ALESSANDRO MANTELERO

DATA PROTECTION ED ATTIVITÀ DI IMPRESA. VERSO DOVE GUARDANO GLI USA?

SOMMARIO: 1. La tutela dei dati nel contesto globale. — 2. Luci e (non poche) ombre del nuovo *framework* delineato dal DoC e dalla FTC: l'equilibrio fra regolamentazione statuale ed autoregolamentazione. — 3. (*segue*) il ruolo del consenso. — 4. Conclusioni.

1. LA TUTELA DEI DATI NEL CONTESTO GLOBALE.

Nel dicembre 2010, con due distinti documenti ufficiali — del Department of Commerce (DOC) e della Federal Trade Commission (FTC)[1] —, gli Stati Uniti hanno palesemente ed espressamente manifestato l'intenzione di affermare la propria visione dell'*informational privacy*, ritenendo sussistente « an urgent need to renew our commitment to leadership in the global privacy policy debate »[2]. Il riferimento alla *leadership* tradisce la consapevolezza che in realtà negli ultimi due decenni la primazia in materia di tutela dei dati personali si sia spostata in Europa.

Gli USA sono certamente « a leader in the global Internet economy »[3] (anche qui non è più un primato incontrastato), tuttavia è stata l'Unione europea a darsi per prima un modello organico e condiviso in grado di rispondere alle esigenze di tutela dei dati personali e di contemperarle con gli altri interessi in conflitto. Non solo, tale modello, grazie ad un'acuta scelta di strategia normativa, è stato esportato al di fuori dei confini dell'Unione, adot-

[1] Cfr. THE DEPARTMENT OF COMMERCE INTERNET POLICY TASK FORCE, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, December 2010, pubblicato in *http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf*, e FEDERAL TRADE COMMISSION, *Protecting Consumer Privacy in an Era of Rapid Change. A Proposed Framework for Businesses and Policymakers. Preliminary FTC Staff Report*, December 2010, pubblicato in *http://www.ftc.gov/os/2010/12/101201privacyreport.pdf*. Tutti i siti web richiamati nel presente lavoro sono stati consultati fra il 10 febbraio 2011 ed il 18 aprile 2011.

[2] Cfr. THE DEPARTMENT OF COMMERCE INTERNET POLICY TASK FORCE, *Commercial Data Privacy and Innovation in the Internet Economy*, citato *supra*, p. 6.

[3] Cfr. *ult. loc. cit.*

tato o usato come esempio per legislazioni di diverse nazioni, ed è divenuto in ogni caso parametro necessario di confronto.

Nello specifico, l'Unione europea con la dir. 95/46/CE, nel definire precise regole per chi voglia ricevere informazioni personali provenienti da *partner* operanti nell'Unione, ha assunto una posizione politica « forte » che ha costretto gli altri Paesi ad implementare *standard* conformi a quelli comunitari, pena il pregiudizio di tutti quei rapporti economici, e sono la quasi totalità, per i quali si rende necessario un trattamento di dati transfrontaliero[4]. Non a caso anche una grande potenza commerciale e politica quale gli Stati Uniti è dovuta venire letteralmente a patti per assicurare alle proprie aziende il perdurare dello scambio di dati con le controllate, i *partner* d'affari ed i clienti europei[5].

Laddove il modello non è circolato a livello normativo, si è poi diffuso per via contrattuale, in virtù del dettato dell'art. 26 della dir. 95/46/CE, ai sensi del quale è possibile fissare per contratto le garanzie minime a tutela dei soggetti interessati dal trattamento, anche avvalendosi di clausole-tipo definite e preventivamente approvate dalla Commissione Europea[6]. In tal maniera si è ulteriormente facilitata l'espansione del paradigma comunitario, rendendo le imprese comunitarie una sorta di vettore per l'affermazione delle politiche e degli *standard* dell'Unione[7].

[4] Cfr. art. 25 dir. 95/46/CE, ove si prevede che il trasferimento verso un Paese terzo di dati personali possa avvenire « soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato », che andrà valutato tenendo conto di tutte le circostanze relative al trasferimento dati (natura dei dati, finalità del trattamento, paese d'origine, paese di destinazione finale, normativa vigente nel paese terzo, regole professionali e misure di sicurezza ivi osservate). Per un elenco dei Paesi che hanno soddisfatto tale requisito, cfr. *http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm*.

[5] Ovviamente la natura della « controparte » ha influito sull'accordo, per cui i *Safe Harbor Privacy Principles*, con le annesse *Frequently Asked Questions*, frutto della negoziazione, benché ritenuti fonte di adeguata protezione (cfr. decisione della Commissione europea 2000/520/CE del 26 luglio 2000), non offrono tuttavia un livello di garanzia comparabile con quello derivante dalla direttiva comunitaria.

[6] Cfr. Decisione della Commissione del 15 giugno 2001, C(2001)1539, poi modificata con Decisione della Commissione del 27 dicembre 2004 C(2004)5271, e Decisione della Commissione del 5 febbraio 2010, C(2010)593. Benché ai sensi dell'art. 26, paragrafo 2, della dir. 95/46/CE, sia comunque possibile fissare contrattualmente in maniera autonoma « adeguate garanzie per i diritti dell'interessato », il ricorso alle clausole-tipo pare tuttavia preferibile poiché esclude l'alea del giudizio di « adeguatezza » sulle pattuizioni *ad hoc* create dai contraenti, esonera dagli adempimenti formali correlati a tale giudizio e, dato non trascurabile in un'ottica d'impresa, azzera i tempi procedurali.

[7] Per completezza va in proposito però osservato come la direttiva comunitaria preveda anche ipotesi di deroga in cui il trasferimento verso Paesi terzi può avvenire a prescindere dal rispetto del criterio dell'adeguatezza, cfr. art. 26 dir. 95/46/CE. Benché quest'ultima norma individui nel consenso dell'interessato e nel perseguimento di finalità contrattuali due elementi sufficienti ad escludere il giudizio sull'adeguatezza, in un'ottica di semplificazione degli adempimenti, di uniformità del trattamento e, soprattutto, di certezza delle situazioni giuridiche, pare tuttavia più agevole per l'impresa il ricorso alla diversa soluzione delle clausole-tipo, che esclude in radice qualsiasi questione interpretativa circa la legittimità dell'applicazione del regime derogatorio, quanto la necessità di provvedere *ex ante* agli opportu-

Il quadro dei rapporti in materia di regolamentazione del trattamento dati alle soglie del secondo decennio del nuovo millennio appare dunque attribuire all'Unione europea un ruolo primario, definendo uno dei campi in cui la normativa comunitaria è presa ad esempio dagli altri Paesi. Cui va aggiunta una tendenza — talora non esente da critiche — emersa di recente a livello comunitario orientata ad una visione pan-europea della *data protection*[8]. Tenuto conto delle implicazioni che tutto ciò comporta in termini di organizzazione dell'attività di impresa e di gestione della ricchezza rappresentata dalle informazioni personali, diviene allora evidente come i recenti ed autorevoli interventi d'Oltreoceano in materia siano mirati ad evitare un'europeizzazione del modello statunitense ed una prospettiva recessiva dello stesso su scala globale.

Al riguardo va infatti ricordato come gli Stati Uniti, pur vantando un significativo retroterra culturale in materia di *informational privacy* che trae origine dal *right to privacy*[9], hanno tuttavia sempre ritenuto di evitare una regolamentazione unitaria e generale a tutela dei dati personali, prediligendo invece interventi settoriali federali[10], cui si sono talvolta affiancati altri provvedi-

ni adempimenti, quale l'acquisizione del consenso *ad hoc*.

[8] Cfr. da ultimo l'intervento del Commissario europeo per la giustizia V. REDING, *Your data, your rights: Safeguarding your privacy in a connected world Privacy Platform*, SPEECH/11/183, Bruxelles, 16 March 2011, p. 3, in *http://europa.eu/rapid/pressReleasesAction.do?reference=-SPEECH/11/183*: « homogeneous privacy standards for European citizens should apply independently of the area of the world in which their data is being processed. They should apply whatever the geographical location of the service provider and whatever technical means used to provide the service. There should be no exceptions for third countries' service providers controlling our citizens' data. Any company operating in the EU market or any online product that is targeted at EU consumers must comply with EU rules... To enforce the EU law, national privacy watchdogs shall be endowed with powers to investigate and engage in legal proceedings against non-EU data controllers whose services target EU consumers ». Si veda anche ARTICOLO 29-GRUPPO DI LAVORO PER LA TUTELA DEI DATI PERSONALI, *Parere 8/2010 sul diritto applicabile*, Bruxelles, 16 dicembre 2010, 27 e 35, in *http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_it.pdf*, secondo cui l'interpretazione estensiva dell'art. 4, paragrafo 1, lett. *c*), dir. 95/46/CE, incentrata sui mezzi/strumenti impiegati per il trattamento, « ha mostrato di avere conseguenze indesiderate, fra cui una possibile applicazione universale del diritto dell'UE »; a tal proposito potrebbe essere utile in termini di certezza del diritto, introdurre « un fattore di collegamento più specifico, che tenga conto dell'eventuale attività mirata a persone [presenti sul territorio dell'Unione europea] », nonché « appoggiare l'applicazione della direttiva a un responsabile del trattamento per l'intero trattamento nella misura in cui il collegamento con l'UE è effettivo e non tenue ». Cfr. anche ARTICOLO 29-GRUPPO DI LAVORO PER LA TUTELA DEI DATI PERSONALI, *Tutela della vita privata su Internet - Un approccio integrato dell'EU alla protezione dei dati on-line* -, Bruxelles, 21 novembre 2000, 30 s., in *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37it.pdf*, nonché i successivi *Parere 1/2008 sugli aspetti della protezione dei dati connessi ai motori di ricerca*, Bruxelles, 4 aprile 2008, 11, e *Parere 5/2009 sui social network on-line*, Bruxelles, 12 giugno 2009, 5.

[9] Sia consentito rinviare, in ragione dell'economia del presente lavoro alla più ampia trattazione svolta in A. MANTELERO, *Il costo della privacy tra valore della persona e ragione d'impresa*, Milano, 2007, p. 1 ss.

[10] Cfr. a riguardo: Health Insurance Portability and Accountability Act (HIPAA) del 1996, Pub. L. No. 104-191 (codificato nel title 42 U.S.C.) 45 C.F.R. 164

menti specifici di fonte statuale. Con particolare riferimento all'attività di impresa è poi prevalsa una strategia orientata a rimettere la tutela dei dati alla negoziazione fra i privati, dando luogo ad un pluralismo che ha sfavorito la definizione di requisiti minimi comuni in materia di informativa, di diritto di accesso e di sicurezza dei dati, ma soprattutto non ha permesso di ravvisare nel consenso espresso ed informato al trattamento dati un momento autonomo e necessario degli accordi contrattuali.

Nello specifico la Federal Trade Commission, nell'ambito della propria competenza in materia di trattamento dati dei consumatori, ha supportato il c.d. « notice-and-choice model », che se da un lato era volto a rendere potenzialmente edotti i consumatori circa le *privacy policies* delle imprese, d'altro canto conviveva con la possibilità di un ampio ricorso al consenso implicito, per giunta in un contesto in cui, come rileva la stessa FTC, « the notice-and-choice model, as implemented, has led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand »[11]. Tale modello ha inoltre trascurato gli ulteriori aspetti che tradizionalmente dovrebbero caratterizzare la tutela dei dati personali, a cominciare dall'esercizio del diritto d'accesso, al rispetto dei principi di necessità e di finalità, nonché all'attenzione per le misure di sicurezza[12].

Sempre in un'ottica di un intervento minimo su questi temi, la FTC ha altresì adottato il c.d. « harm-based model, » rinunciando ad una tutela ad ampio spettro del consumatore con riferimento al trattamento dati ed optando invece per un intervento di protezione in ragione di specifiche tipologie di danno potenziale (« physical security, economic injury, and unwanted intrusions into their daily lives »)[13].

(HIPAA Privacy and Security Rules); Gramm-Leach-Bliley Act (GLBA), Title V del Financial Services Modernization Act del 1999 (codificato nel 15 U.S.C. §§ 6801, 6809, 6821, and 6827); 16 C.F.R. 313; Family Educational Rights and Privacy Act (FERPA) del 1974 (codificato in 20 U.S.C. § 1232g *et seq.*); 34 C.F.R. 99; Individuals with Disabilities Education Act (IDEA) del 1970, come rivisto dal Individuals with Disabilities Education Improvement Act del 2004, (codificato in 20 U.S.C. § 1400 *et seq.*, in specie 20 U.S.C. § 1412(a)(8)); Children's Online Privacy Protection Act (COPPA) del 1998, Pub. L. No. 105-277 (codificato in 15 U.S.C. § 6501 *et seq.*); v. anche 16 C.F.R. part 312. Cfr. in proposito THE DEPARTMENT OF COMMERCE INTERNET POLICY TASK FORCE, *Commercial Data Privacy and Innovation in the Internet Economy*, citato *supra*, p. 60: « Commenters argue that this puzzle results from the sectoral approach having been created backwards. Rather than coming up with an overall picture and then breaking it up into smaller pieces that mesh together, Congress has been sporadically creating individual pieces of ad hoc legislation. Commenters noted that this approach confuses consumers and creates large gaps in consumer protection ».

[11] Cfr. FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, citato *supra*, p. iii.

[12] Cfr. FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, citato *supra*, p. 20.

[13] Cfr. FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, citato *supra*, p. iii. Ad oggi è la stessa FTC ad ammettere la limitatezza di un simile approccio, posto che anche solo il fatto che il trattamento avvenga all'insaputa dell'interessato o in maniera difforme da quanto

Stante tale diversità di orientamento fra le due sponde dell'Atlantico e l'attuale « capacità espansiva » mostrata dalla legislazione comunitaria, si comprende come, anche dai documenti ufficiali statunitensi, emerga una certa ansia nel voler ribadire la bontà del modello americano rispetto a quelli esistenti, quasi a voler sottolineare come l'evidente passo verso una maggior tutela dei dati e disciplina del trattamento non costituisca un mutamento rispetto alle politiche precedenti. In proposito è invece chiaro come questo nuovo corso dell'amministrazione statunitense riveli un cambiamento di orizzonte volgendo lo sguardo dall'impostazione tradizionale, che demandava all'autonomia privata la tutela dei dati, verso una maggior regolamentazione della materia[14], seppur minimale. Da qui l'interrogativo circa l'archetipo a cui guardano i regolatori d'Oltreoceano, onde valutare quanto esso si avvicini a quello comunitario e quanto invece esso non rappresenti uno stadio ancora intermedio rispetto a quest'ultimo, riconfermando così il maggior grado di maturità della riflessione europea, anche alla luce delle attuali istanze di revisione della dir. 95/46/CE.

2. Luci e (non poche) ombre del nuovo *framework* delineato dal DoC e dalla FTC: l'equilibrio fra regolamentazione statuale ed autoregolamentazione.

Prima di procedere alla disamina critica del nuovo *framework*, occorre sottolineare come esso non costituisca un intervento di carattere generale, come fu invece la dir. 95/46/CE, bensì risulti circoscritto alla *commercial data privacy*, ovvero alla tutela dei consumatori. Va tuttavia osservato in proposito come questo rappresenti un limite (in parte giustificato dall'ambito di tutela già assicurato dal generale *right to privacy* e da leggi *ad hoc*[15]) destinato a rivelarsi poco incisivo nel contesto dell'attività d'impresa, posto che i

dichiarato può essere fonte di pregiudizio, a prescindere dall'effettiva produzione di un danno economico, fisico o relazionale; cfr. FTC, *op. cit.*, p. 20: « for some consumers, the actual range of privacy related harms is much wider and includes reputational harm, as well as the fear of being monitored or simply having private information "out there" ».

[14] Diversi progetti di legge federale sono attualmente pendenti, alcuni settoriali, altri di più ampio spettro. In particolare fra i primi si possono ricordare i seguenti introdotti nel 2011: il « Do Not Track Me Online Act » inerente la profilazione degli utenti *on-line* ed il riconoscimento dei diritti di accesso ai dati; il « Financial Information Privacy Act » che prevede l'informativa ed il consenso preventivo alla comunicazione a terze parti, mutando l'attuale regime dell'*opt-out*; l'« Equal Employment for All Act » sul divieto di utilizzo dei rapporti creditizi nel mercato del lavoro. Un approccio generale è invece proprio del « BEST PRACTICES Act » del 2010, in cui vengono fissati i principi generali per il trattamento dati, adottando un modello di *opt-in* per la comunicazione a terze parti dei dati e fissando una disciplina di maggior protezione per i dati sensibili, tra cui figurano anche quelli finanziari. Sempre a carattere generale i più recenti « Consumer Privacy Protection Act » (2011) e « Commercial Privacy Bill of Rights Act » (2011).

[15] Cfr. *supra* nota 10.

dati impiegati per fini commerciali costituiscono una congerie così ampia da comprendere informazioni personali di qualsiasi sorta.

La tecnica normativa cui sembra ispirarsi l'amministrazione statunitense nel definire un *framework* a tutela dei dati è quella della co-regolamentazione. In questo la scelta, comune ad altri ordinamenti, pare condivisibile, sia per la maggior rigidità degli strumenti legislativi nel variare in conseguenza dell'evoluzione del contesto tecnologico, sia per l'opportunità che i processi di formazione delle regole vedano coinvolti direttamente i soggetti interessati, al fine di una maggior consapevolezza dei problemi e condivisione delle soluzioni.

Nel coniugare regolamentazione statuale e auto-regolamentazione[16], nell'orizzonte statunitense della ***data protection***, sembra tuttavia prevalere la seconda sulla prima: definito, ad opera del Governo, « a full set of Fair Information Practice Principles (FIPPs) as a foundation for commercial data privacy »[17], spetterà infatti agli operatori elaborare dei codici di condotta volontari più specifici[18], aventi natura vincolante per chi decida di aderirvi[19].

La scelta di affiancare ad alcune regole di fondo[20] dei codici di autoregolamentazione settoriali, per tipologie di impresa[21], viene

[16] Cfr. FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, citato *supra*, p. 8, ove si ammettono implicitamente i limiti di una soluzione impostata solo sull'autoregolamentazione: « In 2000, the Commission reported to Congress that, although there had been improvement in industry self-regulatory efforts to develop and post privacy policies online, only about one-quarter of the privacy policies surveyed addressed the four fair information practice principles of notice, choice, access, and security. Accordingly, a majority of the Commission concluded that legislation requiring online businesses to comply with these principles, in conjunction with self-regulation, would allow the electronic marketplace to reach its full potential and give consumers the confidence they need to participate fully in that marketplace »; il legislatore statunitense non raccolse tuttavia tale sollecitazione in favore della regolamentazione legislativa.

[17] Cfr. a riguardo UNITED STATES DEPARTMENT OF HEALTH, *Records, Computers and the Rights of Citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, 1973, in *http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm*, nonché i principi adottati dal DEPARTMENTOF HOMELAND SECURITY, *Privacy policy Guidance Memorandum*, 2008, in *http://www.dhs. gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf*, quest'ultimi esplicitamente richiamati nel dettaglio in THE DEPARTMENT OF COMMERCE INTERNET POLICY TASK FORCE, *Commercial Data Privacy and Innovation in the Internet Economy*, citato *supra*, p. 26 s.

[18] Cfr. THE DEPARTMENT OF COMMERCE INTERNET POLICY TASK FORCE, *Commercial Data Privacy and Innovation in the Internet Economy*, citato *supra*, p. 5: « The adoption of baseline FIPPs for commercial data privacy, on its own, is not likely to provide sufficient protection for privacy in the dynamic, global Internet economy. Commercial data privacy policy must be able to evolve rapidly to meet a continuing stream of innovations ».

[19] Cfr. *The department of commerce internet policy task force*, *op. cit.*, p. 5: « Companies would voluntarily adopt the appropriate code developed through this process. This commitment, however, would be enforceable by the Federal Trade Commission ».

[20] Va in proposito osservato come i punti cardine dei FFIPs siano comuni al modello europeo maturato dagli anni '70 del secolo scorso, avendo ruolo centrale il « purpose specification principle » (principio di finalità) ed il « use limitation principle » (principio di pertinenza). I medesimi principi hanno altresì influenzato le soluzioni in materia adottate in ambito APEC, su cui *infra* nota 68.

[21] Si ipotizza una duplice tipologia di

avallata in quanto una « comprehensive baseline FIPPs would maintain the flexibility for each industry sector to develop tailored implementation plans that correspond to the privacy risks posed by their services ». Tuttavia, forse complice l'assenza di una regolamentazione significativa in materia di *data protection*, si assume come certo un dato non pacifico. Che infatti occorrano regole calibrate in maniera specifica per ciascun settore non pare così sicuro.

Certamente è nei vari ambiti operativi e merceologici che le regole generali in tema di trattamento dei dati trovano specifica applicazione, ma questo non implica necessariamente che se ne debbano creare di speciali. Non sono tanto gli aspetti normativi o regolamentari a dover essere declinati in ragione dei diversi contesti, quanto piuttosto quelli di natura procedurale inerenti gli adempimenti da compiersi. Come dimostra anche l'esperienza italiana, salvo casi peculiari, le diverse realtà d'impresa non necessitano di regole diverse, se non al massimo di una maggior o minor gradualità rispetto a certi oneri, in ragione della natura dei dati trattati e della dimensione operativa. Il fulcro della *data protection* è infatti rappresentato dalle modalità di trattamento più che dalla natura dell'autore dello stesso, e le modalità (raccolta, memorizzazione, ecc.) sono in gran parte comuni a qualsiasi tipologia di impresa. Ciò che muta è invece la propensione e la capacità tecnica di adempiere agli obblighi imposti, ed è su questo punto che può divenire opportuna una maggior tipizzazione nell'ottica di una reale efficacia della normativa[22].

codici di condotta: quelli di semplice autoregolamentazione e quelli conformi ai principi della FTC, rispetto ai quali « FTC approval might come through a request by a party to assess how the code meets FIPPs' stipulations. Or, FTC approval could be determined in the context of resolving a specific complaint when the company being investigated asserts a safe harbor defense »; cfr. THE DEPARTMENT OF COMMERCE INTERNET POLICY TASK FORCE, *Commercial Data Privacy and Innovation in the Internet Economy*, citato *supra*, p. 43. L'adesione a quest'ultimi, stante il vaglio delle FTC, implicherà la conformità degli stessi ai FFIPs, ragion per cui l'impresa che adotta correttamente il codice risulterà esente da rilievi e sanzioni. L'inottemperanza ai codici cui si è aderito sarà soggetta ai controlli ed alle sanzioni predisposti dalla FTC o dallo State Attorney General. La stessa FTC dovrebbe vigilare altresì sul rispetto dei FFIPs. La definizione dei codici di condotta, ancorché attribuita ai soggetti appartenenti alle categorie interessate, verrà stimolata e coordinata dal Privacy Policy Office (PPO), organo consultivo che si immagina di costituire all'interno del Department of Commerce, oltre che dalla FTC; è tuttavia esclusa qualsiasi attribuzione di poteri di controllo e sanzionatori in capo al PPO; cfr. THE DEPARTMENT OF COMMERCE INTERNET POLICY TASK FORCE, *op. cit.*, pp. 5 ss. e 44 s.

[22] D'altro canto in THE DEPARTMENT OF COMMERCE INTERNET POLICY TASK FORCE, *Commercial Data Privacy and Innovation in the Internet Economy*, citato *supra*, p. 25, laddove si afferma che « comprehensive baseline FIPPs would maintain the flexibility for each industry sector to develop tailored implementation plans that correspond to the privacy risks posed by their services », lo stesso riferimento ai *privacy risks* implica soprattutto una valutazione in concreto di tipo casistico delle criticità, mediante sistemi di analisi di rischio ed approntamento di misure di sicurezza (quindi pertinenti al profilo degli adempimenti più che a quello della disciplina), piuttosto che la necessaria determinazione di regole *ad hoc*, ancorché di *soft-law*.

La tipizzazione per « industry sector »[23] pare invece fuorviante, poiché, sotto il profilo del trattamento dati, attività imprenditoriali differenti non necessariamente pongono in essere diverse tipologie di azioni, mentre può essere che imprese dello stesso settore merceologico trattino dati in maniera e di natura diversa[24]. La mancanza di una corrispondenza biunivoca fra natura e modalità dei dati impiegati (e conseguenti livelli di rischio e sicurezza), da un lato, e tipologia di attività di impresa, dall'altro, pare costituire dunque l'ostacolo più rilevante all'efficacia di una normativa declinata per « industry sector », foriera di inutili duplicazioni o di aggregazioni di realtà eterogenee. Più efficiente invece una visione dato-centrica che guardi al tipo di informazioni ed al loro trattamento, a prescindere dal contesto operativo in cui avviene, tanto più tenendo conto della crescente trasversalità e della natura intersettoriale delle attività.

Sempre nell'ottica dell'efficacia normativa, va osservato come nell'Unione europea, ancorché in presenza della forza cogente ed uniformante di una direttiva comune (dir. 95/46/CE) e di ulteriori più specifici interventi di settore, la sola azione dei singoli legislatori nazionali abbia dato vita ad un panorama variegato di soluzioni attuative[25]. Viene dunque da chiedersi se davvero con pochi principi comuni affiancati a soluzioni di autoregolamentazione, ancorché stimolate e coordinate dall'amministrazione statunitense, non si raggiungerà un'ancor più elevata frammentazione delle soluzioni adottate.

Proprio la natura dei dati personali, gli incessanti flussi comunicativi di cui sono oggetto ed il loro impiego molteplice, rende la pluralità di modelli regolatori tutt'altro che desiderabile[26]. Gli operatori economici, in primo luogo, trovano assai difficile far fronte a modelli che costringono ad approcci *case by case*, confliggenti con la standardizzazione di un'economia globalizzata. Questo non vuol dire negare il valore della co-regolamentazione, specie alla luce dell'evoluzione tecnologica e della tradizionale difficoltà del legislatore nel recepirla tempestivamente; nel contesto attuale pare tuttavia forte l'esigenza di uniformità delle soluzioni e

[23] Cfr. nota precedente.

[24] Così da un lato, guardando alla categoria merceologica, ad esempio nel settore meccanico, tradizionalmente a basso contenuto di dati personali, può trovare spazio l'impiego di sistemi di rilevamento biometrico per particolari ragioni di sicurezza, mentre d'altro canto, guardando alla natura dei dati, un numero rilevante di dati sensibili sanitari possono essere indistintamente impiegati tanto in ambito biomedico quanto assicurativo.

[25] Cfr. ARTICLE 29 DATA PROTECTION WORKING PARTY-WORKING PARTY ON POLICE AND JUSTICE, *The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, Bruxelles, 1 dicembre 2009, p. 17.

[26] Cfr. THE DEPARTMENT OF COMMERCE INTERNET POLICY TASK FORCE, *Commercial Data Privacy and Innovation in the Internet Economy*, citato *supra*, p. 59 s. vedi i commenti provenienti da Google e Microsoft.

di dar vita ad una regolamentazione puntuale piuttosto che minimale, anche in considerazione dell'ampiezza e della pervasività assunta dai fenomeni di trattamento dati.

Il mutamento della tecnologia, in particolare, è poi una delle ragioni che ha indotto il DoC a prevedere la creazione, all'interno del Privacy Policy Office (PPO) che si vorrebbe costituire[27], di un gruppo composto di soggetti pubblici e privati[28] in grado di definire prontamente[29] le opportune linee guida o variare quelle esistenti, nonché le pratiche in uso[30]. In proposito, seppur la co-regolamentazione o l'autoregolamentazione siano molto più celeri nel rispondere ai mutamenti tecnologici di quanto non lo sia il legislatore, va tuttavia rilevato come la scelta comunitaria di affidare alle autorità garanti per la protezione dei dati personali poteri regolamentari, ancorché nei limiti del quadro definito dal legislatore, consenta una ancor più rapida risposta ai nuovi problemi posti dall'evoluzione tecnologica[31]. D'altra parte non va però disconosciuta la possibile debolezza del modello comunitario correlata al rischio di una personalizzazione degli organi di controllo, specie in presenza di autorità indipendenti aventi un numero limitato di componenti laddove l'impostazione individuale (e talora anche politica) può incidere significativamente sulle modalità di intervento; diversamente in gruppi di lavoro in cui siano rappresentati i vari interessi risulta più probabile l'emersione di posizioni divergenti, ragion per cui la decisione finale dovrebbe dar luogo ad una sorta di mediazione e non riflette il pensiero o l'attitudine del presidente dell'autorità di controllo o di alcuni dei suoi membri.

[27] Cfr. supra nota 21.

[28] Cfr. THE DEPARTMENT OF COMMERCE INTERNET POLICY TASK FORCE, *Commercial Data Privacy and Innovation in the Internet Economy*, citato *supra*, p. 47: « PPO-convened group composed of leaders from key multi-stakeholder institutions and U.S. Government officials could address new commercial data privacy challenges as they arise and develop guidelines for voluntary, enforceable commercial data privacy codes as needed to ensure that no harm occurs while expectations form around new technologies. »

[29] Cfr. THE DEPARTMENT OF COMMERCE INTERNET POLICY TASK FORCE, *Commercial Data Privacy and Innovation in the Internet Economy*, citato *supra*, p. 47: « A dynamic system in which both private and public stakeholders participate would yield privacy practices that are more responsive to evolving consumer privacy expectations than would a traditional rulemaking system. After all, the rate at which new services develop, and the pace at which consumers form expectations about acceptable and unacceptable uses of personal information, is measured in weeks or months ».

[30] Cfr. a riguardo le osservazioni critiche, specie circa all'interazione fra FTC e PPO, esposte in ELECTRONIC FRONTIER FOUNDATION, *Comments of the Electronic Frontier Foundation To The Department of Commerce Internet Policy Task Force Regarding Commercial Data Privacy and Innovation in the Internet Economy: a Dynamic Policy Framework*, 2011, p. 6 s., in *www.eff.org/files/EFF_Comments_to_Commerce.pdf*.

[31] Non è infatti così scontato che all'interno di un gruppo di lavoro rappresentativo dei diversi soggetti interessati — come dovrebbe essere quello in seno al PPO — si trovi tanto rapidamente un accordo su soluzioni comuni, specie in presenza di evidenti interessi contrastanti di tipo economico e politico.

3. (*Segue*) IL RUOLO DEL CONSENSO.

Nel nuovo impianto regolamentare, comunque conseguito, ruolo rilevante viene attribuito all'« informed consent ». In tal senso il DoC, nell'ottica di un *new approach* resosi necessario nell'attuale contesto mediatico, annovera fra i « foundational principles » a tutela della *commercial data privacy* la necessità « to give (or withhold) informed consent before information about them is collected, used, or disclosed in a commercial context »[32]. È tuttavia nel documento della FTC che vengono fornite maggiori e più dettagliate indicazioni a riguardo. Purtroppo però proprio queste specifiche paiono contraddire l'asserita centralità del consenso dell'interessato.

Nel merito si prevede infatti l'ampio ricorso a forme implicite di consenso informato[33] ed è evidente come la valorizzazione del consenso implicito, al di fuori di alcuni limitati ambiti, rischi di tradursi nella pratica in un significativo indebolimento dell'autodeterminazione informativa, che proprio nel consenso informato ed espresso trova maggior garanzia[34]. Più specificatamente la FTC, accanto alle condivisibili ipotesi di consenso implicito relative ai trattamenti motivati da finalità contrattuali[35] o da « public policy reasons », delinea una ben più discutibile ed indefinita fattispecie concernente le attività « sufficiently accepted [...] that companies need not request consent to engage in them »[36]. Ne consegue che una « informed and meaningful choices » verrà riconosciuta all'interessato solamente in relazione ai trattamenti non « commonly accepted »[37], coniugando così la restrizione del ricorso al consenso esplicito con la carenza di determinatezza della

[32] Cfr. THE DEPARTMENT OF COMMERCE INTERNET POLICY TASK FORCE, *Commercial Data Privacy and Innovation in the Internet Economy*, citato *supra*, p. 20.

[33] L'intervento si inserisce nell'ambito di una più ampia revisione delle politiche adottate dalla FTC, che vede tra l'altro come ulteriori punti qualificanti l'implementazione della c.d. « privacy by design » e l'esortazione alle imprese affinché migliorino le proprie *privacy policies*; cfr. FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, citato *supra*, p. v ss. e 41 s. Si rinvia ai paragrafi successivi l'approfondimento degli aspetti da ultimo menzionati.

[34] Benché sia infatti vero che anche il consenso espresso possa in concreto divenire un gesto quasi automatico cui l'interessato non presta attenzione, è altrettanto vero che un indebolimento di tale requisito non va certo nel senso di rafforzare la coscienza dell'atto di disposizione dei propri dati, bensì ne acuisce l'inconsapevolezza.

[35] In queste ipotesi il consenso può essere giustamente ritenuto « obvious from the context of the transaction », cfr. FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, citato *supra*, p. VI e 54.

[36] Cfr. FTC, *op. e loc. cit.* L'indeterminatezza della categoria è d'altra parte dimostrata da quanto successivamente asserito dalla FTC, secondo cui « by clarifying those practices for which consumer consent is unnecessary, companies will be able to streamline their communications with consumers, reducing the burden and confusion on consumers and businesses alike ». Cfr. *amplius infra* nel testo.

[37] La necessità del consenso espresso è inoltre prevista per le modifiche retroattive delle *privacy policies*, cfr. FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, citato *supra*, p. VII: « in addition, all entities must provide robust notice and obtain affirmative consent for material, retroactive changes to data policies »; v. anche p. 76 s.

fattispecie, posto che risulta difficile discriminare — e farlo in maniera univoca —, fra trattamenti « commonly accepted » e « not commonly accepted ». Va inoltre rilevato come l'estensione delle ipotesi di consenso implicito sia destinata ad influire significativamente sulla circolazione dei dati verso terze parti differenti da quella che originariamente ha avuto rapporti con il consumatore, traducendosi nei fatti nella possibilità per una moltitudine di soggetti di raccogliere indirettamente informazioni personali all'insaputa dell'interessato[38].

La scelta per un indebolimento della rilevanza attribuita al consenso dell'interessato mostra la distanza fra l'approccio statunitense e quello comunitario, laddove proprio il requisito del consenso « unambiguously given » riveste ruolo primario nella legittimazione del trattamento degli altrui dati personali[39] e distingue le prime generazioni di leggi in materia di *data protection*[40] da quelle successive alla svolta impressa dalla dir. 95/46/CE.

Non solo, tale scelta mostra anche la mancata ricezione di un'istanza sociale derivante dal nuovo contesto informativo maturato negli ultimi lustri del secolo scorso. Il legislatore comunitario, nel valorizzare l'autodeterminazione informativa anche attraverso il consenso, ha infatti preso atto del valore economico assunto dalle informazioni personali e del mercato creatosi intorno ad esse, tali da far venir meno la legittimazione di un modello che escludeva del tutto l'interessato dalla negoziazione inerente i propri dati.

In tale ottica il consenso è il cardine del sistema attuale della gestione dei dati personali tanto che, anche laddove non è richiesto, se non è lo stesso legislatore a valutare *ex ante* il bilanciamento fra i diversi interessi contrapposti[41], si è in presenza di ipotesi di consenso implicito[42].

[38] In proposito, nuovamente la carenza di una posizione forte a tutela dell'autodeterminazione informativa conduce poi ad opzioni decisamente poco garantiste, cfr. FTC, *op. cit.*, p. 63: « because these companies do not interact directly with consumers, they may not be in a position to provide consumer choice at the point of collection or use. Staff requests comment on choice mechanisms for data brokers, including whether some sort of universal, standardized mechanism would be feasible and beneficial. Another potential approach, which a number of roundtable panelists supported, is to provide additional transparency about data brokers, including byallowing consumers to access the data these entities maintain about them ».

[39] Cfr. art. 7 dir. 95/46/CE.

[40] Le leggi di prima generazione, nate agli inizi degli anni '70 del secolo scorso, erano sostanzialmente incentrate sui diritti d'accesso e sulla previa autorizzazione alla costituzione della banca dati, coerentemente ad un contesto in cui il panorama informatico era costituito da pochi grandi e costosi *mainframe*. Ad esse seguirono nuovi interventi normativi, la c.d. « seconda generazione », ancora basati sui diritti di accesso, ma che prevedevano il superamento del modello autorizzatorio in favore di quello incentrato sulla semplice notifica della costituzione della banca dati. Erano gli anni '80, si andava verso l'informatica distribuita e la progressiva diffusione dei *personal computer*; il valore commerciale dei dati non era però ancora così rilevante ed evidente come sarebbe accaduto nel decennio successivo.

[41] Cfr. art. 7, lett. *c*), *d*), *e*) ed *f*), dir. 95/46/CE.

[42] Cfr. art. 7, lett. *b*), dir. 95/46/CE.

In termini generali risulta dunque corretta l'impostazione statunitense che distingue appunto fra casi di consenso espresso ed implicito, ma essa diviene discutibile a causa della carente definizione delle fattispecie e dell'ampio ventaglio delle stesse. Nel delineare quest'ultime ipotesi si è infatti impiegata la vaga locuzione di « accepted practices » e, quando si è tentato di definirle in maniera più analitica, si sono utilizzate categorie generali troppo ampie e diversificate al loro interno[43]. Così nello specifico sono state considerate « accepted practices » alcune prassi che possono coerentemente reputarsi manifestazioni di consenso implicito (*product and service fulfillment*[44], *fraud prevention*[45] e *legal compliance and public purpose*[46]), tuttavia ad esse sono state affiancate diverse ipotesi in cui non solo tale consenso potrebbe mancare, ma che costituiscono altresì trattamenti volti alla profilazione o alla tracciabilità dell'interessato[47]. A ciò si aggiunga poi che, nel novero delle fattispecie in cui non necessita un'espressa manifestazione di assenso, vengono individuate alcune ipotesi eccezionali per le quali essa è invece comunque richiesta.

Dalle linee guida emerge dunque un contesto complesso, composto da definizioni generali, specificate mediante esemplificazioni, e poi derogate in casi specifici. Risulta così difficile delineare con compiutezza il quadro operativo, laddove la genericità non pare esaustiva e l'analiticità pecca di specialità, rendendo tutt'altro che agevole trovare una risposta alla pluralità di casi cui concre-

[43] Cfr. FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, citato *supra*, p. 53 ss.

[44] Tale fattispecie si realizza quando « Websites collect consumers' contact information so that they can ship requested products. They also collect credit card information for payment. Online tax calculators and financial analysis applications collect financial information to run their analyses for customers », cfr. FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, citato *supra*, p. 53.

[45] A tal riguardo benché le ipotesi individuate paiano effettivamente classificabili come fattispecie di consenso implicito, cfr. FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, citato *supra*, p. 54, tuttavia l'ampiezza della categoria e dei rimedi anti-frode potrebbe ricomprendere anche forme di profilazione rispetto alle quali non è detto che sia possibile ravvisare un consenso implicito in ragione della quantità e entità dei trattamenti posti in essere.

[46] Cfr. FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, citato *supra*, p. 54.

[47] Nello specifico il riferimento è alle « internal operations », laddove si esclude il consenso espresso in relazione ad ipotesi quali i questionari inerenti la customer satisfaction o le informazioni inerenti l'utilizzo di un sito web (« visits and click »), limitandosi in tali casi a richiedere alle imprese di « disclose these practices in their privacy policies in order to promote transparency and accountability ». Anche nel caso di « first-party marketing » si ipotizza poi l'adozione di tecniche di profilazione e *marketing* le quali non è detto che, in ragione della loro accuratezza e complessità, possano sempre considerarsi come assistite da un consenso implicito del cliente. Non pare qui condivisibile la considerazione espressa dalla FTC, secondo cui in questi casi un'efficace tutela dei dati personali andrebbe a detrimento dell'efficienza; cfr. FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, citato *supra*, p. 54, ove si afferma: « staff believes that requiring consumers to make a series of decisions whether to allow companies to engage in these obvious or necessary practices would impose significantly more burden than benefit on both consumers and businesses ».

tamente dà luogo il trattamento dati. Probabilmente non per nulla la stessa FTC pone il seguente quesito per la consultazione pubblica correlata al proprio documento: « Is the list of proposed "commonly accepted practices" described above too broad or too narrow? »[48].

Con riguardo poi alle ipotesi in cui viene attribuito rilievo alla manifestazione di volontà dell'interessato, è poi lasciato ancora aperto il dibattito circa la scelta fra l'*opt-in* e l'*opt-out*[49], benché vengano formulate considerazioni che paiono tradire un certo sfavore per la prima soluzione[50]. Sul punto è evidente come l'adozione del modello dell'*opt-out*, in un contesto che vede già un limitato ricorso all'autodeterminazione del singolo in merito ai propri dati, finirebbe per comprimere ulteriormente tale autonomia. In quest'ultimo senso va anche la diversa soluzione, sempre avanzata dalla FTC, definita come « take it or leave it proposition », in virtù della quale il consenso viene manifestato mediante un comportamento concludente consistente nella fruizione del bene o del servizio[51].

Tanto il meccanismo *take it or leave it*, come quello dell'*opt-out*, considerata l'usuale disattenzione dei consumatori e degli utenti in genere per le informazioni in materia di trattamento dati, nonché la sempre non agevole reperibilità delle stesse o completezza, finiscono per tradurre il consenso al trattamento in un qualcosa di assai dissimile da una scelta consapevole dell'interessato.

Va inoltre osservato come, guardando alle proposte in questione, non pare neppure coerentemente perseguita l'impostazione commerciale caratterizzante l'approccio statunitense: proprio la rilevanza economica delle informazioni, la loro natura di bene, dovrebbe infatti indurre ad una reale negoziazione delle stesse. Quello che si prefigura è invece un sistema evidentemente asimme-

[48] FTC, *op. cit.*, 56.

[49] In proposito la FTC sembra anzi sminuire il rilievo della distinzione fra la necessità di acquisire un'esplicita dichiarazione di consenso da parte dell'interessato (*opt-in*) ed invece presumere il consenso del medesimo salvo che questi affermi il proprio diniego (*opt-out*). Nel testo del FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, citato *supra*, p. 60, si legge infatti: « the time and effort required for consumers to understand and exercise their options may be more relevant to the issue of informed consent than whether the choice is technically opt-in or opt out ». In proposito paiono impropriamente affiancati due diversi profili, quello della chiarezza dell'informativa e quello delle modalità di acquisizione del consenso.

[50] Cfr. 60: « a clear, simple, and prominent opt-out mechanism may be more privacy protective than a confusing, opaque opt-in. Staff has already stated that, regardless of how they are ». Cfr. anche la proposta di legge « BEST PRACTICES Act » del 2010, in cui prevale l'*opt-out*, salvo che per la comunicazione dei dati a terze parti.

[51] Cfr. 61: « Staff also requests comment on whether and in what circumstances it is appropriate to offer choice as a "take it or leave it" proposition, whereby a consumer's use of a website, product, or service constitutes consent to the company's information practices. [...] In particular, how should companies communicate the "take it or leave it" nature of the transaction to consumers? Are there any circumstances in which a « take it or leave it'proposition would he inappropriate? »

trico in cui vengono minimizzate le ipotesi di negoziazione con il detentore originario delle informazioni, ricorrendo a meccanismi che danno per presupposto il consenso. Le posizioni assunte divengono così sperequate in favore delle imprese ed, al più, intenzionate a mitigarne solo parzialmente il predominio nel mercato dei dati, e non paiono certo volte a rendere tale mercato equilibrato nei rapporti di forza.

Non solo è evidente lo squilibrio ingenerato fra le situazioni giuridicamente tutelate, diritti della persona ed attività di impresa, ma ancor più la scarsa stima degli effetti negativi che tali soluzioni possono avere su una società matura e consapevole del valore delle informazioni personali. Va infatti ricordato come la stessa Unione europea, prova ne sono i considerando della dir. 95/46/CE, non fu mossa principalmente dalla volontà di protezione dalla persona nel disciplinare il trattamento dei dati personali, ma ben più prosaicamente dall'esigenza di garantire la possibilità dell'impiego dei medesimi da parte di soggetti pubblici e privati. Tali informazioni, divenute essenziali per ogni attività commerciale e non, sarebbero infatti potute divenire meno disponibili qualora il cittadino si fosse sentito poco garantito circa la propria possibilità di controllo sulla loro sorte e fosse stato escluso dalle dinamiche appropriative di quella che è la nuova ricchezza di questi decenni.

D'altra parte anche sotto il profilo dei diritti di accesso, nucleo primario di tutela del singolo, storicamente antecedente all'affermarsi del ruolo del consenso, le proposte statunitensi paiono deboli. In proposito uno dei punti rilevanti delle linee guida della FTC[52] è l'esortazione rivolta alle imprese affinché migliorino le proprie *privacy policies*[53], sottolineando nello specifico l'opportunità di un « reasonable » diritto di accesso che per esser aggettivato in tal maniera dovrà risultare « proportional to both the sensitivity of the data and its intended use », onde contenere i « significant costs associated with access »[54]. Sono tuttavia le limitazioni intrinseche di tale *guideline* a mostrare alcune criticità: in primo luogo manca di prova la motivazione di tipo economico addotta a giustificazione della restrizione del diritto di accesso, vi sono anzi risultanze empiriche di segno opposto[55]; secondariamente i termini « reasonable » e « proportional » appaiono inadatti a delineare le ipotesi specifiche in cui tale diritto andrebbe riconosciuto[56].

[52] Cfr. FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, citato *supra*, pp. v ss. e 41 s.

[53] Cfr. anche FTC, *op. cit.*, p. 69 ss.

[54] Cfr. FTC, *op. cit.*, p. 73 ss.

[55] Si rinvia a riguardo ai risultati dell'indagine economico-statistica, svolta su oltre centoventi imprese italiane di varie dimensioni, in A. MANTELERO, *Il costo della privacy tra valore della persona e ragione d'impresa*, citato *supra*, p. 290 ss.

[56] Incidentalmente va osservato come anche il modello comunitario faccia riferimento al concetto di ragionevolezza, ma in relazione alla frequenza degli accessi (« reasonable intervals »), onde evitare comportamenti pretestuosi, e non quale restrizione all'accesso medesimo a seconda

4. Conclusioni.

Guardando al quadro generale delineato dai provvedimenti statunitensi, pare emergere un approccio al tema della *data protection* e dei diritti dei singoli sulle informazioni ancora poco sensibile alle diverse sfumature ed alla complessità che connotano la materia. La ragione di questo limite pare individuabile in una scelta consapevole di privilegiare il « mercato dei dati » ad opera delle imprese, circoscrivendo le interferenze dei consumatori a tutto beneficio e lucro di chi tali dati monetizza.

Una simile impostazione, oltre a creare un evidente squilibrio fra le posizioni giuridicamente tutelate (diritti della persona ed attività di impresa), mostra altresì una scarsa stima degli effetti negativi che da essa possono conseguire in una società matura e consapevole del valore delle informazioni personali. Specie con riguardo ai consumatori, lo scarso coinvolgimento dell'interessato nelle opzioni di fondo inerenti il trattamento dei propri dati può tradursi in una minor propensione alla comunicazione degli stessi, con danno per le imprese. Non parendo sufficiente ad incrementare la fiducia dei consumatori la maggior attenzione posta invece al profilo della *security braech notification*[57], laddove si prevede un intervento legislativo federale.

Nelle scelte d'Oltreoceano non si può dunque non scorgere una certa dose di anacronismo rispetto alla percezione delle dinamiche inerenti i dati personali, alle richieste dei consumatori, alle posizioni assunte da molte imprese che della tutela dei dati hanno ormai fatto un *asset* strategico e, non ultimo, alle vie intraprese da diversi legislatori nazionali al di fuori dei confini statunitensi.

Neppure valgono a convincere circa la validità delle conclusioni le osservazioni inerenti i costi. Proprio quest'ultime anzi confermano una riflessione ancora poco matura[58]. Ritenere infatti « cos-

della natura dei dati e del loro impiego; cfr. art. 12, lett. a), dir. 95/46/CE.

[57] Diversi stati hanno adottato specifiche normative a riguardo, si veda ad esempio Cal. Civ. Code §§ 1798.29, 1798.82-1789.84, in *http://www.leginfo.ca.gov*. Si tratta di leggi volte ad imporre, a chi gestisce le banche dati, un obbligo di comunicazione dettagliata alle competenti autorità in caso di compromissione della sicurezza (accessi illegittimi, furti di dati ecc.). Cfr. in argomento S. Romanosky-R. Telang-A. Acquisti, *Do data breach disclosure laws reduce identity theft?*, in *Journal of Policy Analysis and Management*, n. 30 (2), 2011, 256 ss. Con riguardo alla legislazione comunitaria cfr. invece art. 4, paragrafo 3, dir. 2002/58/CE, come modificato dall'art. 2 dir. 2009/136/CE.

[58] Nello specifico non si è fatto tesoro degli studi esistenti sui costi della « privacy » derivanti dall'attuazione della normativa comunitaria, cfr. *Economic Evaluation of Data Protection Directive 95/46/EC*, a cura di Rambøll Management, in *http://ec.europa.eu/justice/policies/privacy/docs/studies/economic_evaluation_en.pdf*. Tanto meno si è considerato come a sedici anni dall'approvazione della direttiva le imprese comunitarie non paiono aver avuto incidenza negativa sui profitti e sulla competitività delle imprese, semmai anzi una maggior attenzione al trattamento dati ha rafforzato i profili inerenti la sicurezza di quest'ultimi e ha reso le imprese europee più adatte a rispondere alla crescente domanda mondiale di gestione corretta, traspa-

tly » l'attività richiesta alle imprese per l'adeguamento alle norme comunitarie, specie in caso di flussi transfrontalieri di dati[59], è recuperare un adagio ormai (non a caso) quasi sopito in Europa, oltre che empiricamente smentito[60]. Esso denota inoltre una scarsa attenzione per la possibilità di valersi di soluzioni efficienti quali sono le clausole-tipo approvate ormai da anni dalla Commissione Europea[61] o le *bindig corporate rules*[62].

In termini generali poi, dietro una rivendicata — pur discutibile — *leadership* statunitense nell'ambito *on-line*[63], pare nascondersi una certa preoccupazione per il dilagare del modello europeo[64] incentrato sulla regolamentazione legislativa del trattamento dati, nella convinzione che i veri ostacoli derivino dalle « regulatory barriers » piuttosto che dal pluralismo dell'autoregolamentazione, ancorché ispirata a principi comuni.

Se questo è l'orizzonte politico statunitense, non sembra facile ipotizzare una mediazione con quello comunitario onde addivenire alla definizione di regole comuni. Tanto più che divergenze emergono non solo sui punti cardine di cui si è detto sopra[65], ma anche su significativi aspetti operativi e sulle stesse strategie globali.

Basti a riguardo notare come negli USA si stia ancora discutendo sull'opportunità di una tutela dei diritti sui dati che non sia solo amministrativa, ma anche giurisdizionale[66], con il rischio

rente ed in sicurezza delle informazioni personali.

59 Cfr. THE DEPARTMENT OF COMMERCE INTERNET POLICY TASK FORCE, *Commercial Data Privacy and Innovation in the Internet Economy*, citato *supra*, p. 6 s.

60 Cfr. *supra* nota 55.

61 Cfr. Decisione della Commissione del 15 giugno 2001, C(2001)1539, poi modificata con Decisione della Commissione del 27 dicembre 2004 C(2004)5271, e Decisione della Commissione del 5 febbraio 2010, C(2010)593.

62 Cfr. ARTICLE 29 - DATA PROTECTION WORKING PARTY, *Working Document: Transfers of personal data to third countries*, 3 June 2003; cfr. anche: ID., *Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules*, April 14th, 2005; ID., *Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From « Binding Corporate Rules »*; ID., *Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules*, 24 June 2008-8 April 2009. Tutti i documenti richiamati sono pubblicati in *http://ec.europa.eu/justice/policies/privacy/binding_rules/tools_en.htm*.

63 Tale *leadership* è indubbia sotto il profilo dei servizi, poiché guardando a tale aspetto la Rete è sicuramente « a stelle e strisce », mentre risulta più opinabile analoga preminenza se si guarda ai volumi attuali e soprattutto futuri delle transazioni *on-line*.

64 Cfr. THE DEPARTMENT OF COMMERCE INTERNET POLICY TASK FORCE, *Commercial Data Privacy and Innovation in the Internet Economy*, citato *supra*, p. 6.

65 La diversa impostazione presente fra le due sponde dell'Atlantico, si rileva anche nella definizione stessa di dato sensibile, laddove la FTC considera « sensitive information » anche i dati finanziari (cfr. FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, citato *supra*, p. 61), mentre l'Unione europea, culturalmente più attenta a tener distinti i profili inerenti la persona da quelli economici, considera bisognosi di un maggior protezione i dati personali « che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale », nonché quelli inerenti la salute e la vita sessuale », cfr. art. 8 dir. 95/46/CE.

66 Cfr. THE DEPARTMENT OF COMMERCE INTERNET POLICY TASK FORCE, *Commercial Data Privacy and Innovation in the Inter-*

di seguire un'impostazione che guarda indietro alle prime leggi europee, incentrate appunto sulla tutela amministrativa offerta dagli organi di vigilanza. Sarebbe questa una soluzione anacronistica, poco coerente con un mercato dei dati legittimato dal consenso informato dell'interessato[67].

Soprattutto a livello di interoperabilità fra le soluzioni adottate nelle diverse nazioni paiono infine carenti le proposte statunitensi, laddove si punta a valorizzare i risultati maturati in ambito APEC (Asia-Pacific Economic Cooperation)[68], secondo un sistema che prevede l'adozione su base volontaria da parte delle imprese di alcuni principi generali e la sottoposizione alla verifica di un « accountability agent » riconosciuto dall'APEC.

Accanto alle diverse criticità sin qui sottolineate va però anche dato conto che su alcuni profili provengono da Oltreoceano indicazioni meritevoli di attenzione, in specie con riguardo al ricorso a soluzioni di tipo tecnologico-organizzativo volte a prevenire l'illecito trattamento dei dati. Così la FTC, tra i punti qualificanti delle linee guida[69], prevede l'adozione da parte delle imprese di un approccio incentrato sul concetto di « privacy by design »[70] volto a creare tecnologie conformate atte ad assicurare il rispetto dei principi di sicurezza, finalità e necessità del trattamento dati[71], principi che come la stessa FTC afferma « are not new, but the time has come for industry to implement them systematically »[72].

Ulteriore elemento significativo di novità ed interesse, suscettibile di essere forse adottato anche in Europa, è l'applicabilità della disciplina sul trattamento dati ogniqualvolta vengano elaborati « data that can be reasonably linked to a specific consumer, computer, or other device »[73], ove si assiste ad una parificazione

net Economy, citato *supra*, p. 29 s. Cfr. invece artt. 22 e 23 dir. 95/46/CE.

67 A tale consenso, sempre più un atto dispositivo volto alla circolazione dell'informazione, avente natura negoziale, ed all'affermata rilevanza economica e commerciale delle informazioni personali, pare infatti logico e necessario accompagnare la tutela in sede giudiziaria nel caso di trattamento illegittimo.

68 Cfr. THE DEPARTMENT OF COMMERCE INTERNET POLICY TASK FORCE, *Commercial Data Privacy and Innovation in the Internet Economy*, citato *supra*, p. 53 ss. Cfr. *APEC Privacy Framework* e *APEC Data Privacy Pathfinder*, entrambi in *http://www.apec.org*. Va rilevato come fra i membri dell'APEC, oltre a Stati Uniti, Australia, Canada e Giappone, figurino anche la Cina e la Russia, non propriamente stati particolarmente sensibili ai temi della tutela dei dati personali, anche se solo limitatamente a quelli di carattere commerciale.

69 Cfr. FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, citato *supra*, pp. V ss. e 41 s.

70 Cfr. A. CAVOUKIAN (Information and Privacy Commissioner of Ontario Canada), *Privacy by Design... Take the Challenge*, 2009, in *http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf*.

71 FTC, *op. cit.*, 44 ss.

72 Va rilevato in proposito come in FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, citato *supra*, pp. V e 44, le imprese vengano sollecitate a « implement and enforce procedurally sound privacy practices throughout their organizations », non solo sotto il profilo della progettazione produzione dei beni o servizi, tipici della *privacy by design*, ma anche della formazione del personale.

73 Cfr. FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, citato *supra*, p. 41.

fra soggetto e dispositivi informatici ai fini della connotazione in termini di natura personale dei dati. In proposito se è vero, ad esempio, che l'indirizzo IP assegnato ad un computer nulla ci dice in merito a chi lo sta usando[74], è altrettanto vero che l'aumento dei dispositivi tecnologici e la loro portabilità ne ha incrementato l'uso esclusivo e personale, così come l'evoluzione delle tecniche di profilazione consente sempre più di rendere individuabile un soggetto attraverso informazioni sparse lasciate dallo stesso durante l'attività *on-line*[75]. In una prospettiva di medio-lungo periodo (essenziale per chi vuole definire delle regole), anche in ragione del concretizzarsi del c.d. *internet of the things*[76], non è dunque da escludersi che i dispositivi di cui ci serviamo divengano una sorta di prolungamento di noi stessi e finiscano per identificarsi con la persona sotto il profilo della tracciabilità dei comportamenti.

Infine va apprezzata la scelta di tener conto nel definire le prescrizioni del fattore dimensionale dell'impresa[77]. In proposito già con riferimento all'attuazione pratica della direttiva comunitaria in Italia si è avuto modo di riscontrare, anche empiricamente, come ad essere avvertita dagli operatori quale principale carenza della regolamentazione sia stata proprio la mancata considerazione del fattore dimensionale e delle peculiarità dei diversi ambiti operativi. Al riguardo, pur mantenendo ferma una disciplina unitaria e generale, evitando la proliferazione di interventi settoriali[78], è pur vero che l'introduzione di singole norme *ad hoc* (di « parte speciale ») può rendersi necessaria in riferimento a specifiche modalità di trattamento realizzate dalle imprese (ad esempio in relazione all'elaborazione dei dati genetici, delle informazioni di *marketing*, ai controlli a distanza). Analogamente, benché non debba trovar spazio un approccio quantitativo nella tutela della persona, parametrando il livello di tutela in ragione del nu-

[74] A riguardo il disegno di legge « BEST PRACTICES Act » del 2010 fa rientrare proprio l'indirizzo IP nell'ambito dei dati personali oggetto di tutela. Sui limiti dell'identificazione dell'utente responsabile di un illecito per mezzo dell'indirizzo IP cfr. recentemente *Media CAT Ltd v Adams & Ors* [2011] EWPCC 6 (08 February 2011), in *http://www.bailii.org/cgi-bin/markup.cgi?doc=/ew/cases/EWPCC/2011/6.html&query=Media+and+CAT&method=boolean*.

[75] Cfr. FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, citato *supra*, p. 43 ove si tiene in considerazione l'assunto secondo cui « the traditional distinction between PII and non-PII continues to lose significance due to changes in technology and the ability to re-identify consumers from supposedly anonymous data ».

[76] L'« internet delle cose » consiste nella capacità di creare reti di comunicazione informatiche avvalendosi di oggetti di uso quotidiano, posti in relazione fra loro.

[77] Cfr. FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, citato *supra*, p. 45: « The level of security required should depend on the sensitivity of the data, the size and nature of a company's business operations, and the types ».

[78] Simili interventi finirebbero per essere ridondanti e, in diversi casi, potrebbero dare origine a dubbi interpretativi circa la disciplina in concreto applicabile a specifici tipi di attività, stante la presenza di imprese operanti in differenti ambiti tra loro interconnessi.

mero dei dati raccolti, può rendersi opportuno definire soluzioni semplificate per le realtà minori, specie in merito agli adempimenti formali, senza con questo mutare i livelli di tutela richiesti.

Se dunque su alcuni punti, soprattutto correlati ai profili tecnologico-organizzativi, paiono esistere assonanze fra le soluzioni ricercate negli USA e nell'UE, si pensi non solo alla *privacy by design*, ma anche al rilievo congiuntamente attribuito da entrambe le sponde dell'Atlantico al principio di *accountability* degli autori del trattamento[79], da rafforzare attraverso sistemi volti alla maggior procedimentalizzazione, alla creazione di *audit* interni ed, eventualmente, al ricorso a forme di certificazione[80], pur tuttavia rimangono rilevanti divergenze su aspetti essenziali della regolamentazione del trattamento dati.

A tal proposito è evidente come la mancata convergenza dei modelli, ancorché le distanze fra gli stessi paiano progressivamente ridursi, è destinata ad incidere negativamente sulle attività di impresa. Il rischio è che negli anni a venire continuino a persistere le divergenze operative che impediscono alle imprese globalizzate di poter affermare *privacy policies* unitarie, oggi ancor più urgenti in un contesto tecnologico ormai rivolto all'*internet of the things*, all'*ubiquitous computing*[81], alla delocalizzazione delle strutture e risorse informatiche attraverso il ricorso al *cloud computing*[82].

Certamente fra Unione Europea e Stati Uniti saranno possibili nuovi *Safe Harbor*, tanto più alla luce delle modifiche della disciplina d'Oltreoceano, ma nel contempo una probabile « offensiva » statunitense volta a propugnare all'estero il proprio modello di tutela dei dati personali verrà ad incrementare lo scontro fra le due differenti impostazione nei Paesi terzi, laddove ad oggi il modello comunitario pareva poter prevalere e rispetto ai quali si gioca una parte assai rilevante della partita inerente la regolamentazione. Sono infatti l'India, i paesi asiatici, ma in prospettiva anche la

[79] Con riguardo al profilo dell'*accountability*, l'ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 3/2010 on the principle of accountability*, Bruxelles, 13 luglio 2010, p. 10, ha giustamente rilevato come « most of the requirements set out in this new provision actually already exist », ma ha tuttavia ritenuto che una specifica indicazione normativa in tal senso, nell'ottica della revisione della dir. 95/46/CE, « does not aim at subjecting data controllers to new principles but rather at ensuring de facto, effective compliance with existing ones ».

[80] Cfr. già in tal senso ARTICLE 29 DATA PROTECTION WORKING PARTY-WORKING PARTY ON POLICE AND JUSTICE, *The Future of Privacy*, citato *supra*. Con riguardo a specifici aspetti si veda inoltre: ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 3/2010 on the principle of accountability*, citato *supra*.

[81] In estrema sintesi con tale termine si identificano le soluzioni informatiche e comunicative in virtù delle quali i processi di elaborazione dati vengono posti in essere avvalendosi degli oggetti di uso quotidiano muniti, ad esempio, di sensori o dispositivi a radiofrequenza.

[82] Il *cloud computing* consiste in un insieme di tecnologie e risorse informatiche (*hardware* e *software*), accessibili direttamente *on-line* grazie allo sviluppo delle reti di comunicazione; per un maggior approfondimento cfr., volendo, *http://staff.polito.it/alessandro.mantelero/cloud-computing.html*.

Cina ed il Sud-America, a rappresentare le attuali e, soprattutto, future destinazioni dei dati personali. In quelle aree del globo, per ragioni sostanzialmente di contenimento dei costi, verranno in essere le grandi *data farm* destinate a contenere miliardi di dati di altrettante diverse imprese dei Paesi più economicamente avanzati. Ne consegue che le soluzioni legislative che verranno adottate in tali stati risulteranno tutt'altro che indifferenti agli interessi delle imprese europee e che la presenza di un modello alternativo a quello comunitario, sponsorizzato dalla superpotenza statunitense, potrà quantomeno creare difficoltà operative o comunque costringere a soluzioni compromissorie.

Urge dunque un rafforzamento del dialogo fra il regolatore statunitense e quello europeo per addivenire il più celermente possibile ad una soluzione maggiormente uniforme, reclamata tanto dalle imprese quanto dai consumatori. La speranza, guardando al futuro dall'Europa, è che la convergenza non imponga una compressione dei diritti dei singoli, anche perché la storia degli ultimi decenni ha dimostrato come la tutela dei dati personali costituisca ormai una necessità, sia reputata rilevante dai consumatori e, non ultimo, abbia un'incidenza in termini di costi minimale, tale da non penalizzare la imprese, come infatti non è accaduto per le imprese europee rispetto ai concorrenti statunitensi.