

**Le nuove frontiere della protezione dei dati
nell'attuale rivoluzione tecnologica:
internet delle cose, blockchain, e-privacy
Workshop 29 marzo 2019 - Roma Università Roma Tre**

*

La legislazione europea: modelli e criticità

Il legislatore europeo, nel disciplinare i vari settori economici, ha da sempre operato una scelte di politica legislativa con un obiettivo minimo ovvero quello di evitare e/o limitare distorsioni del mercato.

La legislazione UE non ha carattere sistematico, non ha alla base delle chiare scelte di politica – economica ma solo l'obiettivo di indirizzare e regolare l'andamento del mercato verso la libera concorrenza.

Con l'avvento delle nuove tecnologie, che stanno avendo sul mercato un effetto disruptive, nasce l'esigenza forte di protezione e tutela delle persone sia in termini socio – economici ed anche e soprattutto in relazione ai dati personali.

La esigenza di tutela in relazione ai dati trova il proprio fondamento nel gap tra i grandi players del mercato, in particolar modo tecnologico, ed il cittadino-consumatore che risulta chiaramente in posizione di debolezza e quasi di subordinazione se non oggetto di vera mercificazione, atteso il grande valore economico dei dati personali per i detti players.

Alla luce della presa d'atto dell'esistenza di un soggetto evidentemente debole, nel tentativo di ridurre il gap o quanto limitare gli effetti negativi dello stesso, va individuato un primo pilastro del sistema di tutele nella indefettibile necessità di una alfabetizzazione tecnologica-informatica del cittadino-consumatore.

Vi è una enorme carenza di comprensione da parte dei cittadini-utenti delle gravi implicazioni, connesse a scelte “leggere”, nel rapporto con i soggetti che dominano il mercato in particolare nel mondo delle nuove tecnologie.

Vi deve essere una formazione informatico-tecnologica di base.

Nelle scuole dovrebbe essere creato un percorso formativo sistematico di base atteso che i millennials, pur essendo nativi digitali nell'utilizzo, sono passivi e leggeri nel valutare gli effetti connessi alla cessione dei propri dati personali in cambio della fornitura di molteplici servizi apparentemente gratuiti.

Il secondo pilastro del sistema delle tutele riguarda l'attività di normazione del legislatore europeo e del singolo stato.

La tecnologia cresce in modo esponenziale e quindi vi è un problema di attualità della regolazione e di grave difficoltà nella attività de jure condendo.

La legislazione UE, storicamente, parte da modelli di creazione delle norme vecchi ed inadatti.

La UE lascia al mercato il compito di autoregolarsi ed interviene solo con norme generali, operando per sistemi autonomi – “silos” verticali.

Vi è un pensiero che, ad un attento esame, costituisce un vizio di origine, ovvero che il mercato non sottoposto a normazione si autoregoli sul medio lungo periodo.

A titolo esemplificativo, si deve necessariamente richiamare quanto accaduto con l'avvento di Internet.

Gli ISP che consentivano di connettersi alla rete operavano in una situazione di carenza assoluta di norme.

In ragione di ciò gli ISP sono proliferati senza controllo e, con una consequenzialità logica e tecnologica vi è stato l'ingresso, diventato vero dominio, degli OTT.

Vi è per così dire, nel legislatore UE quasi rassegnazione nella scelta di non regolare il mercato, siamo di fronte ad un vero laissez faire.

La normativa per “silos” è inadeguata ed in tempi recenti è nata tra le imprese l'esigenza di dettare regole – best practices – codici di condotta per essere compliant alle diverse normative settoriali.

Le imprese hanno quindi intrapreso un significativo percorso di autoresponsabilizzazione ed hanno tentato di autoregolarsi.

In questo panorama si può dire forse che il GDPR costituisca un complesso normativo sia innovativo e trasversale, ma anche vecchio (i lavori iniziati nel 2012) e con certezza detta normativa risulta inadeguata, superata e non efficace poiché non tratta e disciplina in alcun modo gli algoritmi che sono alla base delle nuove tecnologie quali la Blockchain, l'IoT (internet delle cose) e l'Artificial Intelligence.

Dati personali: il valore economico e le forme di tutela

E' in atto una rivoluzione industriale stiamo entrando nella cd. Industry 4.0 ed è forte l'esigenza di tutela del cittadino-consumatore perché la rivoluzione informatica-digitale, avente decisamente carattere disruptive, porta con se gravi rischi di una dittatura socio-economica se non politica.

Vi è un primo livello di incontro-rapporto tra utente-cittadino-consumatore ed i grandi players della tecnologia ed è la “vendita-fornitura” di un servizio “gratuito” a fronte della cessione quantomeno disinvolta del dato personale.

Emerge di tutta evidenza che il dato personale per i grandi players abbia un enorme valore (economico), del tutto non percepito, quasi impalpabile per il cittadino consumatore.

Il GDPR detta regole e principi importanti quali la accountability, la minimizzazione nella raccolta di dati e la richiesta alle aziende di modificare i propri processi aziendali per essere compliant al GDPR, che risulta normativa innovativa e dinamica in termini di concreta tutela del cittadino-consumatore.

Vi è però un superiore livello di contatto con i grandi players del mercato nel quale il cittadino consumatore “proprietario-produttore di dati” utilizza la robotica, gli home assistant, la geolocalizzazione, i pagamenti digitali.

Entra in gioco l’internet delle cose con il suo incalcolabile numero di sensori che costituiscono un formidabile collettore di dati personali e tecnici.

Il volume dei dati già imponente gigantesco ed esploderà con l’implementazione della tecnologia 5G trasformando l’IoT (internet of things) in IFT (internet for things) ovvero nell’internet per le cose.

Il numero immenso di dati raccolti apre altresì il campo ai cd BIG DATA che determinano di fatto la nascita di nuovi soggetti tecnico-economici tipo i data brokers, i data scientist e chi svolge attività di profilazione per creare cluster ovvero macro-categorie di utenti consumatori per individuare e dare valore economico al dato personale.

Si può dire che si stia creando una doppia realtà o meglio una dicotomia tra identità personale e digitale.

Questa identità digitale apre spazio a nuovi e gravi rischi per il cittadino-consumatore quali il condizionamento nelle scelte economiche e politiche ed anche una possibile discriminazione e/o esclusione quali una limitazione nell’accesso al credito o problemi di premi in ambito assicurativo.

Sono i BIG DATA (il numero massivo di dati viene trattato con algoritmi estraendone valore economico) che creano il terreno per tecnocrazia, vi è già in atto un oligopolio dei grandi players.

I dati personali nei cd BIG DATA scompaiono e finiscono per così dire in una blackbox (scatola nera) del tutto inaccessibile che non consente più alcun controllo sui dati che sono quasi oggetto di dematerializzazione.

Vi è una dematerializzazione del dato ma una materializzazione di effetti socio-economici e politici derivanti dall’utilizzo di detti dati parte dei players.

Essenziale come già detto è la consapevolezza del cittadino-consumatore al quale magari ex lege viene richiesto il consenso che però può definirsi di nessun rilievo in termini di efficacia della tutela, poiché spesso non vi è affatto consapevolezza delle conseguenze pratiche ed a volte vi è un forte condizionamento nella decisione di prestare il consenso.

Le tutele, di natura eminentemente giuridica (fermo il GDPR), che possono essere approntate hanno caratteristiche molteplici e diversi livelli di efficacia:

tutela anticipatoria

- l’obbligo di inserire icone e questionari per accessi consapevoli a servizi ed ai siti;
- obblighi stringenti di trasparenza a carico delle imprese (ad esempio la Corte UE in merito alla concessione dei mutui richiede una informazione non astratta ma di natura concreta ovvero viene richiesto di illustrare in modo chiaro e trasparente le conseguenze potenzialmente dannose di importanti scelte economiche.

tutela giudiziale

- class action

- inibitoria art 140 Codice del Consumo.

Si è accennato prima al valore economico del dato e non a caso sono nate APP che aiutano ad individuare il valore dei dati personali ceduti gratuitamente in cambio di determinati “gratuiti” servizi.

In modo ardito, alla luce del valore economico sopra-detto, si possono ipotizzare contratti di durata di vendita dei dati nei quali inserire alcune clausole quali quella sul foro competente o prevedere un onere della prova semplificato per il cittadino-utente.

Un importante scelta di politica legislativa sta per essere adottata in California che a breve emanerà una legge che prevederà il pagamento di Royalties per l’utilizzo del dato personale da parte dei soggetti economici del mercato.