IL NUOVO REGOLAMENTO EUROPEO 2016/679

Il nuovo "**Regolamento Europeo sulla Protezione dei Dati Personali**", che sostituirà l'attuale Direttiva 95/46/CE e supererà l'attuale Codice della Privacy (D.Lgs. 196/03), è stato pubblicato in Gazzetta Ufficiale UE il 4 Maggio 2016 e sarà vigente 20 giorni dopo la pubblicazione in Gazzetta Ufficiale, per diventare definitivamente applicabile, in via diretta, in tutti i Paesi UE, a partire dal **25 maggio 2018**, quando dovrà essere garantito il perfetto allineamento fra la normativa nazionale e le disposizioni del Regolamento.
Nel contempo la Commissione europea, il Comitato europeo per la protezione dei dati (composto dai Garanti di ogni paese) e ogni specifica **Autorità di Controllo** (per l'Italia il Garante Privacy, che cambia solo denominazione) emaneranno specifici provvedimenti che consentiranno di gestire la fase di transizione e dare applicazione pratica alla nuova normativa Privacy.
Nota metodologica: **la lettura delle singole disposizioni deve essere fatta in combinato disposto con i relativi considerando, che altro non sono che la motivazione presupposta della norma**.
Il testo del Regolamento, con tutti i richiami dei considerando riportati per ogni articolo, è scaricabile dal sito del Garante Privacy.

Di seguito un breve riepilogo delle principali novità che verranno introdotte dal nuovo Regolamento Europeo.

a) I principi introdotti dal Regolamento saranno simili a quelli della vecchia Direttiva 95/46/CE, ma la nuova normativa avrà un "approccio più dinamico" e opererà come un "Sistema di gestione" in via preventiva, simile a quello tipico del "sistema di gestione della sicurezza delle informazioni", descritto dalla ISO/IEC 27001 e dalla norma ISO/IEC 15408 (*Evaluation criteria for IT security*, nota anche come "Common Criteria") che definisce i principi ed i concetti generali di sicurezza IT specificando anche un modello generale attraverso il quale valutare le proprietà di un prodotto o sistema IT.

b) Le tutele previste dal nuovo Regolamento si applicheranno alle sole **PERSONE FISICHE**, in relazione al trattamento dei loro dati personali. Per "**dato personale**" si intende: *qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, **dati relativi all'ubicazione**, un **identificativo online (IP)** o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.*

c) Alcune **DEFINIZIONI** subiranno una modifica sostanziale. Ad esempio, il vecchio "incaricato del trattamento", il cui termine veniva utilizzato per indicare le figure con mansioni esecutive, non troverà più una esatta definizione, se non quella di "*chiunque agisca sotto l'autorità del Titolare o del Responsabile del trattamento*". Quindi quest'ultima definizione sostituirà quella attuale di incaricato; vengono introdotte le nuove definizioni di "**profilazione**" e "**pseudonomizzazione**".

d) Gli "**EX DATI SENSIBILI**" e gli "**EX DATI GIUDIZIARI**" troveranno posto solo in parte nell'articolo dedicato alle definizioni; a loro vengono dedicati due articoli ad hoc (**art. 9** e **art. 10**).

e) Saranno soggetti al nuovo Regolamento anche i trattamenti dei dati personali effettuati da un titolare del trattamento o da un responsabile del trattamento non stabilito nell'Unione ma che riguardino interessati stabiliti nell'Unione Europea.

f) L'**INFORMATIVA, che rimane il perno del sistema privacy,** dovrà contenere più elementi rispetto al passato (a titolo di esempio non esaustivo, l'identità e le coordinate di contatto del titolare del trattamento e del suo eventuale rappresentante; le coordinate di contatto dell'eventuale responsabile della protezione dei dati; le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento; l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale; il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare questo periodo; i diritti che l'interessato può esercitare, etc…) ma, le informazioni dovranno essere coincise, facilmente accessibili e comprensibili, utilizzando un linguaggio semplice e chiaro (ad esempio, inglobando simboli grafici, rendendole accessibili via web, etc…); inoltre il Regolamento prevede due tipologie di **INFORMATIVA**, che si distinguono a seconda che i dati vengano raccolti presso l'interessato (art. 13) o non siano stati ottenuti presso l'interessato (art. 14).

g) Il **CONSENSO** (art. 7) dovrà essere sempre espresso (**è esclusa ogni forma di consenso tacito**) mediante un'azione positiva inequivocabile con la quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare che i dati personali che lo riguardano siano oggetto di trattamento (ad esempio mediante dichiarazione scritta, anche elettronica, o orale; ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in questo contesto che l'interessato accetta il trattamento proposto). Il consenso, inoltre, dovrà essere dimostrabile, distinguibile in base alle finalità per cui viene richiesto, in forma comprensibile e facilmente accessibile (utilizzando un linguaggio semplice e chiaro), revocabile in qualsiasi momento.

Per i **MINORI** di 16 anni (o se previsto, per i minori con un età inferiore ma non al di sotto dei 13 anni) occorre che sia espresso o autorizzato dal titolare della responsabilità genitoriale (art. 8).

h) Vengono rafforzati i **DIRITTI (Capo III, sezione I)** sinora riconosciuti agli interessati, adeguandoli all'ambiente virtuale e viene conferito agli interessati un maggiore potere di controllo sui propri dati personali; in particolare, sono sanciti i seguenti diritti:
diritto di accesso dell'interessato (art. 15);
diritto di rettifica (art. 16);
diritto alla cancellazione ("*Diritto all'Oblio*" - art. 17);
diritto di limitazione di trattamento (art. 18);
obbligo di notifica in caso di rettifica, cancellazione o limitazione dei dati (art. 19);
diritto alla portabilità dei dati (art. 20); l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile a macchina i dati personali che lo riguardano forniti ad un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora);
diritto di opposizione (art. 21);
diritto di non essere sottoposto a un processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione (art. 22);
la nuova figura del "**TITOLARE DEL TRATTAMENTO**" (in inglese "***Data controller***") avrà l'obbligo di:
- mettere in atto misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento dei dati personali è effettuato conformemente al presente regolamento –> (viene introdotto il c.d. principio dell'"***Accountability***").
Dette misure sono riesaminate e aggiornate qualora necessario –> (non verranno previsti intervalli prestabiliti di aggiornamento);
- l'obbligo di trattare i dati secondo il principio della "***Privacy By Design***" (tenendo, cioè, in considerazione le tematiche relative alla protezione dei dati, sin dalla fase di progettazione dei sistemi che permettono il trattamento dei dati personali);
- l'obbligo di trattare i dati secondo il principio della "***Privacy By Default***" (mettendo, cioè, in atto meccanismi per garantire che siano trattati, di default, solo i dati personali necessari per ciascuna finalità specifica del trattamento e che, in particolare, la quantità dei dati raccolti e la durata della loro conservazione non vadano oltre il minimo necessario per le finalità perseguite);

i) Viene introdotta la figura del c.d. "**CONTITOLARE**" (in inglese "Joint Controller", art. 26) quando, cioè, due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento dei dati personali.

j) Viene introdotta la figura del c.d. "**RAPPRESENTANTE DI TITOLARI DEL TRATTAMENTO NON STABILITI NELL'UNIONE**" (art. 27), quando, cioè, il trattamento dei dati personali di interessati che si trovano nell'Unione viene effettuato

da un titolare del trattamento o responsabile del trattamento che non è stabilito nell'Unione.

k) La nuova figura del "**RESPONSABILE DEL TRATTAMENTO**" (in inglese, "**Data processor**" – art. 28) dovrà presentare garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento e garantisca la tutela dei diritti dell'interessato. Il responsabile del trattamento non potrà ricorrere ad un altro responsabile senza il previo consenso scritto, specifico o generale, del titolare del trattamento. I trattamenti effettuati dal nominato Responsabile dovranno essere "**contrattualizzati**" (art. 28, comma 3).

l) Permane l'obbligo di nomina e di istruzione degli "**EX INCARICATI DEL TRATTAMENTO**" (art. 29): infatti, "*chiunque agisca sotto l'autorità del Titolare del trattamento o del Responsabile del trattamento e che abbia accesso a dati personali, non può trattare tali dati se non è istruito in tal senso dal responsabile del trattamento*".

m) Viene introdotto l'obbligo di redigere il "**REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO**" (art. 30) dove andranno inserite numerose informazioni sul trattamento dei dati (si tratta di una sorta di *ex* Documento Programmatico sulla Sicurezza).
N.B.: Tale obbligo **NON** si applica alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1 o il trattamento di dati relativi a condanne penali e a reati di cui all'articolo 10. –> (il principio dell'"Accountability" renderà consigliabile per tutti i titolari/responsabili del trattamento di adottare uno strumento simile).

n) "**MISURE DI SICUREZZA**"(art. 32): La loro adozione sarà obbligatoria per tutti i titolari/responsabili del trattamento. Tutti i titolari del trattamento/responsabili del trattamento dovranno mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra l'altro, se del caso: ***a***) la **pseudonimizzazione** e la **cifratura dei dati personali**; ***b***) la capacità di assicurare la continua riservatezza, integrità, disponibilità e **resilienza dei sistemi** e dei servizi che trattano i dati personali; ***c***) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; d) una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. Nel valutare l'adeguato livello di sicurezza, occorrerà tener conto in special modo dei rischi presentati da trattamenti di dati derivanti in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, memorizzati o comunque trattati.

Scompaiono, quindi, le c.d. "Misure minime di Sicurezza", lasciando spazio a **misure adeguate al rischio**, opportunamente individuate attraverso una **adeguata, preventiva e personalizzata Analisi del Rischio** ("Risk Assessment"). Tale valutazione del rischio preventiva assomiglia molto all' analisi dei rischi di cui al D.Lgs. 231/2001 (M.O.G.C.).

o) Viene introdotto l'obbligo di rispettare specifici accorgimenti in caso di eventuale "**DATA BREACH**" (art. 33): il titolare del trattamento, cioè, dovrà segnalare all'autorità di controllo (entro 72 ore, dal momento in cui ne è venuto a conoscenza) eventuali violazioni dei dati personali; qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento dovrà comunicare la violazione anche agli interessati.

p) viene introdotto l'obbligo di svolgere la c.d. "**VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI**" (art. 35, *Data Protection Impact Assessment* - DPIA) per i trattamenti che prevedono, in particolare, l'uso di nuove tecnologie, e che possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Tale valutazione è richiesta nei seguenti casi:
a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata sul trattamento automatizzato, compresa la profilazione e da cui discendono decisioni che hanno effetti giuridici o incidono allo stesso modo significativamente su dette persone fisiche;
b) il trattamento, su larga scala, di categorie particolari di dati di cui all'articolo 9, paragrafo 1 o di dati relativi a condanne penali e a reati di cui all'articolo 10;
c) la sorveglianza sistematica di una zona accessibile al pubblico su larga scala. L'autorità di controllo (leggi Garante) redigerà e renderà pubblico un elenco delle tipologie di trattamenti soggetti al requisito della valutazione d'impatto sulla protezione dei dati; come pure, l'Autorità di controllo potrà redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati.
Questo adempimento sostituisce, di fatto, la *ex* "Notifica al Garante" (che non esisterà più) senza, però, che vi sia l'obbligo di invio telematico della comunicazione all'Autorità di Controllo. Qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenta un rischio elevato, in assenza di misure adottate dal titolare del trattamento per attenuare il rischio, il titolare del trattamento, prima di procedere al trattamento dei dati personali, deve consultare l'Autorità di controllo (procedura di "**PRIOR CONSULTATION**") –> si tratta di una sorta di *ex* "Verifica Preliminare" (art. 36).

q) Viene introdotto l'obbligo di designazione del "**Responsabile della Protezione dei Dati**" (***DATA PROTECTION OFFICER – DPO***, artt. 37, 38 e 39) nei seguenti alternativi casi:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
b) le **attività principali** del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, campo di applicazione e/o finalità, richiedono il controllo regolare e sistematico degli interessati su larga scala;
c) le **attività principali** del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati di cui all'articolo 9) o di dati relativi a condanne penali e a reati di cui all'articolo 10).
Ovviamente la nomina di un "Responsabile della Protezione dei Dati" può essere fatta anche su base facoltativa.
Il Responsabile della Protezione dei Dati:
- dovrà possedere qualità professionali, in particolare la conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati e la capacità di adempiere ai compiti previsti dal Regolamento;
- potrà essere un membro del personale del titolare del trattamento o del responsabile del trattamento oppure adempiere ai suoi compiti in base a un contratto di servizio (consulente esterno dotato di competenze giuridiche);
- dovrà essere coinvolto in tutte le questioni riguardanti la protezione dei dati personali;
- il titolare del trattamento o il responsabile del trattamento dovranno sostenere il responsabile della protezione dei dati nell'esecuzione dei compiti, fornendogli le risorse necessarie per adempiere a tali compiti nonché l'accesso ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica;
- non dovrà ricevere alcuna istruzione per quanto riguarda l'esecuzione dei propri compiti;
- non sarà rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti;
- riferirà direttamente ai massimi superiori gerarchici del titolare del trattamento o del responsabile del trattamento;
- sarà tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti;
- potrà svolgere altri compiti e funzioni che non diano adito a un conflitto di interessi;
- dovrà svolgere almeno i seguenti compiti: ***a***) informare e consigliare il titolare del trattamento o il responsabile del trattamento nonché i dipendenti che trattano dati personali in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati; ***b***) sorvegliare l'osservanza del regolamento, delle altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e gli audit connessi; ***c***) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35; ***d***) cooperare con l'autorità di

controllo; ***e***) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento di dati personali, tra cui la consultazione preventiva di cui all'articolo 36 ed effettuare, se del caso, consultazioni su qualunque altra questione;
- nell'eseguire i propri compiti il responsabile della protezione dei dati dovrà considerare debitamente i rischi inerenti al trattamento, tenendo conto della natura, del campo di applicazione, del contesto e delle finalità del medesimo.

r) Verrà promossa l'elaborazione di "**CODICI DI CONDOTTA**" (artt. 40 e 41) destinati a contribuire alla corretta applicazione del nuovo Regolamento, in funzione delle specificità settoriali e delle esigenze specifiche delle micro, piccole e medie imprese. Inoltre, verranno incentivati i processi di "**CERTIFICAZIONE**" (artt. 42 e 43) o l'acquisizione di "MARCHI" o "BOLLINI" che garantiscano la correttezza e serietà del trattamento. Attesa la complessità degli adempimenti e i potenziali costi di attuazione in capo agli operatori, tali norme sono state pensate per consentire alle c.d. fasce più deboli di conformarsi al Regolamento adottando il Codice di Condotta (art. 40, comma 1 "*Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese*"; l'eventuale adozione di un Codice di Condotta e la certificazione (entrambe le misure sono su base volontaria) comportano una sorta di "presunta conformità al Regolamento" che potrà essere comunque valutata nel merito (sulla scorta dell'esame, da parte del Giudice penale, del M.O.G.C. *ex* 231/2001). Infatti, l'adozione di un Codice di Condotta e/o la Certificazione sono tra gli elementi di valutazione al momento in cui si configura la comminazione di una sanzione amministrativa pecuniaria.

s) Saranno previste regole stringenti in caso di "**TRASFERIMENTO ALL'ESTERO DEI DATI**" (Capo V, artt. 44 – 50) , al fine di valutare se il paese di destinazione dei dati fornisce adeguate garanzie in termini di protezione dei dati.

t) Verrà introdotto il principio del "**ONE-STOP-SHOP**", cioè la possibilità per i cittadini europei di rivolgersi ad una sola delle Autorità Garanti per la protezione dei dati, in caso di violazioni da parte di imprese multinazionali.

u) Vengono sanciti i seguenti ulteriori diritti:
- diritto di proporre **RECLAMO ALL'AUTORITÀ DI CONTROLLO** (art. 77);
- diritto a un **RICORSO CONTRO L'AUTORITÀ DI CONTROLLO** (art. 78);
- diritto a un **RICORSO CONTRO IL TITOLARE DEL TRATTAMENTO O IL RESPONSABILE DEL TRATTAMENTO** (art. 79);
- diritto al **RISARCIMENTO e RESPONSABILITA'** (art. 82, chiunque subisca un danno materiale o immateriale cagionato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento. Il titolare del trattamento o il responsabile del

trattamento è esonerato dalla responsabilità, se dimostra che l'evento dannoso **non gli è in alcun modo imputabile** –> (viene introdotto un principio simile a quello proposto dal D.Lgs. 231/2001).
Il responsabile del trattamento può essere chiamato a rispondere solo per il danno causato a seguito del mancato adempimento degli obblighi diretti ai responsabili del trattamento (ecco che, quindi, diventa molto importante il contenuto del contratto *ex* art. 28, paragrafo 3).

v) Vengono introdotte **SANZIONI AMMINISTRATIVE PECUNIARIE** (art. 83), in funzione delle circostanze di ogni singolo caso, **effettive**, **proporzionate** e **dissuasive**; le nuove sanzioni sono molto più pesanti rispetto al passato.
In particolare, potranno essere irrogate sanzioni amministrative pecuniarie fino a 10.000.000 (dieci milioni) di EURO o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore nel caso delle infrazioni di cui all'articolo 83, paragrafo 4), lettere a), b) e c); sanzioni amministrative pecuniarie fino a 20.000.000 (venti milioni) di EURO o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore nel caso delle infrazioni di cui all'articolo 83, paragrafo 5), lettere a), b), c), d) ed e).
E' espressamente vietato il cumulo materiale delle sanzioni amministrative (art. 83, paragrafo 3) nel caso in cui vengano violate varie disposizione del regolamento, con comminazione dell'importo più elevato tra le sanzioni amministrative pecuniarie.

w) Gli Stati membri possono stabilire (art. 84) "*le norme relative alla altre sanzioni per le violazioni del presente regolamento in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 83, e adottano tutti i provvedimenti necessari per assicurarne l'applicazione. Tali sanzioni devono essere effettive, proporzionate e dissuasive*".
Non ci sono indicazioni in merito a sanzioni di tipo "penale".

x) Nel Capo IX (Disposizioni relative a specifiche situazioni di trattamento - artt. 85 – 91) il regolamento disciplina alcune fattispecie settoriali, tra cui il trattamento e libertà d'espressione e di informazione, il trattamento e accesso del pubblico ai documenti ufficiali (da non confondere con il diritto di accesso dell'interessato *ex* art. 15), il trattamento dei dati nell'ambito dei rapporti di lavoro, norme di protezione dei dati vigenti presso chiese e associazioni religiose.

y) Il nuovo Regolamento entrerà in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea. Esso si applicherà a decorrere da due anni da tale data (**25 maggio 2018**). Da questa data, verrà abrogata la vecchia direttiva 95/46/CE. Il nuovo regolamento sarà obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

z) Bisognerà valutare come verrà gestita la fase di transizione per capire quali, dei tanti provvedimenti attualmente in vigore, rimarranno tali ("Cookie Law",

videosorveglianza, amministratori di sistema, spam, outsourcer, etc…). Il c.d. "Gruppo dei 29" ha già adottato, in data 13 dicembre 2016, le: **1**) Linee Guida sui Responsabili della protezione dei dati (RPD) e **2**) Linee Guida sul diritto alla "portabilità dei dati"; il Gruppo sta lavorando proprio alla gestione della fase di transizione e si attendono dall'Autorità Garante chiarimenti sugli adempimenti da adottare in questa fase.

CONCLUSIONI SINTETICHE

A parere di chi scrive, il Regolamento 2016/679 costituisce l'occasione per una riflessione sistematica sulla filosofia, prima ancora che sulla disciplina della materia, ad oltre vent'anni dalla adozione della normativa base contenuta nella Direttiva 95/46.

La prima riflessione pare soltanto teorica, ma può avere una grande valenza pratico-applicativa: come si evince sin dal titolo del Regolamento, la tutela dei dati personali è emanazione della tutela delle persone fisiche.

La permanenza di una simile prospettiva appare irrinunciabile, specie ove l'ambito in cui si colloca la disciplina è sempre quello del dato personale come "**bene**" destinato alla "libera circolazione", in un'ottica di scambio di mercato senza barriere, tanto più irrinunciabile in termini di concorrenza sovranazionale e di competizione tra ordinamenti sul punto.

In altre parole, il Legislatore Europeo resta saldamente ancorato all'idea dell'ineluttabile circolazione dei dati, che può avere esclusivamente un meccanismo di contrappesi, cui il sistema delle regole in materia è destinato.

In definitiva, nulla muta nel modello binomico "**circolazione/protezione**" dei dati e, d'altro canto non ci si sarebbe potuti attendere niente di diverso, specie in occasione di una disciplina regolamentare.

Si può sicuramente affermare che il Regolamento in esame è il più avanzato ***point of balance*** in argomento, anche se non ha mancato di far segnare crepe e, in certi casi, veri e propri buchi di protezione o, comunque, sbilanciamenti a favore dell'acquisizione/circolazione dei dati rispetto alle prerogative dei soggetti interessati e "potenzialmente" protetti.

Ciò non fosse altro per le crescenti e ricorrenti "emergenze" in cui il bilanciamento finisce per aver luogo.

Ovvio, pertanto, che la ricostruzione secondo cui la circolazione è la regola, l'inaccessibilità dei dati l'eccezione, accompagnato dalla tesi della ***protection/security***, rischia di diventare inefficiente per definizione, atteso che il suo funzionamento fisiologico necessita di interventi equilibrati da un lato e dall'altro, incompatibili con il fiato corto di legislatori sempre più alle prese, invece, con interventi indifferibili, straordinari ed urgenti.
In sostanza, il Regolamento appare ispirato a realismo, ciò sia perché una simile fonte non può e non deve affrontare le scelte di fondo, che invece competono al legislatore delle direttive e sia perché, comunque, sub specie di innovazioni regolamentari, non si smarrisce l'occasione per talune sintomatiche precisazioni di disciplina ed evidenti adeguamenti del testo normativo sia alla giurisprudenza della Corte di Giustizia sia all'evoluzione tecnologica.
E' evidente l'intreccio tra regola giuridica e codice tecnologico (art. 25) che appalesa il nuovo rapporto che si viene ad instaurare tra i dispositivi della tecnica e la tutela della libertà individuale.
Tale relazione si fa inevitabilmente più stretta nella nostra società, definita anche "**società del rischio**"(Beck) e "**società dell'incertezza**" (Baumann), in cui il diritto e la tecnica possono reciprocamente avvalorarsi oppure divaricarsi in forte tensioni.
La scienza e la tecnica, non più chiuse in torri d'avorio come in passato, sono anzi chiamate a concorrere alla stessa effettività dei diritti che si esercitano nel loro campo e anche per tale ragione divengono materia di pubblico scrutinio; esse dunque rivestono materialmente una indubbia funzione politica, la cui esplicazione è massima in materia di protezione dei dati personali.
Ciò emerge in modo palese nella previsione che affida alla componente tecnologica, in dialogo con la regola giuridica, il presidio della libertà individuale e la tutela dei diritti della persona. Se, infatti, con la tutela apprestata attraverso il c.d. **diritto all'oblio** viene riconosciuto in capo al singolo individuo (art. 17) l'interesse a rimuovere **EX POST** informazioni personali a lui riferite, ma la cui diffusione o reperibilità attraverso i sistemi informativi, per legittime (ma sindacabili) motivazioni non siano più desiderate e si vogliano "**dimenticate**", per altro verso la protezione dei dati perseguita attraverso obblighi conformativi degli strumenti tecnologici (art. 25) è soprattutto destinata ad operare **EX ANTE** per discernere le sole – e possibilmente non molte – informazioni necessarie e rilevanti sul soggetto interessato.
Sotto questo aspetto, il Regolamento ha il pregio di ricondurre i nodi dello sviluppo tecnologico al centro della discussione pubblica e, in un ambito di così stretta interazione con l'innovazione tecnologica quale è la tutela dei dati personali, di porre basi per un assetto istituzionale in cui l'artefatto tecnologico rivela e mette in pratica le sue proprietà politiche (Pitto).
I professionisti del diritto non possono rimanere latitanti in questa discussione pubblica ma, al contrario, ne devono assumere il giusto ruolo, sia verso l'esterno, come consulenti nei confronti della parti assistite, sia al proprio interno, in relazione agli aspetti organizzativi dello studio e, in particolare, in relazione alla propria immagine professionale.