Ciberspazio e diritto 2012, Vol. 13, n. 44 (1-2012), pp. 11-27

Lockdown[1]. L'imminente guerra attorno al destino dei computer universali[2]

Cory Doctorow[3]

I computer universali sono stupefacenti. Sono talmente stupefacenti che ancora oggi la nostra società fatica a comprenderli pienamente, a comprendere a cosa servano, a come integrarli nella vita sociale e a come gestirli. Questo ci riporta a un tema che potrebbe avervi annoiato da un po': il *copyright*.

Vi domando, però, di avere pazienza, dal momento che questo discorso riguarda, in realtà, un tema ben più importante. La struttura stessa delle guerre in corso attorno al copyright ci fornisce, infatti, indizi circa un'imminente lotta attorno al destino dei computer universali.

In principio, avevamo software pre-confezionato e *sneakernet*[4]. Avevamo floppy-disk chiusi in buste sigillate, in scatole di cartone appese con le mollette all'interno dei negozi e venduti come se fossero caramelle, o

[1] Il termine *lockdown* scelto dall'Autore nel corpo del titolo significa, come è noto, "chiusura", "bloccaggio". Nel linguaggio comune (e cinematografico) ha anche, però, un significato specifico correlato alla *detenzione* e, in particolare, all'isolamento di un prigioniero in una cella ("chiusa", appunto) dopo un episodio di rivolta. *Lockdown* è infatti anche titolo (o sottotitolo) usato tipicamente per film ad ambientazione carceraria (n.d.t.).

[2] Il testo originario è "general purpose computing" e quindi, letteralmente, "sul calcolo a fini generali", ma si è ritenuta più corretta e scorrevole la traduzione "computer universali" perché più chiara per il lettore (n.d.t.).

[3] Cory Doctorow (Toronto, 17 Luglio 1971) è un giornalista e scrittore che vive a Londra da diversi anni ed è stato coordinatore per l'Europa dell'*Electronic Frontier Foundation*, l'organizzazione senza scopo di lucro che si batte a favore delle libertà digitali. Collaboratore del *Guardian*, del *New York Times*, di *Publishers Weekly e* di *Wired*, è conosciuto in Internet come co-redattore del noto blog *Boing Boing*, tra i primi al mondo per numero di visite uniche (http://boingboing.net/). Nel 2007 è stato definito come uno dei "giovani leader globali" del *World Economic Forum* e una tra le prime 25 *Web Celebrities* elencate dalla rivista *Forbes*. Il presente Articolo è basato sulla relazione tenuta al *Chaos Computer Club* a Berlino nel dicembre 2011 (n.d.t.).

[4] *Sneakernet* è un termine per indicare lo spostamento di supporti magnetici o dati effettuato fisicamente, camminando (di qui, appunto, le *sneakers*, scarpe comode da ginnastica) (n.d.t.).

Abstract

Lockdown. The imminent war surrounding the future of universal computers.

Cory Doctorow in this article assumes a scenario in the near future concerning the world of computer science in general, and the control of content and technology in particular. The discussion ranges from the problem of copyright and its protection (often excessive) with control systems of rights and DRMs, up to assume a "generation" of computers bent on control and the advent of a real war that will focus in computers for common use and of general purpose.

Lockdown. L'imminente guerra attorno al destino dei computer universali.

In questo articolo Cory Doctorow ipotizza uno scenario del prossimo futuro che riguarda il mondo dell'informatica in particolare e il controllo dei contenuti e delle tecnologie in particolare. La riflessione spazia dal problema del copyright, e della sua tutela spesso eccessiva, ai sistemi di controllo dei diritti e ai DRMs sino ad ipotizzare una "generazione" di computer votati al controllo e l'avvento di una vera e propria guerra che avrà ad oggetto i computer ad uso comune e generale.

Ciberspazio e diritto 2012, Vol. 13, n. 44 (1-2012), pp. 29-42

Alcune riflessioni sui rapporti tra diritto (d'autore) e tecnologia (di protezione) a margine dell'articolo di Cory Doctorow

Giorgio Spedicato[1]

Sommario: 1. Premessa. – 2. *Authorized by the authors [and, or, vs.] permitted by law*: ha ancora senso parlare di bilanciamento degli interessi nel diritto d'autore? – 3. *Dura lex, sed autem lex*: perché una cattiva legge è (ancora) il minore dei mali.

1. Premessa.

Come molti bravi autori di *science fiction*, Cory Doctorow ha il pregio di saper vedere lontano. "*Lockdown: The coming war on general-purpose computing*"[2], nel lanciare un grido di allarme contro i danni collaterali tipici di ogni guerra, e dunque anche delle *copyright wars*[3], offre al lettore molte suggestioni e non pochi spunti di riflessione. Da cultore della proprietà intellettuale, mi sembra che siano almeno due quelli che vale la pena di raccogliere e sviluppare in queste brevi note di commento.

Vorrei infatti, in primo luogo, puntare l'attenzione sull'impatto delle norme che nel sistema del diritto d'autore tutelano le cc.dd. misure tecnologiche di protezione (MTP) e, *maxime*, sulle *anti-circumvention provisions* introdotte dagli artt. 11 del *WIPO Copyright Treaty* e 18 del

[1] Giorgio Spedicato, avvocato, è Professore a contratto di Diritto della Proprietà intellettuale presso la Facoltà di Giurisprudenza dell'Università di Bologna (polo didattico di Ravenna) e Dottore di ricerca in Informatica giuridica e diritto dell'informatica. È stato Visiting Research Scholar presso la Benjamin N. Cardozo School of Law di New York e presso il Max-Planck-Institut für Immaterialgüter - und Wettbewerbsrecht di Monaco di Baviera.

[2] L'articolo di Cory Doctorow, pubblicato sul noto blog *Boing Boing*, riprende, ampliandolo, un *keynote speech* tenuto dall'Autore il 27 dicembre 2011 al *Chaos Computer Congress* di Berlino. Su questo Fascicolo è riportata la traduzione in lingua italiana con note integrative.

[3] Sull'origine delle *copyright wars* cfr. P.K. Yu, *The Escalating Copyright Wars*, 32 Hofstra L. Rev. 907 (2004).

Abstract

A number of reflections on the relationships between (copy)rights and (protection) technology in the light of the article by Cory Doctorow.

In this article the author, inspired by the observations of Doctorow, traces the main issues that affect, in the information society, the desire for control of the code and technologies by multinational corporations, instances of protection concerning the right of the authors and the management of content and the delicate relationship between legal protection and self-regulation. The problems are many: from the legal framework in North America to Italian draft legislation aimed at seeking to regulate the circulation of material in violation of copyright, up to moderate proposals of regulation of the current landscape.

Alcune riflessioni sui rapporti tra diritto (d'autore) e tecnologia (di protezione) a margine dell'articolo di Cory Doctorow.

In questo articolo l'autore, prendendo spunto dalle osservazioni di Doctorow, ripercorre le principali problematiche che riguardano, nella società dell'informazione, la volontà di controllo del codice e delle tecnologie da parte delle multinazioni, le istanze di protezione sul tema del diritto d'autore e della gestione del contenuti e il delicato rapporto tra tutela legale e autoregolamentazione. I problemi posti sono molti: dall'analisi del quadro in Nord America ai progetti di legge italiani volti a cercare di disciplinare la circolazione di contenuti in violazione del diritto d'autore, sino ad ipotesi moderate di regolamentazione del panorama attuale.

Ciberspazio e diritto 2012, Vol. 13, n. 44 (1-2012), pp. 45-72

Attivismo digitale: monitoraggio collaborativo e democratizzazione dell'informazione di fonte pubblica

Barbara Coccagna[1]

Sommario: 1. Introduzione: attivismo digitale e trasparenza globale. – 2. L'*hacking* dei dati pubblici. – 3. Monitoraggio collaborativo e *civic engagement*. – 4. Il processo di costruzione sociale della conoscenza. – 5. Reti sociali ampiamente distribuite grazie alle tecnologie mobili. – 6. La costruzione collaborativa dell'attendibilità dei contenuti. – 7. Apertura e semplicità come chiavi di accesso alla conoscenza collettiva. – 8. Scenari futuri: riflessioni conclusive.

1. Introduzione: attivismo digitale e trasparenza globale

Il fascino più grande della rivoluzione tecnologica risiede nella sua imprevedibilità. Lo studioso che si addentra nel mondo digitale, per approfondirne le dinamiche sociali e individuarne la cornice giuridica, ha l'impressione di trovarsi di fronte a un organismo che evolve in una dimensione temporale che ignora i parametri e i ritmi umani. I fenomeni sociali godono nella frontiera elettronica di una tale capacità di amplificazione e rielaborazione da produrre, in pochi mesi, mutamenti che, in passato, avrebbero richiesto decenni. Quella cui abbiamo assistito negli ultimi tre anni è, senza dubbio, una rivoluzione della trasparenza. Trasparenza dei dati, in primo luogo. Sulla scia delle politiche di *open data* inaugurate, nel corso del 2009, dal Presidente degli Stati Uniti d'America, Barack Obama[2], molti Governi, in ogni parte del mondo, hanno in-

[1] Dottore di ricerca in Politiche sociali e Sviluppo Locale presso l'Università degli Studi di Teramo, con una tesi di dottorato sul tema della Peer production e Open Government. Avvocato, già cultore della materia in Informatica Giuridica, Facoltà di Giurisprudenza - Università degli Studi di Teramo.

[2] Il progetto del Governo degli Stati Uniti d'America, denominato *Open Government Initiative*, è consultabile all'indirizzo http://www.whitehouse.gov/Open, mentre il portale per l'accesso ai dati è all'indirizzo www.data.gov. Un elenco dei princi-

Abstract

Digital activism: collaborative monitoring and the democratisation of public information.

In the latest years the wide proliferation of citizen journalism and mobile communication technologies has promoted the germination of a new shape of digital activism which is able to bring about advantages to long lasting democracies as well as to transitional phase and authoritarian Countries. We're talking about projects intended to capitalize on the power of multitudes of occasional witnesses to demonstrate infringements of human rights, acts of violence or corruption in public sector, vote-rigging and other weighty abuses of authority or power, to manage humanitarian emergencies by natural catastrophes and disasters.
Dealing with freedom information and public accountability, this paper's aim is to outline a synthetic global picture of digital activism grounded on collaborative monitoring and civic engagement. The following item points out the great suppleness of a pattern which is able to combine technological tools and human energies to the purpose of collecting and sharing citizens' informations from a positive transparency through a careful survey of tools, technologies and operating patterns.

Attivismo digitale: monitoraggio collaborativo e democratizzazione dell'informazione di fonte pubblica.

L'ampia diffusione del *citizen journalism* e delle tecnologie mobili ha promosso, negli ultimi anni, la nascita di una nuova forma di attivismo digitale, capace di apportare benefici a stabili democrazie, così come ai Paesi in transizione e agli Stati autoritari. Si tratta di sperimentazioni volte a sfruttare il potere della testimonianza visiva per documentare violazioni di diritti umani, episodi di violenza o di corruzione nel settore pubblico, brogli elettorali e altri gravi abusi, gestire emergenze umanitarie in caso di catastrofi naturali e disastri. Scopo del presente contributo è quello di tracciare un quadro sintetico dell'attivismo digitale basato sulla promozione del monitoraggio collaborativo e del *civic engagement*, in tema di *freedom information* e *public accountability*. Attraverso un'attenta analisi degli strumenti, della tecnologie e dei modelli operativi utilizzati, l'articolo evidenzia l'estrema duttilità di un modello capace di coniugare *tools* tecnologici ed energie umane per raccogliere e condividere le informazioni raccolte dai cittadini, in un'ottica di benefica trasparenza.

Ciberspazio e diritto 2012, Vol. 13, n. 44 (1-2012), pp. 75-97

Diritto e procedura penale e criminalità informatica

Il sequestro preventivo di siti web tramite ordine agli ISP: osservazioni sui casi Moncler e Vajont.info

Marco Bettoni[1]

Sommario: 1. Introduzione. – 2. Il caso Moncler. Il sequestro preventivo di 493 nomi a dominio. – 2.1. Il riesame: esorbitanza del provvedimento. – 3. Il caso Vajont.info. Il sequestro preventivo di un sito. – 3.1. Il riesame: eccessività contenutistica del sequestro. – 4. Cenni sul regime di responsabilità degli Internet Service Provider. – 5. Problematiche relative al sequestro preventivo e al blocco di siti dislocati all'estero. – 5.1. Legittimità alla luce dell'art. 322 c.p.p. – 5.2. Proporzionalità e questioni di bilanciamento dei diritti. – 5.3. Questioni di effettività… – 5.4. (segue)… e questioni di opportunità. – 6. Considerazioni conclusive.

1. Introduzione.

Le modalità di attuazione delle decisioni degli organi giudiziari in materia di sequestro di contenuti, che si suppone illeciti, diffusi attraverso Internet sono terreno estremamente sensibile nella prospettiva del conflitto tra libertà di espressione e altri diritti costituzionalmente protetti. La recente giurisprudenza nazionale di merito e di legittimità, oltre che la giurisprudenza della Corte di Giustizia dell'Unione Europea, si caratterizza, infatti, per decisioni dai contenuti molto distanti tra loro.

Le cause di ciò si possono individuare da due prospettive: da un lato le previsioni normative in materia, ormai datate più di un decennio, nel pur nobile intento di fissare principi generali da declinare di volta in volta

[1] Marco Bettoni è dottorando di ricerca in Diritto delle Nuove Tecnologie – *curriculum* in Informatica Giuridica e Diritto dell'Informatica, presso l'Alma Mater Studiorum – Università di Bologna.

Abstract

Preventive seizure of websites through an order to ISPs: comments on Moncler and Vajont.info cases.

This essay addresses the legal and political issues raised by the use, by the Italian courts, of the instrument of preventive seizure of websites located abroad, applied through an order to ISPs to interdict the domain names resolution through DNS. Moving from the decisions taken in the pre-trial phase of two recent court cases, the Moncler and the Vajont.info cases, read in the light of European legislation on ISPs liability and others leading cases of the Italian Supreme Court and the Court of Justice of the European Union, the purpose of this *paper* is to present their implications on freedom of expression.

Il sequestro preventivo di siti tramite ordine agli ISP: osservazioni sui casi Moncler e Vajont.info.

Il presente lavoro affronta le questioni giuridiche e politiche sollevate dal ricorso, da parte della giurisprudenza italiana, allo strumento del sequestro preventivo dei siti web dislocati all'estero, applicato attraverso l'ordine agli ISP di interdizione della risoluzione dei nomi a dominio tramite DNS. A partire dalle decisioni adottate nelle fasi cautelari di due recenti casi giudiziari, il caso Moncler e il caso Vajont.info, letti alla luce della normativa europea in materia di responsabilità dei provider e di altri *leading cases* della Corte di Cassazione e della Corte di Giustizia dell'Unione Europea, lo scopo di questo *paper* è presentarne le implicazioni in punto di diritto alla libertà di espressione.

Ciberspazio e diritto 2012, Vol. 13, n. 44 (1-2012), pp. 99-120

L'introduzione abusiva ed il mantenimento non autorizzato in un sistema informatico nella recente sentenza delle Sezioni Unite. "Abuso" dei profili autorizzativi, "abuso" di poteri da parte del pubblico ufficiale e violazione dello *jus excludendi alios*

Commento a Cass., S.U., 27 ottobre 2011, n. 4694

Roberto Flor[*]

Sommario: 1. Introduzione. – 2. Gli orientamenti interpretativi della giurisprudenza di legittimità. – 3. Il principio espresso dalla sentenza delle Sezioni Unite. – 4. Sulle condotte alternative dell'"introduzione abusiva" e della "permanenza non autorizzata". – 5. La portata del principio espresso dalle Sezioni Unite: "abuso" dei profili autorizzativi ed "abuso" di poteri da parte del pubblico ufficiale. – 6. Rilievi conclusivi.

1. Introduzione.

Con la sentenza del 27 ottobre 2011, n. 4694, le Sezioni Unite della Corte di Cassazione hanno risolto il contrasto giurisprudenziale relativo all'interpretazione dell'art. 615 ter c.p., aderendo alla tesi che individua, *de jure condito*, quale chiave di volta della fattispecie penale la "violazione" dello *jus excludendi* del titolare del sistema informatico: tale violazione esprime il disvalore essenziale del fatto, indipendentemente dai motivi

[*] Roberto Flor è ricercatore in diritto penale e professore aggregato di diritto penale dell'informatica presso la Facoltà di Giurisprudenza dell'Università di Verona. Sulla stessa sentenza delle Sezioni Unite si consenta il rinvio a R. Flor, *Verso una rivalutazione dell'art. 615 ter c.p.? Il reato di accesso abusivo a sistemi informatici o telematici fra la tutela di tradizionali e di nuovi diritti fondamentali nell'era di Internet* (in corso di pubblicazione in *Diritto penale contemporaneo*). Questo ultimo contributo analizza la fattispecie di cui all'art. 615 ter c.p. alla luce olre che della decisione delle Sezioni Unite anche delle fonti sovranazionali, tenendo in considerazione la nascita di "nuovi" diritti fondamentali nell'era di Internet e prospettando concrete soluzioni *de jure condendo*.

o dai propositi perseguiti dall'agente, dall'accesso reale a dati o informazioni e dalla loro natura, nonchè dal loro successivo utilizzo, trovando il reato consumazione nella realizzazione delle condotte tipiche e, con riferimento a quella di permanenza *invito domino*, nella violazione delle disposizioni del titolare.

La pronuncia ha confermato, salvo per quanto attiene al trattamento sanzionatorio, la sentenza della Corte di Appello di Roma del 19 maggio 2009 la quale, in parziale riforma della sentenza di primo grado del 16 ottobre 2007, ha affermato la responsabilità penale di un maresciallo dei carabinieri per il delitto di cui agli artt. 81, co. 2, e 615 ter, co. 2, n. 1, e co. 3 c.p.

Sulla base della ricostruzione dei fatti il pubblico ufficiale, utilizzando le proprie credenziali di autenticazione e di accesso, si era introdotto nel sistema informatico d'ordine pubblico e di sicurezza pubblica S.D.I., protetto da misure di sicurezza, per finalità diverse da quelle istituzionali.

La Corte di appello ha aderito all'orientamento espresso dalla sentenza della Corte di Cassazione del 30 settembre 2008, n. 1727 (Romano)[1], secondo la quale il delitto di cui all'art. 615 ter c.p. sanziona il fatto del pubblico ufficiale che, anche se abilitato a consultare il sistema informatico, si sia però introdotto «con abuso dei poteri o con violazione dei doveri inerenti la funzione o il servizio […] o con abuso della qualità di operatore del sistema».

I ricorsi in Cassazione proposti dagli imputati, fra cui il maresciallo dei carabinieri, sono stati assegnati alla V sezione penale la quale, con ordinanza depositata il 23 marzo 2011, rilevato il contrasto giurisprudenziale in merito all'interpretazione delle condotte tipiche, ha rimesso alle Sezioni Unite la seguente questione di diritto: «se integri la fattispecie criminosa di accesso abusivo ad un sistema informatico o telematico protetto la condotta di accesso o di mantenimento nel sistema posta in essere da soggetto abilitato, ma per scopi o finalità estranei a quelli per i quali la facoltà di accesso gli è stata attribuita». I giudici di legittimità hanno risposto affermativamente, attribuendo però rilevanza alla violazione oggettiva delle regole predisposte dal titolare dello spazio informatico e non, invece, alle finalità del soggetto agente.

[1] In *Cass. pen.*, 2010, 1, 155.

Abstract

The illegal introduction and unauthorised maintenance of an IT system in the recent sentence of the United Chambers. "Abuse" of the authorisation profiles, "abuse" of powers on behalf of public officials and violation of the jus excludendi alios.

The article discusses the hot topic of the improper access to a computer system as addressed by the latest Italian jurisprudence. The author dwells on the orientation of the most important concepts and then discuss the introduction of illegal and unauthorized access. In the last part of the article also discusses the abuse of power by public officials.

L'introduzione abusiva ed il mantenimento non autorizzato in un sistema informatico nella recente sentenza delle Sezioni Unite. "Abuso" dei profili autorizzativi, "abuso" di poteri da parte del pubblico ufficiale e violazione dello jus excludendi alios

L'articolo tratta del tema molto dibattuto dell'accesso abusivo a un sistema informatico o telematico come affrontato dalla più recente giurisprudenza italiana. L'autore si sofferma sugli orientamento più importanti per poi discutere dei concetti di introduzione abusiva e di permanenza non autorizzata. Nell'ultima parte dell'articolo si discute anche dell'abuso dei poteri da parte del pubblico ufficiale.

Ciberspazio e diritto 2012, Vol. 13, n. 44 (1-2012), pp. 121-132

Amministrazione "digitale"

L'effettività del diritto all'uso delle tecnologie nel Codice dell'Amministrazione Digitale. La sentenza del T.A.R. Basilicata n. 478/2011

Pasquale Lopriore[1]

Codice amministrazione digitale – Diritto all'uso delle tecnologie – Posta elettronica certificata (artt. 2, 3, 6, 54 comma 2 ter, del D.Lgs. n. 82/2005)

Massima

La mancata pubblicazione sulla home page del sito istituzionale di una pubblica amministrazione dell'indirizzo di posta elettronica certificata a cui il cittadino possa rivolgersi, ai sensi dell'art. 54 comma 2 ter, del D.Lgs. n. 82/2005 "Codice dell'amministrazione digitale" e dalle "Linee guida per i siti web della P.A. Anno 2010" del Ministero per la pubblica amministrazione e l'innovazione, comporta la violazione degli artt. 3, 6 e 54 della norma citata in quanto l'amministrazione è tenuta a consentire agli utenti di interloquire tramite posta elettronica certificata al fine di rendere effettivo il loro diritto a richiedere ed ottenere l'uso delle tecnologie telematiche.

La sentenza in commento è la prima che applica concretamente il diritto all'uso delle tecnologie da parte dei cittadini e imprese previsto dal D.Lgs. n. 82/2005 "Codice dell'amministrazione digitale" (da ora in poi CAD). Nel caso giunto al vaglio del TAR Basilicata il citato diritto emerge dalla mancata pubblicazione dell'indirizzo di posta elettronica certificata PEC sulla home page del sito istituzionale della Regione Basilicata.

[1] Avvocato esperto in Diritto delle tecnologie informatiche, si occupa di Gare d'appalto telematiche "E-procurement" all'interno della Divisione Informatica e Telematica di InnovaPuglia S.p.A., società in house della Regione Puglia. Componente del gruppo di lavoro di EmPULIA "Centrale di acquisto territoriale della Regione Puglia"

Tale sentenza, pertanto, offre l'occasione per analizzare, anche alla luce delle numerose modifiche subite dal CAD, l'effettività del diritto all'utilizzo delle tecnologie e le sue implicazioni con le altre disposizioni.

La norma chiave sulla base della quale il TAR ha condannato la Regione Basilicata a porre in essere gli adempimenti necessari alla pubblicazione dell'indirizzo PEC è l'art. 3 del CAD. Questo articolo sancisce che i cittadini e le imprese hanno diritto a richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni e con i gestori di pubblici servizi, ai sensi di quanto previsto dal CAD.

Da subito all'art. 3 del CAD è stata riconosciuta una portata innovativa[2], secondo alcuni studiosi un vero è proprio "nuovo diritto"[3] in quanto riconosce per la prima volta al cittadino il diritto ad ottenere forme innovative di partecipazione alla vita amministrativa e politica[4], assumendo in questo modo una posizione centrale quale titolare di una riconosciuta e tutelata pretesa nei confronti della Pubblica Amministrazione[5].

Questo diritto dei soggetti ad accedere agli strumenti informatici era stato già riconosciuto nel nostro ordinamento dalla legge n. 4 del 09/01/2004 "Legge Stanca", la quale afferma all'art. 1 che "La Repubblica riconosce e tutela il diritto di ogni persona ad accedere a tutte le fonti di informazione e ai relativi servizi, ivi compresi quelli che si articolano attraverso gli strumenti informatici e telematici."

Ben si comprende che la portata della Legge Stanca è molto più generale ed è inserita all'interno di un contesto differente, rappresentato dall'accesso dei soggetti disabili agli strumenti informatici.

Pertanto, il diritto all'accesso ai nuovi strumenti, riconosciuto dall'art. 4 della Legge Stanca, è stato rielaborato dal legislatore nella stesura del CAD, con riferimento all'informatizzazione della PA, in quan-

[2] Cfr. E. Belisario, La nuova pubblica amministrazione digitale, Maggioli, 2009.

[3] Cfr. M. Pietrangelo, Il diritto all'uso delle tecnologie nei rapporti con la pubblica amministrazione:luci ed ombre, *in Inf. Dir.* n.1/2005.

[4] Cft. Consiglio di Stato, adunanza del 7 febbraio 2005 Sezione 11995/04.

[5] Cfr. F. Camilletti, La responsabilità della pubblica amministrazione per violazione del diritto all'uso delle tecnologie, Federalismi.it *in Rivista di diritto pubblico italiano, comunitario e comparato*, n. 12/2008.

Abstract

The effectiveness of law on the use of technologies in the Digital Administration Code. The sentence issued by the Regional Administrative Court of Basilicata, No. 478/2011.

The article discusses the right to the use of technologies as outlined in the Italian digital administration code. In particular, the author addresses the issues of certified mail and regulatory developments that has characterized this tool from the point of view of legislative policy. The judgment under review is the first law that applies specifically to the use of technologies by citizens and corporations provided by the code of digital administration. The cited principle arises from the apparent failure to publish e-mail address of certified e-mail on the home page of the istitutional web site of the Region Basilicata.

L'effettività del diritto all'uso delle tecnologie nel Codice dell'Amministrazione Digitale. La sentenza del T.A.R. Basilicata n. 478/2011.

L'articolo tratta del diritto all'uso delle tecnologie come previsto nel codice dell'amministrazione digitale italiano. In particolare, l'autore affronta i temi della posta elettronica certificata e dell'evoluzione normativa che ha caratterizzato questo strumento anche da un punto di vista della politica legislativa. La sentenza in commento è la prima che applica concretamente il diritto all'uso delle tecnologie da parte dei cittadini e imprese previsto dal codice dell'amministrazione digitale. Il citato diritto emerge dalla mancata pubblicazione dell'indirizzo di posta elettronica certificata PEC sulla home page del sito istituzionale della Regione Basilicata.

Ciberspazio e diritto 2012, Vol. 13, n. 44 (1-2012), pp. 133-144

Diritto d'autore

Contrassegno SIAE e aspetti di legittimità: nota a Consiglio di Stato 2 febbraio 2012 n. 584

Maria Rosaria Basilone[1]

CONS. STATO Sez.VI, 02-02-2012, n. 584
Riforma Tar Lazio 24.11.2009, n. 11590

DIRITTI D'AUTORE - DISCIPLINA DEL CONTRASSEGNO DA APPORRE SUI SUPPORTI SIAE - LEGITTIMITÁ - IRRETROATTIVITÁ - (Direttiva 83/189/CE 28 marzo1983; Direttiva 98/34/CE 22 giugno 1998; D.P.C.M. 11 luglio 2001, n. 331; D.P.C.M. 25 ottobre 2002, n. 296; D.P.C.M. 23-02-2009 n. 31; L. 22.04.1941, n. 633, art. 181-*bis*; artt. 171-*bis*, I e II co. e 171 ter I co., lett.d; L. 18-08-2000, n. 248)

Deve ritenersi pienamente legittima l'apposizione del contrassegno Siae su tutti i supporti multimediali contenenti opere dell'ingegno protette dalla legge sul diritto d'autore, e ciò in quanto la prescrizione dell'apposizione del contrassegno risponde all'esigenza di tutelare non solo il diritto di autore in sé, ma anche gli operatori commerciali ed i consumatori dell'opera-esigenza tanto più avvertita a fronte dei diffusi fenomeni di "pirateria" e contraffazione. E il medesimo obbligo deve ritenersi esteso tanto alle opere prodotte e diffuse sul territorio nazionale, quanto a quelle in questo non originate ma che nel mercato interno abbiano diffusione.

La stessa giurisprudenza comunitaria ha chiarito che "in mancanza di normative comuni, gli ostacoli per la circolazione intracomunitaria derivanti da disparità delle legislazioni nazionali relative al commercio dei prodotti di cui trattasi vanno accettati qualora tali prescrizioni, che si applicano indistintamente ai prodotti nazionali e a quelli importati, possa-

[1] Avvocato del Foro di Roma.

Abstract

The SIAE watermark and aspects of legitimacy: note to the Council of State, 2nd February 2012 No. 584.

This article deals with the discipline of the SIAE and of countersigns on the copyright works and some aspects of legitimacy. In particular, the author moves from the general rules and then comment the specific case. The main principle of the judgment is that must be held fully legitimate affixing the SIAE countersign on all media containing works protected by copyright law, especially because the requirement of affixing the countersign responds to the need to protect not only the copyright itself, but also traders and consumers of the work. And the same obligation must be considered extended to works produced and disseminated throughout the Country.

Contrassegno SIAE e aspetti di legittimità: nota a Consiglio di Stato 2 febbraio 2012 n. 584.

In questo articolo si tratta della disciplina del contrassegno SIAE e di alcuni aspetti di legittimità. In particolare, l'autore muove dalla disciplina generale per poi commentare il caso concreto, ossia l'apposizione del contrassegno su supporti multimediali contenenti opere dell'ingegno. Il principio cardine della sentenza commentata è che deve ritenersi pienamente legittima l'apposizione del contrassegno Siae su tutti i supporti multimediali contenenti opere dell'ingegno protette dalla legge sul diritto d'autore, e ciò in quanto la prescrizione dell'apposizione del contrassegno risponde all'esigenza di tutelare non solo il diritto di autore in sé, ma anche gli operatori commerciali ed i consumatori dell'opera, esigenza tanto più avvertita a fronte dei diffusi fenomeni di "pirateria" e contraffazione. E il medesimo obbligo deve ritenersi esteso tanto alle opere prodotte e diffuse sul territorio nazionale, quanto a quelle in questo non originate ma che nel mercato interno abbiano diffusione.