ISSN: 2281-5147

Opinio Juris in Comparatione

Studies in Comparative and National Law

Op. J., Vol. I, n. I/2014

La Gestione di Data e Meta-Data nel *Cloud Computing*: Profili di Proprietà Intellettuale e Questioni di *Privacy*

by

Giulia Schneider

www.opiniojurisincomparatione.org

LA GESTIONE DI DATA E META-DATA NEL *CLOUD COMPUTING*: PROFILI DI PROPRIETÀ INTELLETTUALE E QUESTIONI DI *PRIVACY*

by

Giulia Schneider *

Abstract:

The paper examines the controversial issue of the legal qualification of the information stored on a cloud computing system, and the tension that is likely to arise between the intellectual property regime of protected material flowing through the cloud-platforms and the legal protection of the privacy of cloud consumers, who are more and more relying on such kind of technology as a means of distributing and accessing to protected data.

On the cloud, the conflict between the two legal schemes, and the two legal rights, appears to be much more serious than it was in the pre-digital area, given the peculiar generative nature of the information stored on the cloud: in fact, the duty to control that the usage rights gained by the end user are not violated, encourages a systematic control over the users activities, that leads to surveillance and monitoring practices by means of which the service-providers collect an enormous amount of a specific type of personal meta-data, or secondary data, directly stemming from the primary data of information protected by IP rights, and more specifically directly deriving by the use that consumers make of the accessed intellectual property data.

Three are the control points examined, related to technological protection measures arranged by the providers restricting access to protected material, secondly restricting the usage of it, and thirdly relating to self-help protection measures, assuring adequate reaction against violations of the first two protection parameters, by means of arbitrary cancellations or eventual locking out of users who are intended to create or distribute by the means of the cloud certain kinds of contents or formats.

We will at first focus on the impact of the access measures on the intellectual property regime with specific regards to the European digital copyright and the US fair use doctrine, secondly on the repercussions of the usage controls on the privacy standards.

*Giulia Schneider is undergraduate law student at Sant'Anna School of Advanced Studies in Pisa.

On the one side, the arrangement of access control points enables the providers, and through the cloud providers, also the IP holders to "opt out those parts of the copyright system they dislike"[1].
Furthermore, the centralized structure of the cloud platforms and the verticalization of the digital interaction between users enable the providers to act not only as processors of the protected material, but also as controllers of the amount of personal information directly arising from it, profiling cloud-consumers on the basis of their intellectual inclinations, habits and preferences, in that what some doctrine has defined as a big database of intention.

Ultimately, through the lenses of intellectual property right's safeguard, it becomes clear how in the cloud the right to privacy is jeopardised in the moments of monitoring and surveillance, which determine the loss of control over the personal metadata.

However, another wider significance of privacy directly related to the liberty of self-determination is shown to be affected. In fact the overprotection of works through technical protection measures, obscures the horizon of personal decisional possibilities, by extinguishing fair usages and free possibilities of developing content (collective works, derivative works).

Keywords:
Cloud computing, intellectual property rights, privacy, cloud consumers, monitoring, meta-data, technological protection measures, digital copyright, fair use doctrine, profiling.

1 J. H. REICHMAN (a cura di), *A Reverse Notice and Takedown Regime to Enable Public Interest Uses of Technically Protected Copyrighted Works*, 22 Berkeley Tech. L. J. 981, 988, 995 (2007), 1023.

TABLE OF CONTENTS:

I. INTRODUZIONE

Arduo risulta il tentativo di individuare le coordinate giuridiche per mezzo delle quali qualificare e dunque in parte prevedere, i risvolti sul piano del diritto della nuova tecnologia del *cloud computing*. In questo contesto, come soprattutto la dottrina d'oltreoceano[2] rileva, una delle aree più nebulose rimane proprio quella della proprietà intellettuale, là dove il servizio del *cloud computing* si scopre svincolo di immagazzinamento, elaborazione, e ancora, di vera e propria produzione di dati, da un lato meritevoli di ricevere idonea protezione mediante l'individuazione e l'*enforcement* di diritti di esclusiva riferiti a quella porzione di patrimonio informativo da considerarsi *invenzione industriale*, ovvero *opera dell'ingegno,* dall'altro aventi verosimilmente ad oggetto informazioni personali relative alle modalità d'uso del servizio da parte del *consumer,* di considerevole valore per terze parti e fonte di potenziale guadagno per il *provider* stesso.

La copiosa letteratura relativa all'analisi dei benefici[3] e dei rischi[4] proprie delle piattaforme informatiche di *cloud computing*, non fa che prendere atto della incipiente diffusione di simile tecnologia[5], apprezzabile in relazione ai differenti modelli di business[6] cui essa dà vita[7].

In particolar modo secondo alcuni[8], il principale impatto dell'affermarsi dei servizi in questione sarebbe quello di una sostanziale trasfigurazione della fisionomia dello stesso *web* 2.0, che, da orizzontale, aperto ed eccentrico, sarebbe venuto ad assumere i tratti di una infrastruttura chiusa, contrassegnata da barriere, relative non solo all'accesso, ma anche alla fruizione degli stessi contenuti protetti.

---

2 *Ex multis* si veda in particolar modo HORACIO E. GUTIERREZ, *Peering Through the Cloud: The Future of Intellectual Property and Computing*, 20 Fed. Cir. B.J. 589; PATRICK J. LAYCOCK, *A brief overview of intellectual property issues "in the cloud",* pubblicato online il 16 novembre 2011 su http://www.smart-biggar.ca/en/articles_detail.cfm?news_id=535 ; MARC AARON MELZER, *Enforcing copyright in the cloud,* 21 Fordham Intell. Prop. Media & Ent. L.J. 403; ANNE C. DATESH, *Storms brewing in the cloud: why copyright law will have to adapt to the future of web 2.0,* in 40, 4 Aipla Quaterly J., 685 (2012); TIMOTHY D. MARTIN, *Hey! you! Get off of my cloud: defining and protecting the metes and bounds of privacy, security, and property in cloud computing,* reperibile online su http://works.bepress.com/timothy_martin/3; MARK. H. WITTOW-DANIEL J. BULLER, *Cloud Computing, emerging legal issues for access to data, anywhere, anytime,* in 14, 1 Journal of internet Law, 1 (2010).

3 Sul punto C. YOO, *Cloud Computing, Architectural and Policy implications,* (2011), 9-10, reperibile all'indirizzo http://www.techpolicyinstitute.org/files/yoo%20architectural_and_policy_implications.pdf,

4 *Ex multis* si veda in particolar modo il risultato della ricerca dello European Network and Security Agency (ENISA) pubblicato nel novembre 2009, *Cloud Computing, Benefits, Risks and Recommendations for Information Security.* In ambito italiano, preziose le indicazioni fornite dal Garante per la protezione dei dati personali in *Cloud Computing: indicazioni per l'utilizzo consapevole dei servizi,* reperibile online all'indirizzo http://www.garanteprivacy.it/documents/10160/10704/1819933.

5 Cfr. EXPERT GROUP REPORT, *The Future Of Cloud Computing*, rapporto redatto per la Commissione europea, 2010, reperibile online all'indirizzo http://cordis.europa.eu/fp7/ict/ssai/ docs/cloud-report-final.pdf

6 J. NICHOLAS HOOVER, *Compliance in the Ether: Cloud Computing-Data Security and Business Regulation,* 8 J. Bus. & Tech. L. 255 (2012).

7 Varia è difatti la fenomenologia dei servizi di *cloud* sul piano dei modelli di *business* possibili: accanto a "modalità *in house* per i propri servizi *cloud,* non rari sono i casi in cui le industrie interessate delegano ai terzi *providers* l'attività di archiviazione e gestione dei dati su una piattaforma virtualizzata in rete, che diviene così vera e propria appendice operativa nella forma di database informativo. Sul punto significativo il contributo di A. MANTELERO, *Processi di outsourcing informatico e cloud computing: la gestione dei dati personali ed aziendali,* in *Diritto dell'informazione e dell'informatica*, 24, 4-5, 2010, 673 ss.. Si sofferma sulla complessità di quelle che divengono delle vere e proprie reti di *outsourcing,* nel caso in cui sia lo stesso *cloud provider* a fare ricorso a dei *sub providers,* e sul rischio che esse comportano in relazione alla custosia dei dati, J. NICHOLAS HOOVER, *op. cit.,* 3.

8 Questa la tesi di D. LAMETTI, *The Cloud, Boundless Digital Potential or Enclosure 3.0?,* pubblicato il 5 giugno 2012, reperibile online all'indirizzo http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2077742 e ID., *Cloud Computing, Verso il terzo enclosure movement?,* in *Rivista Critica del diritto privato,* 3, 3, 2012, 363 ss.

La duplice caratteristica di luogo virtuale di orizzontale condivisione di dati tra plurimi *end users*[9], ha infatti come effetto quello di creare database, atti, in virtù della non più limitata capacità computazionale, ad immagazzinare un incommensurabile patrimonio informativo, il quale in virtù della contestuale gerarchica dipendenza che si viene ad instaurare nelle relazioni -economiche e contrattuali- tra gli stessi consumatori ed i *provider* del servizio *cloud,* può divenire oggetto di facili abusi[10], da parte di chi, indipendentemente dalla ancora poco chiara questione di chi sia effettivo titolare dei diritti sui dati archiviati, o ancora, processati nel *cloud*[11], ne possiede sicuramente il controllo in virtù del compito di gestione (*i.e. s*toccaggio ed elaborazione) dei medesimi affidato dai *content providers* ai medesimi *service providers.*

La dimensione che abbiamo definito verticale mette a repentaglio il beneficio della condivisione orizzontale: la dipendenza dal servizio rischia di tradursi in vulnerabilità contrattuale del *cloud consumer,* rispetto alle decisioni del *provider,* non solo in termini di innalzamento dei costi[12], bensì anche anche in riferimento alla creazione di vere e proprie incompatibilità tecnologiche, con pregiudizio della libertà di condivisione, là dove potrà essere condiviso solo ciò che il provider consente[13].

La restrizione dei margini di manovra del singolo utente in relazione alla individuazione dell'oggetto, nella forma e nel contenuto, delle informazioni che possono essere "immesse" nella nuvola, nonché alle modalità di utilizzo (ad esempio l'impossibilità di modificare o disporre i contenuti in un certo modo), e di successivo trasferimento, se non anche conversione, a differenti tipologie di servizi di condivisione digitale, risulta determinata *ex ante* dalla peculiare interazione[14] tra architettura tecnologica[15] e corrispondente assetto contrattuale[16].

---

9 In via puramente generale è possibile individuare due categorie di *cloud users,* identificabili da un lato nel singolo individuo, e dall'altro nelle imprese che divengono utenti *cloud* per ragioni di riduzione dei costi e per la corrispondente necessità di investire nel proprio *core business.* Cfr. A. MANTELERO, *op. cit.,* 674.

10 Cfr. in particolare P. T. JAEGER, J. LINN, J. M. GRIMES (2008), C*loud computing and Information Policy: Computing in a policy cloud?,* Journal of Information Technology & Politics, 5:3, 269-283.

11 C. REED, *Information ownership in the cloud,* Queen Mary University of London, School of law, Research Paper n. 45/2010, reperibile online all'indirizzo http://ssrn.com/abstract=1562461.

12 Cfr. D. LAMETTI, *The Cloud, Boundless Digital Potential or Enclosure 3.0?,* cit., *passim.* Lo stesso successivo innalzamento dei costi da parte del *cloud provider* dovrà essere sopportato dal consumatore là dove questi risultino comunque inferiori agli eventuali *switching costs* di riconversione. In questo senso anche R. CASO, *Relazione introduttiva, Forme di controllo delle informazioni digitali: il digital rights management,* in R. CASO (a cura di), *Digital Rights Management, problemi teorici e prospettive applicative, Atti del convegno tenutosi alla facoltà di giurisprudenza di Trento il 21 e 22 marzo 2007,* 25 ss.

13 Questione ben sintetizzata nella formula di D. LAMETTI "users move from sharing to being shared". ID., *op. ult. Cit.,* 9.

14 Come noto, la tesi per cui alle infrastrutture tecnologiche è da assegnare valore di vero e proprio codice, che necessita di essere recepito anche sul piano normativo, sotto forma di regole giuridiche, è da ascrivere a L. LESSIG in *Code and other laws in cyberspace,* New York, 1999. Sottolineano al contrario la necessità di rimarcare la differenza tra regole informatiche e giuridiche, E. DOMMERING, *Regulating Technology: code is not law,* in E. DOMMERING. L. F. ASSCHER (a cura di), *Coding Regulation: Essays on the normative Role of Information Technology,* The Hague, TMC Asser Press, 10 ss.; per la dottrina italiana si vedano le posizioni di R. CASO, *Un rapporto di minoranza: elogio dell'insicurezza informatica e della fallibilità del diritto d'autore: note a margine del trusted computing, in* R. CASO (a cura di), *Sicurezza informatica: regole e prassi - Atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento il 6 maggio 2005*, Trento, 2006, 5, 44-45.

15 Si rimandi ancora a C. YOO, *Cloud Computing, Architectural and Policy implications, cit.,* 9-10.

16 Per un approfondimento sia consentito il rimando a R. CASO, *Il digital Rights Management, il commercio delle informazioni digitali tra contratto e diritto d'autore,* CEDAM, Padova, 2004, 59 ss.. Si veda inoltre ID., *Relazione introduttiva, Forme di controllo delle informazioni digitali: il digital rights management,* in R. CASO (a cura di), *Digital Rights Management, problemi teorici e prospettive applicative,* Atti del convegno tenutosi alla facoltà di

Essa è tuttavia percepibile anche *ex post* nella perdita del controllo sui dati trasmessi ai terzi *provider,* con notevoli risvolti nel caso in cui tali medesimi dati rilevino (anche) alla stregua di informazioni personali[17].

Accogliendo in questa sede la tesi che ravvede nella tecnologia di *cloud computing* il motore di un terzo movimento di *Enclosure*[18]*,* risulterà come l'utente appaia essere condannato ad una restrizione della libertà di autodeterminazione[19], rilevabile su due distinti piani, da ricollegarsi rispettivamente alla duplice dimensione *micro-* e *macro-cosmica* del servizio *cloud*: da un lato la struttura, e le barriere interne al singolo servizio, dall'altro la infra-struttura, con le rispettive barriere, della dimensione digitale nel suo complesso, come modellata dall'avvento della nuova tecnologia.

In primo luogo si può pertanto individuare una diretta incidenza su due diritti riconosciuti sul suolo europeo come fondamentali[20]: quello di privativa sulle opere frutto di "creazione intellettuale"[21], e quello alla protezione dei dati personali, rilevante non solo dal punto di vista prettamente *informazionale*[22]*,* ma anche sotto il profilo *decisionale*[23]*,* là dove anche nella infrastruttura della nuvola possono riprodursi le

---

giurisprudenza di Trento il 21 e 22 marzo 2007*,* 31, in cui l'A. mette in evidenza come uno dei maggiori esiti della digitalizzazione dell'informazione sia proprio quella della standardizzazione dei contratti e "ad essere espresso in linguaggi (che rispondono a loro volta a standard tecnologici) destinati alle macchine".

17 Si pensi al caso delle informazioni aziendali rilevanti sia in quanto dati personali, protetti nell'interesse del soggetto cui si riferiscono, nonché in quanto informazioni riservate, tutelate mediante lo strumento del segreto aziendale. Cfr. A. MANTELERO, *op. cit.,* 678.

18 Sul punto D. LAMETTI, *op. ult. Cit.,* 365: il c.d. secondo movimento di *enclosure* viene invece individuato sul piano normativo, nelle previsioni in materia di *digital copyright,* quali i Trattati WIPO ovvero lo *US Digital Copyright Millennium Act;* e, sul piano tecnologico, nella messa a punto delle *Technological Protection Measures* (*TPMs*), le quali hanno il principale effetto di diminuire o restringere i punti di accesso alle idee del *public domain.* Cfr. J. BOYLE, *The Public Domain, Enclosing the Commons of the mind,* London, 2008, 15 ss.. Per un'analisi delle disposizioni in materia di *digital copyright* si veda *infra* §2.

19 Vi fanno riferimento in particolar modo D. J. GERVAIS- D. J HYNDMAN, *Cloud control: copyright, global memes and privacy,* 10 J. on Telecomm. & High Tech. L. 53 2012*,* 62 ss.; Sul punto si veda anche R. CASO, *Il digital Rights Management, il commercio delle informazioni digitali tra contratto e diritto d'autore, cit.,*105 ss.; e anche A. PALMIERI, *Digital Rights Management e disciplina europea della protezione dei dati personali,* in R. CASO (a cura di), *Digital Rights Management, problemi teorici e prospettive applicative,* cit.*,* 198 ss.

20 Il diritto sui dati personali è contemplato all'art. 8 della Carta dei diritti Fondamentali dell'Unione Europea. Si ricordi inoltre come la relazione di accompagnamento al Codice in materia di protezione dei dati personali qualifica tale diritto come "diritto fondamentale della persona, autonomo rispetto al più generale diritto alla riservatezza già richiamato dall'art. 1 della legge 675/1996". Per quanto riguarda il diritto di proprietà intellettuale, esso è stato preso in considerazione dalla giurisprudenza comunitaria nel caso *Laserdisken* della Corte di Giustizia 12 settembre 2006, causa 479/04, in *Racc.* 2006, I-8089, punto 65 e parimenti contemplato nella medesima Carta dei diritti Fondamentali all'art. 17.2. Per la dottrina si rimandi a A. OTTOLIA, *Proprietà intellettuale e trattamento dei dati personali: riflessioni su privacy per il sistema e nel sistema,* in *Aida, Annali italiani del diritto d'autore, della cultura e dello spettacolo,* XIX, 2010, 325 ss.

21 Si ricordi come a seguito la decisione della *ECJ Infopaq International A/S v Danske Dagblades Forening* (C-5/08) [2009] E.C.R. I-6569 (ECJ (4th Chamber))*,* si sia dato inizio ad un importante processo di armonizzazione avente ad oggetto la nozione di "opera", da considerarsi "author's own intellectual creation", approccio distante dal parametro inglese *dell'originality* comprensivo delle criteri di *labour, skill,* and *judgment.* Sul punto si vedano i commenti di E. ROSATI, *Originality in a work, or work of originality: the effects of the Infopaq decision,* in European Intellectual Property Review, 2011, 33, 12, 746-755.

22 Relativo cioè al controllo, o per quel che in questa sede rileva, alla perdita di controllo sui dati salvati sulla nuvola. Questa la prospettiva prevalentemente trattata da R. CASO, *op. ult. cit.,* 103 ss. Simile accezione di privacy è da ricondursi concettualmente alla libertà negativa del *right to keep other out,* cui fa riferimento V. MAYER-SCHOENBERGER, *Beyond copyright: managing information Rights with DRM,* 84, Den. Univ. L. Rev., 181, 189 (2006).

23 Questo il profilo messo in luce da P. GUARDA, *Privacy e fruizione della conoscenza scientifica,* in R. CASO (a cura di), *Pubblicazioni scientifiche, diritti d'autore e open access,* Atti del Convegno tenutosi alla Facoltà di Giurisprudenza di Trento il 20 giugno 2008, 99 ss. ; e A. PALMIERI, *op. cit.,* 198 ss.

condizioni per un monitoraggio da parte del *cloud provider* attuantesi nella forma di *profiling*[24], che a sua volta ha l'effetto di suggestionare la costruzione della identità virtuale del singolo[25].

In secondo luogo simile restrizione della libertà di autodeterminazione digitale, del singolo si osserva, più in generale, sul piano concorrenziale, nella stessa compressione della "libertà delle persone nell'uso dei mezzi di comunicazione elettronica"[26], derivante dalla eventuale (e verosimile[27]) violazione da parte del provider dell'obbligo di assicurare "(...) l'interoperabilità dei servizi di tutta l'Unione europea"[28], condizione della c.d. *portabilità* dei dati da una nuvola all'altra.

Attraverso l'analisi del primo dei profili evidenziati, il contributo intende indagare, sul piano teorico, la applicabilità al sistema digitale della nuvola, delle tradizionali categorie dei diritti di proprietà intellettuale e dei diritti sui dati personali, sotto il profilo sia della qualificazione, sia *dell'enforcement,* ed in una prospettiva maggiormente operativa, vagliare i possibili modelli di gestione comune dei dati virtualmente immagazzinati.

II. LE RESTRIZIONI ALL'ACCESSO E ALLA FRUIZIONE DEI CONTENUTI: DIGITAL COPYRIGHT E FAIR USE

Il pendolo ha forse smesso di oscillare. Si è cioè forse compiuto quel graduale processo di passaggio da una soluzione di controllo della fruizione dei contenuti protetti da parte degli stessi consumatori, per mezzo di dispositivi tecnologici, o meno, posti sotto la diretta supervisione di questi, ad una soluzione diversamente "mediata", in virtù della quale i contenuti sono resi accessibili unicamente tramite un *provider* intermediario, che ne regola la distribuzione e il godimento consentito agli *end users*[29]. In questo processo, un ruolo decisivo è da ascrivere all'insorgere delle piattaforme di condivisione di *cloud*

24 Consistente nella catalogazione dei dati personali degli *end users,* corrispondenti agli interessi commerciali dei medesimi, non solo in modo da controllare la gestione del contenuto digitale, di modo da imporgli e se del caso sanzionare le attività a questi consentiti in virtù degli *usage rights* acquisiti, bensì con l'effetto di poter commercializzare lo stesso profilo dell'utente. Così P. GUARDA, *op.cit.,* 102-103. A scopo esemplificativo si possono ricordare le attività oltremodo invasive di *profiling* svolte da *Google Scholar* e da *Google Books*, ricordate da O.TENE, *What Google Knows: Privacy and Internet Service Engines* (ottobre 2007), reperibile all'URL <http://ssrn.com/abstract=1021490>. Sul punto di veda *infra* §3.

25 E' quanto nella dimensione tradizionale del web avviene in virtù dei cosiddetti marcatori elettronici, altresì conosciuti come *cookies.* Analizza le implicazioni di tali dispositivi sulla sicurezza dei dati personali, A. MANTELERO, *Si rafforza la tutela dei dati personali: data breach notification e limiti alla profilazione mediante i cookies,* in *Dir. Dell'informazione e dell'informatica,* 4-5, 2010, 781 ss. Sul punto si veda *infra* §3.1.

26 Art. 3, 1 comma del Codice delle Comunicazioni elettroniche come modificato dal d.lgs. 70/2012 recettivo della direttiva 2009/140/CE.

27 Sul punto LAMETTI, *op. ult. cit., passim.* Si veda anche S. AHMED, *Data portability: Key to cloud Portability,* reperibile online all'indirizzo http://ssrn.com/abstract=1712565.

28 Art. 41 del Codice delle Comunicazioni elettroniche.

29 Il riferimento è al *product-service pendulum* teorizzato da J. ANDERSON, *Stream Capture: Returning Control of Digital AIusic to the Users*, 25 HARV. J.L. & TECH. 159, 167 (2011).

computing: la convenienza del ricorso a simile servizio sembra in effetti assumere dimensioni davvero notevoli in relazione alla particolare aderenza dei diritti d'autore alla infrastruttura tecnologica del *cloud,* come emergente anche dall'analisi delle previsioni normative in materia.

Se infatti la normativa tradizionale in materia di diritto d'autore è da più parti vista entrare in crisi con l'avvento delle nuove tecnologie informatiche[30], le più recenti risposte derivanti dal fronte legislativo sono da rinvenirsi nelle discipline di *digital copyright,* concettualmente costruite attorno ad una determinata *species* di violazione del *copyright,* non più costituita dal classico *infringement for copying,* bensì dall'aggiramento dei lucchetti digitali posti in essere dalle cosiddette *technological protection measures* (*TPM*), e dalla conseguente illecita fruizione, ovvero diffusione, dei contenuti protetti[31]. Più specificamente tale *corpus normativo* fornisce una regolamentazione, nonché tutela giuridica di tali misure tecnologiche, sanzionando l'aggiramento delle medesime mediante dispositivi specificamente prodotti a tale scopo[32].

Di seguito si procederà dunque ad una analisi delle possibili ripercussioni sulla libertà di espressione derivanti dall'applicazione al servizio di *cloud computing* di una simile normativa[33], con specifica attenzione all'impatto che questa può avere sulla validità delle eccezioni al diritto d'autore normativamente previste: come sarà infatti dimostrato, la tutela normativa offerta alle misure di protezione tecnologiche, rischia di vanificare i limiti originariamente posti alla tutela delle opere dell'ingegno[34].

Le fondamenta di simile questione sono da ricercarsi in alcune disposizioni del DMCA[35], ove si rinviene la distinzione tra misure di protezione tecnologica che controllano l'accesso all'opera (*access control*), e misure che proteggono i diritti d'autore (*usage control*).

E' d'uopo osservare come il documento sanzioni esplicitamente solo il raggiro della prima tipologia di misure: la ragione del silenzio in relazione alla seconda è da ricercarsi nella applicabilità in questi casi delle tradizionali previsioni in materia di *copyright*[36], e più precisamente nel fatto che la violazione delle

30 Sul punto si veda nello specifico J.C. GINSBURG, *the author's place in the future of copyright,* 5 Willamette L. Rev. 381 2008-2009, e riguardo al tramonto nell'era del *semantic web* dell'equazione di corrispondenza tra un'opera ed il suo autore, si rimandi a EVAN D. BROWN, *Symposium: internet expression in the 21st century: where technology and law collide: copright on the semantic web: divergence of author and work,* 19 Widener L.J. 829 (2010)

31 Sul punto S. BECHTOLD, *Digital Rights Management in The United States and in Europe,* in *The American Journal of Comparative Law,* 52, 2, 2004, 323-382, 339: "anticircumvention law has little to do with traditional copyright law. They represent a paracopyright law, that deals with controlling the use of and access to arbitrary data, which may or not be protected by copyright law. Furthermore, unlike traditional copyright law, which mainly regulates individual *conduct,* anti-circumvention regulations shift the focus of protection to controlling the production of devices. As in many other areas of Internet law, a trend towards indirect regulation is apparent".

32 Così S. BECHTOLD, *op. cit.,* 331. Nel panorama internazionale sia sufficiente ricordare l'art.11 del *WIPO Copyright Act* e l'art. 18 del *WIPO Performances and Phonogram Treaty*.

33 Numerose sono tuttavia anche gli effetti in materia di antitrust. Sul punto si veda R. CASO, *Il signore degli anelli nel cyberspazio: controllo delle informazioni e Digital Rights Management,* in M. MONTAGNANI- M. BORGHI (a cura di), *Proprietà digitale. Diritti d'autore, nuove tecnologie e Digital Rights Management,* Milano, 2006, 109, *passim.*

34 Cfr. R. CASO, *Digital Rights, Management, Il commercio delle informazioni elettroniche tra contratto e diritto d'autore, cit.,* 91.

35 17 U.S.C. §§1201-1205 DMCA.

36 Si veda *Chamberlain Group, Inc., v. Skylink Technologies, Inc.,* 381 F.3d 1178 (Fed. Cir., Aug. 31, 2004).

misure di protezione poste a salvaguardia degli *usage rights* potrebbe non raramente coincidere con le eccezioni di *fair use* opponibili nei casi di tradizionale *copyright infringement*[37].

Molto complessa appare invece la questione del *fair use* in relazione alle misure poste a protezione dell'*access control.* A questo proposito taluna dottrina[38] ha osservato come nonostante il DMCA provveda a tipizzare le ipotesi di libera utilizzazione[39], prendendo dunque le distanze dal carattere originariamente flessibile del principio del *fair use,* i titolari di diritti di esclusiva potrebbero comunque restringere la altrimenti legittima fruizione di contenuti protetti, proprio attraverso l'applicazione di misure di protezione tecnologiche di *access control*[40], e per quel che in questa sede rileva dunque proprio mediante il ricorso ad infrastrutture tecnologiche di *cloud computing*[41].

In questa prospettiva le previsioni in territorio europeo sembrano innalzare in misura ancora maggiore lo standard di tutela del diritto d'autore, là dove l'art. 6 della Direttiva 2001/29/CE *sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione,* si riferisce *in generale*[42] "all'elusione di efficaci misure tecnologiche"[43] , e l'art. 5, in materia di *eccezioni e limitazioni*[44], prevede al secondo comma che "gli stati membri *hanno la facoltà* (ma dunque non sono obbligati) di disporre eccezioni (..)". Del resto, proprio sulla base dell'art. 6, 4 comma della medesima direttiva, è stato formulato l'art. 71 *sexies,* relativo all'eccezione di copia privata[45]. A seguito della riforma avvenuta nel 2003[46], secondo il comma primo dell'articolo in questione, la copia privata rimane sì possibile se effettuata "da persona

37 Come ricorda S. BECHTOLD, *op. cit.,* 335 v. nota 45.

38 G. JIANG, *Rain or Shine: Fair and other non infringing uses in the context of cloud computing,* 36 J. Legis. 395 (2010), 340 ss.

39 Numerosissime sono state le critiche volte dalla critica americana a tale impostazione. Per tutti si veda J. E. COHEN,*WIPO WIPO Copyright Treaty Implementation in the United States: Will Fair Use Survive?*, in EIPR 1999, 236 ss.

40 Si veda J. H. REICHMAN (a cura di), *A Reverse Notice and Takedown Regime to Enable Public Interest Uses of Technically Protected Copyrighted Works*, 22 Berkeley Tech. L. J. 981, 988, 995 (2007), 1023, in cui si nota il rischio che "copyright owners gain the power to opt out those parts of the copyright system they dislike". *Contra* si vedano le tesi di quella dottrina che sostiene che le misure tecnologiche di protezione, che mettono in atto meccanismi di controllo automatici e pertanto inflessibili, non potranno mai essere in grado di prevenire del tutto gli utilizzi *leciti* del materiale protetto, in quanto quello del *fair use* rimane comunque uno standard per sua natura flessibile, insuscettibile di essere pre-programmato in una misura tecnologica. L'applicazione di MTP di *access control* potrebbe comunque avere il vantaggio di fissare dei margini più precisi allo standard di *fair use. "*Consumers would also benefit because they can develop precise expectations about what uses are and are not allowed and determine if such uses are worth the price", così J. GRIMMELMAN, *Regulation by Software*, 114 Yale L.J. 1719, 175253 (2005).

41 La tecnologia di *cloud computing* sarebbe infatti da considerarsi interamente riconducibile ad una misura di protezione tecnologica di *access control ex* s. 1201(a). così G. JIANG, *Rain or Shine: Fair and other non infringing uses in the context of cloud computing,* cit., 348.

42 E' tuttavia necessario ricordare come non sia in alcun modo estranea alla riflessione europea la distinzione tra le tecniche di controllo dell'accesso e di utilizzo dei contenuti protetti, ed i corrispondenti diritti di accesso e di controllo che sia il legislatore, sia la dottrina ha inteso ascrivere separatamente in capo agli utenti. , lo ricorda R. CASO, *Digital Rights, Management, Il commercio delle informazioni elettroniche tra contratto e diritto d'autore,* cit., 93. "In un sistema di DRM, l'utente non esaurisce il suo interessa nell'accesso, ed anzi si preoccupa maggiormente di quello che potrà fare, successivamente all'accesso, con lo stesso contentuo", *ibid.,* 97. Prendendo in considerazione il diritto di accesso, il legislatore europeo vi fa espressa menzione all'art. 6 della direttiva 2001/29/CE, mentre nella direttiva 98/84/CE sulla tutela dei servizi ad accesso condizionato e dei servizi di accesso condizionato, si trova la nozione di accesso condizionato. Per la discussione dottrinale relativa ai diritti d'accesso sia sufficiente il rimando a A. PALMIERI- R. PARDOLESI, *Gli access contracts: una nuova categoria per il diritto dell'era digitale,* in *Riv. Dir. Priv.,* 2002, 265.

43 Art. 1 e 2. Cfr. R. CASO, *Il signore degli anelli nel cyberspazio: controllo delle informazioni e Digital Rights Management,* cit., 157.

44 L'unica ipotesi obbligatoria di libera utilizzazione obbligatoria prevista dalla direttiva è il caso degli atti di riproduzione temporanea privi di rilievo economico proprio che sono transitori o accessori, e parte integrante e essenziale di un procedimento tecnologico, eseguiti all'unico scopo di consentire, a) la trasmissione in rete tra terzi con l'intervento di un intermediario o b) di un utilizzo legittimo di un'opera o di altri materiali.

45 Sul tema si rimandi in generale a D. GALLETTI, *Le utilizzazioni libere: copia privata,* in AIDA, 2002, 146 ss..

46 Cfr. d.lgs 9 aprile 2003 n. 68.

fisica per uso esclusivamente personale, purché senza scopo di lucro e senza fini direttamente o indirettamente commerciali", ma *unicamente* se le norme tecnologiche di cui all'art. 102 *quater* lo consentono[47].

Qualora le misure di protezione tecnologica siano programmate in modo da impedire l'accesso a specifici contenuti, è evidente come le stessa possano fungere da ostacolo a qualsiasi forma di utilizzo, comprese quelle che la legge consente[48]. Le ricadute di un simile assetto devono essere evidenti anche per quanto riguarda la fruizione di opere non protette, o perché non presentano quei requisiti cui la legge subordina la protezione, o perché cadute nel pubblico dominio[49].

Ad una lettura attenta della direttiva, la applicabilità delle "eccezioni e limitazioni" ai diritti d'autore previste all'articolo 5, sembra poter essere addirittura del tutto esclusa *ex* comma 4 del paragrafo 4 dell'art.6, nel caso in cui le opere ed i materiali protetti siano distribuiti al pubblico mediante servizi *on demand,* quali il *cloud computing,* quando cioè "sulla base di *clausole contrattuali*[50] (…) i componenti del pubblico possono accedere a dette opere e materiali dal luogo e nel momento scelti individualmente"[51]. E' stato acutamente notato come la lettera di simile norma non preveda nemmeno la necessità di una esplicita deroga contrattuale alle eccezioni e limitazioni applicabili alle misure tecnologiche[52].

1. LE RESTRIZIONI ALL'ACCESSO E ALLA FRUIZIONE DEI CONTENUTI: LE SORTI DEL FAIR USE E DELLA LIBERTÀ DI ESPRESSIONE SULLA NUVOLA NELL'ECLISSI DEL DIRITTO D'AUTORE TRADIZIONALE

Alla luce di simili previsioni normative si capisce dunque come il *cloud computing* fornisca una struttura particolarmente rassicurante per i titolari di diritti di privativa[53], là dove le informazioni protette

47 Si faccia riferimento alla tesi di C. GEIGER, *the private copy exception, an area of freedom (temporarily) preserved in the digital environment,* in *IJC,* 2006, 74 ss., ricorda come copiosa dottrina ritenga che la liceità della copia privata verrebbe meno non appena le misure tecniche di protezione riescano a creare adeguati strumenti di protezione della medesima.

48 Cfr. anche S. BECHTOLD, *Digital Rights Management in The United States and in Europe,* cit., 360 in relazione ai sistemi di DRM:"In particular, DRM systems may undermine copyright limitations. They may prevent consumers from copying content for private purposes, even if a copyright limitation allows them to do so without the right's holder permission. DRM systems may also extend their protection to areas that lie outside of the reach of copyright protection".

49 Sul punto si veda il contributo di C. DI COCCO, *circolazione della conoscenza. DRM e limiti del diritto d'autore,* in R. CASO (a cura di), *Digital Rights Management, Problemi teorici e prospettive applicative,* cit., 114 ss..

50 Il corsivo è aggiunto.

51 Dello stesso tenore è la previsione di cui al considerando 53 della medesima direttiva espressamente riferita ai servizi *on demand.*

52 Così R. CASO, *Il signore degli anelli nel cyberspazio: controllo delle informazioni e Digital Rights Management,* cit., 158 vedi nota 116: " qualora ci si attenesse ad una interpretazione letterale la norma suonerebbe davvero come un premio immotivato alle imprese che distribuiscono contenuti digitali in forma *on demand*".

53 Cfr. T. C. WINEGUST, *Work with your Heads in the Clouds: The Impact of Cloud Computing and Content Streaming on the Entertainment industry,* in Intellectual Property Brief 4, no. 1 (2012), 8-15, ove viene offerta un'analisi delle ripercussioni della applicazione della disciplina del *copyright* sulla tutela dei dati protetti immessi nella nuvola. Il ricorso al servizio di cloud computing, in combinazione all'utilizzo di strumenti di *content streaming,* permetterebbe la diffusione dell'opera in via digitale, consentendo all'autore di ritenere non solo i diritti di ripriduzione, bensì anche quelli di distribuzione. Sul primo versante l'A. evidenzia come il trasferimento di materiale artistico-letterario al *cloud provider,* non sia suscettibile di rientrare nella definizione di "pubblicazione" fornita dal §101 del DMCA ("a public performance or display of a work to the

vengono immesse entro scompartimenti tecnologicamente blindati, accessibili unicamente a specifiche condizioni, contrattualmente definite[54]. Anche il piano contrattuale, recettizio del regime di controllo e di razionalizzazione dispiegantesi nel substrato tecnologico, può a sua volta contribuire a rafforzare l'assetto di tutele mediante la inclusione di quelli che sono stati definiti efficacemente definiti da taluna dottrina statunitense *fair use crippling contractual terms*[55].

La biunivoca interazione tra misure di protezione contrattuali e tecnologiche[56] pone pertanto in essere un complesso sistema di barriere protettive, *ex ante* mediante la accettazione delle condizioni di servizio standardizzate[57], *ex post* attraverso la determinazione di specifici margini di manovra virtuali dell'utente, delimitati dalla infrastruttura tecnologica. E' stato notato come un simile assetto renda il contenuto praticamente inseparabile dalla sua protezione tecnologica e contrattuale[58], e come il rischio sia quello di restringere in modo eccessivo le modalità di fruizione, anche altrimenti lecite, dei contenuti[59], generando una sovra-protezione, come visto legittimata dalle più recenti normative in materia di regolamentazione delle misure tecnologiche di protezione, che potrebbe secondo taluni confliggere[60] con le previsioni della disciplina di impronta tradizionale in materia di diritto d'autore, tra i cui cardini è da annoverare l'inderogabilità dell'eccezione di *fair use*[61], e, sul suolo europeo, delle eccezioni di libera utilizzazione[62].

---

public by sale or other transfer of ownership"), il quale prevede che ai fini della pubblicazione vi debba essere una distribuzione di *copie* ad un *gruppo di persone.* Ciò condurrebbe ad un rafforzamento dei diritti d'autore da intendersi in senso sia qualitativo che quantitativo, là dove il titolare potrebbe agire nei confronti di qualsiasi soggetto, diverso dal provider, che eserciti illecite attività di *downloading* o di distribuzione di copie, e la computazione del termine di durata dello stesso copyright sarebbe sospesa fino al momento della pubblicazione. La mancanza di pubblicazione in senso tecnico permetterebbe inoltre di impedire la creazione del mercato "secondario" di diffusione dell'opera, con notevoli incrementi dei *revenue streams* del titolare.

54 E' necessario a tal proposito richiamare le posizioni di taluna dottrina che esorta a non enfatizzare eccessivamente i rischi di restrizione in ordine al solo accesso, giacché le misure tecnologiche di protezione accrescono il controllo dei dati anche in relazione ad altri profili, in particolare attraverso la limitazione delle modalità di fruizione dei materiali così protetti che vanno ben oltre il semplice impedimento della copia privata. Così R. CASO, *Digital Rights Management, Il commercio delle informazioni elettroniche tra contratto e diritto d'autore,* cit.*,* 93.

55 Questa l'espressione di J. H. REICHMAN, *A Reverse Notice and Takedown Regime to Enable Public Interest Uses of Technically Protected Copyrighted Works.,* cit., 1022. A scopo esemplificativo si può ricordare una peculiare clausola del *Supplemental End User License Agreement* di *Microsoft Media Player,* che recita "You agree that in order to protect the integrity of content and software protected by digital rights management ("Secure Content"), Microsoft may provide security related updates to the OS Components that will be automatically downloaded onto your computer. These security related updates may disable your ability to copy and/or play Secure Content and use other software on your computer. If we provide such a security update, we will use reasonable efforts to post notices on a web site explaining the update". E' quanto ricorda A. ROSSATO, *I problemi dell'autotutela digitale,* in R. CASO (a cura di), 186. Sul punto si veda anche G. JIANG, *Rain or Shine: Fair and other non infringing uses in the context of cloud computing,* cit.*,* 348.

56 Cfr. anche S. BECHTOLD, *Digital Rights Management in The United States and in Europe,* cit.*,* 345: " From a legal perspective, this is a very important feature of DRM systems as compliance with the contractual terms may not only be controlled by law, but also by technology: if the contract governing digital content allows a consumer to make only two copies of the content, any further copying will be prevented by the technological meadures of the DRM system, which read the attached metadata in which the contractual terms are encoded".

57 Sul punto R. CASO, *Il signore degli anelli nel cyberspazio: controllo delle informazioni e Digital Rights Management,* cit., 116 ss.

58 Così S. BECHTOLD, *op. cit.,* 381.

59 Cfr. S. BECHTOLD, *op. cit.,* 339.

60 Sul punto ancora G. JIANG, *op. cit.,* 350, il quale invoca una affermazione sul piano normativo della prevalenza delle previsioni in materia di protezione di *copyright,* ed in particolare delle eccezioni del *fair use,* rispetto ai c.d. *TPM-enforced contracts*, là dove le clausole contenenti rinuncia a utilizzi rientranti nel *fair use,* dovrebbero essere sanzionate da nullità per contrasto con le prime.

61 Riflette sul punto anche R. CASO, *op ult. Cit.*, *passim.*

62 Per un analisi delle differenze intercorrenti tra disciplina del *fair use* e il regime delle eccezioni di libera utilizzazione nell'ordinamento comunitario sia consentito il rimando a M. GRANIERI, *Digital Rights Management vs Diritto d'autore,* in R. CASO (a cura di), *Digital Rights Management, problemi teorici e prospettive future,* cit., 86-87.

Le difficoltà di coordinamento tra le due discipline sono da ricondursi alla differente *ratio* a queste sottostanti, là dove la normativa più recente sembra aver attuato una indiretta *normalizzazione* degli strumenti tecnologici, piuttosto che una vera e propria revisione della regolamentazione in materia dei diritti di esclusiva. Le conseguenze di simile differenza sono state rilevate anche sul piano dei rimedi, là dove la determinazione della violazione del diritto d'autore nella sua accezione tradizionale passa necessariamente per la valutazione giudiziale *ex post*[63], mentre la reazione alla elusione delle misure tecnologiche sembra farsi sempre più forte di nuove[64] forme di autotutela[65], tanto più subdole in quanto si confondono e sovrappongono al controllo contrattuale *ex ante* sui contenuti digitali[66]. Ed in questo senso la maggiore esternalità, più che il vero e proprio "paradosso"[67], dell'autotutela sta nel fatto che i soggetti colpiti dall'applicazione di simile norme a tutela delle misure tecnologiche di protezione sono non già i c.d. pirati della rete, bensì proprio gli attori del mondo della scienza, della editoria e della stessa tecnologia[68], con notevoli ricadute sul piano della libertà di espressione, costituzionalmente tutelata[69].

Quest'ultima non può infatti che risultare compressa entro i compartimenti sempre più angusti in cui viene a strutturarsi il *web*, a causa dell'infoltimento delle barriere e dei punti di controllo tecnologicamente predisposti, e legislativamente protetti, ed il ruolo sempre più rilevante occupato dagli stessi *service providers*, non solo come intermediari della condivisione digitale, ma soprattutto in qualità di fornitori e gestori degli strumenti tecnologici entro cui quest'ultima si dispiega.

Non sono da trascurare in quest'ottica i pericoli di cancellazioni arbitrarie[70], nonché, in caso di impossibilità predeterminata di accedere a determinate forme di condivisione e di collaborazione, il venir meno di incentivi alla produzione delle c.d. arti generative, con un eventuale *locked out* ed incriminazione

---

63 R. CASO, *Il signore degli anelli nel cyberspazio: controllo delle informazioni e Digital Rights Management,* Cit., 161.

64 Diversa è la prospettiva adottata da R. CASO, *Relazione introduttiva, Forme di controllo delle informazioni digitali: il digital rights management,* cit., 55, ove la legittimazione dell'autotutela privata compiuta dalle normative in esame viene paragonata agli antichi privilegi librari.

65 Quali ad esempio la negazione all'accesso, la disattivazione di funzionalità, la distruzione di informazioni. Cfr. A. ROSSATO, *I problemi dell'autotutela digitale,* in R. CASO (a cura di), *Digital Rights Management, problemi teorici e prospettive future,* cit., 187 ss.

66 Così R. CASO, *Digital Rights Management, Il commercio delle informazioni elettroniche tra contratto e diritto d'autore,* cit., 110-111. Basti in questa sede ricordare, a scopo esemplificativo, il *Supplemental End User License Agreement* di *Microsoft Media Player,* ove si legge "You agree that in order to protect the integrity of content and software protected by digital rights management ("Secure Content"), Microsoft may provide security related updates to the OS Components that will be automatically downloaded onto your computer. These security related updates may disable your ability to copy and/or play Secure Content and use other software on your computer. If we provide such a security update, we will use reasonable efforts to post notices on a web site explaining the update". E' quanto ricorda A. ROSSATO, *op. cit.,* 186.

67 Questa l'espressione di A. ROSSATO, *op. cit.,* 193.

68 Così R. CASO, *Il signore degli anelli nel cyberspazio: controllo delle informazioni e Digital Rights Management,* cit., 151.

69 Per una riflessione sul fondamento costituzionale dei diritti di proprietà intellettuale ed il contrasto e la necessità di bilanciamento con il diritto alla libertà di espressione, si rimandi a E. BONADIO, *File Sharing, copyright and frredom of speech,* E.I.P.R. 2011, 33(10), 619-631, il quale riporta la opinione dell'Avvocato Generale Pedro Criz Villalon resa il 14 Aprile 2011 nella controversia *Scarlet v. SABAM* (C-70/10), in occasione della quale la Corte di Giustizia era stata investita della questione inerente alla sussistenza della possibilità per le corti nazionali, al fine della protezione dei diritti di proprietà intellettuale, di ordinare agli *internet service provider* di introdurre meccanismi volti alla individuazione della condivisione di *files,* ed alla interruzione della stessa sia al momento della richiesta, sia in quello del trasferimento vero e proprio. L'Avvocato Generale ritenne l'introduzione di simili sistemi restrittiva della libertà di espressione prevista dalla espressamente contemplata dall'art. 10 della *European Convention on human Rights*.

70 A scopo esemplificativo, si ricordi quanto avvenuto nel 2009, quando Amazon ha cancellato una versione dell'opera *1984* di Orwell dalla piattaforma *cloud* di *Kindle e-book,* scopertasi non autorizzata. Cfr. B. STONE, *Amazon Erases Orwell Books from Kindle*, N.Y. TIMES, July 17, 2009, http://www.nytimes.com/2009/07/18/technology/companies/I8amazon.html

degli *users* che intendono procedere alla creazione ed alla diffusione di opere derivate[71]. I costi da annoverare in simile frangente sono da riferirsi anche alla diminuzione delle possibilità di sviluppare opere collettive, quali, in taluni casi, possono essere considerati anche i *software open source*[72].

Spostando pertanto il baricentro dell'analisi dal profilo "oggettivo" della infrastruttura tecnologica, alla contemplazione del piano "soggettivo" inerente alla posizione dei *service providers,* sarà facile notare come la questione relativa al rischio di eclissi della libertà di espressione sulla nuvola, vada ben oltre il problema della preservazione degli spazi di libera utilizzazione che la tutela giuridica delle misure tecnologiche di protezione pone a rischio, per sfiorare la ardente tematica della incidenza della *condotta* degli stessi *providers* sulla riduzione del volume delle interazioni informative in un siffatto contesto.

Come è stato osservato, l'obbligo previsto in capo ai *providers* di rimuovere dai propri *servers* il materiale che terzi abbiano previamente notificato essere illecito[73], potrebbe avere effetti indesiderati là dove questi, in osservanza del "dovere di diligenza che è ragionevole attendersi da loro"[74], implementino determinati *screening devices* "al fine di individuare e prevenire taluni tipi di attività illecite"[75], che potrebbero da un lato condurre alla violazione del principio del "giusto processo", qualora i contenuti vengano eliminati, senza che al soggetto che li ha condivisi mediante il *cloud* sia lasciata alcuna possibilità preliminare di opporsi per dimostrarne la liceità[76]; e dall'altro risolversi in esiti discriminatori, là dove gli stessi *providers,* mediante l'attivazione di strumenti di *access control,* pregiudichino l'interesse all'accesso ai servizi a talune categorie di utenti ritenute meno affidabili[77]. A parziale conforto di simili preoccupazioni si erge il *memento* contenuto al considerando 46 della direttiva 2000/31/CE, ove viene espressamente precisato come il potere decisionale e di controllo attribuito in questo frangente ai *providers,* non possa che dispiegarsi nel rispetto "del principio della libertà d'espressione e delle procedure all'uopo previste a livello nazionale".

---

71 Sottolineano al contrario l'enorme potenziale di produttività culturale insito nel *cloud* C. LEADBEATER, *Cloud Culture:The future of Global Culture relations,* 19-23 (2010), reperibile su http://www.britishcouncil.org/russia-projectscultural-creative-economy-useful-resourcescloudculturecharlesleadbeater. Similmente D. J. GERVAIS-D. J. HINDMANN, *Cloud control: copyright, global memes and privacy,* cit., 65: " there will more to imitate and more ways to imitate. Hundreds of millions of Internet users are downloading, altering, mixing, uploading, and/or making available audio, video, and text content on personal web pages, social sites, or using peer-to-peer technology to allow others to access content on their computer". Cfr. anche LAMETTI, *Cloud Computing, Verso il terzo enclosure movement?,* cit., 366: "La cloud potrebbe ridurre le opportunità per gli utenti di interagire con Internet/Cloud allo scopo di impedirne la partecipazione nella rete in qualità di creatori, collaboratori e condivisori (modalità queste che sono diventate ormai comuni). Ciò significa la diminuzione di attività quali l'ideazione di nuovi contenuti e la ridefinizione delle modalità di interazione basata sui software liberi".

72 In questo senso D. LAMETTI, *op. ult. Cit.,* 12.

73 Così prevede l'art. 14, 1 comma, punto b, della direttiva 2000/31/CE relativa all'*e-commerce.* Simile la previsione di cui al art. 512, 1 comma punto c del DMCA, ove si esclude la responsabilità dei *providers* che a seguito di notifica abbiano immediatamente provveduto al blocco dell'accesso al materiale ritenuto illecito. Si tratta della c.d. *notice and takedown procedure* ampiamente commentata dalla dottrina. Si rimandi sul punto a R. JULIA-BARCELO'-K. J. KOELMAN, *Intermediary Liability, Intermediary liability in the e-commerce directive: so far so good, but it's not enough,* in *Computer Law and Security Report,* 16, 4, 2000, 232 ss.

74 Così recita il considerando 48 della medesima direttiva.

75 *Ibid.*.

76 Così R. JULIA-BARCELO'-K. J. KOELMAN, *op. cit.*, 232.

77 *Ibid.*, 233.

2. LE RESTRIZIONI ALL'ACCESSO E ALLA FRUIZIONE DEI CONTENUTI: VARCHI RIMEDIALI

La riflessione trasporta l'interprete sulla sponda dei rimedi e dunque delle possibili soluzioni proposte.

In conformità all'obiettivo di dilatare i margini della libertà di espressione, taluna dottrina ha proposto di improntare i diritti di privativa non più ad una logica proprietaria, bensì ad una logica di natura compensatoria: in questo senso si estenderebbe la possibilità di condivisione di contenuto, garantendo, ove necessario, un equo compenso[78] al titolare dei medesimi diritti[79].

Altri[80], più attenti alla protezione del principio del *fair use,* osservando come il tessuto normativo, in materia di *digital copyright* si sia rivelato (eccessivamente) permeabile alle ragioni della tecnologia, ritengono i tempi maturi per un processo inverso, da consumarsi sul piano legislativo, in virtù del quale deve essere la tecnologia a non poter più fare a meno di internalizzare le regole giuridiche, attraverso quello che la letteratura d'oltreoceano definisce un *value-sensitive design*[81]. Una simile prospettiva renderebbe forse possibile raggiungere un bilanciamento tra interessi contrapposti come, per quel che qui rileva, l'interesse delle imprese al controllo delle informazioni e quello degli utenti a vedersi garantiti dei margini di libera utilizzazione dei contenuti digitali[82]. L'infrastruttura tecnologica dovrebbe in questo senso far proprie le ipotesi di libera utilizzazione tipizzate sul piano normativo, mentre per quel che concerne i casi maggiormente controversi[83] si fa rifermento alla necessità di una preventiva autorizzazione di un soggetto terzo, responsabile della gestione di alcune chiavi crittografiche di accesso[84].

Non manca tuttavia in questo contesto chi afferma come sia inquadrare le ipotesi di *fair use* in predeterminati schemi normativi, ovvero in ugualmente predeterminati meccanismi tecnologici sconfessi la

78 Sia consentito il rinvio all'ampia trattazione di B. RUGGERO, *Equo compenso e diritto d'autore: un'analisi comparata,* Trento Law and Technology Research Group – Student Paper n. 8, pubblicato nel Gennaio 2012, reperibile online all'indirizzo http://eprints.biblio.unitn.it/2283/1/Trento_Lawtech_Students_Paper_8.pdf.

79 Questa soluzione è caldeggiata anche da L. LESSIG, *The Future of Ideas: the Fate of the Commons in a Connected World*, Random House, 2001, 201-202.

80 Così R. CASO, *Il signore degli anelli nel cyberspazio: controllo delle informazioni e Digital Rights Management,* Cit., 144-145.

81 Cfr.J. E. COHEN, *DRM and Privacy*, in 13 Berkeley Tech. L. J., 2003, 575.

82 Così ancora R. CASO, *op. ult. Cit.,* 145.

83 Controverse giacché non anteriormente predeterminate in virtù di previsioni normative. E questo sarebbe secondo alcuni il caso più frequente, là dove le continue evoluzioni della stessa tecnologia propongono al pubblico sempre nuove modalità di fruizione dei materiali, rendendo impossibile, ed inopportuno, operare una tipizzazione normativa *ex ante,* come è avvenuto in occasione del DMCA, delle ipotesi di *fair use.* " The problem is that as long technology continues to make new uses of copyrighted works possible, it will be impossible to create an exhaustive list of fair uses". Così G. JIANG, *Rain or Shine: Fair and other non infringing uses in the context of cloud computing,* cit., 405.

84 Così J. E. COHEN, *DRM and Privacy,* cit., 614-615. Per un'analisi approfondita sulla regolamentazione dell'attività di simile ente terzo si veda R. JULIA-BARCELO'-K. J. KOELMAN, *Intermediary Liability, Intermediary liability in the e-commerce directive: so far so good, but it's not enough,* cit., 237.

tradizionale vocazione di standard elastico che questo possedeva nell'ordinamento statunitense, per trasformare il medesimo in rigida regola, insensibile alle ragioni di equità individuale[85].

Lungo questa linea di pensiero si profila una soluzione ulteriore, che propone di instaurare un controllo giudiziale *ex post,* non già sulla liceità dell'utilizzo del materiale, sovente già reso inaccessibile *ex ante* indipendentemente dalle caratteristiche del contenuto digitale[86]*,* bensì relativo alla illiceità dei punti di controllo e di blocco responsabili di una *sovra*-protezione del materiale informativo digitalizzato[87]. Ciò dovrebbe avvenire attraverso una procedura "al contrario" di quella di *notice and take-down*[88] che permetta a gruppi di utenti di chiedere, mediante notifica, al titolare dei diritti di esclusiva di disattivare le misure tecnologiche di protezione di specifici contenuti a scopi di libera utilizzazione dei medesimi, e qualora quest'ultimo si rifiutasse, di ottenere, per via giudiziale, una tutela inibitoria (*take-down*) nei confronti del medesimo. Questo meccanismo potrebbe inoltre assicurare, a differenza della soluzione di *value sensitive design*, una maggiore flessibilità in relazione alle modalità sempre nuove di utilizzi rientranti nel *fair use* rese possibili (anche) dalle innovazioni tecnologiche[89]. La tutela inibitoria risulta inoltre l'unico metodo di accedere ai fini di una lecita utilizzazione, al materiale, là dove le misure tecnologiche di protezione predisposte dai *cloud provider* non lo consentano. Queste risulterebbero infatti talmente sofisticate, da essere impossibili da eludere da parte dell'utente medio[90].

Non è tuttavia possibile fare a meno di notare gli svantaggi di un simile meccanismo, sicuramente eccessivamente dispendioso in termini di tempo e costi.

Il criterio dirimente nella scelta tra i due modelli, da un lato basato su architetture tecnologiche di *value sensitive design*e e dall'altro quello di una procedura di *reverse notice and take-down*, potrebbe essere ricercato proprio nella differenza intercorrente tra la disciplina giurisprudenziale di *common law* basata sullo standard del *fair use* e quella europea, normativamente tipizzata[91], delle libere utilizzazioni. L'esigenza della conservazione del carattere flessibile dello standard giurisprudenziale potrebbe dunque suggerire la

85 J. GRIMMELMAN, *Regulation by Software ,* cit.*,* 1752-1753: "fair use is and ought to be a standard and not a rule because only a standard will be attuned to individual equities. We should not expect a rule to capture all the subtleties of human creativity or all the possible uses we might wish to call fair". Vedi sul punto *supra* nota 82.

86 In questa prospettiva si veda anche R. CASO, *Digital Rights Management, Il commercio delle informazioni digitali tra contratto e diritto d'autore,* cit.*,* 96, ove si nota che "persino la lettura di una parola, come sa benissimo chi abbia una conoscenza elementare di Word o di Acrobat Reader, può essere subordinata alla disponibilità di un codice di decrittazione".

87 Questa la proposta di J. H. REICHMAN, *A Reverse Notice and Takedown Regime to Enable Public Interest Uses of Technically Protected Copyrighted Works,* cit.*,* 1032.

88 Cfr. nota 69.

89 Così G. JIANG, *Rain or Shine: Fair and other non infringing uses in the context of cloud computing,* cit.*,* 351: "Thus, the reverse notice and takedown process is the mirror opposite of the notice and takedown process described in DMCA 512(c) and allows for the recognition of new fair uses due to advancements in technology and imagination".

90 *Ibid.*.

91 Cfr. Art. 5 della direttiva 2001/29/CE e per l'ordinamento italiano, artt. 65-71 della legge sul diritto d'autore 433/41 come modificati dal d.lgs recettivo della direttiva 68/2003.

preferibilità della prima soluzione, diversamente dal caso europeo in cui forse parrebbe economicamente più favorevole la seconda.

Rimane tuttavia un ultimo ostacolo, ancora insuperato, ma forse non insuperabile, della dimensione trans-giurisdizionale del *cloud,* di contro alla tradizionale territorialità dei diritti di proprietà intellettuale[92]: lo stesso *end user* non è sovente a conoscenza del luogo in cui i dati si trovano, o vengono elaborati, e non remota è la possibilità che i medesimi siano archiviati in più località, ovvero salvati in modo frammentario su più piattaforme, ed in tempi differenti[93]. Medesime misure tecnologiche di protezione potrebbero blindare allo stesso modo contenuti posti su *servers* allocati in differenti località, e per questo differentemente protetti, a seconda dei regimi normativi diversi, ovvero, in ragione delle discrepanze tra sistemi di eccezioni, non protetti proprio[94].

III ATTIVITÀ DI MONITORAGGIO E AUTOTUTELA: LA QUESTIONE DEI METADATA

La trasmissione di contenuti mediante servizio di *cloud computing* costituisce indubbiamente efficace strumento di protezione contro la pirateria[95], in particolare in riferimento alla riproduzione illecita delle applicazioni interattive non-lineari, come i videogiochi, o le *office suites*: in quanto applicazioni funzionanti sulla base di *software* basati sul *cloud*, nessuna copia "fisica" sarà reperibile o riproducibile, senza la

92 Basti ricordare come nel sistema di *common law* inglese siano degne di protezione quelle opere per la cui creazione sia stato impiegato sufficiente *labour, skill and judgment,* secondo quanto precisa l'art. 3(a) del *Copyright, Designs, and Patents Act 1988 ,* come modificato dal *Copyright and Rights in Databases Regulations* del 1997. Nonostante non sia riconosciuto alcun requisito di creatività, non saranno ritenuti degni di tutela quel materiale per la produzione del quale sia stato un minimo sforzo creativo (si consideri in questo senso la celebre pronuncia *Exxon Corporation v. Exxon Insurance Consultants International Ltd* [1982] Ch 119, ove non si ritenne meritevole di protezione la parola *Exxon*). Per quanto riguarda l'approccio statunitense, pur avendo fatto proprio il parametro della creatività quale requisito imprescindibile ai fini della qualificazione alla stregua di opera dell'ingegno, il grado di creatività richiesto risulta più basso rispetto agli standard europei, secondo quanto enunciato in *Feist Publications Inc. v. Rural Telephone Service Company, Inc.* 499 US 340 (1990) . Sul punto cfr. C. REED, *Information ownership in the cloud,* cit*.,* 10-11 e vedi *supra* nota 20.

93 Rilevano il problema Cfr. D. DESAI, *Beyond Location: Data Security in the 21th century,* in Communications of the ACM, Vol. 56 No. 1, 34-36; e anche P. DE FILIPPI- L. BELLI, *Law of the Cloud vs. Law of Land, challenges and opportunity for innovation,* in *European Journal of Law and Technology*, 3,2, 2012.

94 Similmente R. CASO, *Relazione introduttiva, Forme di controllo delle informazioni digitali: il digital rights management,* cit*.,* 57. "La disciplina delle MTP e delle informazioni sul regime dei diritti si fondano su leggi che incontrano il limite della territorialità. Mentre gli standard delle tecnologie disciplinate sono universali. Ciò innesca dinamiche distorsive del processo di produzione delle tecnologie, e rappresenta un'ulteriore barriera alla circolazione internazionale delle informazioni". A scopo esemplificativo si può considerare la questione dei c.d. *computer generated works,* protetti nell'ordinamento inglese all'art. 9(3) del *Copyright, Designs and Patents Act* del 1988, in virtù del quale l'autore è da identificarsi nella persona "by whom the arrangements necessary for the creation of the work are undertaken". La maggior parte degli ordinamenti non contempla tutta via tale categoria di opere realizzate mediante il ricorso a specifici *software,* rimanendo in tali casi necessario l'accertamento, in concreto, della sussistenza del requisito di creatività. Sul punto vedi C. REED, *Information* ownership *in the cloud, cit.,*16.

95 Cfr. G. JIANG, *Rain or Shine: Fair and other non infringing uses in the context of cloud computing,* cit*.,* 349.

conoscenza del codice sorgente da cui ricavare gli estremi di funzionamento, con la conseguente necessità, a tal fine, di eludere le misure tecniche di protezione[96].

Diverso discorso deve essere fatto per i media c.d. lineari, quali la musica o i film, i quali risultano più facili da riprodurre attraverso strumenti di cattura dei contenuti emessi via streaming[97]. E' tuttavia evidente come la distribuzione di materiale protetto attraverso piattaforme di *cloud computing* possa costituire valida alternativa all'acquisto di copie pirata, là dove il *cloud provider* consenta l'accesso gratuito ai contenuti[98], basando i propri profitti sulla diffusione di messaggi pubblicitari (*advertisement- supported free access model*)[99]. Le compagnie pubblicitarie sono difatti particolarmente favorevoli ad investimenti nell'ambito di servizi *cloud*, in virtù dell'enorme quantità di materiale informativo di cui entrano in possesso i *providers* mediante le statistiche di utilizzo, relativo alle modalità di fruizione dei dati da parte degli utenti, consentendo di individuare con precisione i gusti e le abitudini "culturali" dei *cloud clients*[100].

Ciò è reso possibile dalle molteplici forme di controllo cui i *providers* subordinano la fruizione del servizio predisposto, inerenti non solo all'accesso al contenuto, bensì al controllo sugli usi che i medesimi pongono in atto[101], previa identificazione degli stessi contenuti e dei titolari dei diritti d'autore come dei titolari dei diritti d'uso[102]. Al fine di assicurare il rispetto delle attività consentite all'utente finale in virtù delle licenze da questo acquistate i *cloud providers* pongono in essere un costante monitoraggio delle operazioni effettuate dall'utente. Ecco che il provider diviene in questo contesto *profiler*[103], centro di collezione di un notevole patrimonio di informazioni relative agli utenti, fruitori delle opere d'ingegno archiviate sulla nuvola, a tal punto da creare un vero e proprio *database of intentions*[104]. I dati così raccolti

96 Simile operazione saranno infatti in grado di svolgerla solo degli hacker, costituendo al contrario impresa eccessivamente complicata per l'utente medio. Cfr. G. JIANG, *op. cit.,* 348

97 Per una riflessione della giurisprudenza sul punto si rimandi alla decisione in *Real Networks, Inc. v. Streambox, Inc.*, No. 2:99CV02070, 2000 WL 127311, at 4 (W.D. Wash. Jan. 18, 2000), che offre una accurata descrizione di come sia possibile catturare contenuti emessi in streaming, nonostante la presenza di misure di sicurezza.

98 G. JIANG, *op. cit.,* 348

99 Nonostante l'insuccesso di alcuni esperimenti in questo senso, come nel caso di Imeem, un sito di streaming di musica, acquistata da MySpace, i cui i profitti derivanti dalla pubblicità risultarono insufficienti alla copertura delle spese "operative", e necessarie per l'acquisto delle licenze, così R. NAKASHIMA, MySpace Buys Imeem Music Site for Under $ 1 Million, USA Today, Dec. 8, 2009, http://www.usatoday.com/tech/techinvestor/corporatenews/20091208myspaceimeem_N.htm; numerosi sono gli esempi di riuscita, come ad esempio il diffusissimo *spotify,* cfr. tuttavia MOSCA, *Spotify cambia le regole. E la musica è sempre meno gratis,* pubblicato il 15 agosto 2013 sul sole24ore, reperibile online all'indirizzo http://www.ilsole24ore.com/art/tecnologie/2013-08-15/ecco-come-cambiano-regole-172138.shtml ; o Pandora, un altro servizio di streaming musicale, cfr. G. SANDOVAL, *Westergreen keeps promises: Pandora Profitable,* CNET News, Jan. 12, 2010, http://news.cnet.com/8301310013104333552 61.html.

100 Sul punto si veda A. MANTELERO, *Si rafforza la tutela dei dati personali: data breach notification e limiti alla profilazione mediante i cookies,* cit., 781 ss. Per approfondimento sul tema si veda *infra* in materia di metadata.

101 Sul punto si rimandi alle riflessioni di V. MAYER-SCHOENBERGER, *Beyond copyright: managing information Rights with DRM,* cit., 184, ove l'A. riprendendo talune affermazioni di L. LESSIG, osserva come l'autorità di delimitare i diritti di utilizzo sia sempre più trasferita dal legislatore alle società titolari dei sistemi di DRM, e dunque nel Nostro caso, agli stessi *cloud provider. "*As Lawrence Lessig predicted, the authority to delimit these usage rights shifts from the existing lawmaking and adjudicating institutions in our society to those in control of the DRM system".

102 Così P. GUARDA, *Privacy e fruizione della conoscenza scientifica,* cit., 102.

103 Dei forti incentivi che muovono i *providers* a svolgere l'attività di profilazione parla annche L. CHIARIGLIONE, *Digital Media in Italia,* in R. CASO (a cura di), *Digital Rights Management, Problemi teorici e prospettive applicative,* cit., 263.

104 Così J. BATTELLE, *The database of intentions is far larger than I thought,* in *John Battelle's searchblog,* 5 marzo 2010, reperibile online all'indirizzo http://battellemedia.com/archives/2010/03/the_database_of_intentions_is_far_larger_than_i_thought.php.

possono dunque essere considerati "di secondo grado", giacché direttamente derivanti dai dati oggetto di proprietà intellettuale, e più precisamente, dalla fruizione che di questi viene fatta ad opera degli *end users.*

E' tuttavia necessario muovere alcune precisazioni in merito al profilo della natura giuridica di simili informazioni: se infatti è innegabile che queste ultime attengano alla sfera privata individuata nella dimensione di impiego del dispositivo di condivisione *cloud,* non immediata risulta la qualificazione di simili *metadata*[105] alla stregua di informazioni personali[106], potendo gli stessi divenire altresì oggetto di "nuovi" diritti di proprietà intellettuale, nella forma di *user derived content*[107]*,* quali sono da considerare ad esempio le informazioni inerenti alla organizzazione strutturale di diversi contenuti[108].

Per quanto concerne la natura di diritti personali, questa potrà essere rilevata solamente nel caso in cui gli stessi metadati siano inequivocabilmente riferiti ad un soggetto "identificato" o "identificabile", anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale"[109]. E davvero in questo caso i meta-data derivanti dal monitoraggio dei diritti di utilizzo potrebbero rilevare come dati personali, qualora siano correttamente riferiti all'utente finale[110], e più precisamente ai dati di identificazione di questi, come autenticati[111].

---

105 E' necessario precisare come in questa sede il termine meta-data non viene utilizzato nel suo senso strettamente tecnico di «informazioni che descrivono il contenuto di altri dati», nella forma di veri e propri marcatori digitali costituenti pertanto strumenti di controllo dei diritti di utilizzo acquistati dagli utenti. Cfr. E. PROSPERETTI, *Il DRM come via per la creazione di regole certe,* in R. CASO (a cura di), *Digital Rights Management, Problemi teorici e prospettive applicative, cit.,*281, ed anche V. MAYER-SCHOENBERGER, *Beyond copyright: managing information Rights with DRM,* cit.*,* 192, ove si spiega come i meta-data così intesi siano propriamente incorporati nel contenuto che sono chiamati a monitorare mediante tecniche di criptazione o di steganografia.

106 Cfr. A. MANTELERO, *Si rafforza la tutela dei dati personali: data breach notification e limiti alla profilazione mediante i cookies,* cit.*,* 785.

107 Per una approfondita trattazione del complesso problema relativo alla gestione dello *user generated content* sia consentito il rinvio a D. GERVAIS, *The tangled web of UGC: Making copyright sense of User-generated content,* Vanderbilt University Law School, Public Law and Legal theory, working paper, 9-17, reperibile online all'indirizzo http:/ / ssrn.com/ abstract_id= 1444513.

108 Quali ad esempio l'assetto dato ad un catalogo di fotografie di famiglia. Sul punto anche E. PROSPERETTI, *op. cit.,* 281.

109 Così recita l'art. 4 del d.lgs 196/2003. Per una analisi più approfondita della problematica sia consentito il rinvio a W. HON-C. MILLARD- I. WALDEN, *The problem of "personal Data" in Cloud Computing- What information is regulated?, the cloud of unknowing, part 1,* Queen Mary University of London, School of Law Legal Studies Research Paper No. 75/2011*,* 20 marzo 2011, 15 ss., ove viene presentata una rassegna delle forme di identificazione indiretta, tra cui non solo i numeri di identificazione personale, bensì anche pseudonimi o meccanismi di codificazione, che rendono accessibili i dati, così divenuti personali, una volta identificato il soggetto titolare, solo a specifici *data processors.* A quest'ultimo proposito viene difatti rilevato: "this does not mean, though, that any other data controller processing the same set of coded data would be processing data if within the specific scheme in which those other controllers are operating re-identification is explicitly excluded and appropiate technical measures have been taken in this respect", 18, *cit.*

110 E' necessario precisare che, secondo un'impostazione invalsa nell'ordinamento statunitense, è da qualificare alla stregua di dati personale non solo l'informazione direttamente riferibile ad un soggetto, bensì anche ad uno specifico computer o altro dispositivo. Così è affermato nel documento della *Federal Trade Commission, Protecting Consumer Privacy in an era of rapid change. A proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report,* Dicembre 2010, reperibile online all'indirizzo http://www.ftc. gov/os/2010/12/101201privacyreport.pdf, 41, ove si qualifica come personale "data that can be reasonably linked to a specific consumer, computer or other device". Accoglie in senso positivo simile "parificazione fra soggetto e dispositivi informatici ai fini della connotazione in termini di natura personale dei dati", A. MANTELERO, *Data protection e attività di impresa, verso dove guardano gli usa?,* in *Dir. Dell'informazione e dell'informativa,* 27, 3, 2011, 457 ss., 474, ove l'A., osserva come nonostante non sia immediata l'equazione tra un computer e l'identità del soggetto che lo utilizza, giacché teoricamente più persone potrebbero usare lo stesso dispositivo, l'aumento dei dispsositivi tecnologici e la loro portabilità, nonché le più evolute tecniche di profilazione assicurano una maggiore precisione nell'individuazione dell'identità dell'utente.

111 "Critically, whether information amounts to personal data, including in cloud computing, depends on the circumstances, and consideration of all means likely reasonably to be used to identify individuals- including, in relation to anonymised or pseudonymised data, the strenght of the "anti-identification" measures used", così ancora W. HON- C. MILLARD- I. WALDEN, *The problem of "personal Data" in Cloud Computing- What information is regulated?, the cloud of unknowing, part 1,* cit.*,* 18.

Le tecnologie utilizzate ai fini del monitoraggio, sebbene non sempre chiare nel funzionamento, giacché sovente coperte da segreto industriale[112], sono molteplici, e consistono nella raccolta, effettuata dai *cloud providers,* degli indirizzi IP, propriamente qualificabili come dato personale[113], nell'impiego dei *file cookie,* i quali marcano il *browers* dell'utente finale con numeri univoci di identificazione[114], ovvero, più di recente, nel ricorso alle tecnologie D.A.R.T. (*Dynamic Advertising, Reporting and Targeting*), attraverso cui è possibile tracciare gli spostamenti di sito in sito degli utenti, registrando anche quali pubblicità commerciali questi selezionano nel corso della navigazione[115]. Su un differente versante, tra gli strumenti tecnologici utilizzati ai fini del controllo della fruizione dei contenuti protetti, è indispensabile fare menzione dei cosiddetti *REL* (*rights expression languages*), per mezzo dei quali il *provider* può tradurre in parametri "meccanici", le regole di utilizzo contrattualmente stabilite[116].

1 ATTIVITÀ DI MONITORAGGIO E AUTOTUTELA: LA PANORAMICA NORMATIVA

Risposte normative alla problematica della profilazione degli utenti sono state fornite, seppur nella varietà di approccio su alcuni aspetti, dalle *guidelines* dell'amministrazione statunitense[117], nonché dalle direttive europee in materia di *data protection*[118].

Ripercorrendo brevemente il percorso tracciato dalle normative europee, la disciplina generale in materia di protezione dei dati personali ha già in tempi risalenti fornito postulati teorici, sulla base dei quali poter arginare le attività di raccolta di meta-data personale e la impropria cessione di questi a terzi, i quali ne facciano a loro volta un uso contrario rispetto a quanto stabilito in conformità ai due principi di finalità[119] e pertinenza[120]. Il primo potrà pertanto essere invocato a garanzia del fatto che i dati raccolti non

112 Così precisa R. CASO, *Il conflitto tra diritto d'autore e protezione dei dati personali: appunti dal fronte euro-italiano,* in *Diritto dell'Internet*, 2008, 466 ss., 470.

113 Si veda il parere 2/2002 del Gruppo europeo dei garanti della tutela dei dati personali sull'uso di identificativi esclusivi negli apparecchi terminali di telecomunicazione: "il gruppo mette in evidenza che gli indirizzi IP attribuiti agli utenti Internet costituiscono dati personali", p. 3.

114 Si tratta dei c.d. *unique identifying numbers.* Cfr. P. GUARDA, *Privacy e fruizione della conoscenza scientifica,* cit., 110. si veda anche P. LANOIS, *Caught in the clouds: The Web 2.0, Cloud Computing, and Privacy, ,* 9 Nw. J. Tech. & Intell.Prop. 29 (2010). http://scholarlycommons.law.northwestern.edu/njtip/vol9/iss2/2, 32-33. Per la giurisprudenza sul punto si faccia riferimento in relazione alla specifica problematica dei *cookies,* a *Pharmatrak, Inc., Privacy Litig.*, 220 F. Supp. 2d 4 (D. Mass. 2002), nonché a *DoubleClick, Inc. Privacy Litig.*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001). Cfr. J. COHEN, *DRM and Privacy,* cit., 585.

115 Lo spiega P. GUARDA, *Privacy e fruizione della conoscenza scientifica,* cit., 110.

116 Cfr. sul punto anche V. MAYER-SCHOENBERGER, *Beyond copyright: managing information Rights with DRM,* cit., 186 ss. e anche S. BECHTOLD, *Digital Rights Management in The United States and in Europe,* cit., 344: " one of the most well knonwn RELs is the *eXtensible rights markup language* (XrML). XrML is a general purpose language in XML used to describe the rights and conditions for using digital resources. With RELs such as XrML, the permission to copy, delete, modify, embed, excute, export, (…) may be expressed in machine readable form".

117 Si veda P. LANOIS, *Caught in the clouds: The Web 2.0, Cloud Computing, and Privacy,* cit., 33-36.

118 Sul punto A. MANTELERO, *Data protection e attività di impresa, verso dove guardano gli usa?,* cit., 784.

119 Principio enunciato all'art. 6 lett. B) direttiva 95/46/CE, ed in base al quale i dati personali devono essere trattati per scopi determinati, espliciti e legittimi, e successivamente trattati in modo non incompatibile con detti scopi.

120 Principio enunciato all'art. 6 lett C) direttiva 95/46/CE, ed in base al quale i dati personali siano adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati o successivamente trattati.

vengano utilizzati per trattamenti ulteriori rispetto a quelli in vista dei quali era risultato tollerabile l'immagazzinamento dei dati medesimi, come ad esempio quelli strettamente necessari per la fornitura del servizio informativo; in virtù del secondo risulterebbero al contrario vietate quelle attività di trattamento dei dati personali non strettamente funzionali alla protezione dei contenuti digitali[121]. Il trattamento così definito dovrà inoltre prestare ossequio anche al principio di conservazione limitata dei dati[122], il quale costituisce la base teorica per la forse prossima codificazione di un diritto all'oblio[123].

La stessa direttiva *e privacy* del 2002, ha inoltre inteso restringere le possibilità di ricorso alle tecniche di monitoraggio degli utenti[124], mediante la configurazione in capo ai *service providers*[125] dell'obbligo di fornire adeguate[126] informazioni[127] agli utenti non solo circa le modalità di raccolta dei dati, bensì anche circa gli "scopi del trattamento in conformità della direttiva 95/46/CE, facendo salva "la possibilità di rifiutare tale trattamento da parte del responsabile del trattamento"[128]. In questo contesto, l'utilizzo di *cookies* è ammesso nella misura in cui questi "siano destinati a scopi legittimi, come facilitare la fornitura dei servizi"[129]. L'emendamento compiuto nel 2009[130] eliminerà le ambiguità ancora nascenti dalla lettera della precedente normativa[131], chiaramente subordinando l'utilizzo dei *cookie* alla previa manifestazione del consenso informato dell'utente[132]. Appare in questo senso evidente il passaggio da un modello di *opt out* fatto proprio dalla direttiva del 2002, ad un modello *opt in* promosso dalla direttiva del 2009, maggiormente conforme

121 Così A. PALMIERI, *Digital Rights Management e disciplina europea della protezione dei dati personali,* cit., 209.

122 Cfr. art. 6 lett. E) direttiva 95/46/CE, in virtù del quale sarebbe da ritenersi illecito il controllo sui dati che si protragga per un tempo superiore a quello strettamente necessario per raggiungere gli scopi prefissati.

123 Non essendo in questa sede possibile approfondire la tematica, sia consentito il rinvio a L. MITROU-M. KARYDA, *Eu's data protection Reform and the Right to be forgotten- A legal response to a technological challenge?,* articolo presentato alla 5th International Conference of Information Law and Ethics 2012, Corfu-Greece 29-30 Giugno 2012.

124 Cfr. direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche. Si veda in particolare il considerando n. 25 specificamente relativo ai "marcatori digitali" .

125 Sulla problematica dell'individuazione del soggetto che esegue la attività di installazione di *cookies* e la corrispondente "lettura" e processazione dei dati ricavati dai medesimi, e cui conseguentemente è da ascrivere l'obbligo di predisporre un opportuno prospetto informativo, si veda *Article 29 Data Protection Working Party,* parere 2/2010 sulla pubblicità comportamentale online, adottato il 22 giugno 2010, reperibile *online* all'indirizzo http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_it.pdf, 18-19 : "The Article 29 Working Party notes that pursuant to the working of Article 5(3) of the ePrivacy Directive, the obligation to provide the necessary information and obtain data subjects' consent ultimately lies with the entity that sends and reads the cookie. In most cases, this is the ad network provider".

126 Il considerando numero 25 della direttiva.

127 La direttiva sembra presentare una nozione estesa di "informazione", là dove le stesse informazioni archiviate mediante le tecnologie di monitoraggio sono da riferirsi alla vita privata dell'utente in senso lato. Cfr. il considerando n. 24 in virtù del quale "le apparecchiature terminali degli utenti di reti di comunicazione elettronica e qualsiasi informazione archiviata in tali apparecchiature fanno parte della sfera privata dell'utente". Per una più approfondita riflessione sul tema si rimandi a A. MANTELERO, *Data protection e attività di impresa, verso dove guardano gli usa?,* cit., 785-786. Riflette sul punto anche P. LANOIS, *Caught in the clouds: The Web 2.0, Cloud Computing, and Privacy,* cit., 41.

128 Art. 5, 3 comma della direttiva 2002/58/CE.

129 Così il considerando n. 25.

130 Cfr. direttiva 2009/136/CE

131 In particolare si vedano le riflessioni di P. LANOIS, *op. cit.,* 38, il quale sottolinea come "the 2002 *e-privacy directive* is silent concerning how and when the opportunity to refuse the storage of, or access to the information, needs to be given, leaving each EU member state (or more specifically each country's court system) free to provide its own interpretation on these issues".

132 Cosa che invece la direttiva del 2002 non garantiva. "Under the 2002 *e-privacy* directive it would seem acceptable to use cookies without obtaining the user's prior consent, provided that the use of the cookies is fully explained in a privacy policy which is accessible from every page of a site", *ibid.*.

alle previsioni della disciplina comunitaria generale in materia di *privacy*[133]. In via generale è necessario notare come i due opposti meccanismi di *opt in* e *opt out,* possano dipendere dalla configurazione di *default* del *browser*, cui è da ricondurre una preventiva (ed indiscriminata) accettazione dei *cookies,* ovvero un rifiuto dei medesimi, con i rispettivi riflessi sulle possibilità di profilazione commerciale[134]. Anche nel secondo caso, a prima vista più conforme allo spirito della direttiva del 2009, verrebbe tuttavia a mancare, come è stato opportunamente osservato[135], la specificità del consenso, assicurata unicamente mediante una particolareggiata manifestazione dell'assenso della ricezione dei *cookies* da esprimere di volta in volta. La strategia della impostazione di *default* del *browser* come metodo di acquisizione del consenso nell'un senso o nell'altro, è stata espressamente rigettata dal Gruppo di lavoro per la protezione dei dati personali[136], il quale, rimarcando i caratteri di specificità, nonché di priorità ed inequivocità del consenso, ha sottolineato come l'impostazione di *default* del *browser* nel senso dell'esclusione dei *cookies,* non possa in alcun modo equivalere all'esclusione del consenso ai medesimi che al contrario deve essere espressamente manifestato dall'utente. Sarà inoltre necessario distinguere e "particolareggiare" il consenso rispettivamente in relazione all'impiego di dispositivi di *cookie* ed al conseguente utilizzo e trattamento dei dati (personali) così raccolti[137]. In questo senso, non solo risulterà necessario precisare la portata e gli scopi della elaborazione degli stessi dati[138], ma anche fornire le adeguate specificazioni in ordine alla validità temporale del consenso manifestato, là dove nonostante la lettera della direttiva sembri fare riferimento al carattere unico "dell'offerta di informazioni e del diritto di opporsi"[139], sostanzialmente diverso appare l'orientamento del Gruppo di Lavoro per la protezione dei dati personali, il quale ha in varie occasioni precisato la necessità di fissare adeguate "scadenze temporali", mediante la elaborazione di "modalità per informare periodicamente le persone del monitoraggio in corso"[140].

Le informazioni raccolte attraverso i meccanismi sopra riportati possono dunque essere impiegate per scopi da un lato direttamente funzionali all'esecuzione del rapporto contrattuale di cui è parte il titolare

133 Si veda in particolar modo l'art. 7 della direttiva 95/46/CE sulla protezione dei dati personali-

134 In senso critico si faccia riferimento ancora a P. LANOIS, *op. cit.,* 42-43, il quale mette in evidenza come la configurazione di *default* del *browser* in un senso o nell'altro osti possa impedire, e dunque evitare una legittima manifestazione del consenso, là dove l'utente manchi di modificare le impostazioni di *privacy* del proprio *browser.*

135 Sul punto ancora A. MANTELERO, *op. ult. cit.,* 787.

136 *Article 29 Data Protection Working Party, parere 2/2010 sulla pubblicità comportamentale online*, cit. 17.

137 "users' acceptance of a cookie could be understood to be valid not only for the sending of the cookie but also for subsequent collection of data arising from such a cookie. In other words, the consent obtained to place the cookie and use the information to send targeting advertising would cover subsequent 'readings' of the cookie that take place every time the user visits a website partner of the ad network provider which initially placed the cookie". *Ibid.,* 16.

138 " The data subject should be clearly informed that the cookie will allow the advertising provider to collect information about visits to other websites, the advertisements they have been shown, which ones they have clicked on, timing etc. There should be a simple explanation on the uses of the cookie to create profiles in order to serve targeted advertising". *Ibid.,* 17-18.

139 Si veda in particolar modo il considerando n. 25 della direttiva 2002/58/CE, ove viene precisato che "l'offerta di informazioni e del diritto di opporsi può essere fornita *una sola volta* per l'uso dei vari dispositivi da installare sull'attrezzatura terminale dell'utente durante la stessa connessione *e applicarsi anche a tutti gli usi successivi,* che possono essere fatti, di tali dispositivi durante successive connessioni".

140 Cfr. *Article 29 Data Protection Working Party,* parere 2/2010 sulla pubblicità comportamentale online, *cit.*, 18.

dei dati[141], e dall'altro per finalità che, esulando dal tracciato sinallagmatico, appaiono diversamente legate al valore economico di cui può profittare l'impresa entrata in possesso dei medesimi[142]: in quest'ultimo caso, anche il nostro Garante della Privacy[143] ha precisato come il trattamento dei dati identificativi le abitudini dei clienti, non raccolti in forma aggregata o anonima, sia da considerarsi illecito se il titolare del trattamento non presta documentazione scritta del consenso informato[144], notificando lo stesso trattamento al Garante[145], e rendendo adeguata informativa agli interessati.[146]

Da questo contesto emerge chiaramente la natura "generativa" dei dati protetti da diritti di proprietà intellettuale archiviati sui dispositivi di *cloud*: questa è da ricondursi direttamente alla struttura centralizzata[147] delle piattaforme di interconnessione entro le quali il *provider,* nelle vesti di *processor,* svolge di riflesso anche attività di *controller*[148] *,* in quanto detentore di un generale potere di controllo sulle informazioni scaturenti dalla gestione e della conseguente messa a disposizione al pubblico dei contenuti protetti[149].

Complessa risulta a proposito la possibilità di configurare in capo al *provider,* dei diritti (*database rights*) sulla collezione dei meta-dati raccolti mediante la predisposizione del servizio di *cloud computing*[150]*,* qualora "per scelta o per disposizione del materiale" possano rilevare come "creazione dell'ingegno"[151]. E' tuttavia inevitabile in questa prospettiva menzionare la difficoltà della individuazione dei requisiti cui subordinare la qualifica di banca dati: se la disciplina europea fa leva sul profilo dell'"investimento rilevante sotto il profilo qualitativo e quantitativo"[152], complicazioni potrebbero sorgere nei casi in cui i *servers* siano allocati in territorio statunitense, dove la banca dati viene protetta solo là dove sia rilevabile un sufficiente apporto creativo da parte del suo autore[153]. Ne deriva che lo standard statunitense appare più alto rispetto a quello

141 Cfr. art. 24 del Codice in materia di protezione dei dati personali in virtù del quale il trattamento può essere effettuato anche senza il consenso dell'interessato qualora esso sia "necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato, o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato".

142 Riflette sul punto anche A. OTTOLIA, *Proprietà intellettuale e trattamento dei dati personali: riflessioni su privacy per il sistema e nel sistema,* cit., 328.

143 Provvedimenti a carattere generale del Garante della Privacy del 25 giugno 2009, in Boll. N 106/giugno 2009.

144 *Ex* art. 23 del Codice in materia di protezione dei dati personali.

145 Cfr. artt. 37, 1 comma lettera d) e 38 del Codice.

146 Art. 13.

147 Cfr. P. DE FILIPPI- S. MC CARTHY, *Cloud Computing: Centralization and data sovereignty,* in *European Journal of Law and Technology* 3, 2 (2012) *, passim.*

148 Sulla differenza tra data processors e controllers sia consentito il rimando a P. BALBONI, *Data protection and data security issues related to cloud computing in the EU,* Tilburg University Legal Studies Working Paper Series No. 022/2010, August 21, 2010, 5 ss.

149 "To the extent that publishers act as data controllers they are bound by the obligations arising from Directive 95/46/EC regarding the part of the data processing under their control", così si legge nell' *Article 29 Data Protection Working Party,* parere 2/2010 sulla pubblicità comportamentale online, *cit.,* 12.

150 Tratta del problema C. REED, *Information ownership in the cloud, cit.*, 11.

151 Così art.1 della direttiva 96/9/CE del Parlamento europero e del consiglio, dell'11 marzo 1996, relativa alla tutela giuridica delle banche dati.

152 Cfr. art. 7, 1 comma della direttiva 96/9/CE

153 Questo quanto enunciato nella celebre controversia *Feist Publication Inc. v. Rural Telephone Service Company, Inc.* 499 US 340 (1990). Nel caso in cui la banca dati non sia tutelabile secondo la disciplina in materia di *copyright,* questa è considerata quale un insieme di informazioni fattuali, non protetti da alcuna forma di tutela particolare. Cfr. C. REED, *op. cit.,* 15.

europeo, con riflessi particolarmente apprezzabili sul piano dei rimedi: qualora infatti sia rilevabile il diritto d'autore sulla banca dati solamente alla stregua della disciplina europea, il titolare avrebbe a disposizione i rimedi[154] contro tutte le "operazioni di estrazione e/o reimpiego della totalità o di una parte sostanziale del contenuto della stessa"[155] avvenute in suolo europeo, mentre nessuno strumento di *enforcement* sarebbe rinvenibile qualora le attività illecite siano effettuate in territorio statunitense[156].

2 ATTIVITÀ DI MONITORAGGIO E AUTOTUTELA: FUNZIONI E RIFLESSI SULLA LIBERTÀ DI ESPRESSIONE

Indipendentemente dalla qualificazione, la gestione di simile *asset* informativo da parte del *provider* viene ad assumere duplice funzione: da un lato, come visto, quella del controllo della fruizione del contenuto digitale effettuata dall'utente[157], cui corrisponde la facoltà di sanzionare[158] le attività non consentitegli in base alla licenza finale, e dall'altro quella della individuazione degli interessi commerciali di questo, così da rendere possibile la commercializzazione del profilo ricavato[159], mediante la attuazione di strategie di *direct marketing,* nonché di *behavioural advertisement*[160].

La dottrina italiana come d'oltreoceano[161] ha sottolineato come queste duplici funzioni abbiano ripercussioni su due distinte accezioni di *privacy,* l'una "spaziale", l'altra "informazionale", altresì detta "decisionale" [162], entrambe riconducibili alla più ampia dimensione della libertà individuale di autodeterminare il proprio consumo intellettuale[163].

E' stato già precedentemente messo in evidenza come la complessa architettura del *cloud computing*, attraverso l'impiego di tecnologie di *access control,* restringa *ex ante* le possibilità di fruizione dei contenuti disponibili, con evidente condizionamento dell'*an* e del *quomodo* del consumo intellettuale del singolo[164], e la

154 Cfr. art. 12 della direttiva 96/9/CE

155 Art. 7, 1 comma, *ibid.*

156 Così C. REED, *op. cit.,* 15 nota 39.

157 Sul punto S. BECHTOLD, *Digital Rights Management in The United States and in Europe,* cit., 327: " In order to provide a secure distribution platform for digital content, DRM systems not only have to protect content against copying, they must offer means to identify and manage content. In order to facilitate the auomated trading of digital content and associated digital rights, DRM systems use so called "meta-data" to formally describe digital content and related parameters. With meta-data, the provider is able to control, in a very fine-grained manner, which consumer may access and use content, under what circumstannce and for what purpose", *ivi.*

158 Mediante blocco dell'accesso ai contenuti. Vedi *supra* in tema di autotutela.

159 P. GUARDA, *Privacy e fruizione della conoscenza scientifica,* cit., 102.

160 Sul punto A. MANTELERO, *Data protection e attività di impresa, verso dove guardano gli usa?,* cit., 781 ss.

161 Si veda in particolar modo J. COHEN, *DRM and Privacy,* cit., 576 ss. e per la dottrina italiana ancora una volta R. CASO, *Digital Rights Management, Il commercio delle informazioni elettroniche tra contratto e diritto d'autore,* cit., 103.

162 Sul punto R. CASO, *Digital Rights Management, Il commercio elettronico delle informazioni tra diritto d'autore e contratto,* cit.,104, il quale sottolinea come "la dimensione informazionale della *privacy* delimiti uno spazio (intellettuale) nel quale il pensiero può liberamente esprimersi", a differenza di quella spaziale, delimitante uno spazio (fisico) nel quale la persona è libera di esplorare i propri interessi intellettuali".

163 In questo senso J. COHEN, *op. cit.,* 580 ss. e A. CAMERON, *The nexus between copyright and intellectual privacy,* Ottawa, Canada, 2012, reperibile online all'indirizzo http://www.ruor.uottawa.ca/en/bitstream/handle/10393/22798/Cameron_Alexander_Dugan_2012_thesis.pdf?sequence=3, 84 ss..

164 Così R. CASO, *op. ult. Cit.,* 105.

conseguente compressione dell'autonomia decisionale in relazione alle condizioni di godimento del materiale reso accessibile, là dove, di fronte ad una sempre più capillare standardizzazione contrattuale e tecnologica, si giunge ad un'omologazione dei comportamenti possibili[165].

La successiva operazione di monitoraggio e di eventuale autotutela[166] compiuta dai *providers* grazie alla collezione di metadata e la formazione di vere e proprie banche dati[167] frutto dell'osservazione da un lato degli interessi intellettuali degli utenti[168], dall'altro delle modalità lecite o meno, entro le quali simili interessi vengono soddisfatti, conducono a diversi e non immediatamente percettibili pregiudizi alla sfera privata[169].

In primo luogo la sistematizzazione e la automatizzazione[170] dell'acquisizione e registrazione di informazioni relative alle abitudini dei consumatori, minano la libertà "negativa" di escludere terzi dalla interferenza negli *spazi* privati di individuale consumo intellettuale[171], ma incidono anche sulla facoltà "positiva" di detenere il pieno controllo sulle attività di indagine intellettuale personalmente scelte[172]. In questo senso è necessario ricordare come le stesse funzionalità di autotutela, le quali sono poste in essere in combinazione con quelle di monitoraggio, costituiscano una ulteriore barriera eretta a compromissione della libertà del consumo intellettuale[173]. In specie le tecnologie volte a sanzionare gli usi non autorizzati, disabilitandoli, si riflettono in due diverse compressioni della *intellectual privacy*[174].

In primo luogo infatti, l'utente necessariamente esce dalla dimensione di seppur precario anonimato in cui versa fino a quel momento insieme agli altri consumatori di contenuti[175], per divenire, una volta

165 Così J. COHEN, *op. cit.,* 577-578: "the inexorable pressure toward conformity generated by exposure, and by loss of control over uses of gathered information, violates rights of self-determination by coopting them. Additionally, surveillance and exposure devalue the fundamental dignity of persons by reducing the exposed individuals to the sum of their profiles".

166 Cfr. J. COHEN, *op. cit.,* 582 ss.

167 Più nello specifico, il *provider,* accedendo al *licensing module,* potrà compiere delle statistiche aggregate dell'utilizzo dei contenuti, ovvero visualizzare il profilo di un determinato utente, "abbinando le informazioni contenute nel *logging program* con quelle salvate nella banca dati che, invece, raccoglie le informazioni personali degli utenti". Così P. GUARDA, *op. cit.,* 106-107.

168 Particolarmente approfondita appare la riflessione giurisprudenziale statunitense sul punto. In particolare si vedano *Specht v. Netscape Communications Corp.* 306 F.3d 17 (2d Cir. 2002), inerente ad una invasione della privacy compiuta dal provider attraverso la installazione di browser "plug in" per monitorare le attività del consumatore; similmente *RealNetworks, Inc., Privacy Litig.*, No. 00-1366, 2000 WL 631341 (N.D. Ill. May 8, 2000).

169 Sul punto si rimandi a J. COHEN, *DRM and Privacy,* cit., 577-578: " surveillance and compelled disclosure of information about intellectual consumption threaten rights of personal integrity and self-definition in subtle but powerful ways. Although a person cannot be prohibited from thinking as she chooses, persistent, fine-grained observation subtly shapes behavior, expression, and ultimately identity. The inexorable pressure toward conformity generated by exposure, and by loss of control over uses of the gathered information, violates rights of self-determination by coopting them. Additionally, surveillance and exposure devalue the fundamental dignity of persons by reducing the exposed individuals to the sum of their 'profiles'".

170 Sul punto cfr. R. CASO, *op. cit.,* 106: "Il fatto che la raccolta dei dati avvenga mediante funzionalità automatizzate non diminuisce la minaccia che le banche dati – potenzialmente accessibili ai titolari dei contenuti ed a terzi – pongono alla privacy legata al consumo intellettuale".

171 Così anche A. CAMERON, *The nexus between copyright and intellectual privacy,* cit., 76.

172 Similmente J. COHEN, *op. cit.,* 585: " DRM technologies that monitor user behavior create records of intellectual consumption. Indirectly, then, they create records of intellectual exploration, one of the most personal and private of activities".

173 Similmente R. CASO, *Digital Rights Management, Il commercio elettronico delle informazioni tra diritto d'autore e contratto,* cit., 106-107.

174 Per un'approfondita riflessione sul concetto si rimandi a A. CAMERON, *op. cit.,* 38 ss.

175 In questo senso ancora J. COHEN, *op. cit.,* 587: "The punitive quality of self-help, impicates privacy interests in one way that technologies of direct constraint do not. The identification of a particular consumer as a target for self-help measuresentails loss of the relative anonymity formerly enjoyed by that individual as one among many customers".

individuato e classificato, diretto bersaglio di una misura di autotutela. E' evidente come quest'ultima abbia natura profondamente differente dalle altre misure restrittive sopra esaminate, quali quelle all'accesso e quelle costituite dalle successive attività di sorveglianza compiute dal *provider*: se simili misure interessano in modo più o meno uniforme[176] la totalità dei clienti di un determinato servizio, in ragione dell'efficacia "diffusa" delle norme tecnologiche e contrattuali come standardizzate, l'autotutela ha carattere particolare, e svela la effettività del meccanismo di profilazione compiuta attraverso il monitoraggio.

Secondariamente è stato infine osservato come le architetture *cloud* così strutturate, foriere di un controllo sempre più privato dei contenuti[177] rischino di dare vita a nuove forme di "autoritarismo decentrato"[178], qualora oggetto di simili misure risultino non più solo comportamenti contrari alle norme giuridiche, e più specificamente contrattuali, bensì condotte da considerarsi riprovevoli secondo specifiche norme sociali, fatte proprie dal sistema informatico come configurato[179].

Rischi successivi sono da ravvisarsi nella possibilità per il *provider* entrato in possesso di simile patrimonio informativo di trasferirlo a terzi[180], interessati all'acquisto[181], primi tra tutte le compagnie pubblicitarie: in questo senso si dà concretamente luogo alla commercializzazione dei profili, avente come effetto primario quello del condizionamento degli oggetti di fruizione intellettuale, e da ultimo la eso-imposizione di interessi latamente culturali[182].

176 E ciò dipenderà ad esempio dalla portata delle licenze acquisite dai singoli consumatori.

177 Nel senso proposto da C. DI COCCO, *Circolazione della conoscenza, DRM e limiti del diritto d'autore,* in R. CASO, *Digital Rights Management, problemi teorici e prospettive applicative, Atti del convegno tenutosi alla facoltà di giurisprudenza di Trento il 21 e 22 marzo 2007*, cit., 123-124, ossia di un controllo sempre più privato dei contenuti. Si veda anche D. J. GERVAIS-D. J. HYNDMAN, *Cloud control: copyright, global memes and privacy,* cit., 64, ove si mette in evidenza come la regolazione, che da una struttura gerarchica così deriva, del traffico dei dati ammessi ed immessi, non solo ponga a repentaglio la neutralità della rete, ma la stessa natura aperta di Internet, dominato da codici proprietari progettati per la massimizzazione del profitto, anziché della ampliamento dell'accesso.

178 Questa l'espressione utilizzata da R. CASO, *Digital Rights Management, Il commercio elettronico delle informazioni tra diritto d'autore e contratto,* cit., 107.

179 Questo il pericolo paventato in particolare da J. COHEN, *DRM and privacy,* cit., 587-588: "By inserting automatic enforcement functions into private spaces and activities, these technologies elide the difference between public/rulegoverned behavior and private behavior that is far more loosely circumscribed by applicable rules and social norms. (…) In other cases, however, looseness of fit between public rules and private behavior serves valuable purposes. Where privacy enables individuals to avoid the more onerous aspects of social norms to which they may not fully subscribe, it promotes tolerance and pluralism". Ciò costituirebbe di fatto una inammissibile violazione di quella dimensione spaziale della *privacy,* intesa dalla stessa Autrice come "freedom to explore areas of intellectual interest that one might not feel free to explore in public", *ibid.,* 579.

180 Lo scambio delle informazioni personali tra imprese deriva dal notevole valore economico da assegnare alle stesse, e sul quale taluna dottrina intendere giustificare la qualificazione delle medesime alla stregua di diritti di esclusiva a contenuto patrimoniale. Così ad esempio L. UBERTAZZI, *I diritti d'autore e connessi,* 5 Quaderni di Aida, 2003, 140 ss. La questione sarà comunque affrontata *infra* §5.

181 Sul punto anche L. BYGRAVE, *Digital Rights Management and Privacy, Legal Aspects in the European Union,* E. Becker et al. (Eds.) Digital Rights Management, LNCS 2770, 418–446, 2003, 436 ss..

182 Ciò è evidente se si considerano i contenuti monitorati come veicoli di veri e propri "prodotti culturali", sul punto anche A. PALMIERI, *Digital Rights Management e disciplina europea della protezione dei dati personali,* cit., 198. Sul punto degni di nota sono i rilievi compiuti da D.J. GERVAIS-D. J. HYNDMAN, *op. cit.,* 69-70: "The real concern is that when those technologies suggest content, they may interrupt a chain of events (initiated by a user's search) thath might have led one to a completely different place. They reinforce the past but at the potential expense of different futures. When Amazon suggests a book for instance, one may end up buying that book and not wander in a different cultural "direction". (…) However, beacuase "cloud suggestions" (and default choices made for users) are based on one's past actions and preferences, intuitively they will tend to reinforce what one already knows and who that person is rather than allow one to take different path. In other words, they might expose each of us to "more of the same". The risk is that this may, in time, impoverish the social and cultural discourse.".

3 ATTIVITÀ DI MONITORAGGIO E AUTOTUTELA: INFORMATION FOR INFRINGEMENT

Peculiare momento di *vulnus* della tenuta della sicurezza dei dati personali, a tutto vantaggio dell'affermazione dell'inviolabilità dei diritti di autore appare in questo senso l'ipotesi della cessione ai titolari di questi ultimi diritti da parte del *cloud provider,* del patrimonio informativo raccolto attraverso le tecniche di monitoraggio, e funzionale alla promozione di azioni giudiziali e stragiudiziali volte a colpire direttamente gli utenti sospetti di violazioni[183].

Numerosi sono a questo proposito i rilievi ricavabili dalla riflessione giurisprudenziale[184], da un lato riconducibili alla affermazione della illiceità delle operazioni di *tracking* specificamente funzionali al monitoraggio di attività sospette[185], e dall'altro inerenti alla questione se si possa, o meno, desumere dalla normativa europea la sussistenza di un imposizione in capo agli stati membri di istituire un obbligo di trasmettere dati personali al fine di assicurare la effettiva protezione dei diritti di autore nell'ambito di un procedimento civile.

Rilevanti in questo senso le precisazioni espresse dal Garante della Protezione dei Dati Personali nel febbraio 2008[186], in cui si precisa che simili attività di monitoraggio, compiuta in specie attraverso la raccolta di indirizzi IP da parte dei terzi *providers*, sono da considerarsi illecite, quando siano compiute in violazione dei principi di trasparenza e correttezza sanciti dalle direttive europee[187], nonché degli stessi principi di pertinenza[188] e necessità[189].

Passando alla seconda problematica, in occasione della controversia *Promusicae*[190], è emersa la difficoltà di risolvere la questione relativa alla possibilità di configurare "l'obbligo di conservare e *mettere a disposizione* i dati sulle connessioni ed il traffico generati dalle comunicazioni effettuate durante la

183 Cfr. R. CASO, *Il conflitto tra diritto d'autore e protezione dei dati personali: appunti dal fronte euro-italiano,* cit., 466 ss. Sul punto si è espresso anche il Gruppo di Lavoro per la Protezione dei dati personali, nel *Working Document on data protection issues related to intellectual property rights,* cit., 6-7.

184 Pur trattandosi di vicende non specificamente riguardanti il servizio di *cloud computing*, bensì da ricondursi al sistema di condivisione digitale del *Peer-to-Peer*, si ritiene che le linee fondamentali delle argomentazioni proposte possano essere adeguatamente estese e riferite anche alla particolare tipologia di servizio informatico in questa sede preso in esame.

185 R. CASO, *op. ult. Cit.,* 474.

186 Reperibile online all'indirizzo http://www.garanteprivacy.it/web/guest/home/docweb/-/docwebdisplay/docweb/1495246. Il documento è stato sollecitato dalle vicende giudiziarie della controversie Peppermint, in occasione del quale il Tribunale di Roma ha finito per declinare la richiesta avanzata dalla società in questione alle autorità giudiziarie affinché queste ordinassero a taluni fornitori di servizi di comunicazione elettronica di rivelare le generalità degli utenti sospetti di violazione dei diritti dalle prime rivendicati. Trib. Roma, ord. 22 novembre 2007, Foro it., 2008, I, 1329, con nota di E. TUCCI. Cfr. anche R. CASO, *Il conflitto tra copyright e privacy nelle reti peer to peer-profili di diritto comparato,* in *Diritto dell'Internet*, 2007, 471 ss.

187 Il riferimento è in particolare all'art. 5 della direttiva 2002/58/CE.

188 Cfr. i rilievi del Gruppo di Lavoro per la protezione dei dati personali, nel *Working Document on data protection issues related to intellectual property rights,* cit., 7, "The Working Party insists on the legal restrictions applying to the re-use of personal information. The content of databases, be they public or not, can only be processed and further used for a purpose compatible with the one for which they were first collected".

189 «I dati che gli utenti mettono in rete possono essere utilizzati per le finalità per le quali tale pubblicazione avviene […]. L'utilizzo dei dati dell'utente delle reti peer-to-peer può, quindi, avvenire per le finalità sue proprie e non già, in modo non trasparente, per scopi ulteriori, quali quelli perseguiti da Logistep, Peppermint e Techland», *ibid.*

190 Causa C- 275/06, *Productores de Musica de Espana (Promusicae) v. Telefonica de Espana SAU.*

prestazione di un servizio della società dell'informazione"[191] da ascrivere " agli operatori di rete, e di servizi di comunicazione elettronica, *ai fornitori di accesso alle reti di telecomunicazione ed ai fornitori di servizi si archiviazione di dati"*[192], là dove pur dovendosi escludere, sulla base delle previsioni esistenti, un *vincolo* in questo senso[193], la Corte di Giustizia, ha rimarcato la sussistenza della *facoltà* che gli stessi Stati membri hanno di prevedere simili obblighi[194], al termine di un bilanciamento tra i contrapposti interessi da condursi caso per caso, entro i confini dei singoli ordinamenti[195].

Come infatti riflesso nelle parole dell'Avvocato Generale Juliane Kokott, irrinunciabile risulta la necessità del concreto contemperamento, da operarsi nel solco del principio di proporzionalità, tra diritti di *eguale rango fondamentale*[196] secondo la Carta dei diritti fondamentali dell'Unione europea, quali il diritto d'autore, e quello alla tutela giurisdizionale ed alla riservatezza[197].

La prevalenza del diritto alla riservatezza[198], promossa sulle basi del principio cardine del divieto all'autotutela[199], sembra in questo senso derogabile unicamente in prossimità di "fattispecie particolarmente gravi", riconducibili "ad infrazioni commesse a scopo di lucro, ossia ad un uso illecito di opere protette, tale da pregiudicare gravemente il realizzo economico del titolare del diritto (d'autore)"[200], tali da giustificare l'affermazione del diritto d'autore. E difatti di fronte al "guado" di una disciplina comunitaria che, pur non imponendo l'obbligo di divulgazione dei dati personali nell'ambito di un procedimento civile, tuttavia non

191 *Ibid.* Questo l'oggetto della domanda pregiudiziale di cui il *Jugzado de lo Mercantil b.5 de Madrid* ha deciso di investire la Corte.

192 *Ibid.*. Corsivo aggiunto.

193 Questa sarà infatti la conclusione della Corte: " l'art. 15, 1 comma (dir. 2002/58) non può essere interpretato nel senso che, nelle situazioni che elenca, esso vincola gli Stati membri". Simile obbligo non discenderebbe nemmeno dalla considerazione delle direttive 2001/29, 2004/48 e 2000/31. Cfr. sul punto R. CASO, *Il conflitto tra diritto d'autore e protezione dei dati personali: appunti dal fronte euro-italiano,* cit., 473-474. Risulta a riguardo necessario rilevare una sostanziale differenza di orientamento intercorrente tra la giurisprudenza europea ed americana: infatti per quanto riguarda l'ordinamento statunitense, vi è una espressa previsione del DMCA, riguardante la c.d. *subpoena,* disciplinata alla 17 U.S.C. §512 (m), che consente ai titolari di diritti d'autore di richiedere, sulla base del mero convincimento in buona fede dell'avvenuta violazione dei diritti di esclusiva, ad alcune categorie di ISP l'identità degli utenti sospetti di violazione. Come rilevato in occasione della controversia *Recording Indus. Ass'n of Am. V. Verizon Internet Servs, Inc.*, 351 F. 3d 1229 (D.C. Cir. 2003), la norma in esame non sarebbe tuttavia da applicarsi agli *access providers. Ibid.*, 476.

194 E' necessario difatti considerare le previsioni di ci all'art. 13, 1 comma della direttiva 95/46, che autorizza gli Stati Membri a limitare la portata dell'obbligo di riservatezza dei dati personali, nei casi in cui ciò sia necessario per la tutela di altri diritti e di altre libertà altrui. *Ibid.*.

195 Cfr. D. SARTI, *Privacy e proprietà intellettuale: la Corte di giustizia in mezzo al guado,* in *Aida,* 2008, 435, ove l'A ritiene come l'effetto di tale pronuncia sia quello di porre in atto una sostanziale *disarmonizzazione* della disciplina contenuta nella nell'art. 8, 1 comma della direttiva di *enforcement* 2004/48/CE. Sul punto riflette anche A. OTTOLIA, *Proprietà intellettuale e trattamento dei dati personali: riflessioni su privacy per il sistema e nel sistema,* cit., 326. Vedi *infra* §4.

196 Cfr. *supra* nota 19.

197 L'Avvocato generale sembra in questo senso rifarsi al precedente espresso in occasione della pronuncia *Lindqvist* (causa 101/01, in *Racc.* 2003, I, 12971), ove nell'ambito di un conflitto tra privacy e libertà di espressione, la Corte ha precisato come sia necessario tutelare entrambi i diritti, attraverso la ricerca del giusto punto di equilibrio tra i medesimi. Cfr. D. SARTI, *op. cit.,* 435.

198 Cfr. A. OTTOLIA, *op. cit.,* 334 ss., ove si sottolinea come, sia nell'ordinamento italiano, sia a livello propriamente europeo, le risposte normative al problema del contemperamento tra l'interesse della tutela dei dati personali, e le "esigenze probatorie del giudizio civile", sembrino chiaramente volgersi a favore del primo. La stessa giurisprudenza italiana ha sottolineato come i diritti fondamentali alla segretezza delle comunicazioni ed alla riservatezza, di rilievo costituzionale, risultino suscettibili di compressione unicamente per la superiore esigenza di tutelare beni ritenuti rilevanti alla stregua della normativa penale. Così Trib. Roma, ord. 22 novembre 2007, cit..

199 Così ricorda R. CASO, *Il conflitto tra diritto d'autore e protezione dei dati personali: appunti dal fronte euro-italiano,* cit., 478.

200 Questi le affermazioni dell'Avvocato generale Juliane Kokott, le quali sembrano trovare pieno riscontro nel nono considerando della direttiva 2004/48/CE, da cui emerge la necessità dell'affermazione del diritto d'autore nel caso di infrazioni commesse in rete, là dove queste siano specificamente inscrivibili nel contesto di criminalità organizzata.

sembra nemmeno vietarlo[201], il vantaggio commerciale connesso alla violazione potrebbe essere criterio decisivo cui orientare il bilanciamento proposto[202].

Al concreto bilanciamento tra gli opposti interessi richiama lo stesso Gruppo per la Protezione dei Dati Personali, nella lettera inviata alla Commissione[203], in occasione della pubblicazione nel 2010 del *draft* dell'*Anti-counterfeiting Trade Agreement,* ove l'inserimento della disposizione in materia di *information related to infringement*[204] - la quale assicura l'accesso alle informazioni relative all'identità di soggetti sospetti a scopi di tutela dei diritti di esclusiva[205]- è subito apparsa del tutto incompatibile agli standard di protezione europea dei dati personali[206], e foriera di una diretta imposizione dell'obbligo del trasferimento di dati personali dal service provider al titolare di diritti sui materiali protetti, fino a questo momento lasciato alla libera discrezionalità degli Stati Membri[207].

La versione ultima del trattato, cui nel gennaio 2012 hanno aderito anche maggior parte degli Stati Membri dell'Unione[208], non sembra aver pienamente preso in considerazione i rilievi del Gruppo di Lavoro: scorre difatti tra le righe del testo, ancora, l'invito rivolto agli stati parte a promuovere- includendole nelle legislazioni nazionali- restrizioni all'accesso dei contenuti, nonché attività di monitoraggio da parte dei *service providers*, all'espresso fine della identificazione degli autori di infrazioni. L'esito ultimo, quello di una inammissibile regolarizzazione di un sistema di controllo delle informazioni personali di milioni di utenti,

201 In questo senso si è espresso anche il Gruppo di lavoro per la protezione dei dati personali, nel *Working Document on data protection issues related to intellectual property rights,* cit., 7, si sottolinea come "the Working Party recalls that no systematic obligation of surveillance and collaboration can be imposed on ISPs, pursuant to article 15 of Directive 2000/31 on electronic commerce".

202 *Ibid.,* 8: "A fair balance shall have to be found between the legitimate interests of copyright holders and individuals concerned. The criteria of the commercial advantage linked with the infringement may be decisive in this respect". In questa direzione sembra guardare anche CASO, O, *Il conflitto tra diritto d'autore e protezione dei dati personali: appunti dal fronte euro-italiano,* cit., 474.

203 Lettera del Gruppo di Lavoro per la protezione dei dati personali, indirizzata al membro della Commissione Karel de Gucht, inerente a "data protection and Privacy mplications of the Anti-counterfeiting Trade Agreement (ACTA)" del 15 luglio 2010, reperibile online all'indirizzo http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2010_07_15_letter_wp_commissioner_de_gucht_acta_en.pdf.

204 Art. 11 dell'*Anti-counterfeiting Trade Agreement Act*: "Without prejudice to its law governing privilege, the protection of confidentiality of information sources, or the processing of personal data, each Party shall provide that, in civil judicial proceedings concerning the enforcement of intellectual property rights, its judicial authorities have the authority, upon a justified request of the right holder, to order the infringer or, in the alternative, the alleged infringer, to provide to the right holder or to the judicial authorities, at least for the purpose of collecting evidence, relevant information as provided for in its applicable laws and regulations that the infringer or alleged infringer possesses or controls".

205 Espone la problematica A. C. SILVA, *Enforcing intellectual Property rights by diminishing privacy: how the Anti-counterfeiting Trade Agreement Jeopardizes the Right to Privacy,* PIJIP Research Paper No. 11. American University Washington College of Law, Washington, DC, pubblicato il 9-1-2010, reperibile online all'indirizzo http://www.auilr.org/pdf/26/26.3.4.pdf, 19-20: "On the contrary, ACTA seems to privilege expeditious access to data, without mentioning either substantive or procedural safeguards".

206 Proprio in questo senso è da interpretarsi la aggiunta, nell'articolo definitivo (art.11), della premessa "without prejudice to its law governing privilege, the protection of confidentiality of information sources, or the processing of personal data", più estesa rispetto alla originaria formulazione dell'art. 2.4 del *Draft* del 18 gennaio 2010, reperibile online all'indirizzo http://www.laquadrature.net/wiki/ACTA_20100713_version_consolidated_text, ove ci si limitava a precisare "Without prejudice to its domestic law that concerns the protection of confidentiality of information sources".

207 Si vedano sul punto i rilievi di A. C. SILVA, *op. cit.*, 17: "The obligation to identify subscribers set forth by ACTA has a broad scope also. They seem not limited to copyright enforcement, but intellectual property; additionally they extend not only to piracy and counterfeiting, as it was suggested by negotiating parties, but, also, to criminal and civil enforcement of intellectual property rights in general".

208 Tra i paesi non firmatari si ricordano anche Germania e Paesi Bassi.

che in virtù dell'automatizzazione dei processi, andrebbe ad interessare milioni di cittadini europei, indipendentemente dal fatto che siano, o meno, bersaglio di sospetti di violazione[209].

IV TUTELA DELLA PROPRIETÀ INTELLETTUALE E DEL METADATO PERSONALE ATTRAVERSO LE LENTI DEL SISTEMA: ESIGENZE CONTRAPPOSTE?

E' stato sopra osservato come nel trapasso alla digitalizzazione dei dati, le tensioni tra esigenze dell'utente finale alla privacy, e dei titolari dei diritti d'autore alla protezione dei loro contenuti si sia inasprita notevolmente[210].

L'accostamento derivante dalla comune caduta dei dati personali e dei dati oggetto di proprietà intellettuale, nell'orbita dell'indistinto flusso informativo attraversante il *web*, si è trasformato in vero e proprio conflitto dei diritti in esame, là dove l'applicazione di misure tecnologiche di protezione da parte di strutture privatizzate e altamente centralizzate, quali quelle predisponenti servizi di *cloud computing,* è riuscita a realizzare modelli di gestione di dati per mezzo delle quali lo scoraggiamento delle pratiche di pirateria, è andata di pari passo da un lato all'annichilimento degli spazi di libero utilizzo, e dall'altro alla creazione di un ineludibile sistema di controllo dei contenuti protetti, fondato sul monitoraggio delle attività e abitudini di consumo degli utenti.

La interazione in esame sembra assumere tratti del tutto particolari all'interno delle piattaforme di condivisione predisposti da terzi *cloud provider,* i quali, nel processo di archiviazione e distribuzione dei materiali, facilmente vengono a svolgere funzioni non solo di *processors* delle informazioni immesse sulla nuvola dai *content providers* titolari dei diritti d'autore*,* ma anche di *controllers* delle informazioni auto-generatesi dalla fruizione del materiale diffuso, e quindi di *profilers* nell'attività di costruzione di vere e proprie banche dati in cui ogni utente diviene centro gravitazionale di una sempre crescente catalogo di meta-dati scaturenti dalla relazione di volta in volta instauratasi tra utente stesso ed i contenuti protetti archiviati.

Necessario tuttavia rilevare come la collisione tra i due diritti in questione, non si consumi solo nel rapporto verticale tra *end user*, titolare di diritti personali, e *cloud provider,* gestore della struttura tecnologica alla cui sicurezza il *content provider* affida il proprio contenuto protetto, ma, in una prospettiva

209 "WP29 emphasizes that any form of large scale monitoring or systematic recording of data of EU citizens would be contrary to the provisions of Directive 95/46/EC since that would affect millions of individuals, regardless of whether or not they are under suspicion". Così si legge nella lettera "data protection and Privacy mplications of the Anti-counterfeiting Trade Agreement (ACTA)"*,* così si legge nella Lettera del Gruppo di Lavoro per la protezione dei dati personali, indirizzata al membro della Commissione Karel de Gucht, inerente a "data protection and Privacy mplications of the Anti-counterfeiting Trade Agreement (ACTA)", cit., 2.

210 Cfr. R. CASO, *Il conflitto tra diritto d'autore e protezione dei dati personali: appunti dal fronte euro-italiano,* cit., 469 .

diametralmente opposta, arrivi ad investire anche la relazione orizzontale tra più *end users,* là dove la natura generativa dell'informazione immagazzinata sulla nuvola dianzi discussa, potrebbe rendere possibile la creazione di diritti di proprietà intellettuale avente ad oggetto contenuti condivisi, costituiti da materiale informativo qualificabile (anche) alla stregua di dati personali protetti dalla disciplina in materia di *privacy*. Basti pensare, a scopo esemplificativo, a peculiari casi di *user generated content-* come un album fotografico, ovvero un video rappresentativo di più scene di vita quotidiana- in cui il materiale derivante dalla violazione della riservatezza, ovvero originato dalla "violazione della stessa mediante un consenso insufficiente a determinare la legittimità del trattamento"[211], possa essere al contempo tutelabile da diritti di esclusiva, in virtù dei peculiari caratteri di creatività apportati nella disposizione o nella specifica selezione dei frammenti[212]. In questi casi è stato notato come il conflitto verrebbe più precisamente ad instaurarsi tra il diritto alla riservatezza del soggetto ritratto, ed il diritto di iniziativa economica di rango costituzionale, fondamento positivo del diritto sull'opera dell'ingegno così creata[213].

In generale, sul piano sistematico, il dominio digitale della protezione del diritto d'autore sembra essersi espanso al punto da comprimere notevolmente l'opposto diritto del singolo alla tutela della propria sfera privata, nella sua duplice declinazione del più generale diritto alla riservatezza, e del più specifico diritto al controllo da parte del soggetto titolare, sui propri dati personali[214].

Come si è tentato di dimostrare nelle pagine precedenti, questa compressione non avviene unicamente in relazione al diritto individuale al controllo dei dati personali come pregiudicato nei momenti di sorveglianza traducentisi nella raccolta e catalogazione dei meta-dati, qualificabili alla stregua di dati personali giacché aventi ad oggetto modalità di fruizione dei contenuti da riferirsi inequivocabilmente alla persona degli utenti.

L'assetto strutturale del *cloud computing* viene difatti a deformare in senso restrittivo anche la seconda, più ampia accezione di *privacy*[215]*,* direttamente tangente alla libertà di autodeterminazione che, secondo la ricostruzione compiuta dalla dottrina statunitense, passa attraverso la libera scelta dell'oggetto, nonché delle modalità del consumo intellettuale: ciò viene evidentemente ostacolato dalle misure tecnologiche di protezione poste a baluardo delle opere dell'ingegno, nella rigida definizione, in via

211 Ovvero, costituito mediante " violazione della stessa mediante un consenso insufficiente a determinare la legittimità del trattamento", come sottolinea A. OTTOLIA, *Proprietà intellettuale e trattamento dei dati personali: riflessioni su privacy per il sistema e nel sistema,* cit.*,* 333 alla nota 55.

212 La giurisprudenza ha a riguardo ritenuto come la presenza di una colonna sonora possa essere in questo senso determinante. Cfr. Trib. Roma 15 gennaio 1996, ord., in *Dir. Inf.,* 96, 255.

213 Sul punto riflette ancora A. OTTOLIA, *op. cit.,* 333, nota 55.

214 A. OTTOLIA, *op. cit.,* 324-325. Per una approfondita riflessione sulla differenza tra diritto alla riservatezza e diritto alla tutela dei dati personali, si rimandi a R. PARDOLESI, *Dalla riservatezza alla protezione dei dati personali, una storia di evoluzione e discontinuità,* in ID. (a cura di), *Diritto alla riservatezza e circolazione dei dati personali,* Milano, Giuffrè, 2003.

215 Cfr. J. LITMAN, *Lawful personal use,* 85 Tex L. Rev. 1871 (2007), 1915: "Intelectual Privacy advances liberty by giving us freedom to think without surveillance and is a crucial aspect of any liberty worth having".

predeterminata, delle condizioni di accesso e di utilizzo delle medesime, così da eliminare ogni possibilità di sviluppo di spazi di libera utilizzazione.

Due sono dunque i profili di contatto tra la proprietà intellettuale e la privacy, che potremmo rispettivamente definire, dal punto di vista della prima, di natura endogena ed esogena.

Il primo aspetto rimane interamente confinato nella dimensione della protezione dei diritti d'autore: si tratta del problema della sovra-protezione apportata dalle misure tecnologiche, che a sua volta, sebbene in via indiretta, si proietta sull'annichilimento del diritto di libero godimento e soprattutto di libera elaborazione dei contenuti (si pensi al riflesso che ciò può avere in relazione alle opere derivate, ovvero a quelle collettive), il quale oscura l'orizzonte privato delle possibilità decisionali[216].

Il secondo profilo attiene invece più specificamente alla questione del controllo e dunque della sicurezza dei dati personali scaturenti dalla connessione stabilita dal sistema tecnologico tra identità dell'utente ed il contenuto protetto di cui egli fruisce entro gli schemi prefissati.

Il conflitto tra privacy e proprietà intellettuale consumantesi all'interno di servizi basati sul *cloud computing* può tuttavia assumere connotati nettamente differenti nell'ambito della tutela giurisdizionale dei diritti di esclusiva, là dove risulti necessario trattare i dati dei soggetti sospetti di violazioni.

In quest'ultimo caso appare profilarsi una diversa accezione di privacy[217], in prossimità della quale il trattamento delle informazioni personali avviene in funzione dell'applicazione delle regole dell'ordinamento relative alla giustiziabilità dei diritti ed in specie dei diritti di privativa.

Il conflitto tra opposti interessi permane, ma esso appare esulare dalle logiche di scambio e di utilizzo caratterizzanti i rapporti orizzontali tra privati, ossia tra *end user* e titolari dei diritti di proprietà intellettuale, per svilupparsi lungo una diversa direttrice che vede mutato il secondo elemento del contrasto: come taluna dottrina ha inteso mettere in evidenza infatti, il diritto al mantenimento del controllo sui dati personali rischia in simili casi di soccombere non tanto dinnanzi alla esigenza della protezione delle opere digitali, bensì di fronte al diverso diritto alla tutela giurisdizionale delle medesime[218].

A proposito è d'uopo osservare come, se da una parte ci si trovi in mancanza di una disciplina europea di sistematizzazione delle fattispecie di contrasto tra l'esercizio dei diritti in oggetto, la situazione di asimmetria così delineata tra gli ordinamenti nazionali, si trova d'altra parte ad essere mitigata da una

216 *Ibid.,* "permitting private uses advances important copyright and noncopyright interests".

217 A. OTTOLIA, *Proprietà intellettuale e trattamento dei dati personali: riflessioni su privacy per il sistema e nel sistema, passim*, definisce questa valenza della nozione di privacy come privacy *per* il sistema, in cui il dato personale, o meglio, la sua acquisizione, è "precondizione per l'applicazione di regole" da distinguersi dalla differente privacy *nel* sistema, ove il diritto alla privacy può ragionevolmente prevalere nei casi in cui l'esercizio dei diritti di privativa appaia illegittimo, come nei casi di sovra-protezione dei medesimi sopra ricordati. Secondo questa interessante ricostruzione sarebbe pertanto da distinguere una situazione di "conflitto tra valori omogenei (ovvero l'esercizio dei diritti fondamentali)" ed un'altra ove "si confrontano un diritto legittimamente esercitabile e un trattamento dei dati personali meramente strumentale all'attuazione delle norme dell'ordinamento". *Ibid.,* 333-334.

218 *Ibid.,* 334.

istanza di armonizzazione codificata nell'art. 8, 1 comma della direttiva di *enforcement*, secondo la quale gli Stati Membri "assicurano che, nel contesto di procedimenti riguardanti la violazione della proprietà intellettuale, (…) l'autorità giudiziaria competente possa ordinare che le informazione sull'origine, e sulle reti di distribuzione di merci o di prestazione di servizi che violano un diritto di proprietà intellettuale siano fornite dall'autore (...)" o, per quel che in questa sede maggiormente rileva, da "persona implicata nella (…) fornitura" dei servizi ove la violazione è venuta a consumarsi.

La individuazione dei due piani di contrasto contribuisce, secondo la ricostruzione della dottrina in esame[219], a spiegare la possibilità di coesistenza, entro le falde dell'ordinamento europeo, tra una generale condizione di "disarmonia" -inerente al bilanciamento tra diritti fondamentali aventi pari dignità gerarchica- lasciata volutamente irrisolta anche da parte della Corte di Giustizia[220], ed una norma, quale quella ora ricordata, che definisce in termini rigidamente chiari il rapporto tra proprietà intellettuale e privacy "per il sistema", nella lettera del terzo comma[221], ove si fanno salve le limitazioni poste dalle discipline nazionali a tutela di quest'ultima, e si rende così implicita la prevalenza della stessa rispetto alla protezione dei diritti di privativa. A ben vedere tuttavia, la armonizzazione attuata dalla disposizione in esame risulta confinata ad un piano del tutto superficiale: attribuendo infatti il giusto peso alla eccezione di cui alla lettera d) dell'ultimo comma, non si può fare a meno di notare come il contemperamento tra diritto alla privacy e diritto di esclusiva, anche nella sua declinazione giurisdizionale, diventi attuale unicamente in riferimento alle particolari normative in materia di trattamento dei dati.

La rilevazione della disomogeneità concettuale dei diversi momenti di contrasto sembra dunque, in questa prospettiva, perdere la sua pregnanza sul piano operativo, ove, in assenza di adeguate risposte provenienti dal fronte europeo, sono ancora le normative ed ancor più, i giudici nazionali a (sop)portare il carico dell'ineluttabilità del bilanciamento.

---

219 *Ibid.*.

220 Risulta infatti necessario precisare come sebbene il caso *Promusicae* sopra trattato abbia ad oggetto una situazione di conflitto tra i due interessi alla privacy ed alla protezione dei diritti di esclusiva, più propriamente qualificabile alla luce della impostazione qui accolta, alla stregua dell'interesse alla tutela giurisdizionale dei medesimi diritti di esclusiva, si ritiene come i rilievi mossi dalla Corte di Giustizia trattando la questione alla luce del più generale e generico problema del bilanciamento tra le opposte istanze, possano essere applicati anche agli ulteriori casi di contrasto che sono state concettualmente distinte dalla specifica ipotesi della protezione da accordare ai diritti di privativa in sede di giudizio civile.

221 Cfr. art. 8, 3 comma lett. d) della direttiva 2004/48/CE, in conformità del quale ""i paragrafi 1 e 2 si applicano fatte salve le altre disposizioni regolamentari che (…) disciplinano la protezione o la riservatezza delle fonti informative o il trattamento di dati personali".

V FUORI DAL SISTEMA: OLTRE LA DIVERSITÀ SISTEMATICA, LA DIVERSITÀ OPERATIVA DEI DATI. PARALLELISMI NEI MODELLI DI GESTIONE.

Se si è visto come, a livello di sovrastruttura giuridica, dalla digitalizzazione delle informazioni scaturiscano pretese di tutela sempre più aspre nel loro rapporto di alternatività, diverse sembrano essere le prospettive sul piano della concreta interazione operativa, là dove la natura ibrida dei meta-data, generati dalla fruizione di contenuti protetti, ora qualificabili alla stregua di dati personali, ora oggetto di "nuovi" diritti di proprietà intellettuale[222], anche nella forma di veri e propri *database rights,* mostra la strettissima interdipendenza *fattuale* delle due tipologie di dato in esame. Proprio la natura "generativa" dell'informazione transitante sulla nuvola, rende impellente una preliminare indagine *empirica* circa le tipologie dei medesimi dati transitanti sul *cloud*, sia sotto forma di *imput* (*i.e.* dati già esistenti al di fuori della nuvola ed ivi immessi), sia sotto forma di *output* (*i.e.* dati generati all'interno delle stesse piattaforme di *cloud*)[223], per muovere da qui la successiva indagine in ordine alle possibilità di qualificazione giuridica di simile materiale informativo[224], nonché di allocazione dei diritti così rilevati[225].

Di qui, la esigenza della ricerca di modelli di gestione necessariamente comuni rivela come risulti scarsamente funzionale una impostazione sistematica volta a giustificare sulla base della diversità intrinseca dei diritti, un differente assetto di tutele desunte dai distinti sistemi di privacy e di proprietà intellettuale.

Prima ancora che oggetto di differenti diritti, al fine di individuare la strada per la ricomposizione del conflitto[226], sarà opportuno considerare gli stessi dati come appartenenti ad una uniformante categoria di informazione digitale[227], da cui muovere per individuare le regole di corretto *management* del flusso informazionale[228].

---

222 Cfr. D. J. GERVAIS , *The tangled web of UGC: Making copyright sense of User-generated content,* cit., 9 ss.. Sul punto si vedano anche le riflessioni di C. REED, *Information ownership in the cloud,* cit., 8 in relazione alle informazioni generate all'interno del *cloud* e qualificabili alla stregua di *trade marks* o *know-how*.

223 Si ricordi la classificazione compiuta da S. AHMED, *Data portability: Key to cloud Portability,* cit., 6 ss., ove l'A. effettua una accurata distinzione tra *user data, associated data* e *system data.*

224 C. REED, *op. cit., passim.*

225 Cfr. W. ODOM- A. SELLEN- R. HARPER- E. THERESKA, *Lost in translation, Understanding the possession of Digital Things in the Cloud,* CHI'12, May 5–10, 2012, Austin, Texas, USA, reperibile online all'indirizzo http://research.microsoft.com/pubs/158029/odom2012.pdf.

226 In questo senso P. GUARDA, *Privacy e fruizione della conoscenza scientifica,* cit., 115.

227 *Ibid.*: "Meglio sarebbe cominciare ad interrogarsi sul fatto che essi possono essere considerati per quello che sono nel mondo digitale, cioè informazioni, e, dunque, ripensare regole, tecnologie e costumi alla luce di questa categoria uniformante".

228 *Ibid.,* 115-116. Sulla stessa linea anche V. MAYER-SCHOENBERGER, *Beyond copyright: managing information Rights with DRM,* cit., 1863. "information privacy governance happens largely beyond individual enforcement of individual privacy rights, and is taking place through governance mechanisms that information privacy intermediaries utilize. This yields a system of information privacy protection that is much larger, more complex and varied, and likely more effective, than individual information privacy rights. This is not peculiar to information privacy. We can find a similar system beyond rights in the area of copyright (in the United States) and authors' rights (in the European Union), in which a range of special intermediaries play a central role".

Ed infatti, con il profilarsi di misure tecnologiche di protezione tanto sofisticate, da identificarsi, in virtù del controllo operato, con i contenuti che intende proteggere[229], si capisce come taluna dottrina abbia avuto ragione di parlare in questo contesto di un processo di "assimilazione" delle informazioni[230], ugualmente espresse nella forma di *bit stream*[231].

Simile *reductio ad unum* sul piano fattuale, risulta diretto frutto di una standardizzazione dei processi di elaborazione dei dati, per cui sarà possibile gestire allo stesso modo modo informazioni personali, protette da diritto d'autore[232], o da entrambe[233], o ancora anche informazioni libere[234].

Nonostante sia stato affermato come questa meccanizzazione dei trattamenti sia resa possibile da un sostanziale "agnosticismo tecnologico"[235] in relazione alla natura giuridica dei dati processati, è evidente come la configurazione in un modo o nell'altro degli standard di funzionamento abbia diretta incidenza sulla tenuta degli opposti diritti, e di conseguenza sul grado di protezione a questi accordato. In questa prospettiva non si può fare a meno di notare come la precedentemente inneggiata neutralità della rete[236] sia fortemente venuta meno in costanza di strutture di gestione digitale dei dati nettamente sbilanciate a favore della tutela dei contenuti protetti, a tutto pregiudizio delle facoltà di controllo sui dati personali messi a disposizione a favore dell'utente[237].

Ciò è enormemente accentuato nella dimensione del *cloud computing*, là dove gli stessi dati personali vengono esportati su piattaforme allocate nelle più differenti parti del globo, ed in cui la eventuale presenza di *sub-providers* rende poco chiaro il numero degli addetti che hanno accesso ai medesimi dati[238].

Il problema del controllo di quel sovra-strato informazionale, generato dalla fruizione del materiale protetto messo in circolazione attraverso le piattaforme di *cloud computing,* induce alla considerazione *fattuale*

---

229 Vedi *supra,* nota 57.

230 A. OTTOLIA, *Proprietà intellettuale e trattamento dei dati personali: riflessioni su privacy per il sistema e nel sistema,* cit., 321.

231 In questo senso V. MAYER-SCHOENBERGER, *Beyond copyright: managing information Rights with DRM,* cit., 189: " Technically, these different types of content are all the same: stream of bits (…)".

232 Sul punto A. OTTOLIA, *op. cit.,* 321

233 Si rimandi a L. UBERTAZZI, *I diritti d'autore e connessi,* cit., 140 ss.

234 Sia consentito il rinvio a P. SAMUELSON, *Mapping the Digital Public Domain: Threats and Opportunities,* 66 Law and Contemp. Probs. 2002, 1135 ss..

235 L'espressione è tratta da V. MAYER-SCHOENBERGER, *op. cit.,* 189: "As DRM systems are built to control access to "digital" information, they are fundamentally rights agnostic—that is, they can in principle restrict any digital bit stream".

236 Obbligato il rimando a T. WU, *network neutrality broadband discrimination,* Journal of Telecommunications and High Technology Law, Vol. 2, p. 141, 2003. Il tema della neutralità della rete e della sua diminuzione di fronte alla diffusione di servizi di telecomunicazione di *broadband* era stato già messo in evidenza da L. LESSIG-M. LEMLEY, *The end of the end-to-end: preserving the Architecture of the Internet in the broadband Era,* 48 UCLA law Rev., 925-972 (2001). Per rilievi inerenti al fronte europeo si veda la Consultazione sulla neutralità della rete disposta dalla Commissione europea, il 30-6-2010, reperibile online all'indirizzo www.ec.europe/information_society.

237 La questione dell'influenza che la regolazione del livello dei contenuti, ed in particolare quella dei dati personali, ha sul modello di infrastruttura aperta o chiusa, è stata più volte messa in evidenza dalla dottrina che ha analizzato la interdipendenza del c.d. livello logico (*software* e standard tecnologici utilizzati) e quello della architettura della rete. Per una rassegna di posizioni si rimandi a A. OTTOLIA, *op. cit.,* 320, in particolare nota 7.

238 Cfr. A. DEVORE, *Cloud Computing: Privacy storm on the horizon?,* 20. ALB. L.J. SCI. & TECH. 365 (2010), 370. Sottolinea inoltre i forti rischi legati alla divulgazione di tali dati di natura personale sedimentati sulla nuvola, ai poteri pubblici, C. SOGHOIAN, *Caught in the cloud: Privacy, Encryption, and government back doors in the web 2.0 era,* Journal on Telecommunications and High Technology Law, Vol. 8, No. 2, 2010, 396 ss., 393-394.

dei dati oggetto dei differenti diritti: in questa prospettiva, le opposte esigenze giuridiche della protezione dei contenuti e della sicurezza delle informazioni personali, sembrano ricomporsi nel frangente operativo dei modelli di gestione suggeriti.

Al fine di individuare un regime comune di gestione delle differenti informazioni[239], sulla scia di una corrente dottrinale che ha individuato la *intellectual property* come la più efficiente forma di *information privacy*[240], l'ipotesi della riconduzione, operata da taluni sul piano teorico[241], dei diritti sui dati personali[242] e dei diritti di proprietà intellettuale al comune denominatore dei diritti di proprietà[243], è stata trasposta al settore dei sistemi digitali attraverso la proposizione di modelli gestionali, entro i quali il trattamento dei (meta)dati personali verrebbe ad essere razionalizzato attraverso le medesime misure tecnologiche poste a protezione della proprietà intellettuale[244], e più nello specifico, mediante le stesse tecnologie di *digital rights management*[245].

Le forti incoerenze teoriche[246] che un simile approccio presenta, sono nondimeno accompagnate da notevoli complicazioni anche sul piano della fattibilità tecnologica[247].

---

239 Riflette sul punto anche A. OTTOLIA, *Proprietà intellettuale e trattamento dei dati personali: riflessioni su privacy per il sistema e nel sistema,* cit., 324.

240 Questa è la soluzione sondata, anche se poi declinata da P. SAMUELSON, *Mapping the Digital Public Domain: Threats and Opportunities,* cit., 1135 ss.. L'argomento è stato trattato anche da L. LESSIG, *The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRAC. 56, 58 (1999),e per un contributo più recente si veda P. M. SCHWARTZ, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2058 (2004).

241 La tesi è particolarmente caldeggiata da R. C. DREYFUS, *Warren and Brandeis Redux: Finding (more) privacy protection in intellectual property law,* Stan. Tech. L. Rev. 8 (1999)

242 Sulla sensibilmente diversa concezione della *privacy* tra Europa e Stati Uniti, cfr. P. SAMUELSON, *Privacy as intellectual property?,* 52 *Stan*. L. Rev., 1125, 1130 (2000). Preziose le indicazioni di A. OTTOLIA, *op. cit., passim.*

243 Nel panorama della dottrina italiana si volge in questo senso anche L. UBERTAZZI, *I diritti d'autore e connessi,* cit., 137 e 146, in cui l'A. preferisce ricondurre il diritto al controllo sui dati personali alla categoria dei diritti di esclusiva, piuttosto che a quelli della personalità, individuando nella necessità della prestazione del consenso come condizione di utilizzo dei dati personali, sottenda la natura disponibile, e pertanto patrimoniale dell'interesse protetto; inoltre si sofferma sulla considerazione che la disciplina della *privacy* interessi anche le persone giuridiche, in relazione alle quali non si può parlare di interesse della personalità. Rimane tuttavia dominante, in Europa, la considerazione del diritto alla privacy, in particolare nella sua accezione di diritto alla riservatezza, come diritto fondamentale della persona, e pertanto indisponibile. Sul punto A. OTTOLIA, *op. cit.,* 324-325, con particolare riguardo alla nota 22. Si veda inoltre *supra,* nota 19.

244 Cfr. V. MAYER-SCHOENBERGER, *Beyond copyright: managing information Rights with DRM,* cit., 190: «Intellectual property is but one right over information our legal system recognize. DRM systems could potentially be used to manage other rights over information. Given how much we expose personal information on the Internet and the extent to which this exposure is abused, one obvious candidate for such an extension could be informational privacy- the management and protection of personal information».

245 Lo stesso Gruppo di Lavoro per la tutela dei dati personali nel, ha sottolineato come "guardando al futuro i sistemi di gestione di diritti digitali (DRM- Digital Rights Management) potrebbero essere in grado di definire e securizzare, fino ad un certo punto, l'accesso o l'impiego di dati personali in modo individuale e su base contrattuale. Tali applicazioni non sono mature, perché esistono solo in qualche laboratorio di ricerca e richiedono il supporto di un quadro normativo stabilito". Così si legge alla pag. 3 del "Documento di lavoro sulle piattaforme informatiche fidate, in particolare per quanto riguarda il lavoro effettuato da Trusted Computing Group (Gruppo TCG)" adottato il 23 gennaio 2004, consultabile all'indirizzo http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp86_it.pdf .

246 Inevitabilmente diversa appare difatti la *ratio* posta a giustificazione della proprietarizzazione degli uni e degli altri diritti. Se infatti la teoria c.d. utilitarista intende giustificare l'attribuzione all'autore di diritti di proprietà sulle opere create, di modo da rendere possibile la commercializzazione della stessa, ed il conseguente godimento dei frutti così ottenuti, di modo da creare incentivi alla produzione di nuove opere, così promuovendo il progresso delle "Arti e della Scienza", la proprietarizzazione dei dati personali avrebbe la opposta, auspicata funzione di restringere il flusso e la diffusione dei medesimi. Cfr. P. SAMUELSON, *op. cit*., 1143-1144. Non trascurabili si rivelano inoltre i rischi pratici connessi alla totale perdita di controllo sulle informazioni personali in caso di alienazione a terzi. Sul punto riflette anche V. MAYER-SCHOENBERGER, *op. cit.,* 196: " Through the act of propertization, the originator loses control of her personal information and cannot stop it from being used by others who have legitimately obtained "ownership" rights over it". In senso critico rispetto alla applicazione della teoria dei property rights all'informazione, anche R. CASO, *Il signore degli anelli nel ciberspazio,* cit., 136-137, ove si osserva come "diversamente dalle cose materiali le informazioni, che sono per natura non escludibili e non rivali, non soffrono del problema della scarsità e del sovrasfruttamento. Si può costruire un sistema di esclusiva per incentivare la produzione di informazione, ma tale sistema non è l'unico possibile".

Ravvisata la scarsa fattibilità di applicare ai dati personali le medesime misure tecnologiche di protezione ideate in funzione della protezione dei diritti d'autore, si profila un'ulteriore alternativa, costituita da infrastrutture di gestione comune tecnicamente sensibili delle differenze intercorrenti tra i diritti, e dunque tra gli interessi a queste ultime connesse[248].

La vivacità della sfida[249] della ricerca di strategie tecnologiche funzionali al bilanciamento delle differenti istanze in gioco, è riflessa nei numerosi progetti di *Trusted Cloud Computing* che stanno andando diffondendosi[250], ed alcuni interessanti spunti possono in questo senso essere ricavati anche dal Progetto sorto in territorio italiano del Digital Media[251].

Da notare come la questione della ricerca di adeguati modelli di gestione dei dati presenti profili di alta problematicità proprio in relazione al governo di quelle informazioni personali, indicate in questa sede con il termine di metadati e specificamente ricavati e archiviati attraverso il monitoraggio della fruizione dei contenuti protetti mediante apposite misure tecnologiche di protezione, quali i sistemi di *digital rights management*[252]. In questo senso, la adozione di misure di anonimizzazione degli stessi dati[253] potrebbe costituire adeguato rimedio al rischio della mercificazione del patrimonio informativo avente ad oggetto le abitudini di consumo dei *cloud clients*, giacché una volta reciso il legame tra informazione stessa ed il suo

---

247 Come è stato infatti notato, le misure tecnologiche di protezione, ed in specie i sistemi di DRM, si basano su tag e marcatori di controllo: difficile sarebbe in questo senso costruire un sistema di tal fatta in relazione alla gestione dei dati personali, là dove le dimensioni contenutistiche di questi ultimi risulterebbero spesso inferiori a quelle dello stesso marcatore che deve essere in questi ultimi incorporato ai fini del controllo Cfr. V. MAYER-SCHOENBERGER, *Beyond copyright: managing information Rights with DRM,* cit., 193: "In such cases the meta-data defining permissible usage would be substantially bigger than the informational content it intends to protect, requiring DRM system builders to fundamentally adjust their systems, while steganography and similar methods of "hiding" and "embedding" meta-data would have to be replaced by more robust mechanisms that work without depending on a relative size difference between meta-data and protected content".

248 *Ibid.,* 196-198. In questa direzione si volge anche Il Gruppo di Lavoro per la tutela dei dati personali, nelle righe conclusive del "Working document on data protection issues related to intellectual property rights", pubblicato il 18 gennaio 2005, reperibile online all'indirizzo http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp104_en.pdf, ove si legge: "the working Party calls for a development of technical tools offering privacy compliant properties, and mor generally for a transparent and limited use of unique identifiers, with a choice option for the user".

249 Così A. PALMIERI, *Digital Rights Management e disciplina europea della protezione dei dati personali,* cit., 200.

250 Cfr. N. SANTOS-K. GUMMADI-R. RODRIGUES, *Towards Trusted Cloud Computing,* Hot Cloud 2009, reperibile all'indirizzo http://www.usenix.org/event/hotcloud09/tech/full_papers/santos.pdf.

251 Nel documento "Digital Media in Italia" , recante il titolo di "Specifiche funzionali, azioni normative e governance per la realizzazione della proposta dmin.it" , reperibile online all'indirizzo http://www.dmin.it/proposta/proposta-operativa.htm, si sottolinea, in relazione ai sistemi DRM, come "la «la concorrenza tra diverse tecnologie DRM possa instaurarsi anche su parametri attinenti alla 'qualità giuridica' (in particolare, il rispetto dei diritti e degli interessi degli utenti finali). In un contesto in cui gli utenti di *digital media* possono scegliere DRM con restrizioni tecnologiche meno rigide, processi di negoziazione trasparenti e bidirezionali (cioè capaci di allargare il ventaglio delle scelte dell'utente rispetto al "prendere o lasciare" tipico della contrattazione standardizzata), nonché un monitoraggio della fruizione meno invasivo della *privacy,* il mercato potrebbe essere orientato verso una concorrenza virtuosa nella quale accanto al prezzo e ad altri parametri figuri la "qualità giuridica" del DRM".

252 Per quanto riguarda il problema generale della protezione dei dati personale, basti ricordare, per quanto non costituisca oggetto della presente trattazione, che adeguati sistemi di protezione degli stessi dati transitanti attraverso piattaforme di cloud computing, sono già stati implementati, mediante il ricorso a tecniche di criptazione, funzionanti attraverso chiavi create dallo stesso utente e di cui il *cloud provider* non entra in possesso. E' quanto avviene con Weave Software di Firefox. Lo spiega C. SOGHOIAN, *Caught in the cloud: Privacy, Encryption, and government back doors in the web 2.0 era,* cit., 396 ss.: "Mozilla baked privacy into the product at the design stages, stating that a key principle of the project that "users own their data, and have complete control over its use. Users need to explicitly enable third parties to access their data." As a result, the data that Weave users store on Mozilla's servers is encrypted with a key created by that user, which is not shared with anyone else". Come viene affermato, questa soluzione non è destinata a rimanere isolata, e sono già stati pubblicati numerosi studi sul tema. Cfr. KAMARA-LAUTER, *Cryptographic cloud storage,* reperibile online all'indirizzo http://research.microsoft.com/pubs/112576/crypto-cloud.pdf.

253 Come codificazione, pseudonimizzazione irreversibile, data *aggregation* o *barnadisation,* W. HON-C. MILLARD- I. WALDEN, *The problem of "personal Data" in Cloud Computing- What information is regulated?, the cloud of unknowing, part 1,* cit., 21.

titolare[254], questo potrebbe essere liberamente messa in circolazione, ed essere, ad esempio, comunicata a terzi per scopi statistici. A proposito è stato tuttavia notato come l'efficacia di simili strumenti risulti in concreto compromessa dalle sempre più sofisticate tecniche di associazione e combinazione dei dati medesimi, le quali, a loro volta, si riflettono in un più ampio grado di identificabilità dei soggetti titolari[255].

Appare allo stesso modo difficilmente praticabile la via della criptazione delle informazioni in questione, là dove questa generalmente avviene per mano dell'utente prima del trasferimento al *provider,* mentre maggiormente improbabile, sebbene non da escludere del tutto[256], appare l'ipotesi che quest'ultimo provveda a criptare i dati generati dalla fruizione del suo stesso servizio da parte del cliente.

Oltre alle grida di coloro[257] che invocano l'implementazione di *policies* più attente al valore della *privacy*[258]*,* e una più rigida applicazione dei principi normativi sopra richiamati, primi tra tutti quelli di finalità e pertinenza del trattamento[259], vi è chi, cerca il perno dei rimedi in supporti di natura prettamente tecnologica[260], mediante la costruzione di sistemi *privacy-oriented*[261]*,* ossia conformati in funzione del rispetto dei principi di sicurezza, finalità e necessità del trattamento dei dati[262].

Come è stato osservato, gli stessi provider potrebbero avere incentivi all'adozione di simili modelli, in quanto la stessa riduzione del volume dei dati identificativi collezionati ed archiviati, riducendo il diametro del controllo e dunque del monitoraggio esercitabile, restringerebbe al contempo i rischi di scivolare nelle ipotesi di responsabilità vicaria[263].

Proprio l'inscindibile legame che si instaura in questi dati personali e quelli oggetto di diritti d'autore rende ancora più urgente la necessità di giungere ad espedienti tecnologici, che vadano ad agire, sanandoli,

---

254 Sostenitrice di simili tecniche di anonimizzazione risulta anche J. COHEN, *DRM and privacy*, cit., 612: "designers should consider whether the desired benefit can be achieved without capturing the precise identity of the user, *or withou tying users to content*". Corsivo aggiunto.

255 "this reinforces the present reality that current techniques, such as removing or scrambling direct identifiers, and/or aggregating data, may be of little effect in anonimysing data irreversibly", così W. HON-C. MILLARD- I. WALDEN, *The problem of "personal Data" in Cloud Computing- What information is regulated?, the cloud of unknowing, part 1,* cit., 22.

256 "However the provider may also apply cryptography to data, to enable it to use or sell the anonymised or pseudonymised data (by applying 1-way or 2-way cryptography to identifiers and the like), or to enable it to store data more securely (applying 2-way cryptography to the full data set)". *Ibid*., 23.

257 Sul punto si rinvia a A. PALMIERI, *Digital Rights Management e disciplina europea della protezione dei dati personali,* cit., 200-201.

258 Interessanti a riguardo i rilievi formulati dalla *Federal Trade Commission* nel documento *Protecting Consumer Privacy in an era of rapid change. A proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report, cit.,* 44, ove si esortano le imprese ad "implement and enforce procedurally sound privacy practices throughout theri organizations" anche mediante una più funzionale formazione del personale, volta a prevenire il rischio dei c.d. *insider breaches*. Sul punto anche A. DEVORE, *Cloud Computing: Privacy storm on the horizon?,* cit., 370.

259 Specifica la questione S. BYGRAVE, *Digital Rights Management and Privacy, Legal Aspects in the European Union,* cit., 436 ss. Parla dell'esigenza di *Building intellectual privacy into law,* nel tentativo di passare in rassegna standard utili a tal fine anche COHEN, *op. cit.,* 588 ss..

260 Così quella parte di dottrina che pone l'attenzione a soluzioni del già citato *value sensitive design. Ex multis,* per un'analisi approfondita sul tema si rinvia ancora a J. COHEN, *op. cit.,* 609 ss.

261 Cfr. A. PALMIERI, *op. cit.,* 210 ss. Cfr. anche C. SOGHOIAN, *Caught in the cloud: Privacy, Encryption, and government back doors in the web 2.0 era,* cit., 396 ss. Per ulteriori precisazioni si veda *infra.*

262 Si confrontino a riguardo i considerando 9 e 30 della direttiva 2002/58. Riflette sul punto anche A. MANTELERO, *Data protection e attività di impresa, verso dove guardano gli usa?,* cit., 473.

263 Questa la tesi di A. PALMIERI, *Digital Rights Management e disciplina europea della protezione dei dati personali,* cit., 212, cfr. anche R. JULIA-BARCELO'-K. J. KOELMAN, *Intermediary Liability, Intermediary liability in the e-commerce directive: so far so good, but it's not enough,* cit., *passim.*

proprio su quei momenti di *vulnus*, in cui la legittima necessità della *privacy* intellettuale impallidisce dinnanzi alla ragione della tutela della proprietà intellettuale.

In questa prospettiva, nelle pagine precedenti sono state individuati tre distinti punti critici, consistenti rispettivamente nelle restrizioni all'accesso, nel successivo monitoraggio, nonché nell'attivazione di strumenti di autotutela. Al fine di impedire una intollerabile compromissione della sfera privata dell'utente, le proposte addotte vanno nel senso della declinazione della progettazione delle infrastrutture del servizio di *cloud computing,* lungo le direttrici delle tre corrispondenti garanzie, inerenti in primo luogo alla conservazione di idonei margini di libertà nella fruizione del contenuto stesso, quindi alla riduzione delle possibilità di trattamento dei dati personali da parte del *provider,* ed infine alla limitazione dell'utilizzazione di misure di autotutela[264].

E' in questo modo che nei casi in cui la nuvola divenga veicolo di opere dell'ingegno, risulta necessario procedere alla "incorporazione del bilanciamento di interessi contrapposti"[265], attuando così il riequilibrio della bilancia valoriale, ad ora eccessivamente pendente da un lato.

La chiamata in giudizio della ingegneria informatica non rende tuttavia meno impellenti più decise soluzioni da parte dell'ingegneria normativa: nella convinzione che le risposte siano da ricercarsi *anche,* ma non *solo* nella macchina[266], non si affievolisca la curiosità dell'interprete di scorgerle tra le righe del prossimo regolamento generale sulla protezione dei dati[267], nella forma, ad esempio, della definizione di più precisi strumenti di *accountability*[268]*,* volti ad assicurare una maggiore e più effettiva aderenza delle pratiche dei *data processors* e/o *controllers,* ai principi generali già sedimentati nel bacino della disciplina in materia di *data protection*[269].

264 Queste le soluzioni cui giunge J. COHEN, *DRM and privacy,* cit., 610 ss..

265 Così R. CASO, *Il signore degli anelli nel ciberspazio,* Cit., 144.

266 C. CLARK, *The answer to the machine is in the machine*, in B. HUGENHOLZ (a cura di), T*he future of copyright in a digital environment*, Kluwer, L'Aja, 1996, 139 ss.

267 Si veda a riguardo la *Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali ed alla libera circolazione di tali dati,* Bruxelles, 25 gennaio 2012, reperibile online all'indirizzo http://eur-lex.europa.eu/LexUriServ/LexUriServ.douri=COM:2012:0011:FIN:IT:PDF.

268 Cfr. Gruppo di Lavoro per la protezione dei dati personali nella *Opinion 5/2012 on Cloud Computing,* adottato il 1 luglio 2012, reperibile online all'indirizzo http://ec.europa.eu/justice/dataprotection/article29/documentation/opinionrecommendation/files/2012/wp196_en.pdf, 16: "IT accountability is particularly important in order to investigate personal data breaches, where cloud clients, providers and sub-processor may each bear a degree of operational responsibility. The ability for the cloud platform to provide reliable monitoring and comprehensive logging mechanisms is of paramount importance in this regard".

269 In questa direzione si volge ancora una volta il Gruppo di Lavoro per la tutela dei dati personali, come emerge dalle precisazioni contenute nella *Opinion 3/2010 on the principle of accountability,* adottato 13 luglio 2010, reperibile online all'indirizzo http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf, 10, ove si rileva come "the new provision does not aim at subjecting data controllers to new principles but rather at ensuring de facto, effective compliance with existing ones".