema che prevede interazioni umane e non-umane, il suo utilizzatore potrebbe doversi trovare a fornire una *probatio diabolica*: come esimersi da responsabilità quando magari i log (prodotti dal sistema stesso) proveranno il contrario? Tuttavia, i prodotti informatici non sono di per sé neutrali: sono degli strumenti che possono consentire il perseguimento degli scopi più diversi e in simili casi è necessario presuppore che i relativi produttori possano non agire necessariamente in buona fede, prevedendo così delle garanzie effettive. Eppure, se il codice è segreto, diviene impossibile assicurarsi che quei log sono effettivamente la traccia di ciò che è realmente accaduto in un determinato sistema (ad esempio, in un autoveicolo a guida autonoma). Ancora, la progressiva diffusione di strumenti di uso comune (come gli elettrodomestici) dotati di funzionalità intelligenti implica una profilazione continuativa di ciascun utilizzatore, indipendentemente dalla sua volontà. Così, un semplice elettrodomestico può monitorarne le abitudini e comunicarle al suo produttore; come qualsiasi dato personale, esse sono tuttora, e saranno sempre, più tradotte digitalmente in informazioni da utilizzarsi per le finalità più diverse, ma generalmente commerciali. L'opacità, in questi casi, giunge a coprire le tracce informatiche di tali informazioni, sostanzialmente impossibili da seguire.
Queste ragioni sono sufficienti per argomentare la necessità di un approccio prudente all'opacità dei sistemi intelligenti. In tal senso, può pensarsi a una opacità variabile e condizionata, imposta dal legislatore con modalità differenti a seconda delle peculiarità delle tipologie dei sistemi e dei rischi che essi pongono, come proposto al paragrafo successivo in riferimento alle problematiche di sicurezza informatica.

5. Prospettive di una terza via fra regolazione e tecno-regolazione

Le considerazioni sin qui svolte evidenziano una molteplicità di problemi che rendono sempre più stringenti ed attuali alcune domande. Può il diritto regolare la tecnica raggiungendo un corretto equilibrio fra progresso tecnologico e tutela dei diritti? O deve piuttosto affidarsi alla tecno-regolazione ed intervenire solo ove si presentino conseguenze avverse? Come regolamentare i sistemi intelligenti operanti su scala globale? In sostanza, come affrontare questa nuova "sfida tecnologica"?
Queste domande, innanzi tutto, evidenziano l'impossibilità di adottare soluzioni univoche ed estremamente settoriali poiché presuppongono un utilizzo pervasivo di tecnologie sempre più evolute nella Società dell'informazione.
Bisogna quindi trovare una terza via nell'ambito di una dicotomia duplice: quella fra trasparenza e segretezza, da un lato, e fra regolazione e tecno-regolazione, dall'altro. Innanzi tutto, il diritto può regolare la tecnica ma non può spingersi sino a realizzare una regolamentazione minuziosa sia perché essa potrebbe non avere i caratteri della

generalità e dell'astrattezza sia perché sarebbe di difficile comprensione non solo per gli operatori del diritto ma già per tutti coloro i quali sono sottoposti alle regole medesime. Una componente di tecno-regolazione è presumibilmente ineliminabile, ma essa può realizzarsi mediante la promozione della definizione di *best practices* che siano implementate dagli operatori di ciascun settore di riferimento e ciò può anche mitigare quelle problematiche di carattere globale che inevitabilmente caratterizzano la Società dell'informazione.
In sostanza, si può propendere per una terza via, rifuggendo da soluzioni troppo nette e rigide che non consentirebbero di trovare delle soluzioni adeguate alla molteplicità delle fattispecie ipotizzabili.
In linea generale, bisogna raggiungere un compromesso fra trasparenza e segretezza, giungendo ad una opacità bilanciata. Gli interessi in gioco, infatti, sono tanti e vi sono aspetti positivi e negativi in entrambe le vie: essi mostrano anche l'obiettivo di dimostrare la necessità di un loro contemperamento non solo con le esigenze degli utilizzatori e dei terzi, ma anche degli stessi produttori.
In particolare, si può pensare a una opacità parziale e condizionata, distinta a seconda della tipologia di ciascun prodotto o servizio. In questo senso, l'opacità consente di mediare fra i due estremi della trasparenza e della segretezza.
Le soluzioni possono essere implementate in modo diverso, ma il punto fondamentale è quello di superare il paradigma della segretezza assoluta del codice per contemperarlo con quello della trasparenza. Ciò può avvenire trovando una terza via fra regolazione e tecno-regolazione, che appare come una via mediana: pertanto, bisogna interrogarsi su soluzioni che permettono di operare un bilanciamento corretto fra gli interessi delle parti in gioco.
La correttezza può stabilirsi facendo riferimento a parametri e criteri generali e sostenibili che trovino la loro fonte primaria in una considerazione della persona in quanto tale più che in essa come consumatore o utente. Una realizzazione concreta di questa tesi può rinvenirsi nelle seguenti soluzioni che qui si propongono per una regolamentazione di alcuni profili dei sistemi intelligenti nella società contemporanea.
Una prima soluzione può consistere nella obbligatorietà di una sorta di «garanzia estesa» per ciò che concerne la sicurezza dei prodotti, come già anticipato. Ovviamente, sussistono diverse problematiche, come l'ipotesi del fallimento di un determinato produttore e la vendita o la fornitura di servizi su scala globale, ma sono questioni che possono essere previste e risolte mediante appositi strumenti giuridici, come già avviene in diversi settori in casi analoghi (basti pensare ai fondi di garanzia).
Una seconda soluzione è invece relativa a una problematica che, in linea più generale, tocca gli agenti intelligenti: quando capire se hanno operato in modo corretto? Secondo Russell e Norvig, un agente razionale è colui che effettua la cosa giusta. Ma cosa significa effettuare la cosa giusta? Si può qui fare riferimento alle conseguenze della condotta dell'agente. Quando un agente è calato in un ambiente, produce una sequenza di azioni in risposta alle percezioni che riceve. Questa sequenza di azioni fa sì che l'ambiente attraversi una sequenza di stati. Se la sequenza è desiderabile, l'agente si è comportato correttamente. Questa nozione di desiderabilità è valutabile

facendo riferimento alle specifiche sequenze degli stati dell'ambiente, non agli stati dell'agente[35].
Pertanto, da un punto di vista tecnico può sostenersi che anche in un sistema complesso una valutazione tecnica nei termini di cui sopra possa aiutare a capire se esso abbia funzionato «correttamente». In tal modo si può controbattere la possibile argomentazione difensiva da parte del fornitore o prestatore circa l'impossibilità di prevedere la condotta dei propri agenti intelligenti. Ma già normalmente un datore di lavoro non può prevedere la condotta dei propri dipendenti e ciò nonostante essere comunque ritenuto responsabile di loro eventuali atti illeciti, in applicazione delle già ricordate regole sulla responsabilità vicaria.
Tuttavia, nelle ipotesi in cui si debbano valutare eventuali illeciti compiuti direttamente dall'agente e si vogliano prendere in considerazione gli elementi tecnici sin qui considerati, bisognerebbe poter effettuare le opportune verifiche sul sistema. Il produttore o prestatore, però, gode di una posizione di indubbio vantaggio, mentre il danneggiato deve fornire una prova che seppur non diabolica è estremamente difficile da raggiungere. Il primo normalmente si opporrà a qualsiasi richiesta di accesso al proprio codice, invocando le normative in materia di proprietà intellettuale, mentre al secondo non resterà che cercare di provarne il dolo o (più presumibilmente) la colpa effettuando deduzioni a posteriori. Per risolvere tale questione, sarebbe necessario modificare la ripartizione dell'onere della prova, riequilibrando un rapporto altrimenti del tutto squilibrato.
Una terza soluzione può consistere nell'obbligo del deposito del codice presso apposite banche date pubbliche, assicurandone la confidenzialità e consentendo l'accesso solo in determinate ipotesi. Ovviamente, tali banche dati dovrebbero essere costantemente aggiornate e altrettanto ovviamente una siffatta previsione sarebbe osteggiata dai vari produttori e prestatori di servizi.
Una quarta soluzione potrebbe consistere nella previsione di una sorta di «data di scadenza» nei prodotti non aggiornati o insicuri, che dovrebbero essere disattivati automaticamente e quindi resi inutilizzabili[36]. Ma ciò dovrebbe essere chiaramente evidenziato prima dell'acquisto e potrebbe costituire uno strumento per potenziare o addirittura realizzare l'obsolescenza programmata.
Nessuna soluzione, comunque, è indolore.

[35] S. Russell, P. Norvig, *Artificial Intelligence. A Modern Approach*, op. cit., p. 36.

[36] In tal modo si applica a questo ambito la proposta avanzata da V. Mayer-Schönberger di stabilire una «data di scadenza» per le informazioni digitali (Id., *delete. The Virtue of Forgetting in the Digital Age*, Princeton University Press, Princeton and Oxford, 2011).

N. 1 - 2017 · pp. 250-255

L'analisi di un "cold case" delitti nell'astigiano negli anni '90: serial killer o differenti autori?

Agostino Raso[1]

Abstract: Per "cold case", si intendono i c.d. "casi freddi" o "piste fredde", con riferimento ai delitti più gravi, irrisolti, che anche a distanza di numerosi anni possono essere oggetto di nuove indagini eseguite in particolare attraverso l'utilizzo delle moderne tecniche investigative. Tra questi rientrano per eccellenza gli omicidi rimasti senza colpevole. Numerosi sono i casi di cronaca più o meno recenti che, specie con il supporto delle scienze forensi, sono stati oggetto di nuove indagini, talvolta risolutive. Per far fronte a tale esigenza sia l'Arma dei Carabinieri che la Polizia di Stato hanno creato di recente specifici Reparti di investigazione, all'interno delle proprie strutture centrali di Polizia Giudiziaria.

"Cold case" is an unsolved major crime (mainly homicide or abduction), which, after long time, can be re-examined by using modern technologies for their investigation. Unsolved homicides are typical examples of "cold case". Many crime news' cases (either recent or past) have undergone new examinations, with the support of forensic science. In some cases, these new activities have led to crimes' solution. In order to face this new need, both "Carabinieri" and "Polizia di Stato" have established recently specific units as part of their own Criminal Investigation Department.

Parole chiave: cold case (caso freddo), serial killer (assassino seriale), investigazioni, criminal profiling (profilo criminologico).

(L'articolo è tratto dal capitolo IV della tesi di Laurea discussa nella sessione invernale dell'a.a.2015/2016, Corso di Laurea in Scienze dell'amministrazione e della Sicurezza, Curriculum Sicurezza e Investigazioni)

---

[1] Maresciallo Capo nei Carabinieri, in servizio come Ufficiale di Polizia Giudiziaria presso il Comando Stazione Carabinieri di Nepi (VT). Dottore in Scienze dell'Amministrazione e della Sicurezza, Curriculum Sicurezza e Investigazioni, titolo conseguito presso l'Università degli Studi di Roma Unitelma Sapienza. L'argomento di interesse nazionale, è stato presentato in sede di seduta di tesi di Laurea durante l'anno accademico 2015-2016 .E-mail: agostino.raso.roma@gmail.com

[2] Documentazione acquisita, previa autorizzazione dell'A.G., dagli atti contenuti nei fascicoli processuali custoditi presso il Tribunale e la Procura della Repubblica di Asti, a cura di Agostino Raso e Riccardo Mazzei.

Articolo pervenuto il 16 Febbraio 2017, approvato il 20 Marzo 2017

1. Introduzione

La ricerca e l'analisi di un possibile cold case rinvenuto sul territorio nazionale, nell'ambito di doverose attività di sistematizzate ricerche investigativo-scientifiche, prende spunto dall'analisi dell'arresto di un operaio quarantenne, Massimo Delù, residente nella provincia di Asti, avvenuto in data 15 aprile 2001 e già oggetto di esame nella letteratura criminologica. L'uomo aveva tentato di strangolare mediante una corda una prostituta albanese, dopo aver cercato di stordirla con uno spray. Grazie alla reazione della malcapitata e all'intervento di un'altra prostituta accorsa in aiuto, il delitto non veniva portato a termine e l'autore, rintracciato poco dopo i fatti, veniva fermato.
Da alcuni articoli apparsi su quotidiani locali a seguito del fatto e tutt'ora reperibili in rete, venivano portati all'attenzione del pubblico alcuni omicidi insoluti, avvenuti negli anni Novanta nella stessa area geografica, in danno di prostitute, supponendo che i delitti potessero essere stati commessi per mano di un *serial killer*, che la stampa lasciava intendere essere Massimo Delù.
L'ipotesi prospettata dalla stampa in ordine ai delitti in questione, che ha prima vista presentavano alcuni elementi in comune, dava inizio alla ricerca degli atti processuali riferiti ai casi degli omicidi in danno di: Marina Zaio, il cui cadavere era stato rinvenuto in San Marzano Oliveto (AT) nel 1992; Piera Melania Vico, uccisa nel febbraio 1995 in Castello di Annone (AT) e Jessica Moore, rinvenuta cadavere il 27 gennaio 1999, sempre in Castello di Annone (AT). La prima attività di analisi della serie di delitti, veniva intrapresa attraverso l'acquisizione degli atti d'indagine e processuali, presso gli uffici giudiziari di Asti, ad eccezione di quelli riferiti all'omicidio di Marina Zaio, purtroppo non reperiti.

2. L'omicidio di Piera Melania Vico

Piera Melania Vico, abitante nella provincia di Cuneo, ha 42 anni, quando durante l'esercizio della prostituzione scompare nell'Astigiano in data 10 febbraio 1995. Due giorni dopo un interlocutore mai identificato contatta il 112 e riferisce che presso un casale in Loc. Crocetta del Comune di Castello di Annone (AT) c'è il cadavere di una donna. Dopo circa due ore lo stesso soggetto contatta nuovamente il 112, riferendo che il cadavere si trova in Loc. Alberone dello stesso Comune. Poco dopo personale dei Carabinieri rinviene il corpo senza vita di Piera Melania Vico, nel cortile di un casolare ubicato nella seconda località indicata.
Il corpo esanime della donna è riverso sul fianco sinistro e scoperto nelle parti intime. Viene immediatamente constatato che la vittima è stata ferita con numerose coltellate di cui una più profonda al collo.
Sulla scena del crimine vengono rinvenuti alcuni reperti tra i quali la confezione di un preservativo e poco distante un preservativo con all'interno probabile liquido

biologico. Sia agli inquirenti che al medico legale appare evidente che la donna prima di essere stata uccisa abbia avuto un rapporto sessuale.
Sulla causa della morte il medico legale non ha dubbi che sia stata provocata dalla ferita inferta nella parte anteriore del collo, con un'arma da taglio. Tale ferita nella relazione è descritta: *"… sulla superficie anteriore del collo, da destra a sinistra, a forma di mezzaluna, lunga cm.12 è presente un'ampia ferita da taglio…"*. Circa l'arma utilizzata, il consulente espone: *"…si potrebbe supporre, allora, che sia stato fatto uso di un coltello, verosimilmente ad un tagliente, a lama probabilmente larga e sufficientemente pesante…"*
Le indagini portano a sospettare di due prostitute e un uomo che probabilmente in contrapposizione con la donna assassinata, per ragioni legate al business connesso all'esercizio della prostituzione della zona, avevano deciso di dare una lezione alla stessa, degenerata nell'omicidio. Nei giorni immediatamente successivi al delitto, una delle persone indagate aveva avviato il proprio veicolo alla rottamazione pur essendo in buone condizioni. Il mezzo viene però rintracciato e sequestrato dagli inquirenti che acquisiscono su di esso reperti contenenti tracce biologiche. Le persone sospettate, sottoposte a fermo, vengono incarcerate.
La perizia finalizzata all'estrazione del DNA da tali reperti e la successiva comparazione con quello della vittima, fornisce però esito negativo e pertanto gli indagati vengono liberati e il procedimento a loro carico archiviato.
Dagli atti non risulta però mai essere stato analizzato il reperto consistente nel preservativo usato, rinvenuto sulla scena del crimine e quindi mai valutato ai fini dell'estrazione del profilo genetico del DNA per successivi confronti.

3. L'omicidio di Jessica Moore

Jessica Moore, era una prostituta nigeriana di 27 anni, la quale, come spesso accaduto ad altre sue connazionali, era giunta in Italia alla ricerca di lavoro, finendo verosimilmente vittima della criminalità intraetnica e costretta a prostituirsi. La donna si era stabilita a Torino ed esercitava la prostituzione in strada, nella provincia Astigiana. La ragazza scompare la sera del 06 gennaio 1999 e viene ritrovata cadavere il 27 gennaio 1999, in un fossato posto fuori dal centro abitato di Castello di Annone (AT), nei pressi del fiume Tanaro.
Sulla scena del crimine il cadavere si presenta supino e con evidenti ferite provocate da fendenti praticati con un'arma da taglio, nonché con il padiglione auricolare destro reciso. Poco distante dal cadavere vengono rinvenuti alcuni preservativi, di cui uno contenente liquido seminale.
Dalla lettura del verbale di sopralluogo e dell'esame autoptico emergono alcuni singolari elementi. La donna presentava numerose ferite da taglio, superiori a dieci, tra le quali una più importante sotto l'arcata mandibolare sinistra.
Tale lesione era stata provocata da un'arma della lunghezza di almeno 12/14 cm, che

aveva prodotto ferite riconducibili ad una lama particolarmente robusta, scrive a tal proposito il Medico Legale *"…del tipo di quelle proprie delle baionette militari…"*, concludendo circa la diagnosi medico-legale che *"…un simile quadro lesivo è indicativo in modo perentorio di una modalità omicidiaria"*.
D'altra parte la volontà di uccidere appariva evidente anche dal fatto che gli oggetti ornamentali ed i gioielli indossati dalla vittima, non erano stati asportati, escludendo pertanto l'ipotesi che il delitto aveva avuto uno scopo di rapina, degenerato poi nell'omicidio.
Le indagini, dopo aver battuto piste legate a clienti o persone comunque conosciute alla vittima, nonché al racket della prostituzione, finivano per arenarsi, senza individuare alcun autore.
Dagli atti emerge, anche in questa circostanza, che non risulta mai essere stato analizzato il reperto consistente nel preservativo rinvenuto sulla scena del crimine e quindi estratto il relativo profilo genetico del DNA, accertamento che oggi avrebbe permesso un eventuale confronto.

4. Il tentato omicidio di Seva Dayana

Si tratta dell'evento che ha permesso l'arresto di Massimo Delù e che ha fornito lo spunto per l'avvio della presente ricerca, come descritto in premessa.
L'evento risale alla notte del 14 aprile 2001, vigilia della Santa Pasqua. Massimo Delù si apparta in un'area industriale di Castello di Annone (AT) con la prostituta albanese Seva Dayana di 27 anni. Ad un certo punto, secondo la ricostruzione processuale, mentre i due consumano un rapporto sessuale, l'uomo spruzza sul viso della donna il contenuto di una bomboletta spray comunemente utilizzata per l'avviamento di motori, di seguito con una corda cinge il collo della sventurata, la quale però riesce a sfuggire alla presa e prima di allontanarsi toglie le chiavi dall'auto, gettandole all'esterno. Seva Dayana con le sue urla riesce ad attirare l'attenzione di un'altra prostituta che richiederà l'intervento della Polizia di Stato.
Il personale intervenuto sul posto rinviene all'interno e nei pressi del veicolo in uso all'indiziato, il materiale utilizzato per l'esecuzione del reato, la bomboletta spray e la corda, nonché un coltello a serramanico, detenuto sul cruscotto dell'autovettura.
Nella stessa notte gli inquirenti individuano Massimo Delù mentre cerca di rientrare presso la sua abitazione celato all'interno dell'autovettura di un amico. Presso l'appartamento sottoposto a perquisizione verranno rinvenuti numerosi coltelli, lacci, corde, oltre ad oggetti disposti accanto ad una sorta di altarino adornato da ciondoli, statue di Buddha ed altro, nonché una foto di una giovane donna non identificata. Nella camera da letto dell'uomo viene documentata la presenza di numerosi crocefissi.
Massimo Delù verrà condannato dal Tribunale di Asti per tentato omicidio di Seva Dayana alla pena definitiva di anni sei, poi ridotta in appello.

Ma il materiale sequestrato nell'occasione, sia sulla scena del delitto che presso la sua abitazione, appare di particolare interesse, per ipotizzare alcune affinità con i delitti insoluti riportati ai paragrafi precedenti, desumibili sia dai mezzi utilizzati, che dalle modalità dell'azione.

5. L'ipotesi di omicidi seriali. Analogie tra i casi

Procedendo nell'analisi dei delitti descritti, in maniera unitaria, emergono senz'altro alcune importanti analogie tra di essi, suscettibili di ulteriore approfondimento.

Se da un lato non è possibile, allo stato, ipotizzare che i delitti siano seriali e riconducibili con certezza alla mano di Massimo Delù, non possono essere trascurati alcuni elementi che verranno di seguito evidenziati.

Le analogie riportate sono quelle oggettivamente riscontrate dalla lettura ed analisi degli atti acquisiti all'interno dei fascicoli processuali aperti in relazione ai reati, acquisiti durante la ricerca:

- **Le vittime prescelte sono tutte donne dedite alla prostituzione su strada e come tali naturalmente più vulnerabili, in pratica "facili prede";**
- **Le scene del crimine sono tutte ubicate nel Comune di Castello di Annone (AT), luogo di nascita e domicilio di Massimo Delù;**
- **L'esecuzione dei delitti è preceduta da un rapporto sessuale tra autore e vittime, circostanza desumibile dal rinvenimento su entrambe le scene del crimine riferite agli omicidi di Piera Melania Vico e Jessica Moore, di preservativi con all'interno liquido biologico (circostanze emerse dalla lettura dei verbali di sopralluogo della scena del crimine, eseguiti rispettivamente in data 12/02/1995, da personale del Comando Stazione Carabinieri di Castello di Annone e in data 27/01/1999, da personale del Gabinetto di Polizia Scientifica della Questura di Asti). Analogamente anche l'esecuzione del tentato omicidio di Seva Dayana, è riscontrato dagli atti essere preceduta da un rapporto sessuale (elemento emerso all'esito del processo a carico di Massimo Delù, definito con sentenza di condanna, emessa in data 27/02/2002, dal Tribunale di Asti, divenuta irrevocabile in data 11/07/2003);**
- **I decessi di Piera Melania Vico e di Jessica Moore, sono stati entrambi causati dalle gravi ferite inferte alla gola, mediante un'arma da taglio dalla lama robusta (così come accertato attraverso le consulenze Medico Legali, redatte rispettivamente in data 02/03/1995, dal Dr. A. Gaglio e in data 20/05/1999, dal Dr. R. Testi); nel caso di Seva Dayana la vittima viene dopo un tentativo di stordimento, cinta con una corda al collo e a bordo del mezzo in uso al Massimo Delù viene rinvenuto un coltello a serramanico,** arma tipicamente a lama robusta, come riscontrato dalla fotografia sotto riportata, acquisita all'interno del fascicolo fotografico redatto per il caso, da personale del Gabinetto di Polizia Scientifica della Questura di Asti, in data 14/04/2001:

Anche presso l'abitazione dello stesso Massimo Delù, verranno rinvenute armi da taglio, illegalmente detenute, come riportato nella sentenza sopra citata;

- In entrambi gli omicidi si denota una particolare ferocia e malvagità nell'esecuzione del crimine, le vittime sono attinte da numerose coltellate con il fine, più probabile, di arrecare dolore e solo una di queste è inferta per uccidere, come dettagliatamente descritto attraverso gli esami autoptici eseguiti dai Medici legali attraverso le consulenze tecniche già indicate.

D'altra parte l'ipotesi di delitti seriali emerge anche dalla lettura della richiesta di convalida del fermo eseguito a carico di Massimo Delù, scrive a tal proposito il Pubblico Ministero, Dott.ssa A. Ricci: ***"…l'assoluta gratuità del gesto realizzato, nonché dei mezzi usati e le modalità della condotta potrebbero addirittura far ipotizzare un delitto seriale…",*** **(estratto della richiesta di convalida del fermo avente data 16/04/2001, Procura della Repubblica di Asti).**

I casi riportati, per quanto emerso, possono essere certamente oggetto di nuove indagini, nonché di analisi Criminal Profiling, potendo, nella fattispecie, rientrare in uno dei profili di serial killer analizzati e studiati da esperti del settore, così da fornire utili elementi per un'eventuale riapertura delle inchieste allo stato archiviate. A tal fine è altresì ipotizzabile un confronto tra il profilo genetico del DNA riferito a Massimo Delù, che per quanto emerso dagli atti non risulta mai essere stato prelevato, con i profili del DNA estratti attraverso la perizia effettuata sui reperti acquisiti nell'ambito dell'omicidio di Piera Melania Vico, conservati agli atti del fascicolo d'indagine.