Privacy, qual è il valore reale del dato personale?

Negli ultimi decenni il contesto socio-culturale è cambiato profondamente, modificando anche le modalità di comunicazione degli individui. Tale cambiamento ha avuto un profondo impatto anche sul rapporto esistente tra individuo e norma giuridica, soprattutto riguardo alla tutela della persona. Sono numerosi gli interventi legislativi che hanno dovuto modificare norme giuridiche o crearne nuove per adattarsi alla realtà virtuale del web.

In effetti, da un lato è noto che la diffusione di Internet e delle piattaforme di social networking abbiano inciso favorendo la possibilità di interazione tra gli individui; dall'altro, l'evoluzione tecnologica, soprattutto attraverso smartphone e tablet, ha favorito detta interazione in mobilità non essendo più necessario un computer.

Ciò ha determinato un mutamento delle modalità di comunicazione, che non è più solo verbale (nelle sue ampie accezioni) o scritta ma anche basata su immagini e contenuti multimediali, con un conseguente impatto sul comportamento delle persone nella loro quotidianità.

L'essere umano ha bisogno di comunicare (primo assioma della Scuola di **Palo Alto**)[1] e il vantaggio offerto da Internet di poter interagire con altre persone anche a distanza ha avuto successo. Del resto, sono numerosi i contributi divulgativi e scientifici che hanno descritto questa evoluzione (o involuzione, a seconda del punto di vista) di carattere sociale, che può avere indubbi riflessi di natura giuridico-legale.

Va riconosciuto che la “nuova” modalità di comunicazione per certi versi costituisce un miglioramento in termini puramente sociali. Tuttavia, se si registra un vantaggio sociale della “nuova” comunicazione non può dirsi altrettanto per il contesto culturale che, molto spesso, denota, purtroppo, una involuzione.

La “nuova” modalità di comunicazione, paradossalmente, favorisce in maniera esponenziale la comunicazione tra gli individui, e la velocità di interazione ha fatto scaturire la consuetudine (divenuta ormai il modello) della celere (e comoda) consultazione dei contenuti presenti sul web (senza alcun discernimento delle fonti) anche con finalità, purtroppo, di apprendimento. In effetti, le fonti consultabili (non sempre corrette) sono fondamentalmente sul web e i contenuti sono poco articolati perché devono risultare facilmente leggibili e in breve tempo.

Accedere (comodamente e rapidamente) alle fonti presenti sul web consente di realizzare in maniera distorta il processo di autoformazione (o apprendimento autodiretto o autoapprendimento – *self learning*) in quanto “*la criticità nel tema dell’autoapprendimento è legata al fatto che per auto-apprendere, le persone devono avere una specifica competenza sul come sia possibile auto-apprendere*” e, quindi “*c’è bisogno di sviluppare una competenza ad auto-apprendere che non può essere data per scontata*“[2]. Il processo di autoapprendimento generalizzato può determinare un abbassamento del livello culturale.

In sostanza, l’esigenza di una comunicazione sempre più veloce molto spesso richiede altrettanta celerità nella acquisizione di nozioni e nell’accrescimento del profilo culturale che, invece, può subire un decremento sia in ragione della moltitudine di fonti presenti sul web alle quali si accede senza selezionare quelle certe e accreditate sia riguardo alla necessaria competenza per auto-apprendere.

La nostra vita quotidiana è incentrata sulla comunicazione e sull'imprescindibile utilizzo degli strumenti necessari alla esecuzione della stessa. Le 24 ore (anche quelle notturne) sono quasi completamente impegnate dall'utilizzo di device (computer, tablet, smartphone) fondamentalmente per comunicazioni di natura lavorativa o personale.

Le app più note consentono una comunicazione multimediale che non si limita alla sola scrittura di testo, ma include anche la trasmissione di contenuti quali immagini, video o messaggi vocali. Gli utenti, però, scelgono le app seguendo il criterio della loro maggiore diffusione (spesso per moda o per essere parte di un gruppo) invece di prestare attenzione alla protezione delle informazioni che vengono veicolate. Paradossalmente, gli utenti preferiscono continuare ad utilizzare app potenzialmente meno sicure ma molto diffuse invece che riflettere sulle conseguenze dei rischi connessi alla sicurezza dei dati. A fronte dell'invito rivolto alle persone di riflettere sui potenziali rischi di sicurezza, si sente rispondere che quella o quelle app sono le più utilizzate; prevale, quindi, il criterio (imprudente?) delle scelte operate dalla maggioranza degli utenti (inconsapevoli). È altrettanto vero che gli sviluppatori hanno l'obbligo di rispettare le norme sulla protezione dei dati personali e in particolare il principio sancito dall'art. 25 del **GDPR** sulla "protezione dei dati fin dalla progettazione e protezione per impostazione predefinita" (**Data Protection by Design** and **by Default**).

Del resto, le scelte degli utenti sono al contempo indirizzate verso app che si assumono poter essere utilizzate gratuitamente senza alcuna riflessione sul reale costo da pagare che, quasi sempre, corrisponde ai dati degli utilizzatori (dati personali, indirizzi IP, data e ora di accesso e di utilizzo, metadati, ecc.). La smania di accedere a determinati servizi o di utilizzare le app prevale sul minimo buon senso che viene ampiamente prevaricato sia dalla

accettazione incondizionata delle condizioni generali e delle privacy policy (quasi sempre non lette) sia dal disinteresse per i rischi, anche minimi, connessi alla sicurezza delle informazioni (valutabili con tre banali domande: “A chi e dove invio i miei dati, da chi essi saranno trattati e dove gli stessi saranno salvati”?).

Molti utenti trasmettono messaggi vocali senza riflettere affatto sui rischi a cui potrebbero andare incontro nel caso in cui venisse acquisito da terzi il campionamento vocale, alterato e utilizzato per fini impropri.

Quale dato più personale della propria voce? Tuttavia, l’irrefrenabile desiderio di attestare la propria presenza (sulla rete o comunque mediante app) prevale sulla sicurezza per i propri dati personali e quelli delle altre persone.

In conclusione, al di là delle esigenze di comunicazione, emerge anche un desiderio, tipico dell’essere umano, che è quello dell’esibirsi e dell’apparire[3].

Essere o apparire: il tema è ovviamente antico e non si scopre l’acqua calda.

Comportamento e fattore umano

Abbiamo assistito, nel corso degli ultimi anni, alla proliferazione delle piattaforme di comunicazione sul web, dai forum ai social network.

È profondamente cambiato lo stile di vita (*lifestyle*) delle persone, sia in ambiente lavorativo sia in ambito privato.

Le persone, a volte anche consapevolmente, nel corso degli anni hanno alimentato – e continuano a farlo – le piattaforme di comunicazione con quantità enorme di dati, anche personali. È immaginabile quanto sia vertiginoso l’aumento della quantità di dati da parte dei provider delle piattaforme.

Il numero di utenti della rete (quasi 4 miliardi e mezzo e cioè oltre il 50% della popolazione mondiale) consente di immaginare facilmente la enorme quantità di dati che vengono quotidianamente trasmessi (sms, app e sistemi di messaggistica, **Whatsapp, iMessage, Facebook, LinkedIn, Twitter**, pagine web, ecc.) e numerose sono le piattaforme da cui è possibile, anche solo indicativamente, avere idea del traffico di dati trasmessi (secondo Cisco[4] in un secondo il traffico di rete è di circa 24.000 GB e in un mese di 91,3 EB, oltre 98 bilioni di GB).

A ciò si aggiunga che l'evoluzione tecnologica ha consentito lo sviluppo di sistemi intelligenti, basati sulla **Intelligenza Artificiale** e sul **Machine Learning**, attraverso i quali è possibile ottenere risultati di analisi anche di grandi quantità di dati (Big Data) trasmessi dai singoli utenti, oltre ai cosiddetti metadati (informazioni aggiuntive rispetto al contenuto trasmesso, quali – ad esempio – indirizzo IP, data e ora, dati EXIF per le immagini, URL, HTTP GET, pagine web, file, email, transazioni con carte, ecc.).

Lo scenario descritto – sebbene sintetico e non esaustivo – illustra come, al di là dell'utilizzo di sistemi di mascheramento di alcune informazioni, la maggior parte dei dati che transitano sulla rete risultano identificabili.

Peraltro, la libertà di pubblicare contenuti sulla rete non trova il corrispondente opposto nella volontà dell'individuo di poter cancellare i medesimi contenuti quando si vuole, in ragione della possibile indiscriminata diffusione degli stessi contenuti su internet. In sostanza, una volta pubblicato un contenuto (che sia un like, un post, un'immagine, un articolo, o qualunque altra risorsa) non si ha la certezza che esso possa essere rimosso come se non fosse mai stato pubblicato.

Il fattore umano suscita sempre particolare attenzione, sia in ambito sociale per l'analisi dei comportamenti sia in ambito più tecnico per la valutazione dei rischi relativi alla

sicurezza in generale. I comportamenti umani possono essere prevedibili e condizionabili ma resta sempre l'incognita della mente umana che appartiene all'imponderabile; una persona può porre in essere azioni o omissioni che sono il risultato della sua capacità di autodeterminazione, tanto da potersi discostare dalle proprie comuni abitudini o consuetudini. In sostanza, il fattore umano, considerato sia sul piano del comportamento sia sul piano dei rischi per la sicurezza, potrebbe avere conseguenze dirompenti in ragione di decisioni imponderabili.

I contenuti pubblicati online, anche su piattaforme ad accesso riservato, non escludono il rischio consistente nell'utilizzo non autorizzato, e quindi abusivo, di determinate informazioni personali (a volte anche sensibili) appartenenti all'interessato.

Ogni contenuto generalmente lascia la sua traccia indelebile sulla rete.

Il 12 luglio 2019 è stato pubblicato sul sito del Comitato europeo per la protezione dei dati (**EDPB**) il documento dal titolo "*Guidelines 3/2019 on processing of personal data through video devices*"[5], in consultazione pubblica sino al 6 settembre 2019.

Il predetto documento si riferisce al trattamento dei dati personali effettuato tramite dispositivi video; nel paragrafo 1 della sezione 'Introduzione' si legge che l'uso intensivo di dispositivi video ha un impatto sul comportamento dei cittadini e le implicazioni sulla protezione dei dati sono enormi (*The intensive use of video devices has an impact on citizen's behaviour. … Data protection implications are massive*.).

Si legge, inoltre, che sussiste un rischio potenziale, consistente nell'abuso dei dati acquisiti dalle videocamere, che è direttamente proporzionale alla dimensione dello spazio

monitorato e al numero di persone che frequentano detto spazio. L'EDPB evidenzia correttamente il "**comportamento**" dei cittadini quale conseguenza dell'utilizzo di sistemi video, ove il presupposto ("*behaviour*") è connesso all'impatto delle tecnologie sulla privacy e sui dati personali.

Del resto, il comportamento è stato già oggetto di attenzione in relazione al fenomeno "*behavioural advertising*" (pubblicità comportamentale), con alto rischio di profilazione.

Si tratta di un provvedimento sul tema della video sorveglianza ove le preoccupazioni sono focalizzate sull'uso improprio dei dati anche mediante tecniche di analisi video intelligenti; non vi è dubbio che queste linee guida avranno effetti anche in ambito nazionale, con impatto sui provvedimenti già adottati in materia dal Garante.

Emerge dal citato provvedimento dell'EDPS l'importanza del comportamento, il "*behaviour*" che è imprevedibile, comunque strettamente connesso alla personalità di ciascun essere umano, e potrebbe trasformarsi in una potenziale fonte di rischio.

La smania dell'apparire, che pervade l'essere umano, costituisce lo spunto motivazionale che potrebbe indurre le persone a pubblicare i più disparati contenuti nell'ottica della massima libertà di espressione. In questo modo si contribuisce ad alimentare il "contenitore" di dati di ciascun provider ma soprattutto dei fornitori di social network.

Se da una parte si possono registrare soggetti "più attivi" socialmente, dediti alla pubblicazione smodata di informazioni, dall'altro non si può escludere l'abusivo utilizzo di informazioni appartenenti ad alcuni individui da parte di soggetti che potrebbero diffonderle.

Com'è evidente sussistono rischi per i dati personali. E allora, che fare?

Consapevolezza ed etica

Oggigiorno c'è l'esigenza di parlare di etica per consentire un approccio corretto alla dignità umana così come è necessario che si lavori per consolidare e accrescere una vera consapevolezza del valore della persona e dell'intera sfera di ciascun individuo.

La prevalenza dell'apparire rispetto all'essere si esplica *in toto* nel comportamento umano, senza possibilità di essere contenuta o mitigata con rimedi preventivi e specifici. Le sanzioni (successive al fatto) hanno un mero significato punitivo di un comportamento contrario alle norme dell'ordinamento giuridico.

Una adeguata consapevolezza e un approccio etico riguardo a ciò che si sta compiendo e soprattutto alle conseguenze che ne possono derivare potrebbero però costituire un valido strumento preventivo per ridurre il rischio in capo a ciascun soggetto per sé e per gli altri. Consapevolezza ed etica non costituiscono decisamente "la soluzione", ma componenti del processo sulla protezione dei dati personali.

In un'epoca come quella attuale, in cui si assiste al vertiginoso sviluppo delle innovazioni tecnologiche e alla conseguente incidenza sulla digital economy, il focus va ricercato nella reale consapevolezza del valore attribuito al dato personale e in una attenta e corretta analisi di ciò che accade nel resto del mondo in questa materia.

Molto spesso la voglia di apparire prevale sulla consapevolezza in quanto l'attuale società è del tutto condizionata dall'utilizzo delle tecnologie nonché dalla smania di confermare la propria presenza in numerosi contesti digitali. Anche un solo like attesta una presenza, un "ci sono".

Tutto ciò non deve però demotivare dalla diffusione della

cultura della consapevolezza e dell'etica, entrambe finalizzate a sensibilizzare gli utenti sulla importanza e sul rilievo che assumo i dati personali.

Il trattamento dei dati personali

Ulteriore riflessione è quella relativa alla "gestione", al trattamento dei dati che vengono forniti alle numerose piattaforme che ne sono responsabili.

Fino a qualche tempo fa gli utenti "si fidavano" (quasi ciecamente) dei social network provider riguardo al rispetto delle leggi vigenti in materia di protezione dei dati personali.

Tuttavia, il noto caso "*Cambridge Analytica*" ha dimostrato quanto sia debole il sistema basato sul "trust" e sulla accettazione e approvazione (unilaterale?) incondizionata delle privacy policy proposte (in questo caso da Facebook, titolare del trattamento). Il social network provider ha l'obbligo di rispettare le norme in materia di protezione dei dati personali e i singoli utenti.

Non è questa la sede opportuna per approfondire i dettagli del caso "*Cambridge Analytica*" ma appare evidente che le informazioni personali (a volte sensibili) di soggetti presenti su Facebook sono state utilizzate senza il loro consenso per finalità di analisi e condizionamento delle loro scelte per il raggiungimento di altri risultati diversi dalle finalità del titolare del trattamento.

Se non si considera l'alto valore dei dati personali, si corre il rischio di favorire – in un'ottica pericolosamente e apparentemente legittima ma del tutto illecita – la mercificazione delle informazioni personali anche corrispettivo per eventuali servizi forniti anche mediante l'utilizzo di applicazioni.

Il fenomeno già noto in passato, tanto che ha ricevuto adeguata attenzione da parte dell'EDPS, sta serpeggiando e tornando in auge. Sono addirittura sorti i *data broker*[6] per l'acquisto di set di dati.

È evidente che un simile fenomeno è inaccettabile, oltre che essere illecito in ragione delle norme vigenti, soprattutto perché comporta lo svilimento dell'alto valore proprio dei dati personali come si è illustrato.

Le ricerche dimostrano anche un altro aspetto di rilievo: è emerso che l'utilizzo dei social network attesti un alto livello di analfabetismo funzionale[7] in quanto la "*partecipazione non è andata di pari passo con un miglioramento delle capacità di comprensione del testo, nel senso di interpretarlo, di saper leggere fra le righe elaborando delle conclusioni proprie*".

Si tratta di uno scenario sconcertante che contribuisce ad aumentare le preoccupazioni circa la assoluta mancanza di consapevolezza sia sul valore del dato personale sia sugli effetti della pubblicazione e propagazione dei contenuti sui social network.

Quale **etica** alla base di un simile comportamento ?

Quanta **consapevolezza** da parte degli utenti ?

Per entrambe le domande, le risposte possono essere molto semplici, posto che il tutto si è basato (ma tuttora è lo stesso) sulla totale o parziale assenza di consapevolezza e comunque mancanza di etica.

Digital economy, e-Democracy e dati personali

I più grandi player a livello globale da tempo sanno che il vero capitale è costituito dai dati personali.

D’altra parte accade, invece, di rado che le persone effettuino scelte etiche consapevoli quando agiscono anche solo come utenti nel “sistema” delle piattaforme digitali.

Ogni azione, che sia un like, un post o una condivisione, sarà fagocitata dagli algoritmi basati sulla IA e fornirà ai provider precise indicazioni sul comportamento degli utenti: si tratta della c.d. *Big Data Analytics*.

Ciò consente ai provider di orientare le proprie scelte a seconda del comportamento degli utenti.

L’apparente libertà di espressione si tramuta in un vero e proprio condizionamento globale governato da chi ha il controllo dei potenti algoritmi di IA, che finisce per esplicarsi in una profilazione globale basata sul comportamento degli utenti sottoposti al monitoring delle proprie scelte.

Consapevolezza, allora, significa conoscere la realtà, apprendere e sapere quali sono le conseguenze di ogni comportamento per poi decidere se essere parte del “sistema” e in che modo.

È ovvio che da qualsiasi analisi di grandi quantità di dati si possono estrarre risultati di ogni tipo, non esclusi quelli su singoli profili.

Uno dei rischi maggiori è quello di perdere il pieno controllo delle proprie informazioni dopo averle pubblicate, qualora esse siano state oggetto di condivisione e replicate altrove.

I dati personali, pertanto, governano la *digital economy* e possono essere utilizzati per influenzare le scelte.

Il panorama così osservato e descritto, ricomprende, inoltre, ipotesi di gravi conseguenze anche riguardo ai rischi per un distorto esercizio della democrazia.

L’attuale contesto è evidentemente votato, ad una democrazia

digitale – *e-Democracy* – nella sua più ampia accezione, realizzata mediante l'utilizzo sempre più massiccio delle tecnologie.

Il tema è particolarmente delicato e merita il rinvio ad altra sede per gli opportuni approfondimenti.

L'utilizzo delle tecnologie costituisce un indubbio vantaggio anche in democrazia nelle diverse accezioni in cui si esplica, tra le quali, e-Government, e-Governance, e-Participation, e-Inclusion, e-Procurement. In questo generale contesto, però, l'uso incondizionato delle tecnologie può comportare rischi per la sicurezza e per i diritti fondamentali degli individui, tra cui quello alla protezione dei dati personali.

Il quadro diviene più nitido se si considera il fenomeno delle *fake-news*, a volte frutto di attività realizzate in laboratorio mediante la manipolazione di video con l'aggiunta di una base vocale diversa da quella originaria, ovvero attraverso l'utilizzo di un profilo digitale non ufficiale ma identico a quello, la manipolazione delle informazioni, ecc.

Le incertezze sulla impossibilità di avere pieno e sicuro controllo delle tecnologie e delle fonti di informazione ufficiali potrebbe costituire un rischio per la democrazia digitale. Se questi rischi, poi, sono connessi a dati personali è immaginabile come sia elevato il livello di preoccupazione.

Norme giuridiche e visione globale

Il **GDPR** è una pietra miliare in materia di protezione dei dati personali in quanto trasforma radicalmente il relativo sistema, comportando un profondo rinnovamento scientifico e culturale, attuabile modificando l'approccio a questa materia.

Tuttavia, a distanza di oltre un anno dalla sua applicazione, sembra opportuno guardare anche al di fuori dell'Europa per

avere una visione completa della incidenza delle tecnologie sui dati personali e sulla privacy. Non si può prescindere dalla osservazione di quanto accade al di fuori del perimetro nazionale o europeo in questa materia.

Infatti, prima di approfondire specifiche tematiche in materia di protezione dei dati personali e privacy, è necessario avere preventivamente chiari gli scenari europei e quelli dei principali Paesi del mondo, mediante un'efficace e corretta analisi di carattere generale. In un mondo globalizzato e decisamente condizionato dall'uso di Internet e delle tecnologie non è più possibile occuparsi di questi temi unicamente soffermandosi all'interno dei propri confini nazionali o europei.

Il GDPR, sappiamo, è applicabile – in presenza di specifiche condizioni – anche a soggetti che sono fuori dall'Unione, i quali, spesso, hanno approcci diversi alla protezione dei dati personali e alla privacy. In un sistema globale ove le tecnologie direttamente e indirettamente incidono sulla vita privata di ogni persona, non si può prescindere da valutazioni che – sebbene generali – riguardano anche altri sistemi giuridici.

L'analisi di altre realtà, dove possono essere utilizzati istituti giuridici diversi da quelli che conosciamo o ruoli non utilizzati nei nostri sistemi (es. *Data Custodian* in Canada), consente di avere un quadro più ampio e chiaro per poter affrontare correttamente e con le necessarie competenze le singole questioni. Esiste una matrice comune che riguarda privacy e protezione dei dati personali, ma gli approcci possono essere differenti a seconda del contesto territoriale.

È noto che negli USA e in Canada questa materia sia descritta come "*Data privacy and protection*", quasi come se tale approccio esprimesse la primazia della privacy rispetto alla protezione dei dati personali. Ciò induce a considerare la privacy e la protezione dei dati personali in termini globali

senza considerare confini, possibilmente con un comune standard privacy framework, così come descritto nel contributo dal titolo "***Privacy and Security in the Internet of Things***" pubblicato nel 2013 su *Cutter IT Journal*[8] (Vol. 26, No. 8 August 2013).

In Europa abbiamo il privilegio di fare riferimento ai diritti fondamentali contenuti nella Carta dei Diritti Fondamentali dell'Unione Europea.

Tuttavia nel confronto con soggetti di altri continenti potrebbe risultare complesso discutere, a livello generale, del valore del dato personale con riferimento a principi codificati nella legislazione europea.

La protezione dei dati personali in Europa è un diritto fondamentale, ma l'assenza di normativa che attribuisca dignità alla privacy (il riferimento è a-tecnico e esteso anche alla protezione dei dati personali) non vuol dire poter ignorare o ridimensionare la portata.

Una valutazione che faccia riferimento alla persona e alla dignità umana porterebbe inevitabilmente ad attribuire un valore elevato e nobile al dato personale per il solo fatto che esso appartiene a una persona ed è intrinsecamente connesso ad essa. Infatti, la qualifica di valore assoluto deriva proprio dalla natura delle informazioni strettamente appartenenti a una persona fisica.

Con il termine valore, in questo caso, si intende affermare una qualità di particolare pregio che contraddistingue le informazioni personali poiché esse sono strettamente connesse alla persona e ne costituiscono il suo elemento ontologico. La vita al contempo è e ha un valore in senso assoluto, così come tutto ciò che appartiene ad una persona; per questo il regime di appartenenza alla persona consente a ciascun elemento ad essa afferente di acquisire lo stesso valore, pregio e condizione e, quindi, merita identico trattamento.

Questo approccio non è strettamente correlato alla normativa e all'ordinamento giuridico ma, più in generale, all'utilizzo di un criterio che si basi su consapevolezza ed etica andando ben oltre l'impianto del diritto.

Allo stesso modo, il lavoro per la realizzazione di standard tecnici di portata internazionale (tra i molti, "*Ontological Standard for Ethically Driven Robotics and Automation Systems*[9]" che mi vede direttamente coinvolto) molto spesso comporta delle difficoltà per la corretta applicabilità delle relative norme in Paesi dove alcuni concetti possono essere diversi o inesistenti.

Tutto quanto precede è necessario per ancorare un concetto che si ritiene essere basilare. Si discute di protezione dei dati personali e privacy solo e unicamente in quanto esistono norme *ad hoc*, diversamente non ci si porrebbe il problema di soffermarsi sulla essenza e sul rilievo dei dati personali.

La disciplina giuridica certamente costituisce l'elemento principale da considerare per valutare il rispetto delle regole in materia di protezione dei dati personali.

Pertanto, il processo logico e metodologico che viene adottato è quello della tutela o protezione dei dati personali, procedendo dall'elemento principale costituito dalle norme esistenti. Il riferimento immediato, infatti, è costituito dalle norme vigenti al fine di interpretarle per affrontare le singole fattispecie.

Non si può trascurare, però, che il dato personale debba essere considerato come valore in senso assoluto, anche attraverso un approccio etico e comunque prescindendo da qualsiasi norma.

L'analisi e la valutazione di una fattispecie in materia di privacy e protezione dei dati personali, oggigiorno, non possono essere affrontate basandosi – correttamente peraltro – unicamente sul dato normativo alla ricerca di una soluzione;

è, invece, necessaria una preventiva valutazione della fattispecie procedendo con un criterio che si basi su consapevolezza ed etica, aspetti che si collocano su un livello superiore rispetto a quello normativo.

Del resto, avere un previo e chiaro scenario internazionale su un aspetto specifico afferente privacy e protezione dei dati personali, consente di poter affrontare le relative questioni con consapevolezza. In uno Stato in cui non esiste una normativa in materia di protezione dei dati personali, infatti, qualora non si procedesse dalla consapevolezza e dall'etica considerando il dato personale un valore, verrebbe consentita qualunque azione fondamentalmente in pregiudizio della persona.

L'approccio descritto – che considera quale "**prerequisito**" il criterio preventivo basato sul principio secondo il quale il dato personale è un valore assoluto e richiede consapevolezza ed etica – è il vero e reale punto di partenza, non codificato, che si pone come elemento ultragiuridico.

Infatti, la normativa in materia di protezione dei dati personali esiste proprio perché vanno tutelate le informazioni appartenenti ad una persona, nel pieno rispetto della dignità umana.

In questo modo, con il criterio proposto, ci si posiziona ad un livello antecedente a quello delle norme giuridiche risultando lo ***starting-point***.

Il "**livello zero**", vero punto di partenza, è la considerazione anche etica dell'alto valore attribuibile al dato personale; senza questo assunto difficilmente si può avere un idoneo approccio alla normativa. Il "**livello uno**" sarà quello delle norme giuridiche.

In conclusione, consapevolezza ed etica senza prescindere dalle norme, possono condurre a risultati più efficaci: è una sfida.

[1] Secondo la Scuola di Palo Alto, il cui maggior esponente fu Paul Watzlawick, si distinguono 5 assiomi: 1. Non si può non comunicare; 2. All'interno di ogni comunicazione si possono individuare due livelli (contenuto "notizia o informazione" e relazione "comando"); 3. Il flusso comunicativo è espresso secondo la punteggiatura degli eventi; 4. La comunicazione avviene attraverso i canali verbali (digitale) e non verbali (analogica); 5. Gli scambi di comunicazione sono simmetrici o complementari, a seconda che siano basati sull'uguaglianza o sulla differenza. Tra i numerosi contributi, Alessandro Ferrari, "*I 5 assiomi della comunicazione umana*".

[2] Autoformazione o autoapprendimento, *Intervista Franco Bochicchio dell'Università del Salento.*

[3] *È vero che quella di oggi è la società dell'apparire, che è una società edonistica, che è una società che fa la fortuna dei chirurghi plastici, giacché tutti vogliono essere perfetti, tutti vogliono sembrare belli.* – "La società dell'apparire: intervista al sociologo Francesco Pira".

[4] https://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html#~complete-forecast

[5] Guidelines 3/2019 on processing of personal data through video devices

[6] Intel Executive: Rein In Data Brokers

[7] Analfabeti funzionali e social network: la situazione in Italia?

[8] https://www.cutter.com

[9] https://standards.ieee.org/project/7007.html

email: info@fabiano.law

Copyright (Nicola Fabiano) Tutti i diritti riservati. All rights reserved.

https://www.key4biz.it/privacy-qual-e-il-valore-reale-del-dato-personale/268586/