Informatica e diritto, XXXV annata, Vol. XVIII, 2009, n. 1, pp. 123-134

Privacy e *design*

UGO PAGALLO*

SOMMARIO: *1. Introduzione – 2. Teoria giuridica del* design *– 3. Il* design *nella protezione dei dati personali – 4. La posta in gioco tra informatica e diritto – 5. Conclusioni*

1. INTRODUZIONE

Nella prima edizione di *The Sciences of Artificial*, pubblicato per i tipi della MIT Press nel 1969, Herbert A. Simon lamentava lo stato di abbandono, teoretico e accademico, in cui versava la "scienza del *design*"[1]. A giudizio del futuro premio Nobel, "rispetto alle norme prevalenti, la rispettabilità accademica esige che le materie trattate debbano essere intellettualmente robuste, analitiche, formalizzabili ed insegnabili. Nel passato, molto, se non la maggior parte, di ciò che sapevamo attorno al *design* e le scienze artificiali era intellettualmente sommesso, intuitivo, informale e artigianale"[2].

Trent'anni dopo, in *Code and Other Laws of Cyberspace*, era il turno di Lawrence Lessig per stigmatizzare il fatto che, malgrado il ruolo cruciale svolto dall'architettura, o "codice", nel perseguimento di finalità sociali o collettive, i giuristi avessero per lo più riservato scarsa attenzione all'impatto del *design* nei rapporti intersoggettivi[3].

Molta acqua, da allora, è passata sotto i ponti.

Innanzitutto, lo stesso Simon ricorda nella terza edizione di *The Sciences of Artificial* (1996), come, a partire dalla metà degli anni settanta, con la fondazione del *Design Research Center* presso la Carnegie Mellon University, sia venuta emergendo e consolidandosi una vera e propria "scienza del *design*". "In sostanza, la teoria del design mira ad ampliare le capacità dei

* L'Autore è professore ordinario di Filosofia del diritto alla Facoltà di Giurisprudenza dell'Università di Torino, Faculty del Center for Transnational Legal Studies di Londra.

[1] Il richiamo va sin d'ora alla terza edizione di H.A. SIMON, *The Sciences of Artificial*, Cambridge, Mass.-London, MIT Press, 1996. Si tenga presente che, sempre nel 1969, appariva la prima edizione di N. POTTER, *What Is a Designer*, London, Hyphen Press, 2002.

[2] H. A. SIMON, *The Sciences of Artificial*, cit., p. 112.

[3] Si v. infatti L. LESSIG, *Code and Other Laws of Cyberspace*, New York, Basic Books, 1999, pp. 91-92.

computer nel dare aiuto al design, attingendo ai mezzi della intelligenza artificiale e della ricerca operativa"[4].

Nel frattempo, è venuta del pari maturando la consapevolezza dei giuristi, nonché dei legislatori e autorità garanti in materia di tutela dei dati personali, a proposito del ruolo svolto dal *design* sul piano delle relazioni intersoggettive. Dopo il fugace richiamo nel considerando 46 della direttiva 95/46/CE – dove il termine *design* è reso nella versione italiana come "momento della progettazione" – la formula *privacy by design* è stata coniata alla fine degli anni novanta dal Commissario per la *privacy* dell'Ontario, in Canada, Ann Cavoukian. La formula, poco più tardi, sarebbe stata ripresa in alcuni testi ufficiali, tra cui il *Privacy Design Principles for an Integrated Justice System* presentato, nell'aprile 2000, dal Dipartimento della giustizia nordamericano e dal Commissario per la *privacy* dell'Ontario. Più di recente, il 1° dicembre 2009, il Gruppo di lavoro *ex* art. 29 D-95/46/CE, insieme al Gruppo di lavoro per la polizia e la giustizia, ha pubblicato un documento su "Il Futuro della Privacy", in cui viene dato ampio spazio, appunto, al "nuovo principio della *privacy by design*".

Il crescente interesse dei giuristi per i temi (informatici) del *design*, specie in materia di tutela e trattamento dei dati personali, rischia tuttavia di ingenerare un equivoco. Secondo il titolo del presente saggio e come già capitato ad altri e ben più autorevoli scritti – penso solo a *Verità e metodo* di Hans-Georg Gadamer, o a *Dio e stato* di Hans Kelsen – bisogna infatti stabilire se la "e" del rapporto tra *privacy* e *design* abbia un senso congiuntivo o disgiuntivo. Se, cioè, si propugni la tutela della *privacy* come *design* o il *design* come una modalità di tutela dei dati personali.

Al fine di chiarire i termini della questione, il presente saggio è suddiviso in quattro parti.

In primo luogo, illustro i termini generali del problema, vale a dire come il *design* incida sul fenomeno giuridico e sulla disciplina delle relazioni intersoggettive.

Secondariamente, spiego come le prospettive in tema di *design* siano state in concreto declinate in materia di tutela dei dati personali.

[4] H.A. SIMON, *The Sciences of Artificial*, cit., p. 114.

Quindi, esamino sia le tesi sulla *privacy* come *design* sia quelle del *design* come *una* modalità di tutela nel trattamento dei dati personali.

Dopo di che, sarà giunto il momento di trarre le conclusioni.

2. Teoria giuridica del *design*

È stato indubbiamente merito di Lessig aver attirato l'attenzione dei giuristi sui modi in cui il *design* determini e/o condizioni il comportamento dei soggetti, sia nel mondo reale sia nel mondo virtuale di internet[5].

Per quanto riguarda il mondo reale, è sufficiente menzionare i ponti di Long Island, costruiti in modo da bloccare il transito degli autobus, oppure l'impiego dei dossi nei fondi stradali per ridurre la velocità delle automobili (dossi che, con la consueta sagacia tropicale, sono soprannominati in Venezuela "poliziotti sdraiati"). Per quanto attiene al mondo virtuale di Internet, si rifletta invece sui "codici" TCP/IP e http, nell'intreccio con questioni di anonimato in rete e *spamming*, oltre ai temi relativi alla tutela del *copyright* con l'uso di DRM (*Digital Rights Management*).

Ulteriori ricerche sono state condotte nell'ambito del diritto penale[6], dell'architettura di Internet e del suo impatto sul piano delle garanzie costituzionali[7], e via dicendo.

Ma, si deve forse a Karen Yeung il primo tentativo di elaborare una compiuta teoria generale del *design* in ambito giuridico[8].

In questa sede, possiamo concentrarci sui due aspetti più rilevanti della tassonomia proposta.

[5] Cfr. L. Lessig, *Code and Other Laws*, cit., pp. 90-98.

[6] Si v. ad esempio N.K. Katyal, *Architecture as Crime Control*, in "Yale Law Journal", 2002, 111, pp. 1039-1139; nonché Id., *Digital Architecture as Crime Control*, in "Yale Law Journal", 2003, 112, pp. 101-129.

[7] J. Zittrain, *The Future of the Internet and How to Stop It*, New Haven, CT, Yale University Press, 2008.

[8] Cfr. K. Yeung, *Towards an Understanding of Regulation by Design*, in Brownsword R., Yeung K. (eds.), "Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes", London, Hart Publishing, 2007, pp. 79-108. In questa sede possiamo lasciare in parentesi altre utili suddivisioni come, ad esempio, quella proposta da N. Potter, *What Is a Designer*, cit., p. 4, per cui occorre distinguere tra oggetti (*design* di prodotto), luoghi (*design* ambientale) e, infine, messaggi (*design* di comunicazione).

In primo luogo, occorre prestare attenzione all'*oggetto* che volta per volta si regola attraverso uno specifico *design*: la progettazione può infatti riguardare non solo spazi e luoghi (i ponti di Long Island o i dossi stradali ricordati precedentemente), oppure prodotti e processi produttivi (come nel caso dei DRM). In realtà, il *design* concerne anche la riconfigurazione di organismi viventi come piante, animali ed esseri umani: nell'ordine, è il caso degli OGM, dei salmoni geneticamente modificati e di tutto l'odierno dibattito in tema di post-umano e *cyborgs*.

In secondo luogo, bisogna far caso alle stesse *modalità* del *design*: la progettazione può avere il fine di modificare il comportamento dei soggetti, oppure, di ridurre l'impatto di eventi dannosi o, infine, di prevenire del tutto la possibilità che quel presunto evento dannoso si verifichi.

Per illustrare la prima ipotesi, è sufficiente tornare al *design* dei dossi come forma per invogliare un comportamento più prudente: perfino il più incallito automobilista italiano emulo di Alonso dovrebbe pensarci su due volte prima di sfrecciare a centoventi in una strada nella quale egli sa che corre il rischio di sfasciare la propria macchina!

Quanto alla seconda modalità di *design* e rimanendo nell'universo delle automobili, basti citare l'*air-bag*.

Infine, rispetto all'obiettivo di garantire una prevenzione totale tramite *design*, è sufficiente menzionare le macchine intelligenti in grado di arrestarsi o ridurre la velocità a seconda che siate stanchi o ubriachi oppure delle congiunture dell'ambiente circostante[9].

Delle nove combinazioni possibili proposte dallo schema, quali, dunque, i casi più pertinenti al tema della *privacy* e *design*? Esclusi, va da sé, i casi di progettazione su piante e animali come i salmoni geneticamente modificati, quali le ipotesi più interessanti riguardo al trattamento e tutela dei dati personali?

[9] Lungi dall'essere un mero esempio di *science fiction*, segnalo al lettore che su questi temi va lavorando la Cattedra UNESCO in "*data privacy* e comunicazioni macchina-macchina" presso Tarragona, in Spagna. Oltre alle pubblicazioni in rete di Josep Domingo-Ferrer, si v. la sua comunicazione *The "Backwards, Forwards and Sideways" Changes of ICT*, in Arias-Oliva M., Bynum T.W., Rogerson S., Torres-Corona T. (eds.), "ETHICOMP 2010", Tarragona, URV, 2010.

3. Il *design* nella protezione dei dati personali

Nei lavori di Ann Cavoukian, alla quale dobbiamo, forse, non solo la formula *privacy by design* ma altresì quella di PETs ossia *Privacy Enhancing Technologies*, troviamo una guida efficace per cominciare a chiarire il rapporto tra *privacy* e, appunto, *design*[10].

In sostanza, l'idea è che le misure a tutela della *privacy* debbano essere presenti sin dalla fase di progettazione degli strumenti preposti al trattamento ed elaborazione dei dati, affinché, secondo il principio di minimizzazione, tali sistemi possano raccogliere, processare e utilizzare la minore quantità possibile o, se del caso, nessun tipo di dato personale. Con gli esempi proposti dai Gruppi di lavoro comunitari[11], si pensi ai sistemi di video-sorveglianza nel settore dei trasporti pubblici, che dovrebbero essere progettati in modo tale da non permettere il riconoscimento dei volti (salvo, ovviamente, per il caso di delitti); oppure, si considerino i sistemi di elaborazione dei dati negli ospedali, in cui i nomi dei pazienti ed altri elementi identificativi dovrebbero essere tenuti rigorosamente separati dai dati sullo stato di salute e relativi trattamenti medici.

Oltre al rispetto del principio di minimizzazione, i sistemi per la raccolta e il trattamento dei dati dovrebbero essere progettati al fine di garantire l'effettivo controllo degli interessati sui propri dati personali, di pari passo con la trasparenza del sistema, vale a dire che i titolari dei dati possano essere sufficientemente informati sulle modalità operative del sistema stesso. Ad esempio, il disegno degli interfaccia informatici dovrebbe essere "intuitivo" per l'utente o, come suole dirsi, *user friendly*. Tra i vari meccanismi, è il caso dell'inserimento di collegamenti semplici ed efficaci per la richiesta d'informazioni o l'inoltro di reclami da parte degli utenti, impostando al contempo il sistema in modo tale che la minimizzazione della raccolta e la condivisione dei dati avvengano, specie nei servizi di *social network*, per *default*[12].

[10] Cfr. A. Cavoukian, *Privacy by Design*, Ottawa, IPC Publications, 2009.

[11] Si v. il documento, presentato il 1° dicembre 2009 dal Gruppo di lavoro *ex* art. 29 D-95/46/CE e dal Gruppo di lavoro per la polizia e la giustizia, "Il Futuro della Privacy" – 02356/09/EN WP 168, specie parr. 44-53.

[12] La questione, sollevata dal Gruppo di lavoro *ex* art. 29 nell'Opinione 5 del 12 giugno 2009 (01189/09/EN - WP 163), è stata al centro del convegno su *Intelligent Privacy*

Tra i vari approcci informatici, una particolare menzione va fatta al settore delle ontologie giuridiche[13]. L'obiettivo di questi sistemi consiste infatti nel rappresentare la conoscenza *iuris et de iure* con la formalizzazione dei concetti tradizionalmente impiegati dai giuristi – come norme, diritti o doveri – affinché una macchina possa comprendere e processare tale informazione. Distinguendo i compiti tra le ontologie che elaborano tutti i concetti più rilevanti del dominio interessato con l'uso di tassonomie, e le ontologie che includono le sole regole e restrizioni concernenti quello stesso dominio, l'obiettivo è di offrire maggiori garanzie nelle fasi di accesso, conservazione, gestione e uso degli archivi informatici contenenti dati personali, automatizzando i processi di tutela e trattamento di quei dati.

Naturalmente, gli accorgimenti a tutela della *privacy* non soltanto riguardano il *design* dei prodotti o dei processi produttivi. Come ricordato dai Garanti europei nel parere su "Il Futuro della Privacy", sarebbe opportuno che gli strumenti di identificazione biometrica non rinviino alle informazioni contenute in banche dati ma, sotto forma di *smart card*, che tali dati siano piuttosto tenuti sotto il diretto controllo degli interessati.

Tuttavia, che dire sulle finalità di questi accorgimenti? Si tratta di trasformare il comportamento dei soggetti e ridurre il rischio che accadano eventi dannosi? E se invece l'idea fosse quella di eliminare alla radice la stessa possibilità che quell'evento dannoso accada?

A ben vedere, è proprio quest'ultimo il punto principale che finisce per dividere spesso il parere di politici ed esperti. Attraverso le accortezze del *design*, si mira a rendere effettivo il quadro normativo e le sanzioni previ-

Management Symposium, organizzato presso l'Università di Stanford, CA., il 22-24 marzo 2010, cui hanno partecipato alcuni dei giganti del settore quali Google, Facebook, Apple, ecc. Il programma su http://research.it.uts.edu.au/magic/privacy2010/.

[13] Si v. ad esempio D. Abou-Tair e S. Berlik, *An Ontology-based Approach for Managing and Maintaining Privacy in Information Systems*, in "Lectures notes in computer science", Heidelberg, Springer, 2006, n. 4275, pp. 983-994; H. Mitre, A. Gonzalez-Tablas, B. Ramos, A. Ribagonda, *A Legal Ontology to Support Privacy Preservation in Location-based Services*, in "Lecture notes in computer science", Heidelberg, Springer, 2006, n. 4278, pp. 1755-1764; nonché G. Lioukadis, G. Lioudakisa, E. Koutsoloukasa, N. Tselikasa, S. Kapellakia, G. Prezerakosa, D. Kaklamania, I. Venierisa, *A Middleware Architecture for Privacy Protection*, in "The International Journal of Computer and Telecommunications Networking", 2007, 51(16), pp. 4679-4696.

ste dai legislatori competenti, come suggerito dalle Autorità garanti per la *privacy* in Europa, oppure, come propende il Commissario per la *privacy* in Ontario, è forse il caso di sostituire progressivamente quelle norme e sanzioni, spesso del tutto inefficaci, con automatismi tecnici?

4. La posta in gioco tra informatica e diritto

La concreta possibilità di automatizzare molti meccanismi di tutela a presidio della *privacy* sembra per molti versi auspicabile, tenuto conto dei problemi, non solo tecnici ma latamente culturali, sorti con l'impiego delle nuove tecnologie dell'informazione e della comunicazione (ICT). Per dirla con le stesse Autorità garanti europee, "gli utenti dei servizi di ICT – dal business al settore pubblico e certamente gli individui – non sono in condizione di assumere da soli rilevanti misure di sicurezza al fine di proteggere i dati personali propri o di altri soggetti. Ne consegue che tali servizi e tecnologie dovrebbero essere progettati [*designed*] implementando la *privacy* per *default*"[14].

Gli automatismi a presidio della *privacy*, d'altra parte, sembrano in grado di far fronte a molte delle deficienze caratterizzanti l'odierno stato dell'arte sia nel limitare la discrezionalità dei burocrati, riguardo al ri-uso della informazione nel settore pubblico, sia, come riferisco nel prossimo paragrafo, per quanto concerne le questioni di competenza e giurisdizione[15].

Di fronte al progresso tecnologico, non di meno, sussistono fondati motivi di perplessità rispetto all'ipotesi di automatizzare l'applicazione della legge, fino al punto da renderla "perfetta" a fini di prevenzione. Secondo il giudizio di Jonathan Zittrain, "la perfetta applicabilità [della legge] fa svanire la pubblica comprensione del diritto in quanto la sua applicazione [automatica] elimina un utile interfaccia tra i termini della legge e la sua imposizione. Parte di ciò che ci rende umani sono le scelte che facciamo ogni giorno su quel che rappresenta alcunché di giusto o

[14] Si v. il par. 45 del più volte citato documento su "Il Futuro della Privacy".

[15] Me ne sono ampiamente occupato in *Sul principio di responsabilità giuridica in rete*, in "Il diritto dell'informazione e dell'informatica", XXV, n. 4-5, 2009, pp. 705-734, nonché, con E. Bassi, in *The Future of the EU Working Parties' "The Future of Privacy" and the Principle of Privacy by Design*, in Bottis M. (ed.), "Proceedings of the Third International Seminar on Information Law" (Corfù, 24-25 giugno 2010), INSEIT (in corso di pubblicazione).

sbagliato (…). In un ambiente monitorato e sorvegliato del tutto, quelle stesse scelte svaniscono"[16].

Oltre a motivi di natura morale e filosofico-giuridica, ci sono poi questioni prettamente pratiche che finiscono per incidere sulle scelte politiche di fondo. Come ricorda Karen Yeung, "non solo è inevitabile il rischio di fallimenti operativi, ma la finalità di disegnare standard che siano in grado di raggiungere l'obiettivo desiderato dal regolatore in forma precisa e accurata, non può che essere, con ogni evenienza, un'impresa improba"[17]. La ragione la spiega esaurientemente uno dei massimi esperti del settore, Eugene Spafford: "L'unico sistema [informatico] realmente sicuro è quello che sia stato spento, messo dentro a un blocco di cemento e sigillato a piombo in una stanza attorniata da guardie giurate – e anche così avrei i miei dubbi"[18].

Del resto, ritroviamo con Spafford alcuni dei problemi emersi con le ricerche di ontologie giuridiche di cui al paragrafo precedente[19].

La formalizzazione delle disposizioni normative in materia di tutela dei dati personali non solo ha a che fare con nozioni rigorosamente definibili in termini di ruoli, processi o relazioni, come ad esempio avviene con le tradizionali categorie dell'obbligo, del divieto o del permesso. Molti dei concetti chiave in tema di *privacy* dipendono strettamente dal contesto in cui essi vanno inseriti: a partire dall'idea di dato personale, basta far caso alla definizione di "responsabile del trattamento" che, a giudizio del Gruppo di lavoro *ex* art. 29 D-95/46/CE, deve essere inteso come "un concetto funzionale, volto a stabilire le responsabilità in rapporto alle circostanze del caso e, per ciò, basato su un'analisi di tipo fattuale più che di stampo analitico"[20].

[16] Cfr. J. ZITTRAIN, *Perfect Enforcement on Tomorrow's Internet*, in Brownsword R., Yeung K., "Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes", London, Hart Publishing, 2007, pp. 125-156.

[17] K. YEUNG, *Towards an Understanding of Regulation by Design*, cit., p. 106.

[18] S. GARFINKEL, G. SPAFFORD, *Web Security & Commerce*, Sebastopol, O'Reilly, 1997, p. 9.

[19] Un quadro d'assieme nell'*Introduzione* a Breuker J., Casanovas P., Klein M.C.A., Francesconi E. (eds.), "Law, Ontologies and the Semantic Web: Channelling the Legal Information Flood", Amsterdam, IOS Press, 2008, specie pp. 12-14.

[20] Si v. l'Opinione 1, adottata il 16 febbraio 2010, sui concetti di "controllore" e "processore" (00264/10/EN – WP 169), p. 9.

L'obiettiva difficoltà di formalizzare alcuni concetti cardine della disciplina ha per ciò consigliato di adottare una strategia "dal basso verso l'alto" che, individuando soluzioni per classi di sotto-problemi nonché per specifiche attuazioni della normativa, possa approdare per gradi a un approccio globale della materia[21].

Più in dettaglio, la procedura prevede che, dopo la fase preparatoria relativa all'individuazione dei requisiti ontologico-giuridici relativi al campo prescelto, segua la fase di sviluppo del progetto con l'acquisizione della conoscenza tramite il sapere degli esperti, con l'inserimento dei documenti normativi e il possibile riutilizzo delle informazioni. La formalizzazione in classi, relazioni, proprietà e casi del modello dovrà poi essere sottoposta nuovamente al parere degli esperti e, infine, testata nella fase di valutazione del modello stesso attraverso l'analisi della consistenza interna e la verifica empirica che Herbert A. Simon illustrava come "ciclo del test dinamico"[22].

Come ben si vede, siamo ben lungi dalle tentazioni di garantire una "perfetta applicazione della legge"; almeno nell'ambito della tutela e protezione dei dati personali, l'alternativa secca tra la *privacy* come *design* e il *design* come una modalità di attuazione della legge, appare allo stato astratta e pure fuorviante. I timori per una "applicabilità automatica" della legge si traducono, più prosaicamente, nell'odierno dibattito sull'impostazione dei servizi di Google Buzz e, cioè, se lo scambio dei dati e informazioni debba avere per *default* natura "pubblica" o "privata"[23].

L'intenzione non è però di suggerire, attraverso le difficoltà cui vanno incontro le ricerche sulle ontologie giuridiche applicate alla *privacy*, un

[21] La difficoltà non rileva naturalmente nel solo ambito della tutela dei dati o per gli approcci dell'ontologia giuridica ma, piuttosto, in linea generale, dipende dalla necessità di ridurre la complessità informativa di sistemi, come quelli giuridici, soggetti a evoluzione nei propri concetti e rapporti. Me ne occupo in *As Law Goes By: Topology, Ontology, Evolution*, in Casanovas P., Pagallo U., Sartor G., Ajani G. (eds.), "AI Approaches to the Complexity of Legal Systems", Heidelberg, Springer, 2010, pp. 5-11.

[22] Cfr. H.A. SIMON, *The Sciences of Artificial*, cit., pp. 128-130.

[23] Si v. infatti la lettera aperta che, lo scorso 19 aprile 2010, il Commissario per la *privacy* in Canada, Jennifer Stoddart, insieme alle Autorità Garanti di Francia, Germania, Israele, Italia, Irlanda, Nuova Zelanda, Olanda, Regno Unito e Spagna, hanno mandato al capo esecutivo di Google, Eric Schmidt, a proposito delle nuove questioni di tutela dei dati personali sollevate da Buzz.

salomonico compromesso per cui il tradizionale apparato repressivo della legge andrebbe integrato con la progressiva estensione degli ambiti affidati all'automatismo tecnologico. Piuttosto, i limiti dell'odierna tecnologia con i suoi sistemi esperti invitano a riflettere sui vicoli ciechi che affliggono, nell'odierna società dell'informazione, la canonica rappresentazione del diritto come insieme di comandi suffragati da sanzioni fisiche.

In sede conclusiva, occorre ritornare al caso chiave dei conflitti di competenza e giurisdizione cui si è fatto cenno in precedenza.

5. Conclusioni

Tra i profili giuridici più rilevanti della "rivoluzione informatica"[24], spicca il fatto che quanto per secoli era l'eccezione, sta diventando la regola, ovvero che eventi e transazioni tra individui finiscano per avere sempre, virtualmente, natura e carattere transnazionali[25].

Nel caso della tutela dei dati personali, un esempio lampante per mostrare cosa ciò significhi sul piano delle garanzie e competenze giurisdizionali, è dato dai *cookie*, vale a dire i *file* di testo posti sul disco rigido del vostro computer da parte dei siti *web* che state per lo più visitando nel navigare in Internet. Provate soltanto a disattivare la funzione *default* del vostro apparecchio!

Sin dal 30 maggio 2002, con il documento 5035/01/IT – WP 56, il Gruppo di lavoro *ex* art. 29 D-95/46/CE ha avanzato la tesi che l'uso dei *cookie* debba essere inteso alla stregua degli "strumenti" previsti dall'art. 4.1(c) della predetta normativa comunitaria. Se l'obiettivo dichiarato è di "garantire che una persona non sia priva di tutela per quanto riguarda il trattamento effettuato nel suo paese per il solo fatto che il responsabile non è stabilito sul territorio comunitario", la tesi, nondimeno, finisce per confliggere sia con la lettera che con lo spirito della direttiva, conducen-

[24] Cfr. T.W. Bynum, *Introduzione* a Floridi L., "Infosfera. Etica e filosofia nell'età dell'informazione", Torino, Giappichelli, 2009.

[25] Il punto è stato segnalato con forza, ormai due lustri or sono, da David Post nella sua critica alle tesi tradizionali di Jack Goldsmith sul diritto internazionale pubblico e privato. Si v. J. Goldsmith, *Against Cybernarchy*, in "University of Chicago Law Review", 1998, 65, pp. 1199-1250; e D. Post, *Against "Against Cyberanarchy"*, in "Berkeley Technological Law Review", 2002, 17, pp. 1365-1383.

do a esiti paradossali: le giurisdizioni europee sarebbero infatti competenti anche nel caso in cui un indiano o un cinese dovessero mai visitare un 'proprio' sito *web* durante le loro vacanze a Capri…

Più pragmaticamente, nell'Opinione del GEPD, ossia del Garante europeo per la protezione della *privacy*, Peter Hustinx, c'è da dire che questo approccio "non garantirà la piena protezione ai soggetti europei in una società disposta a rete, in cui le frontiere fisiche perdono importanza (…): l'informazione su internet è onnipresente, ma la giurisdizione del legislatore europeo non lo è"[26].

Tra le soluzioni prospettate dal GEPD per sopperire ai limiti di competenza delle autorità, non solo comunitarie, in materia di *privacy*, va annoverata l'elaborazione di un "quadro globale" per la protezione dei dati personali, sulla base delle linee guida elaborate dall'ONU e dall'OCSE; marco entro il quale sviluppare la cooperazione con altri organismi internazionali e con paesi terzi, anche in materia giurisdizionale, tramite accordi di stampo bilaterale o multilaterale.

Avendo, però, presente altri fattori rilevanti quali la corruzione e le istanze censorie di molti Paesi[27], nonché marcati contrasti politici tra le stesse istituzioni e Stati membri dell'UE[28], sembra proprio necessario integrare il "quadro globale" del GEPD con alcuni degli accorgimenti tecnologici discussi in questa sede.

Come detto, l'intento non è garantire un'"automatica applicazione della legge" in modo da prevenire del tutto la possibilità che si verifichi una qualsiasi trasgressione della *privacy*. Piuttosto, tramite il *design*, occorre attenuare il rischio che si verifichino eventi dannosi, consentendo agli individui di approntare da sé misure di sicurezza a tutela dei dati altrui o propri. È sotto questo punto di vista che può dunque scorgersi la possibile con-

[26] Si v. il par. 42 dell'Opinione del 25 luglio 2007 (EDPS, 2007/C 255/01).

[27] Cfr. solo R.J. Deibert, J.G. Palfrey, R. Rohozinski, J. Zittrain, *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge, Mass., MIT Press, 2008.

[28] Tra i casi più significativi si pensi al regime del trattamento dati PNR, di cui mi sono ampiamente occupato in *La tutela della privacy negli Stati Uniti d'America e in Europa*, Milano, Giuffrè, 2008, pp. 157-196. Più di recente si v. E. Brouwer, *The EU Passenger Name Record (PNR) System and Human Rights: Transferring Passenger Data or Passenger Freedom?*, CEPS Working Document n. 320, settembre 2009.

vergenza tra le tesi delle Autorità Garanti europee nel ricordato documento su "Il Futuro della Privacy" e le considerazioni del Commissario per la *privacy* in Ontario, secondo cui "dovesse mai crescere bene nel futuro, la privacy per design garantirebbe il futuro della privacy"[29].

Non si tratta, infatti, di rovesciare semplicemente le idee di chi, in nome dei ricavati tecnologici, si è peritato di annunciare nel corso degli ultimi anni la morte della *privacy*[30].

Si tratta al contrario di maturare la consapevolezza che molti dei problemi che affliggono l'odierna protezione dei dati personali s'intrecciano con le questioni coltivate ormai da tempo in altri campi, circa i profili di natura cognitiva, psicologica e tecnica del *design*[31].

Senza pretendere che gli accorgimenti tecnici del *design* ci indichino quale sarà mai il futuro della *privacy*, c'è da credere che proprio dal *design* avremo modo di comprendere molto sulla *privacy* del futuro.

[29] A. CAVOUKIAN, *Privacy by Design*, cit., p. 7.

[30] Tra i vari profeti mi limito a ricordare C. SYKES, *The End of Privacy. The Attack on Personal Rights at Home, at Work, On-Line, and in Court*, New York, St. Martin's Griffin, 1999; S. JARFINKEL, *Database Nation. The Death of Privacy in the 21st Century*, Sebastopol, O'Reilly, 2000; nonché D.H. HOLTZMAN, *Privacy Lost. How Technology Is Endangering Your Privacy*, San Francisco, Jossey-Bass, 2006.

[31] Si v. ad esempio D.A. NORMAN, *The Design of Future Things*, New York, Basic Books 2007; e S. KRUG, *Don't Make Me Think*, Indianapolis, New Riders, 2005.