filodiritto
APPROFONDISCI SEMPRE
Tribunale Bologna 24.07.2007, n.7770 - ISSN 2239-7752
Direttore responsabile: Antonio Zama

Fabbriche digitali, big data e protezione dei dati personali

11 Giugno 2019
Stefania Calvello

Indice

1. Le Fabbriche Digitali: profili introduttivi

Con la Quarta Rivoluzione industriale si è consolidato il processo di digitalizzazione all'interno delle imprese, divenuto parte integrante delle cc.dd. Fabbriche Digitali, affermatesi quale strumento di competitività, per fare fronte alle sfide poste dagli sviluppi della globalizzazione e dalle attuali tendenze dei mercati.

A questo riguardo, la stessa Commissione UE nella Comunicazione "*Digitalizzazione dell'industria europea – Cogliere appieno i vantaggi di un mercato unico digitale*" ha espressamente riconosciuto che la digitalizzazione e, in particolare, il ricorso ad alcune specifiche tecnologie (tra cui, l'IoT, i *big data* e il *cloud computing,* la robotica, l'intelligenza artificiale e la stampa 3D) "*consentono all'industria di rispondere alle richieste dei consumatori odierni, che sono più esigenti e chiedono personalizzazione, maggiore sicurezza, maggiore comodità, efficienza energetica ed efficienza nell'impiego delle risorse*" rilevando come ad esempio "*la combinazione di sensori avanzati e* big data *nei processi industriali può ridurre il consumo energetico e la quantità di materie prime utilizzata*".

Le Fabbriche Digitali si pongono, pertanto, come un modello che si fonda su un nuovo approccio nella organizzazione e controllo di tutto il ciclo di vita dei prodotti, dalla ideazione e progettazione, allo sviluppo e fabbricazione fino alla consegna dei prodotti al cliente finale e sono orientate a soddisfare le esigenze della clientela in maniera sempre più individualizzata e personalizzata.

Tra i componenti di cui si avvalgono le Fabbriche Digitali figurano – quale elemento essenziale – i cc.dd. *Big Data* e i *Data Analytics*, identificati dal Parlamento Europeo nella Risoluzione del 14 marzo 2017 sulle implicazioni dei Big Data per i diritti fondamentali come uno strumento che si riferisce "*alla raccolta, all'analisi e all'accumulo ricorrente di 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 determinate correlazioni, tendenze e modelli (analisi dei Big Data)*".

La definizione fornita dal Parlamento Europeo si presenta come una delle più aderenti alla realtà operativa, in quanto ne evidenzia sia l'aspetto quantitativo sia quello qualitativo, per la molteplicità e varietà dei dati raccolti ed analizzati e delle relative fonti.

Certamente, come evidenziato dall'Autorità per le Garanzie nelle Comunicazioni in un proprio recente studio, il ricorso ai *big data* si è nel tempo sempre più ampliato, tanto da essere qualificato come un "*fenomeno dirompente*", per l'incremento delle fonti dei dati, oltre che per la continua innovazione ed evoluzione delle strumentazioni tecnologiche.

Nell'ambito delle Fabbriche Digitali, va, in particolare, considerata la crescente diffusione di nuove sorgenti di dati, quali, ad esempio, l'Internet delle cose (c.d. "*Internet of Things - IoT*") nonché i sensori, in grado di "gestire le risposte" per esigenze di controllo e di ottimizzazione del processo produttivo e conseguentemente di intercettare valori via via crescenti di dati.

Ma l'ampliamento, per effetto di tali tecnologie, della produzione ed analisi sistematica di dati – peraltro, qualitativamente eterogenei, in quanto comprendenti, nel caso di *big data*, anche dati di tipo non strutturato – pone inevitabilmente considerevoli oneri per le imprese, tenute – in forza del principio di *accountability* – a **valutare sin dalla fase della progettazione le implicazioni in ambito *data protection* e a porre in essere una serie di misure ed adempimenti nell'attuazione dei propri programmi di adeguamento al Regolamento UE 2016/679 ("GDPR") e alla legislazione nazionale in tema di protezione dei dati personali**.

2. *Big Data vs. personal data*

Con riferimento ai *big data*, uno dei primi aspetti che necessita di essere considerato riguarda la verifica della **natura dei dati trattati** e, in particolare, la valutazione se dalle operazioni di *Data Analytics* possano derivare operazioni di trattamento di dati personali.

Su questo punto, lo stesso Parlamento Europeo nella propria Risoluzione del 14 marzo 2017 ha espressamente rilevato che "*dall'impiego dell'analisi dei Big Data si osserva **una confusione tra i dati personali e quelli non personali, il che può portare alla creazione di nuovi dati personali***".

Le sintetiche indicazioni del Parlamento Europeo comportano un inevitabile innalzamento del grado di responsabilizzazione delle imprese e del livello di indagine nell'impiego dei *Big Data*, in quanto ne deriva una esortazione ad effettuare **un'analisi attenta e capillare dei dati** oggetto dei trattamenti e delle correlazioni che possono derivare dalle operazioni di *Data Analytics*, per effetto delle quali **è altresì possibile re-identificare un soggetto anche attraverso dati apparentemente anonimi**.

L'approccio "investigativo" di cui sopra risulta, altresì, giustificato alla luce della **definizione ampia di "dato personale"** contenuta nel GDPR e delle relative indicazioni interpretative.

Significativo, in proposito, è il considerando n. 26, in cui il legislatore UE evidenzia che "*è auspicabile applicare i principi di protezione dei dati a tutte le informazioni relative a una persona fisica identificata o identificabile*" precisando, al contempo, che "*per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente*" ed escludendo, infine, dall'applicazione del GDPR le sole informazioni anonime, vale a dire "*informazioni che non si riferiscono ad una persona fisica identificata o identificabile*".

Come si può notare, con tale "considerando" il legislatore UE– con il chiaro intento di ampliare la protezione delle persone fisiche con riferimento al trattamento dei dati personali e di favorire conseguentemente lo sviluppo di un clima di fiducia verso l'economia digitale – ha inteso **estendere l'ambito applicativo del GDPR anche ai casi cc.dd. di *"singling out"*, laddove sia possibile l'individuazione di un soggetto nell'ambito di specifici contesti**.

In tale linea interpretativa si collocano anche le precedenti osservazioni rese dallo stesso **Gruppo di Lavoro *ex* art. 29 nel parere n. 4/2007 sul concetto di dati personali**, che portano a considerare talune informazioni come "concernenti" una persona, qualora **informazioni in sé neutre (in quanto, ad esempio, riferite ad oggetti), siano comunque collegabili a persone fisiche e, conseguentemente, suscettibili di essere qualificate come dati personali**.

> **Conclusivamente, si può, dunque, affermare che, nell'ottica dei *big data*, l'elemento dirimente ai fini della valutazione della natura dei dati concerne il fattore dell'identificabilità del soggetto: in sintesi, l'analisi del titolare del trattamento dovrà spingersi fino a verificare se dall'applicazione della *Data Analytics* sia, comunque, possibile risalire a persone fisiche, anche per effetto di aggregazioni di dati, che singolarmente potranno essere di per sé non identificativi e rientrare nell'accezione di dati anonimi.**

Tale approccio trova conferma anche nelle affermazioni di A. Soro, Presidente del Garante per la protezione dei dati personali, nel suo recente intervento in tema di "*Big Data e Libertà nella dimensione digitale*", in cui l'analisi delle dinamiche di gestione dei *Big Data* conduce a riconoscere come ***la nozione di dato anonimo stia subendo una "contrazione speculare all'estensione del concetto di dato personale, in funzione ampliativa della tutela***".

In sintesi, le ragioni dell'estensione dell'applicabilità del GDPR, con riferimento ai *Big Data,* risiedono nelle peculiari potenzialità della *Data Analytics,* che comprendono – come sopra indicato – anche possibili re-identificazioni di dati in apparenza anonimi.

3. GDPR: alcuni strumenti a disposizione delle imprese nel campo dei *Big Data*

Dalla nuova lettura delle nozioni di "dato anonimo" e di "dato personale" deriva conseguentemente un ampliamento dell'ambito applicativo del GDPR.

A questo riguardo, con specifico riferimento ai *Big Data*, il Consiglio d'Europa nelle proprie Linee Guida del 27 Gennaio 2017 sui *Big Data* ha fornito una serie di indicazioni di carattere operativo.

Tra queste, particolare importanza riveste la **valutazione del rischio**, che incombe sui titolari del trattamento e che, per la particolare complessità del fenomeno in questione, il Consiglio d'Europa suggerisce che sia svolta con **l'ausilio di figure professionali dotate di conoscenze e competenze specifiche, tali da consentire di valutare l'impatto complessivo, *"including the legal, social, ethical and technical dimension"***.

Nel caso dei *Big Data* e *Data Analysis*, considerata la "*natura, l'oggetto, il contesto e le finalità del trattamento*" e tenuto conto, altresì, della complessità intrinseca dell'analisi dei *Big Data*, è ulteriormente opportuno che il titolare – in linea con quanto già previsto dall'articolo 35 del GDPR – effettui, prima di procedere al trattamento, una o più **valutazioni d'impatto**, al precipuo fine di considerare i rischi connessi all'utilizzo dei *Big Data.*

Peraltro, come anche riconosciuto dal Presidente del Garante per la protezione dei dati, **il GDPR contiene** "***alcune norme e garanzie di particolare interesse per i trattamenti su larga scala*** *quali quelli realizzati sui Big Data*", intendendosi per "trattamenti su larga scala" – come specificato nel considerando n. 91 – un insieme di operazioni "*che mirano al trattamento di una* ***notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato….ad esempio per i diritti e le libertà degli interessati, specialmente qualora tali trattamenti rendano più difficoltoso per gli interessati l'esercizio dei propri diritti***", specificandosi nello stesso considerando che "*E' opportuno altresì effettuare una valutazione d'impatto sulla protezione dei dati nei casi in cui i dati personali sono trattati per adottare decisioni riguardanti determinate persone fisiche in seguito ad una valutazione sistematica e globale di aspetti personali relativi alle persone fisiche, basata sulla profilazione di tali dati…*".

Inoltre, come rilevato dal Consiglio d'Europa, in linea con il principio di trasparenza, gli esiti delle valutazioni del rischio effettuate dal titolare dovrebbero essere rese conoscibili agli interessati, allo scopo di **renderli partecipi degli effetti derivanti dall'utilizzo dei *Big Data***.

> **Sempre nell'ottica della valutazione complessiva del fenomeno *Big Data*, uno strumento espressamente individuato dal GDPR e particolarmente indicato è rappresentato dalla c.d. "*privacy by design*" volta nello specifico a consentire di individuare "*sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso*" misure tecniche ed organizzative adeguate, al fine di mettere in atto interventi volti ad una riduzione dei dati oggetto di trattamento nell'ottica del principio di minimizzazione nonché misure tecniche (tra cui può essere considerata la pseudonimizzazione), al precipuo scopo di ridurre i rischi a carico degli interessati.**

Ancora, qualora per effetto della *Data Analysis* siano possibili re-identificazioni di persone fisiche, i titolari saranno tenuti, nella valutazione di tale rischio, a considerare l'adeguatezza o meno delle misure adottate e ad aggiornare periodicamente tale valutazione, anche alla luce degli sviluppi in ambito IT, con particolare riferimento alle misure tecniche da applicare, tra cui quelle concernenti l'anonimizzazione dei dati od anche la crittografia, purché, come specificato dal Parlamento Europeo, non siano rese possibili ai fornitori di servizi di crittografia le cc.dd. "*backdoor*".

Infine, uno strumento di effettiva utilità per le imprese, sia per consentire di acquisire un quadro chiaro e completo con riferimento alle attività in ambito *data protection* sia per contribuire ad una efficace valutazione dei rischi, ancor più nel campo dei *Big Data,* è sicuramente rappresentato dal **registro delle attività di trattamento**.

Data la specificità e complessità dei trattamenti inerenti a *Big Data* e *Data Analysis*, potrebbe essere consigliabile **prevedere nei registri una sezione *ad hoc*, in cui "ove possibile" siano inserite le informazioni richieste dall'articolo 30 del GDPR**: la condizione sopra indicata, con riferimento ai *Big Data* appare d'obbligo, tenuto conto del fatto che, in tale specifico contesto, non sempre è possibile avere un quadro chiaro delle finalità dei trattamenti *ex ante* e conseguentemente dei termini di cancellazione dei dati.

4. GDPR: alcune criticità nell'applicazione ai *Big Data*

Nonostante il GDPR sia stato impostato con lo specifico intento di adeguare le norme a tutela delle persone fisiche con riferimento al trattamento dei dati personali alle nuove istanze e scenari dell'economia digitale, alcuni snodi fondamentali di tale atto normativo risultano di non agevole applicabilità al fenomeno *Big Data.*

Ci si riferisce, in particolare, ai **principi elencati all'articolo 5**, di cui lo stesso legislatore UE ha sottolineato e ribadito l'importanza, tanto da prevedere espressamente "*sanzioni amministrative pecuniarie fino a 20.000.000 EUR o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore*", in caso, *inter alia,* di violazione dei "*principi di base del trattamento, comprese le condizioni relative al consenso a norma degli articoli 5,6, 7 e 9*".

Ci si chiede, in particolare, nel contesto specifico dei *Big Data,* come possano trovare completa applicazione alcuni tra i principi elencati all'articolo 5 del GDPR, quali in particolare, quelli di minimizzazione, limitazione della finalità e di esattezza.

Partendo dal primo dei principi sopra elencati non vi è chi non veda come **la logica della c.d.** " **minimizzazione**" non si attagli adeguatamente alle logiche dei *Big Data,* che, per la natura e conformazione degli stessi, rischiano di porsi in contrasto con le indicazioni fornite dal legislatore UE, volte a richiedere che, in applicazione di tale principio i dati siano "*adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*".

Analoghe criticità emergono con riferimento al **principio della limitazione della finalità**, in base al quale è previsto che i dati siano trattati per finalità "*determinate, esplicite e legittime"* e con l'ulteriore previsione che gli stessi non possano essere utilizzati per scopi incompatibili con le finalità inizialmente individuate.

Con riferimento ai *Big Data,* il principio di limitazione delle finalità rischia di risultare di non facile e piena applicazione, data l'intrinseca difficoltà nei *Big Data* stessi di individuare, sin dalla fase iniziale, le finalità della raccolta e del trattamento dei dati.

Da ultimo, anche **il principio di esattezza** rischia di non essere pienamente applicato in realtà complesse quali i *Big Data*, proprio in virtù del fatto che in tali contesti le ingenti quantità di dati raccolti possono derivare da molteplici fonti, senza che sia possibile *ab origine* verificare l'esattezza dei dati raccolti.
Infine, lo stesso **consenso dei soggetti interessati** – individuato tra le basi giuridiche del trattamento – in ambito *Big Data* può dare luogo a criticità, in quanto riferito all'utilizzo di ingenti quantitativi di dati e al trattamento degli stessi per effetto di strumenti analitici automatizzati.

5. Considerazioni conclusive

Le osservazioni che precedono sono specificamente riferite alla realtà operativa delle imprese e, in particolare, all'utilizzo dei *Big Data* per esigenze di ottimizzazione del processo produttivo. Nella trattazione che precede, inoltre, per esigenze di sintesi, non si è tenuto conto delle ulteriori problematiche conseguenti alla pluralità dei soggetti che, in particolar modo nell'ambito dei *Big Data*, possono essere coinvolti nelle operazioni di raccolta e *Data Analysis*.
Certamente, con riferimento alla realtà delle imprese, il GDPR contiene utili prescrizioni e strumenti in grado di consentire ai titolari di orientarsi negli adempimenti per la protezione dei dati personali, ma data la complessità, specificità oltre che prevedibile estensione del fenomeno, sarebbero auspicabili interventi legislativi *ad hoc*, in modo da contribuire a fornire ai titolari un quadro normativo chiaro, adeguato e completo.

Letture consigliate

M. Rossi – M. Lombardi. *La Fabbrica Digitale – Guida all'Industria 4.0,* Tecniche Nuove, 2017;
Commissione UE, *Comunicazione "Digitalizzazione dell'industria europea – Cogliere appieno i vantaggi di un mercato unico digitale"*, (COM (2016)180 final;
Manuale sul diritto europeo in materia di protezione dei dati, edizione 2018 (in particolare, pp. 389 e ss.);
L. Bolognini, E. Pelino, C. Bistolfi, *Il Regolamento Privacy Europeo,* Giuffrè, 2016 (in particolare, pp. 50 e ss. e pp. 81 e ss.);
F. Pizzetti, *Intelligenza artificiale, protezione dei dati personali e regolazione,* Giappichelli, 2018;
R. Ducato, *La crisi della definizione di dato personale nell'era del web 3.0.,* in *Università degli Studi di Trento – Le definizioni nel diritto – Atti delle giornate di studio 30-31 ottobre 2015,* 2016;
I. M. Alagna, *Big Data e People Analytics: nuove sfide e opportunità per liberare valore,* in *Ciberspazio e diritto*, 2018, pp. 339 e ss.;
Council of Europe, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data,* 2017;
Parlamento Europeo, *Risoluzione del 14 marzo 2017 sulle implicazioni dei Big Data per i diritti fondamentali: privacy, protezione dei dati, non discriminazione, sicurezza e attività di contrasto;*
A. Soro, *Big Data e Libertà nella dimensione digitale,* 23 Agosto 2018;
AGCOM, *Big data – interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 217/17/CONS* – 2018;
Articolo 29 Gruppo di Lavoro per la protezione dei dati personali, *Parere 4/2007 sul concetto di dati personali* – 20 giugno 2007.

TAG: *big data, accountability, privacy*