La tutela dei dati personali tra big data ed algoritmi di I.A.

Gli Stati Generali del Diritto di Internet

Prof. Avv. Gianluigi Ciacci

Studio Legale Ciacci

Intelligenza Artificiale

L'Intelligenza Artificiale, al di là delle varie definizioni, e dal dettaglio dei suoi contenuti, sicuramente è un fenomeno di rilevante, e crescente, interesse: che quindi la sta portando ad essere di grande … "moda".

Il rischio di tale situazione ?

Forse il distrarsi con aspetti secondari del fenomeno, anche se … di "successo" (almeno mediatico: ad esempio il tema della guida autonoma)

Uber, la polizia scagiona l'auto a guida autonoma: «Incidente inevitabile»

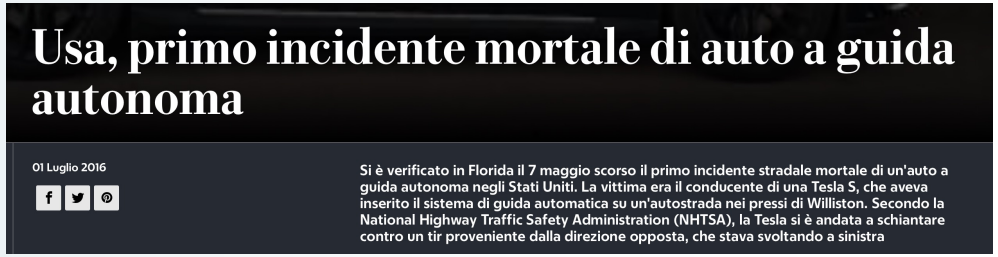
Dalle prime rilevazioni, la vittima è sbucata all'improvviso e non era possibile, neanche per l'intelligenza artificiale, evitare l'impatto. I precedenti

di Michela Rovelli

1 di 7

Il caso Uber: «Impatto inevitabile»

Le indagini sono solo all'inizio. Si sa poco di ciò che è successo nelle trade di Tempe, sobborgo di Phoenix, nello stato dell'Arizona, nella notte tra domenica 18 marzo e lunedì 19. Un Suv Volvo del 2017, con tecnologia Autopilot di Uber integrata, ha investito e ucciso Elaine Herzberg, una donna di 49 anni, mentre attraversava la strada trasportando a mano la sua bicicletta fuori dalle strisce pedonali. La vettura era in modalità autonoma e, sebbene ci fosse alla guida una



Usa, primo incidente mortale di auto a guida autonoma

01 Luglio 2016

Si è verificato in Florida il 7 maggio scorso il primo incidente stradale mortale di un'auto a guida autonoma negli Stati Uniti. La vittima era il conducente di una Tesla S, che aveva inserito il sistema di guida automatica su un'autostrada nei pressi di Williston. Secondo la National Highway Traffic Safety Administration (NHTSA), la Tesla si è andata a schiantare contro un tir proveniente dalla direzione opposta, che stava svoltando a sinistra

successo che quindi spesso "condiziona" anche chi se ne occupa, professionalmente e a livello istituzionale: 2 esempi.

Descrizione dell'evoluzione storica I.A.

Da una monografia sul tema ...

- 1939 Atanasoff-Berry Computer (ABC)
- 1950 test di Turing
- 1959 machine learning
- 1966 Shakey the Robot
- 1970 WABOT 1
- 1995 chatbot Alice
- 1997 Deep Blue
- 2000 ASIMO
- 2011 Watson
- (…)

- 1942 Asimov, le 3 leggi della robotica
- 1968 "2001 Odissea nello spazio"
- 1977 "Star Wars"
- 1984 "Electric Dreams"
- 2001 "AI - Artificial Intelligence"
- 2004 "Io, robot"
- 2013 "Her (Lei)"
- (…)

In premessa di una fonte ufficiale*

" (…) considerando che, dal mostro di Frankenstein ideato da Mary Shelley al mito classico di Pigmalione, passando per la storia del Golem di Praga e il robot di Karel Čapek, che ha coniato la parola, gli esseri umani hanno fantasticato sulla possibilità di costruire macchine intelligenti, spesso androidi con caratteristiche umane"

*(Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica)

Intelligenza Artificiale

Ma in realtà a parte il rischio evidenziato, non si deve ignorare l'opportunità creata dal forte interesse per questa realtà, rappresentata dalla nuova domanda di conoscenza legata alla necessità di comprendere l'I.A.: che porta al moltiplicarsi di eventi, di pubblicazioni non solo divulgative, ma anche tecniche (e con riferimento ai diversi campi applicativi).

Domanda di conoscenza che assume una grande importanza, soprattutto nel nostro Paese, dove la carenza di competenze nelle nuove tecnologie ha sempre rappresentato uno dei suoi grandi problemi, ancor di più se si pensa alla mancata percezione della necessità di un approccio culturale alle stesse. Carenza oggi sempre più grave.

Intelligenza Artificiale

Lo sviluppo di un'attenzione "diffusa" per l'I.A., conseguenza anche del moltiplicarsi delle sue applicazioni nella quotidianità degli utenti (ad esempio con gli assistenti virtuali nei cellulari o in *device* casalinghi) oltre a portarla al di fuori della discussione tra esperti, ha fatto nascere un dibattito sulla necessità di trovare un equilibrio fra due opposte esigenze:

- non rallentare, o addirittura bloccare, il progresso del settore, e quindi le conseguenze positive dello stesso;
- impedire che tale progresso avvenga in danno dei suoi utenti.

Una realtà strettamente collegata all'I. A.
i c.d. Big Data

Parlando di “società dell’informazione” ...

Quando ci si occupa delle nuove tecnologie, e non solo, è oramai costante il richiamo alla c.d. "società dell'informazione", e all'importanza fondamentale acquisita dai dati ("il nuovo petrolio").

L’informazione è dunque diventata il motore dell’economia, e l’evoluzione negli anni delle tecnologie dell'informazione e della comunicazione ha portato ad una sua trasformazione diventando automatica, e quindi informatica.

Parlando di "società dell'informazione" ...

L'ulteriore evoluzione degli ultimi anni ha portato un cambiamento nelle modalità di creazione, acquisizione, gestione, comunicazione, ..., delle informazioni.

La tecnologia ha quindi modificato il Volume, la Velocità, la Varietà, (la Veridicità), il Valore economico dei dati … e la possibilità di utilizzo, analisi e sviluppo degli stessi, in una realtà di autoalimentazione che genera quotidianamente miliardi di informazioni.

Realizzando la realtà dei c.d. "**Big Data**".

“Big Data”

"*ingenti quantità di dati, compresi i dati personali, provenienti da una serie di fonti diverse, che sono oggetto di un trattamento automatizzato mediante algoritmi informatici e tecniche avanzate di trattamento dei dati, che usano sia informazioni memorizzate sia in streaming, al fine di individuare*"

(Risoluzione del Parlamento europeo del 14 marzo 2017 sulle implicazioni dei Big Data per i diritti fondamentali: privacy, protezione dei dati, non discriminazione, sicurezza e attività di contrasto)

"Big Data"

I Big Data si pongono in stretta correlazione con l'Intelligenza Artificiale: da un lato ne "alimentano" l'apprendimento (ad esempio nei sistemi di *machine learning*), dall'altro rappresentano il risultato dell'applicazione degli algoritmi.

Se questo è il contesto, se i dati hanno assunto questa importanza, allora è diventato fondamentale proteggere il loro valore, insieme alla necessità sempre più sentita di sviluppare l'I.A.

Ma se poi i dati di cui si parla sono … "personali", cioè sono riferiti (o riferibili, anche indirettamente) ad individui, non basta più proteggere il loro *valore*, e non si può pensare solo a diffondere l'utilizzo di I.A., ma diventa prioritariamente necessario tutelare *i soggetti* a cui si riferiscono, la loro dignità.

Big Data, Intelligenza Artificiale e protezione dei dati personali

la tutela dei dati personali ...

Ed eccoci alla normativa che tutti cercano di evitare …

Infatti quando ci si occupa di "privacy", di protezione dei dati personali, soprattutto con riferimento al nostro Paese, si entra in contatto con un'anomalia "paradigmatica".

L'idea generalizzata è quella che vede la disciplina sulla "privacy" assolutamente inutile, burocratica, anzi, dannosa per chi vuole oggi fare impresa … appunto, qualcosa da cui difendersi

la tutela dei dati personali ...

Di conseguenza la diffusione di una "cultura" della protezione dei dati personali, l'attenzione politica al problema, il livello di adeguamento delle strutture dei vari titolari, privati e anche pubblici, è stata fortemente carente negli anni.

La situazione è migliorata con l'avvento del Regolamento 2016/679, il c.d. GDPR, di cui tutti parlano, molti si attivano per poterlo rispettare, ma alla fine non così tanti riescono ad approfondirne i diversi temi per arrivare a conoscerlo.

la tutela dei dati personali ...

Ad ogni modo, l'ingente importo delle sanzioni, l'introduzione di un sistema basato sulla responsabilizzazione del titolare, una serie di scelte ... "strategiche" nella costruzione della normativa (ad esempio la previsione della figura del DPO, del registro dei trattamenti come momento di "autoconsapevolezza" del titolare, l'obbligo di denuncia dei c.d. *data breach*, il principio di *accountability*, ...), hanno trasformato il sostanziale fallimento della disciplina degli anni '90 in un successo.

Il Regolamento 2016/679 rende la disciplina "sostanzialista", non risolvendosi solo nel rispetto formale degli obblighi come in quella precedente: si è passati da una logica di adempimento a quella di "sistema" (di protezione).

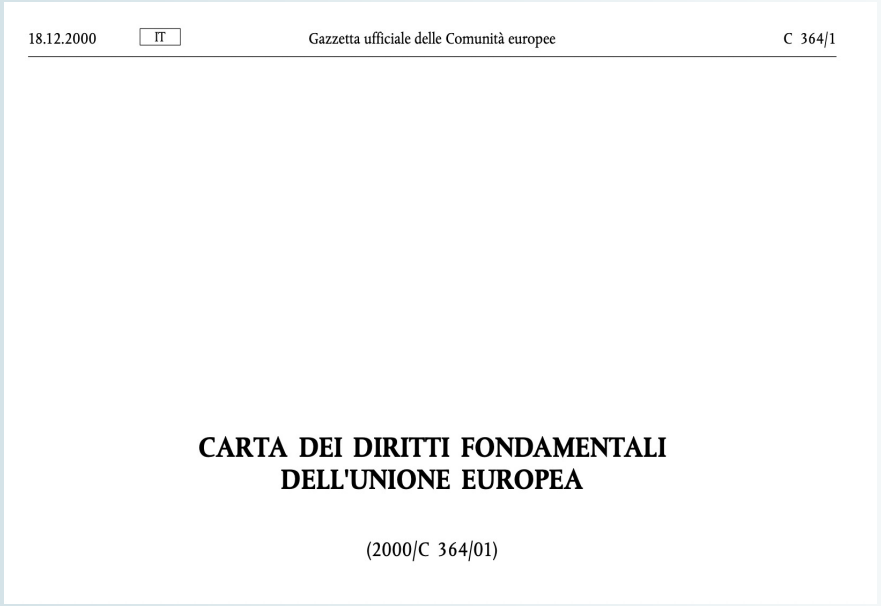
la tutela dei dati personali ...

Ancora, il cambiamento ha riguardato proprio l'oggetto della disciplina, la sua finalità: in particolare

- prima (Direttiva 95/46/CE) si voleva assicurare la protezione dei dati personali e la loro libera circolazione;
- ora il Regolamento 2016/679 invece inquadra la protezione dei dati personali quale diritto fondamentale e inviolabile della persona, ritiene prioritario rafforzare la fiducia degli interessati sulla tutela forte delle informazioni, stabilendo un quadro normativo adeguato allo sviluppo dell'economia digitale.

la tutela dei dati personali ...

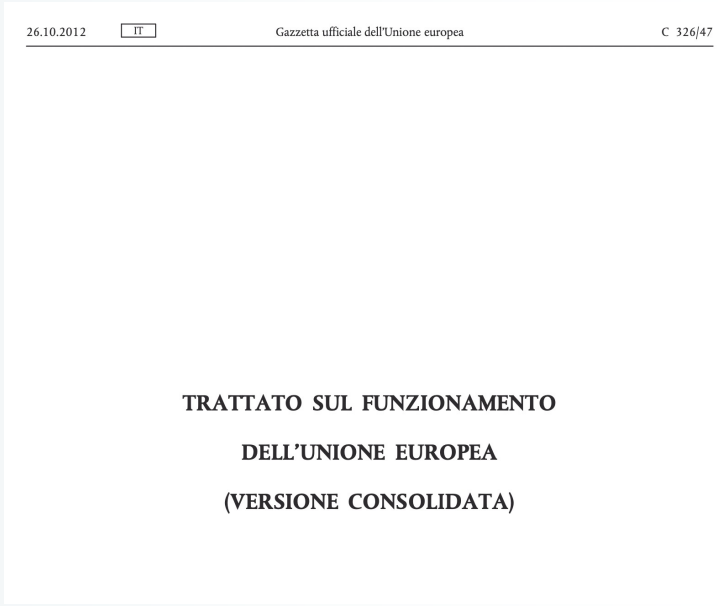
Cambiamento di impostazione che riporta centrale proprio l'importanza della tutela delle informazioni relative agli individui, come previsto in due fonti di primaria importanza per l'Europa



18.12.2000 IT Gazzetta ufficiale delle Comunità europee C 364/1

CARTA DEI DIRITTI FONDAMENTALI DELL'UNIONE EUROPEA

(2000/C 364/01)



26.10.2012 IT Gazzetta ufficiale dell'Unione europea C 326/47

TRATTATO SUL FUNZIONAMENTO DELL'UNIONE EUROPEA

(VERSIONE CONSOLIDATA)

la tutela dei dati personali ...

Nella Carta dei diritti fondamentali della UE, all'art. 7 ("*Rispetto della vita privata e della vita familiare*") dispone

- "*ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni*"

e all'art. 8 ("*Protezione dei dati di carattere personale*") sancisce

- "1. *ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano*; 2. *tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica*; 3. *il rispetto di tali regole è soggetto al controllo di un'autorità indipendente*"

la tutela dei dati personali ...

Nel Trattato sul funzionamento della UE, il cui art. 16 prevede

- par. 1 "*Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano*", e al
- par. 2 "*Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti*"

Ma il Regolamento ha funzionato ?
Problemi dell'applicazione della disciplina privacy

In linea di massima sì, ha funzionato, e sta funzionando ... anche se in realtà c'è ancora molto da fare, propri per le peculiarità della normativa e della "situazione privacy".

Così, alcune difficoltà sono generali della disciplina: a partire dall'efficacia del sistema in generale (si conosce ? viene rispettato ? è controllato ? funziona l'apparato sanzionatorio ?), ad alcuni concetti di difficile determinazione (quando un dato è effettivamente "anonimo" ?), ad importanti necessità non abbastanza sottolineate (mi riferisco all'obbligo di formazione).

Altre sono legate all'approccio "sociale" alla materia, ritenuta, come detto, inutile e burocratica, una vessazione.

Gli aspetti della disciplina in materia di protezione dei dati personali di rilievo per le attività di trattamento collegate all'I.A.

Il Regolamento Europeo

« … protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali»

(art. 1 comma 2)

I temi interessanti o problematici del Regolamento 2016/679 ...

- ✓ ambito di applicazione (target)
- ✓ principi generali
  - in particolare liceità/correttezza/trasparenza, minimizzazione, finalità, limitazione conservazione, accountability e quelli dell'art. 25
- ✓ la figura del titolare
- ✓ l'informativa
- ✓ il consenso / le basi giuridiche del trattamento
- ✓ i diritti dell'interessato e la procedura per il loro esercizio
- ✓ il Garante
- ✓ le sanzioni

Big Data, Intelligenza Artificiale e protezione dei dati personali ... problemi e possibili soluzioni

I problemi dell'applicazione della disciplina privacy ai Big Data e all'I.A.

Le caratteristiche del "sistema GDPR" portano, come detto, diversi problemi nella sua applicazione alla realtà dell'I.A. e dei Big Data.

Si pensi alla redazione dell'informativa secondo quanto richiesto dall'art. 14, o alla configurabilità di una base giuridica del trattamento consensuale, o comunque all'individuazione di quella giusta; come, in linea di massima, appaiono non applicabili, o comunque non facilmente, i principi generali del trattamento, o effettiva la possibilità concreta di esercizio dei diritti da parte dell'interessato.

I problemi dell'applicazione della disciplina privacy ai Big Data e all'I.A.

Altre difficoltà sono legate alla tipologia di trattamento dati legati a tali realtà.

Ad esempio, in genere le informazioni risalgono a una lunga catena di acquisizioni, e solo alla fine vengono aggregate
ed esaminate/utilizzate da titolari che possono non coincidere con coloro che li hanno raccolti.

Ancora, spesso l'intervento di sistemi di I.A. sulla massa di dati portano a creare nuove informazioni impreviste, e imprevedibili, nel momento dell'inizio della raccolta.

E, tra l'altro, i player di questi sistemi sono in genere gli OTT di difficile "gestione" (2 esempi: Google Analytics e Microsoft cloud).

Big Data, I.A. e privacy

Nel tentare di ipotizzare alcune soluzioni al problema della protezione dei dati personali compresi nei c.d. Big Data, e di conseguenza sottoposti all'applicazione di sistemi di I.A., procediamo per temi.

Iniziando con l' analizzare l'unica norma attualmente dedicata a disciplinare uno degli aspetti applicativi di tali sistemi: quello dell'art. 22 del Regolamento 2016/679.

Regole per l' I. A.: l'art. 22 GDPR

Il suo titolo è "*Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione*", che quindi individua il settore dell'I.A. di interesse. In particolare il disposto del suo primo comma prevede:

L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

Regole per l' I. A.: l'art. 22 GDPR

Quindi, proprio a tutela dei diritti e delle libertà fondamentali, della dignità delle persone fisiche, si prevede la possibilità di rifiutare l'applicazione esclusiva di un sistema automatizzato nelle decisioni che le riguardano.

Affermazione che ha poi alcune eccezioni nel comma 2, nella specie se la decisione

- ✓ sia necessaria per la conclusione o l'esecuzione di un contratto
- ✓ sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento
- ✓ si basi sul consenso esplicito dell'interessato

Regole per l' I. A.: l'art. 22 GDPR

Eccezioni che comunque sono equilibrate dall'applicazione di una regola generale a garanzia della persona coinvolta ("*il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione*"), e che comunque hanno a loro volta una eccezione, stabilita dall'ultimo paragrafo dell'art. 22 (che le esclude in ogni caso in cui si tratti di "categorie particolari di dati personali").

le fonti (qui su IA e privacy)

European Parliament

The impact of the General Data Protection Regulation (GDPR) on artificial intelligence

EDPB-GEPD

Parere congiunto 5/2021

sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale)

Big data, artificial intelligence, machine learning and data protection

ico.
Information Commissioner's Office

Strasburgo, 25 gennaio 2019 T-PD(2019)01

COMITATO CONSULTIVO (CD. T-PD) DELLA CONVENZIONE SULLA PROTEZIONE DELLE PERSONE RISPETTO AL TRATTAMENTO AUTOMATIZZATO DI DATI A CARATTERE PERSONALE
(Convenzione 108)

LINEE-GUIDA IN MATERIA DI INTELLIGENZA ARTIFICIALE E PROTEZIONE DEI DATI

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

ICDPPC
International Conference of Data Protection & Privacy Commissioners

DECLARATION ON ETHICS AND DATA PROTECTION IN ARTIFICAL INTELLIGENCE

40th International Conference of Data Protection and Privacy Commissioners

Tuesday 23rd October 2018, Brussels

Regole per l' I. A.: altre fonti

In genere, tutte usano una formulazione ... "condizionale", ma prevedono già in questa fase indicazioni ben precise: ribadendo e sottolineando l'importanza del rispetto dei diritti fondamentali dell'individuo, in particolare quello alla protezione dei suoi dati personali.

Prendiamo ad esempio la "*Risoluzione del Parlamento europeo del 12 febbraio 2019 su una politica industriale europea globale in materia di robotica e intelligenza artificiale*": numerose sono le norme sul punto, ad iniziare dal paragrafo 4.2 intitolato "Dati personali e riservatezza".

Regole per l' I. A.: altre fonti

L'art. 126 ad esempio

"*ribadisce che il diritto al rispetto della vita privata e il diritto alla protezione dei dati personali, quali sanciti dagli articoli 7 e 8 della Carta dei diritti fondamentali e dall'articolo 16 del trattato sul funzionamento dell'Unione europea si applicano a tutti i settori della robotica e dell'intelligenza artificiale e che il quadro giuridico dell'Unione per la protezione dei dati deve essere pienamente rispettato*" ed

"*evidenzia che i progettisti di sistemi robotici e intelligenza artificiale sono responsabili di sviluppare prodotti che siano sicuri e adeguati agli scopi previsti e di applicare le procedure per il trattamento dei dati rispettando la legislazione esistente e garantendo la riservatezza*"

Regole per l' I. A.: altre fonti

Ancora, l'art. 140 introduce un altro tema, quello della cooperazione tra Commissione, Stati membri e mondo accademico per

"*rafforzare la condivisione delle conoscenze e promuovere l'istruzione e la formazione*

- *per i progettisti, relativamente alle implicazioni etiche, alla sicurezza e al rispetto dei diritti fondamentali, e*
- *per i consumatori, per quanto riguarda l'utilizzo della robotica e dell'intelligenza artificiale, con una particolare enfasi sulla sicurezza e la riservatezza dei dati*".

Regole per l' I. A.: altre fonti

Altro esempio si può riscontrare nelle "*Linee Guida relative ai principi dell'intelligenza artificiale dell'OEDC (OCSE)*" del 22 maggio 2019, in particolare nel par. 1.2 (Valori incentrati sull'uomo ed equità) che dispone

"*Gli attori dell'IA devono rispettare lo stato di diritto, i diritti umani e i valori democratici, durante tutto il ciclo di vita del sistema di IA. Questi includono la libertà, la dignità e l'autonomia, la privacy e la protezione dei dati, la non discriminazione e l'uguaglianza, la diversità, l'equità, la giustizia sociale e i diritti del lavoro riconosciuti a livello internazionale.*"

possibili soluzioni ?

Proviamo quindi, ad immaginare le possibili soluzioni:

- ✓ portare tutti i player del settore (comunque "titolari del trattamento") ad adeguarsi correttamente al sistema della protezione dei dati personali previsto dal Regolamento 2016/679;
- ✓ sviluppare il più possibile una tutela "dal basso", partendo da una corretta formazione e informazione degli interessati (non solo "tecno-entusiasmo");
- ✓ potenziare il più possibile la tutela "dall'alto" (normativa e in particolare Autorità Garante, nella sua qualità e possibilità concreta di operare).

possibili soluzioni ?

Utopia ?

Sicuramente le soluzioni proposte sono ambiziose, e allo stesso tempo, riguardando la … "privacy" (con tutte le difficoltà ad essa correlate, di cui si è detto: in particolare l'approccio negativo alla materia, e in generale la mancata conoscenza della stessa), di difficile realizzazione, e comunque non in tempi brevi.

possibili soluzioni ?

Occorre però capire (e spero che il mio intervento contribuisca a questo) che non si può non decidere, accorciando i tempi, e avendo ben chiaro che la scelta si pone, su un livello più ampio, tra

- la limitazione, o addirittura la rinuncia a un diritto fondamentale, a causa dell'importanza (economica) del settore,
- ed invece un "salto culturale" che deve portare al successo (al 100%) del sistema di protezione dei dati personali, anche rispetto agli innovativi sistemi di I.A.