D'AMMASSA & ASSOCIATI

STUDIO LEGALE

Avv. Giovanni d'Ammassa
Avv. Andrea Marco Ricci, Ph.D.
Avv. Andrea Michinelli

OF COUNSEL

Avv. Alessandra Fiumara
Avv. Carlo Sala
Diritto Industriale
Avv. Giuseppe Vaciago
Diritto Penale

IL NUOVO REGOLAMENTO EUROPEO DELLA PRIVACY *DE IURE CONDITO* E *DE IURE CONDENDO*. PRIME IMPRESSIONI SUI MARGINI DI INTERVENTO DEGLI STATI MEMBRI: QUALE UNIFORMITÀ APPLICATIVA?

14 gennaio 2016 - Avv. Andrea Michinelli – a.michinelli@dammassa.com

1 - Premessa

Dopo diversi anni di gestazione e lotte fra interessi contrapposti, finalmente le autorità comunitarie hanno predisposto il testo definitivo[1] dell'emanando **Regolamento comunitario in materia di trattamento dei dati personali** (di seguito "Regolamento")[2], il quale sarà pubblicato a gennaio 2016 nella Gazzetta Ufficiale UE e che concederà, comunque, due anni di tempo dalla pubblicazione per la sua applicazione[3].

Le novità in campo sono numerose, il tempo permetterà di colmare i tanti dubbi e risvolti applicativi che entreranno in gioco. Decisivo sarà constatare quanto i singoli Stati membri potranno e dovranno intervenire localmente – come previsto dal Regolamento stesso – onde, di fatto, creare differenze potenzialmente rilevanti da Paese a Paese. Un effetto

[1] Reperibile al seguente URL: *http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf*. I presenti riferimenti ai numeri dei considerando e degli articoli probabilmente muteranno, in alcuni casi, alla pubblicazione del testo definitivo in Gazzetta Ufficiale UE.

[2] Come noto, il mezzo regolamentare è previsto dall'art. 288 TFUE con portata generale per tutti gli Stati membri e di diretta applicabilità verso Stati, persone e istituzioni destinatarie, salva – come nel caso in parola – la necessaria integrazione locale che renda possibile l'esecuzione concreta di parte del provvedimento comunitario se necessita di integrazione attuativa.

[3] V. l'art. 91.d del Regolamento. Salva l'apposizione di un termine particolare come questo, di norma i Regolamenti entrano in vigore previa *vacatio legis* di 20 giorni dalla pubblicazione in Gazzetta Ufficiale UE: si vuole dare tempo a Stati e imprese, soprattutto, di approntare quanto necessario alla complessa nuova gestione dei dati, tra procedure di *privacy assessment* e provvedimenti di riordino legislativo.

paradossale che si voleva certamente evitare nelle intenzioni iniziali, come testimonia l'adozione dello strumento regolamentare invece di quello della Direttiva; i compromessi raggiunti hanno creato diverse "zone grigie" nell'impianto che lasciano aperta la porta a svariate interpretazioni e difformi applicazioni, rischiando di ricreare quella selva di regole stratificate che finora ha reso la materia spesso inestricabile e lontana dall'auspicata certezza del diritto[4], senza menzionare la comprensibilità e chiarezza che si vorrebbero sempre presenti nei provvedimenti indirizzati anche ai semplici cittadini[5]. Ciò che si vuole proporre di seguito è una breve panoramica di quali incertezze si profilino *de iure condito* all'orizzonte già a una prima lettura del provvedimento, sperando che vengano colmate da un'effettiva e tempestiva attività uniformatrice *de iure condendo*.

2 – Abrogazioni e integrazioni sul trattamento dei dati personali

Riepilogando brevemente alcuni dei punti più rilevanti *prima facie*[6], si può aiutare la complessa lettura con un'elencazione analitica, quasi "radiografica": il testo è ricco di ben 135 considerando e 91 articoli[7], disegnando un sistema complesso[8] e dotato di un'organicità ancora da verificare e che sarà terreno fertile per autorevoli commentatori. Trattando anzitutto delle fonti, si deve tenere conto quale premessa che con l'entrata in vigore del Regolamento:

[4] Si pensi alle diverse interpretazioni rese tuttora da autorità e diversi organi nazionali, chiamati a pronunciarsi in materia di dati personali o comunque in ambiti che vi si intersecano, come il Garante della Privacy e la Cassazione: ad es. la seconda, con sentenza n. 22611 dell'11 giugno 2012, ha ammesso la possibilità di adottare sistemi di videosorveglianza dei lavoratori in mancanza delle preventive procedure di accordo sindacale o con la DTL, qualora vi sia comunque un assenso contrattuale di tutti i lavoratori aziendali, ai sensi del previgente art. 4 l. 300/1970; il Garante italiano è più volte intervenuto in casi analoghi, d'altro canto, ribadendo la non ammissibilità di una procedura siffatta in deroga a quella di accordo sindacale o amministrativo, cfr. il provvedimento generale del Garante del 29 aprile 2004 (doc. web 1003482) e quello dell'8 aprile 2010 (doc. web 1712680).

[5] Il paradosso si è confermato con la recente innovazione del Codice del Consumo (D.Lgs. 206/2005) a opera del D.Lgs. 21/2014, generando un testo di difficile lettura e coordinamento anche per i professionisti.

[6] Si propone qui una traduzione *ad hoc* di vari termini ed espressioni, non essendo ancora disponibile un testo ufficiale in lingua italiana. Per i termini già adottati nella precedente Direttiva si è sfruttata la traduzione impiegata nel recepimento confluito nel D.Lgs. 196/2003.

[7] Di seguito, salvo diversa indicazione, si farà sempre riferimento ad articoli del Regolamento.

[8] Ricordiamo che la Direttiva precedente di disciplina generale del trattamento dei dati personali, la 95/46/CE, era di soli 34 articoli.

a) (art. 88) si abroga l'attuale **Direttiva 95/46/CE** alla predetta entrata in vigore; gli effetti possono includere, pertanto, l'abrogazione anche delle normative nazionali emanate in applicazione di tale Direttiva, come il **D.Lgs. 196/2003**[9], almeno nelle parti di diretta trasposizione di tale Direttiva;

b) (art. 89) resta invece vigente la **Direttiva 2002/58/CE** sulla privacy nelle comunicazioni elettroniche, recepita nel nostro ordinamento con specifiche disposizioni collocate sempre nel corpo del D.Lgs. 196/2003[10] – si prospetta pertanto, in linea con quanto visto sopra, un intervento normativo nazionale che chiarisca quali disposizioni del D.Lgs. 196/2003 subiranno l'abrogazione e quali no, oppure si potrà varare un provvedimento nazionale che *ex novo* recepisca la Direttiva 2002/58/CE[11] quanto ai vari profili integrativi-esecutivi;

c) (art. 89b) gli **accordi internazionali tra UE e Stati extra-UE** per il rispetto delle tutele nel trattamento, stipulati prima dell'entrata in vigore del Regolamento, restano immutati[12]; si badi che all'art. 41.5b si prevede la possibilità che le autorizzazioni già rilasciate dagli Stati o Autorità nazionali in passato possano essere integrate, sostituite o abrogate dalla mera Autorità nazionale;

d) si menziona una **futura Direttiva**[13] che dovrà disciplinare l'uso giudiziario e investigativo dei dati personali, sostituendo la decisione quadro del Consiglio UE sulla protezione dei dati e risalente al 2008.

---

[9] Vale a dire il nostro Codice per il trattamento dei dati personali, detto di prassi "Codice della Privacy", che aveva sostituito la prima legge organica in materia ovvero la l. 675/1996.

[10] Non è di poco conto tale sopravvivenza, considerato che la Direttiva armonizza la disciplina di realtà in evoluzione come i *cookies*, le reti di comunicazione elettronica e non, le comunicazioni pubblicitarie indesiderate, ecc. Si è, evidentemente, ritenuta tuttora valida e sufficientemente aggiornata questa disciplina, pur a fronte di vari riferimenti in tale Direttiva a quella precedente del 1995 (ad es. all'art. 1 si stabilisce che la Direttiva del 2002 precisa e integra la Direttiva del 1995, all'art. 2 si rimanda alle definizioni della medesima, ecc.). La giustificazione potrebbe rinvenirsi nel dato per cui la Direttiva del 2002 risulta emendata di recente, con l'importante Direttiva 2009/136/CE (indicata spesso come "cookie law") e recepita in Italia nel 2012 mediante integrazione nel testo del D.Lgs. 196/2003.

[11] Tale ultima strada sarebbe quella più chiara per disegnare una nuova disciplina, soprattutto se si includerà nello stesso atto normativo nazionale quanto andrà ad attuare facoltà od obblighi regolamentari comunitari.

[12] Non certo, quindi, la già invalidata autorizzazione comunitaria intercorsa con gli Stati Uniti e denominata "*Safe Harbour*" del 2000, a opera della Corte di Giustizia UE nella causa n. C-362/14 Maximillian Schrems/Data Protection Commissioner.

[13] Con relativo recepimento nella normativa nazionale: sarebbe utile che accadesse con lo stesso provvedimento nazionale di integrazione del Regolamento.

3 – Le facoltà degli Stati membri

L'impianto deciso in sede comunitaria fa emergere una realtà in cui gli Stati comunitari **potranno** adottare specifici provvedimenti normativi nazionali (generando potenziali differenze a macchia di leopardo nel territorio comunitario, giocoforza) quanto a svariati profili, riassumibili come segue:

- (considerando 6a) viene concesso il potere agli Stati membri di **specificare o restringere l'applicazione del Regolamento** innestando parti dello stesso all'interno di norme nazionali, per quanto necessario all'uniformità applicativa comunitaria e per rendere la normativa comprensibile ai destinatari del singolo Stato membro (come si può prevedere nell'utilizzo di istituti giuridici che possono avere diverse sfaccettature da Paese a Paese o addirittura essere assenti in alcune normative locali);
- (considerando 23aa) il Regolamento non si applica al trattamento dei dati di **defunti**, potenzialmente disciplinabile dallo Stato se ritenuto opportuno;
- (art. 6.2.a) si potranno adottare provvedimenti specifici di adattamento nazionale del Regolamento in occasione (art. 6.1.c) dell'adempimento di **obblighi legali** (es. contrattuali) del titolare o (art. 6.1.e) di **esecuzione di compiti di interesse pubblico o da parte di organi della P.A.**;
- (art. 8) quanto all'**età minima** per la quale è richiesto il consenso da parte dell'esercente la patria potestà, di base il limite è di 16 anni (pari all'età minima per l'Italia tale da consentire l'emancipazione del minore[14] e altre limitate attività, come quelle lavorative o per il pieno esercizio dei propri diritti d'autore[15]), la riduzione nazionale potrà però abbassare il limite fino a 13 anni; sarà interessante vedere il riscontro italiano e se e come verrà motivato un eventuale abbassamento dell'età minima;
- (art. 9.5) vi potranno essere provvedimenti specifici, anche limitativi, circa il trattamento di **dati sanitari, biometrici o genetici nel territorio nazionale**;

[14] V. art .84 c.c.
[15] Cfr. art. 108 l. 633/1941.

- (art. 17.1.e) la **cancellazione** di dati (in ottemperanza al **diritto all'oblio**, ora riconosciuto normativamente[16]) dovrà avvenire nei casi eventualmente previsti come obbligatori anche da norme locali;
- (art. 17a) il blocco del trattamento dei dati, richiesto dall'interessato, può non essere rispettato – tra l'altro – per motivi non ben precisati di "pubblico interesse" sanciti dallo Stato membro[17];
- (art. 20) è derogabile il divieto di utilizzare decisioni (e dunque le profilazioni alla loro base) ricavate da processi automatizzati, qualora abbiano effetti legali e sempre che lo Stato membro lo preveda per legge; contestualmente lo Stato dovrà stabilire le misure di salvaguardia dei diritti, delle libertà e dei legittimi interessi dell'interessato;
- (art. 21) ogni Stato potrà limitare per legge l'ambito di applicazione di numerosi articoli del Regolamento[18] concernenti i diritti dell'interessato e il loro esercizio, qualora – pur nel rispetto dei diritti e delle libertà fondamentali e sempre in maniera proporzionata a quanto necessario in una società democratica – lo Stato ravvisi un interesse preminente tra quelli elencati nel medesimo art. 21, tra cui troviamo: la difesa e sicurezza nazionale, le indagini giudiziarie, importanti scopi di generale pubblico interesse (soprattutto economico, finanziario, fiscale, di salute pubblica o previdenza sociale), l'indipendenza giudiziaria, il rispetto dell'etica professionale per le professioni regolamentate, ecc.;
- (art .24.1) nel caso di titolari congiunti[19], la legge statale può prevedere la ripartizione delle rispettive responsabilità tra i molteplici titolari; in mancanza, dovrà sussistere un contratto tra le parti per stabilire tale suddivisione;
- (art. 26.2.a) il responsabile potrà trattare i dati solo in base a istruzioni documentabili (quindi in forma scritta o loro equivalente, inteso in chiave probatoria) ricevute dal titolare, salvo che una legge statale non preveda l'operazione di trattamento come obbligatoria a prescindere; in tale ultimo caso, il titolare dovrà segnalare

[16] In precedenza ammesso dalla Corte di Giustizia UE con la discussa sentenza del 13 maggio 2014, n. C-131/12.C-131/12 Mario Costeja Gonzalese e AEPD contro Google Spain e Google Inc.
[17] Gli altri casi di eccezione comprendono: il consenso dell'interessato, l'instaurazione o esercizio o difesa di propri diritti, la protezione dei diritti di terzi.
[18] In particolare, quanto previsto agli artt. 5, 12-20, 32 del Regolamento in esame.
[19] Si tratta di più titolari che decidono congiuntamente scopi e mezzi del trattamento, con relative responsabilità.

previamente al responsabile questo requisito legale, salvo che la legge non disponga diversamente per ragioni di pubblico interesse;

- (art. 26.2.g) nuovamente riguardo alla figura del responsabile, questi dovrà procedere alla cancellazione dei dati su richiesta del titolare, salvo che non vi sia una legge che prescriva, al contrario, il mantenimento dei dati; si pensi ad es. al caso nazionale del mantenimento obbligatorio dei dati di fatturazione a fini fiscali per 5 anni a carico degli imprenditori;
- (art. 27) il responsabile e altri soggetti deputati al trattamento potranno effettuare il trattamento anche in mancanza di apposite istruzioni del titolare ma solo se così consentito da norme comunitarie o statali;
- (art. 34.7a) potrebbe stabilirsi come obbligatoria una preventiva procedura di consultazione dell'Autorità nazionale, qualora il titolare compia trattamenti nel pubblico interesse (ad es. per ragioni attinenti alla previdenza sociale o alla salute pubblica);
- (art. 35.4) la nomina[20] del *data protection officer* ("responsabile della protezione dei dati") – nuova figura professionale di tutela dei dati personali[21] che dovrà essere competente non solo del rispetto della normativa privacy ma anche della protezione in sé dei dati (personali o meno) – potrà essere imposta in capo al titolare, oltre che nei casi già previsti dal Regolamento all'art. 35.1, anche in nuove fattispecie dettate da norme comunitarie o nazionali; oltretutto sarà soggetto alle normative nazionali e comunitarie circa il rispetto del segreto professionale nell'espletazione della sua attività;

[20] Ex art. 35.1 si apprende che la nomina può avvenire non solo da parte del titolare ma anche del responsabile; si possono avere dei dubbi perché l'articolo in parola recita che titolare "e" responsabile dovranno procedere alla designazione, dunque non è chiaro se la nomina debba avvenire con atto congiunto o se sia possibile anche disgiuntamente (come sembra avvalorato dall'art. 35.4 ove troviamo la congiunzione "o" in merito ai soggetti designanti).

[21] Disciplinato agli artt. 35-37 del Regolamento, si tratta di un esperto nel trattamento dei dati di un titolare, che sia un interno o un esterno all'organizzazione dello stesso; di fatto si potrà incaricare un dipendente o un professionista a contratto. È una figura difforme da quella del responsabile ex art. 29 D.Lgs. 196/2003 e che, pare, non può cumularsi nella stessa persona del responsabile. Particolarmente importanti sono i casi in cui la nomina è obbligatoria (art. 35.1), ovvero: a) trattamento dei dati da parte della Pubblica Amministrazione; b) quando le attività principali del titolare o del responsabile comportino un regolare e sistematico monitoraggio degli interessati, su larga scala; c) qualora le attività principali del Titolare o del Responsabile comportino su larga scala il trattamento di dati sensibili e giudiziari. Sarà tutto da vedere quale uniformità interpretativa si potrà imporre circa il significato di "larga scala": le bozze precedenti del Regolamento presentavano parametri oggettivi numerici (es. numero minimo di interessati), questo risultato pare un compromesso dall'incerto futuro.

- (art .38) si potrà incoraggiare a livello nazionale la stesura di codici di condotta rivolti ai titolari per l'attuazione del Regolamento, tenuto conto di vari interessi come le esigenze delle PMI locali;
- (art. 39) analogamente, analoghi incentivi si potranno dedicare alle procedure di certificazione e "bollini" di *compliance* privacy ai sensi del Regolamento, sottolineando che il livello comunitario – per una maggiore uniformità applicativa - dovrà essere quello dedicato con particolare attenzione a tali attività; gli organismi di certificazione saranno comunque (art. 39a) oggetto di verifica statale quanto alla rispondenza ai parametri nazionali;
- (art. 44.5a) per importanti ragioni di interesse pubblico, si potranno stabilire limiti nazionali al trasferimento di determinate categorie di dati personali in Paesi terzi o a organizzazioni internazionali;
- (art. 53.4) si possono assegnare ulteriori poteri in capo all'Autorità Garante nazionale, oltre a quelli già previsti dal Regolamento a mente dell'art. 54;
- (art. 76) è facoltativa l'attribuzione a organismi associativi, o comunque enti no profit, del diritto di agire (giudizialmente o amministrativamente) avverso violazioni della normativa in parola, sia in rappresentanza di un singolo soggetto leso che per tutela di un interesse generale al rispetto della normativa in discussione (in quanto rientrante tra gli scopi dell'ente esponenziale);
- (art. 79.3b) può stabilirsi se e in che misura le sanzioni amministrative (nei casi più gravi, potranno arrivare a 20 milioni di euro o al 4% del fatturato del titolare, a seconda di quale risulti la sanzione più elevata) possono essere applicate alla Pubblica Amministrazione; qualora non si voglia applicarle a livello nazionale, sarà comunque opportuno un meccanismo che in qualche modo incentivi la P.A. al rispetto della normativa;
- (art. 79.5, v. anche considerando 119) se non sono previste sanzioni amministrative nazionali in conseguenza della violazione del Regolamento (incluso il sequestro dei profitti realizzati grazie alla violazione), si potrà applicare l'impianto sanzionatorio dell'art. 79 del Regolamento mediante un riparto analogo a quello già esistente in Italia, ovvero con un'Autorità nazionale competente come il Garante italiano che in prima battuta eroga la

sanzione e successiva possibilità di intervento giudiziario (con relativo potere coercitivo) per l'esecuzione;

- (art. 80b) si possono stabilire specifiche condizioni locali di trattamento di codici identificativi nazionali o di generale applicazione (ad es. del codice fiscale o partita IVA);
- (art. 82) per legge o tramite contratto collettivo (anche aziendale o di prossimità, pare, visto che non viene precisato che debba essere nazionale) si possono stabilire ulteriori e più specifiche regole per il trattamento dei dati nell'ambito del rapporto di lavoro, ad es. quanto all'assunzione, all'esecuzione del rapporto, salute e sicurezza, ecc.; in tal caso si dovranno sempre prevedere misure adeguate al rispetto della dignità umana e dei diritti fondamentali, oltre ai casi di trasferimento dei dati fra gruppi societari e alla sorveglianza dei luoghi di lavoro;
- (art. 83) deroghe e salvaguardie analoghe al caso precedente potranno essere adottate da norme nazionali in materia di trattamento per scopi di interesse pubblico, scientifico, storico o statistico;
- (art. 84, v. anche considerando 127) si potrà adottare una specifica normativa quanto al rispetto del segreto (professionale e non) da parte dell'Autorità preposta (come il Garante italiano e la delegata Guardia di Finanza[22]) ad accedere ai dati e ai locali del Titolare[23] per le verifiche ispettive di legge[24].

4 – Gli obblighi degli Stati membri

Quanto sopra non va confuso con diverse previsioni del testo comunitario di taluni obblighi in capo agli Stati membri UE, quali requisiti di esecuzione di svariate disposizioni del Regolamento. Le distinguiamo in ordine:

[22] Ovvero il Garante italiano per la tutela dei dati personali, http://www.garanteprivacy.it, disciplinato dal D.Lgs. 196/2003; forse il Garante dovrà trovare una nuove fonte nazionale di disciplina, alla luce di quanto detto *supra*.

[23] Utilizziamo qui la convenzionale traduzione di "titolare" al posto di "controller" e di "responsabile" al posto di "processor", come attuato nel D.Lgs. 196/2003 in ottemperanza alla Direttiva 95/46/CE.

[24] Si pensi ad es. ai problemi analoghi, in sede di accertamento tributario, che hanno portato alla l. 413/1991 poi riversata nell'art. 52 DPR 633/1972, senza tuttavia che si sia considerato risolto il profilo di tutela del segreto in sede ispettiva.

- (art .34) vi sarà consultazione preventiva obbligatoria dell'Autorità nazionale da parte dello Stato in sede di redazione legislativa (o regolamentare) nazionale in merito al trattamento di dati personali;
- (art. 46) è prevista l'istituzione di una o anche più Autorità per la tutela dei dati (resta da vedere se si possono integrare attribuzioni a enti già esistenti, ad es. si potrebbe attribuire all'AGCM, Autorità competente per la tutela dei consumatori, anche il campo della tutela dei dati personali degli stessi consumatori; come già in passato, le Autorità dovranno essere di effettiva indipendenza (art. 48) e con l'assegnazione di un budget annuale pubblico; in Italia permarrà il Garante della privacy, come ovvio, a fronte di alcune possibili revisioni; peculiare risulta la previsione ex art. 85 del Regolamento, onde per cui lo Stato potrebbe designare un'Autorità specificamente competente a controllare il rispetto della normativa da parte di chiese ed enti religiosi;
- (art. 79b) si dovranno determinare sanzioni penali applicabili a livello nazionale, soprattutto quanto alle fattispecie non coperte da sanzioni amministrative, garantendo che le sanzioni siano effettivamente implementate e che siano effettive, proporzionate e dissuasive; si tratta di un'integrazione prevedibile e giustificata dal sistema stesso dell'Unione Europea, posto che sul piano comunitario non è possibile predeterminare sanzioni di tipo penale bensì sono riservate alla competenza nazionale: vedremo se verrà confermato l'impianto sanzionatorio già dettato nel D.Lgs. 196/2003, discutibile in più punti, oppure se si deciderà di inasprirlo o ampliarlo;
- (art .80) si dovrà conciliare la tutela della privacy con il trattamento dei dati per scopi di libera manifestazione del pensiero, di informazione, accademici e di espressione artistica o letteraria; lo strumento dovrà essere quello di norme nazionali in deroga alla disciplina del Regolamento, se necessarie per garantire l'equilibrio tra la protezione dei dati e il diritto di libera espressione e informazione[25]; principio analogo è sancito all'art. 80a quanto all'equilibrio tra interessi contrapposti nel caso di un diritto di accesso agli atti amministrativi da parte della P.A.

[25] Auspichiamo che tale importante presidio trovi una migliore espressione rispetto all'attuale norma nazionale, ovvero l'art. 136 del D.Lgs. 196/2003, di incerta interpretazione e applicazione soprattutto quanto al comma 1 lett. c).

5 – Conclusioni

Alla luce di quanto sopra, cosa ci si deve attendere dal futuro a disegnare le istruzioni per l'uso dei dati personali: il Regolamento e un profluvio di norme locali integrative? Oppure innumerevoli provvedimenti del Garante nazionale, degli enti sovranazionali e degli organismi di coordinamento, atti spesso di incerta collocazione quanto al sistema delle fonti[26]? Insomma, si arriverà sotto questo profilo a un'Unione Europea comune nelle premesse e poi attaccata ai propri localismi in sede attuativa? Viene da chiedersi come potrà essere raggiunta l'uniformità applicativa del Regolamento, il quale tuttavia fornisce uno strumento precipuo: agli artt. 57 ss. si prescrivono adempimenti in ambito di cooperazione tra istituzioni comunitarie e nazionali (ovvero ciò che negli ultimi anni non ha dato miglior prova di sé nell'attuazione del disegno comunitario generale). Oltretutto, quando gli Stati derogheranno al Regolamento avranno l'onere di darne notizia alla Commissione Europea (la quale, dunque, dovrà monitorare le svariate applicazioni nazionali) e in ogni caso le Autorità nazionali competenti (come il Garante italiano) dovranno (art. 46.1a) contribuire all'applicazione uniforme di tutto l'impianto del Regolamento. È un rinnovato ruolo per il nostro Garante, chiamato a fungere sia da guardiano locale del Regolamento sovranazionale che delle norme nazionali collegate, ricordandosi che sarà anzitutto l'autorità giudiziaria il soggetto tenuto a dover sempre ritenere la fonte comunitaria prevalente sulla legislazione nazionale contrastante, in forza dell'art. 11 Cost., oltre a dover attuare un'interpretazione conforme, cioè il più possibile aderente al diritto comunitario[27].

Altro strumento di uniformità potrà essere, in aggiunta, la certificazione (prevista agli artt. 39-39a del Regolamento) che permetterà ai titolari di ottenere attestati di *compliance*

[26] Nel tempo si è ravvisato criticabile che il Garante, da autorità amministrativa indipendente, possa pubblicare provvedimenti in Gazzetta Ufficiale con forza di legge ai sensi dell'art. 154 comma 1 lett. c) e d) D.Lgs. 196/2003.

[27] Si tratta di un principio interpretativo riconosciuto dalla Corte Costituzionale ex art. 117 Cost.

privacy validi in tutta Europa[28], una volta che si sarà provveduto a stabilire procedure uniformi di certificazione volontaria[29].

Sia chiaro, l'occasione di avere un ombrello unico a livello comunitario non era scontata, come evidenzia la lotta che ha portato a questo risultato: visibilmente aspra, politicamente parlando[30], giunta infine a un traguardo comunque significativo. Toccherà alle varie Autorità garanti nazionali, alla Commissione europea ma soprattutto al nascente Comitato[31] Europeo per la Protezione dei Dati[32], inaugurare un inedito coordinamento che possa in concreto portare a regole condivise[33] e affidabili in tutta Europa, senza che si generi una Babele di provvedimenti integrativi, nazionali e non[34]. Come detto *supra*, un ruolo preminente l'avranno gli stessi Stati nazionali in sede legislativa, chiamati a emanare provvedimenti e a effettuare valutazioni integrative di non poco conto. Auspicando che si arrivi a semplificare, invece di complicare, un settore che necessita, ancora più di altri

[28] Almeno auspichiamo sia così perché in effetti l'art. 39.1 sancisce che sarà "*in particolare*" a livello comunitario il piano in cui si dovranno incoraggiare i meccanismi di certificazione, lasciano aperta la possibilità per ognuno dei soggetti coinvolti – singoli Stati membri e Autorità nazionali incluse – di provvedere in proprio.

[29] Come già accade con le norme internazionali e linee guida ISO, in particolare per la certificazione qualità di imprese e professionisti.

[30] Un confronto tra le numerose versioni precedenti della bozza di Regolamento era, di per sé, già eloquente di quali interessi fossero in gioco, si pensi proprio ai casi in cui era obbligatoria l'implementazione del *data protection officer*.

[31] Oppure "Consiglio" o "Commissione", a seconda della traduzione che verrà preferita in sede comunitaria alla pubblicazione in italiano.

[32] Ovvero lo *European Data Protection Board* che nel testo del Regolamento, in più punti (es. art. 58 del Regolamento, considerando 113 poi rispecchiato all'art. 66 del Regolamento, ecc.), assume il ruolo di guida, arbitro e fonte di fondamentali linee guida, raccomandazioni e *best practices* del settore. La disciplina istitutiva si trova agli artt. 64 ss. del Regolamento.

[33] Non solo: ad es. l'art. 56 del Regolamento chiarisce che molto potrebbe cambiare sul piano applicativo, ove un'Autorità nazionale ne incarichi un'altra estera per effettuare accertamenti sovranazionali di proprio interesse o competenza, realizzando davvero un ombrello comunitario di pari ed effettiva tutela dei dati personali. Ricordando che se nel caso concreto entreranno in gioco difformi concezioni locali del trattamento, sarà difficile capire quale potrà prevalere.

[34] Resta il dubbio che non si sia voluto osare un approccio di maggior rottura quanto al sistema comunitario di tutela dei dati personali varato in precedenza, in particolare quanto alle nuove tecnologie: si pensi ad es. al perdurante *iter* imposto ai Titolari del trattamento e ancorato alla sequenza *informativa-consenso-trattamento* verso gli interessati, defatigante se calato in un contesto tecnologico di svariati accessi giornalieri alle svariate fonti informatiche di trattamento (si pensi alle molteplici *app* in uso negli *smartphone* odierni, ai siti web di e-commerce, alla messa a disposizione al pubblico di *user generated content* tramite i social network, per esempio). Anche la frequente irritazione per l'onnipresente banner informativo circa il trattamento web dei cookies testimonia lo stridente contrasto tra ragionamento normativo e realtà degli utenti ma soprattutto degli interessati stessi!

ambiti, di un'opera di revisione continua che rincorra gli incessanti mutamenti tecnologici, aventi notevoli ricadute circa il trattamento dei dati personali[35]. È prevedibile, infatti, che una stratificazione normativa troppo complessa risulti lesiva degli interessi - oltre che degli Stati - anche dei medesimi destinatari dei provvedimenti, se si pensa ad es. a un'azienda che debba tenere il passo con quanto prescritto e che per farlo debba immergersi in un *mare magnum* di provvedimenti e fonti[36], senza una bussola chiarificatrice, condivisa e il più possibile schematica. Il mercato comunitario e nazionale se ne gioverebbe, oltre a garantire un maggiore rispetto dei dati personali dei cittadini stessi[37].

[35] Basti pensare alle obsolete misure minime di sicurezza, dettate nell'Allegato B del D.Lgs. 196/2003, oppure all'emergente problema del trattamento dei *big data*, non ancora all'orizzonte all'epoca della precedente Direttiva 95/46/EC.

[36] Non è insolito il disorientamento che spesso sovviene a chi si avvicini *ex novo* alla materia e che approcci il profluvio di provvedimenti presenti sul portale del Garante italiano, per fare un esempio.

[37] È sotto gli occhi di tutti la quasi inefficacia del sistema del Registro Pubblico delle opposizioni gestito dalla Fondazione Bordoni (http://www.registrodelleopposizioni.it) e che avrebbe dovuto contenere il fenomeno delle chiamate commerciali indesiderate. La riforma regolamentare è l'occasione giusta per rivedere meccanismi farraginosi e inconcludenti come questo.