IL DIRITTO NEL RAPPORTO TRA FILOSOFIA E INFORMATICA:

I "BIG DATA" CI AIUTANO A VIVERE MEGLIO O LIMITANO LE NOSTRE LIBERTÀ INDIVIDUALI?

INTERVISTA A FABIO CAPRABIANCA

ABSTRACT: THE LAW IN THE RELATIONSHIP BETWEEN PHILOSOPHY AND COMPUTER SCIENCE: DO THE BIG DATA HELP TO LIVE BETTER OR RESTRICT INDIVIDUAL FREEDOM?
In this interview Fabio Caprabianca highlights the question and concern about Big Data, i.e. how the reduction of the existent in data is going to modify also the sense of things and the concept of knowledge.

S&F: S&F_scienzaefilosofia.it

FC: Fabio Caprabianca

S&F: Come impostare correttamente la questione "Big Data"?

FC: *Negli ultimi anni la società, in esito allo sviluppo delle tecnologie dell'informatica e delle telecomunicazioni, è stata oggetto di un rapidissimo cambiamento sia dal punto di vista della comunicazione e del rapporto sociale, sia da quello cognitivo, ponendo l'individuo di fronte a una serie di problematiche delle quali, molto spesso, si ignora la natura. Lo sviluppo tecnologico e, in particolare, la diffusione di smartphone e tablet abilitanti all'uso dei social media, mentre da un lato hanno contribuito a facilitare la diffusione dei dati e delle informazioni, nonché a*

migliorare il rapporto tra il cittadino e la società, dall'altro hanno sottoposto il cittadino a una serie di rischi causati anche dalla mancata regolamentazione di tali strumenti tecnico-informatici e del loro utilizzo. Ciò in parte dovuto alla rapidità eccessiva di questo sviluppo tecnologico a cui, fisiologicamente, la macchina del diritto ineluttabilmente più lenta fatica molto ad adeguarsi. Conseguentemente il cittadino risulta esposto a una serie di vulnerabilità e criticità causate dall'utilizzo inconsapevole di tali tecnologie che, di fatto, stanno cambiando anche la comunicazione e il rapporto sociale con diverse implicazioni, come la questione del "digital divide", della "new economy" e degli impatti sul lavoro e sulla formazione.

In una società in cui emerge un effettivo rapporto di dipendenza dalla tecnologia dell'informazione, assume carattere centrale la questione del "datismo", ovvero di come la riduzione dell'essente in dato sta modificando anche la percezione e il concetto di conoscenza. Alcuni ritengono che ciò di cui si ha bisogno oggi siano le sole informazioni che provengono dai dati i quali, a causa della loro mole così smisurata, non possono essere interpretati dall'intelligenza umana poiché non in grado di contenerli tutti per elaborarne le caratteristiche principali e costruire sui medesimi una nuova conoscenza. Di conseguenza i dati costituiscono de facto il fulcro della nostra società cosiddetta dell'informazione in cui si assiste, alla stregua della "febbre dell'oro" di un paio di secoli fa, alla corsa da parte delle grandi aziende multinazionali ad accaparrarsi più dati possibile e in modo più o meno esplicito e/o consapevole da parte del cittadino-utente. Ciò con l'intento di profilare gruppi e/o sottoinsiemi di persone in base a determinati criteri per le finalità più differenti, per scopi che spaziano dalla sfera prettamente commerciale a quella più personale in cui si cercano di tracciare modelli e/o profili sulle abitudini, i gusti, i pareri circa determinati argomenti e/o opinioni di pensiero: ad

esempio basti pensare ai "like" o "dislike" che si mettono sui post sulle reti social (e.g. Facebook, LinkedIn, Twitter, etc.), ovvero al numero di volte in cui è stato condiviso un post per capirne il livello di diffusione/condivisione e rilevanza dell'item. Ci si trova così proiettati con una seconda personalità in questo universo digitale, il Cyberspazio, in cui si ha un vero e proprio scollamento tra l'io tradizionale e quello digitale. Nel Cyberspazio si ha così la possibilità di alterare le caratteristiche e la percezione di un soggetto o un ente in genere, con l'introduzione di nuovi dispositivi di gestione e controllo del "parco umano" ad esempio attraverso le reti social, da cui la questione della verità.

In questo particolare momento storico di fervente dinamicità e cambiamento, è bene fermarsi a riflettere su alcuni temi anziché agire in maniera impulsiva e sottovalutando l'impatto sociale del "progresso" tecnologico. Un organismo vivente non può essere considerato un complesso di algoritmi eterogenei e non si può ritenere "intelligente" la decisione elaborata da un automa/algoritmo che non si basi sull'assunzione consapevole di responsabilità rispetto alle conseguenze eventuali.

Ma tutti questi dati come sono stati acquisiti? Dove sono custoditi? E per quanto tempo? Come sono tutelati da eventuali accessi da parte di terzi?

È solo apparente il vantaggio nell'utilizzo di un App che in cambio ci chiede il consenso per la condivisione di alcuni nostri contenuti personali o l'invio di dati geo-referenziati dal nostro smartphone, senza informarci adeguatamente sulle finalità e sull'effettivo utilizzo di tali dati.

Forse appare opportuna una riflessione in merito...

S&F: Quale la tutela dei dati e delle libertà individuali dei cittadini UE da parte delle aziende alla luce del nuovo

Regolamento UE n.2016/679 (c.d. GDPR, General Data Protection Regulation)?

FC: *Il nostro Paese, tra i primi a rilevare l'importanza della questione privacy riconoscendo come diritto fondamentale quello della protezione dei dati personali con la famosa "legge sulla privacy" del Prof. On. Stefano Rodotà (legge n.675/1996) in recepimento della direttiva 95/46/UE, ha contribuito alla redazione del nuovo Regolamento UE n.2016/679 (c.d. GDPR, General Data Protection Regulation) di recente attuazione che abroga la precedente direttiva 95/46/UE ed emenda il Codice Privacy (cfr. d.lgs. n.196/2003). A differenza di una direttiva UE il GDPR, in qualità di regolamento generale UE, non ha bisogno di essere recepito da ciascuno dei singoli stati membri ed è direttamente applicabile (con efficacia differita ex art. 99 GDPR) in modo uniforme in tutti i paesi dell'UE quando i dati trattati si riferiscono a cittadini europei.*
Principio cardine del Regolamento Europeo 2016/679 è quello della protezione delle persone con riguardo al trattamento dei dati e della conseguente necessità, per ogni ordinamento, di approntare meccanismi di reazione a condotte che danneggino le persone.
Il GDPR rappresenta in sé una specie di rivoluzione, in quanto impone una sorta di uniformità di trattamento dei dati delle persone introducendo il concetto di dato come valore/asset della persona (c.d. Interessato) e che, in quanto tale, va tutelato con adeguate misure di sicurezza da parte sia del Titolare del trattamento (cioè di colui che determina le finalità del trattamento, le modalità e gli strumenti utilizzati, ivi compreso il profilo della sicurezza), sia da parte del Responsabile del trattamento (cioè di colui che tratta i dati secondo le direttive del Titolare che deve essere in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei

diritti dell'interessato). Nascono delle nuove figure all'interno delle aziende e/o organizzazioni, come il Responsabile della Protezione dei Dati (c.d. RPD oppure DPO, c.d. Data Protection Officier), con il compito di valutare e organizzare la gestione del trattamento di dati personali, e dunque la loro protezione, all'interno di un'azienda, di un ente o di una associazione, affinché questi siano trattati in modo lecito e pertinente, operando con autonomia decisionale. Viene introdotto il concetto di valutazione del rischio nel trattamento dei dati, di "Privacy by default"/"by design" e Accountability, che potremmo riassumere come responsabilità e adeguatezza del trattamento dei dati, implementando tutti quei meccanismi e quelle tutele tali da rendere le misure di sicurezza idonee al valore dei dati trattati. Inoltre, si introduce anche il principio dello Sportello Unico (c.d. One Stop Shop), che stabilisce l'unicità per i titolari del trattamento dell'Autorità di Controllo (solitamente il Garante Privacy nazionale o della sede principale dell'azienda/organizzazione) a livello UE, secondo principi di coerenza e mediante elezione di una "leading authority" in modo tale che, di volta in volta, una decisione emessa dall'Autorità di controllo designata divenga valida in tutto il resto dell'Unione.

In questo contesto appare evidente che il GDPR sia una evoluzione più che una rivoluzione nella tutela dei dati delle persone, introducendo i principi di responsabilizzazione e rischio, maggiore proattività nella tutela dei dati, "europeizzazione" e omogeneizzazione delle procedure, nuovi diritti per l'interessato quali la limitazione del consenso nel trattamento, il diritto alla portabilità dei dati, il diritto a essere informati e il diritto all'oblio; il ruolo dell'Autorità di controllo secondo il principio dello sportello unico e meccanismi di coerenza, nonché un sistema sanzionatorio tendenzialmente uniforme in tutta l'Unione.

S&F: Veniamo dunque al problema della "sicurezza informatica": come pensare un approccio integrato che consideri la rilevanza sociale, economica, organizzativa, giuridica e tecnica nella protezione dei dati?

FC: *Per quanto precedentemente considerato, al fine di poter tutelare i dati degli interessati con le adeguate misure di sicurezza prospettate dal GDPR e quindi garantire l'applicazione di idonei meccanismi di sicurezza informatica, non si può seguire un approccio esclusivamente tecnico.*
Valutare la sicurezza dei dati delle persone è un'attività molto complessa, per gli impatti e le conseguenze che possono derivare da una perdita accidentale o da un eventuale furto (c.d. data breach). Di conseguenza il problema della sicurezza informatica deve necessariamente essere trattato in modo integrato in quanto la sicurezza deve preservare il valore dei dati, quindi è necessario considerarne la rilevanza sotto diversi profili: economico, sociale, organizzativo, giuridico oltre che tecnico.
La sicurezza informatica è un elemento centrale senza il quale la Società dell'informazione non potrebbe esistere o essere definita tale. La sua rilevanza economica è facilmente intuibile, soprattutto per i dati pubblici e aziendali quando sono completi, aggiornati, validi e accessibili in forma digitale e riferiti a un particolare soggetto o raggruppamento di soggetti. Ci rendiamo conto del valore dei dati soltanto quando li "perdiamo" o li regaliamo in modo spesso inconsapevole alle reti social o alle aziende gestori di servizi e/o telecomunicazioni. La rilevanza sociale della sicurezza informatica attiene la conservazione e la gestione dei patrimoni informativi digitali, sia nelle banche dati che nelle reti, ivi compresi i dati personali, i patrimoni tecnologici, i dati relativi alla sicurezza fisica e logica delle persone, la qualità delle informazioni. Essere consapevoli della rilevanza sociale della sicurezza informatica rende più elevata la

sicurezza fisica delle persone. Per quanto attiene l'aspetto organizzativo, la sicurezza informatica dei dati è strettamente correlata ai modelli organizzativi e ai processi di digitalizzazione e gestione elettronica delle informazioni adottati in azienda. Mentre la rilevanza tecnica della sicurezza informatica è piuttosto intuitiva, quella giuridica può essere considerata come l'elemento di coesione di tutte le altre, atta così a garantire la validità giuridica dei dati. Caratteristiche quali integrità intesa come non-modificabilità, accessibilità intesa come disponibilità e riservatezza intesa come prevenzione dall'uso non autorizzato delle informazioni sono i principi su cui si basa la sicurezza informatica.

S&F: Dunque: limiti e responsabilità nell'utilizzo dei big data. Il problema della profilazione e della persistenza dei dati nel cyberspazio, il diritto all'oblio (i.e. il diritto a essere dimenticati dal web) e il rapporto tra diritto alla privacy e interesse pubblico alla notizia.

FC: *Negli anni passati, anche prima del GDPR, ci sono state numerose vicende giudiziarie legate all'utilizzo non autorizzato dei cosiddetti "big data" da parte di soggetti che operano nel settore dell'informatica, in particolare nella gestione dei motori di ricerca e delle reti social, ovvero ai gestori di servizi IT e/o delle telecomunicazioni (e.g. Google, Facebook, etc.).*
Con l'entrata in vigore del GDPR si sono poste molte questioni legate agli aspetti accennati in precedenza, soprattutto per quanto attiene alla persistenza dei dati nella rete internet, preso atto che i vari motori di ricerca (e.g. Google, Yahoo, etc.) continuano a conservare copie di tali dati anche dopo la cancellazione del dato originario che diventa così praticamente ineliminabile.

Attualmente, per poter eliminare tali dati, sia ha solo la possibilità di deindicizzarli dai vari motori di ricerca dopo aver vinto un procedimento giudiziario oneroso (cfr. motori di ricerca e diritto all'oblio nella vicenda giudiziaria della Corte di Giustizia nel caso Google Spain).

La consapevolezza da parte del cittadino-utente circa le finalità dei dati forniti a fronte dell'utilizzo dei servizi e delle applicazioni informatiche (i.e. App, web, reti social, etc.) accessibili da personal computer, tablet e smartphone, anche riguardo ai processi decisionali automatizzati ivi compresa la profilazione, rientra nelle previsioni del GDPR e nei nuovi diritti dell'interessato quale, ad esempio, il diritto alla spiegazione nelle procedure automatizzate inteso come diritto di contestare la decisione basata sul trattamento automatizzato.

Il fatto è che questo tema è particolarmente delicato e complesso, in quanto impatta molteplici aspetti sia della sfera sociale sia di quella personale. La norma può dare delle indicazioni, ma non può prescindere dal buon senso e dalla consapevolezza da parte di tutti, aziende/organizzazioni e cittadini.

In ogni caso è doveroso operare un bilanciamento fra i vari interessi coinvolti, cercando di orientare il ragionando sulla tutela dell'interesse del cittadino, inteso come individuo ed elemento sostanziale della società che ha il diritto fondamentale alla tutela dei suoi dati, anche quando è coinvolto l'interesse pubblico (che spesso viene sfruttato da parte di taluni giornalisti d'assalto).

Poiché la rete internet non ha la capacità di dimenticare, nel senso che è molto difficile cancellare un'informazione una volta pubblicata (in quanto essa persiste anche oltre la sua cancellazione sui vari motori di ricerca),emerge la necessità di responsabilizzare e formare i cittadini-utenti alla comprensione delle tecnologie informatiche disponibili e al loro utilizzo consapevole, in modo da evitare sbilanciamenti nella messa a

disposizione di dati che, opportunamente correlati, potrebbero fornire ad alcuni "soggetti" quelle informazioni utili a gestire e controllare il "parco umano" e, di conseguenza, limitare la libertà dei cittadini-utenti della Società dell'informazione.

FABIO CAPRABIANCA è docente di Sistemi Erp e Real-Time presso il Dipartimento di Ingegneria Industriale e dell'Informazione dell'Università degli Studi della Campania Luigi Vanvitelli

fabio.caprabianca@unicampania.it