UNIVERSITÀ DEGLI STUDI DI PAVIA

DIPARTIMENTO DI GIURISPRUDENZA

DOTTORATO DI RICERCA IN DIRITTO PRIVATO, DIRITTO ROMANO E CULTURA GIURIDICA EUROPEA
CURRICULUM PROPRIETÀ INTELLETTUALE E CONCORRENZA

LA CIRCOLAZIONE DEI DATI E L'ANALISI BIG DATA

RIFLESSIONI SUGLI ASPETTI RELATIVI ALLA PROTEZIONE DEI DATI PERSONALI, ALLA PROPRIETÀ INTELLETTUALE E ALLA CONCORRENZA

TUTOR

Chiar.mo Prof. Andrea Ottolia

Dissertazione di dottorato di

Giacomo Braschi

LA CIRCOLAZIONE DEI DATI E L'ANALISI BIG DATA

RIFLESSIONI SUGLI ASPETTI RELATIVI ALLA PROTEZIONE DEI DATI PERSONALI, ALLA PROPRIETA' INTELLETTUALE E ALLA CONCORRENZA

INDICE

Introduzione

CAPITOLO I

GLI STRUMENTI GIURIDICI PER LO STUDIO DEI DATI PERSONALI

1. Premesse: sulla circolazione e lo studio dei dati personali……18

2. Premesse sul rapporto tra analisi big data e statistica……26

3. Il trattamento dati a fini statistici……...39

4. La profilazione……...56

CAPITOLO II

GLI STRUMENTI GIURIDICI VOLTI A REGOLARE LA CIRCOLAZIONE DEI DATI.

1. La duplice tutela delle banche di dati……..66

2. Banche dati e privacy …….....77

3. Il segreto industriale e il brevetto……84

4. Altre tecniche per regolare la circolazione dei dati……91

CAPITOLO TERZO

DIRITTO DI PROPRIETÀ O DIRITTO D'ACCESSO AI DATI

1. La configurabilità di un diritto di proprietà sui dati……97

2. Abuso di posizione dominante……103

3. (segue) Alcuni esempi di abuso di posizione dominante nell'utilizzo dei dati e correttivi per migliorare l'attuale assetto concorrenziale……112

Bibliografia

Introduzione

Il presente elaborato ha lo scopo di analizzare e ricostruire gli assetti normativi che caratterizzano la circolazione dei dati, con particolare attenzione alla tematica dei dati personali. Come si vedrà nel presente elaborato, big data è un termine estremamente ampio che può riferirsi sia a studi su dati personali che non personali. Quando nell'analisi vengono coinvolti dati personali è fondamentale che la normativa posta a protezione dei dati personali venga rispettata[1].

Nel nostro ordinamento l'attenzione alla protezione dei dati personali è abbastanza recente. Basti pensare che in Italia è Rodotà negli anni settanta che arriva a dare una definizione al diritto alla protezione dei dati personali, intendendolo come il diritto dell'individuo a controllare l'uso delle informazioni che lo riguardano[2], in altri termini il diritto dell'individuo all'autodeterminazione informativa. È con la diffusione dei primi computers ed elaboratori elettronici che incomincia a porsi il problema non solo della riservatezza, ma anche del controllo sulla circolazione dei dati personali, ossia il diritto alla protezione dei propri dati personali. Questo problema diventa poi particolarmente pressante ed importante negli anni 90 con l'avvento di internet e lo sviluppo delle tecnologie telematiche[3], è del 1995 la direttiva privacy che per la prima volta interviene ad armonizzare la materia all'interno della Comunità Europea, imponendo all'Italia l'adozione della legge n. 675 del 1996. La privacy acquisisce un ulteriore accezione, non vi è solo l'esigenza dell'individuo di escludere i terzi dalla conoscenza di vicende personali e familiari. Alla libertà negativa tipica della concezione riassumibile nella celebre frase "right to be let alone"[4] si affianca la libertà positiva

---

[1] Per un richiamo a porre attenzione alla normativa a protezione dei dati personali nell'effettuazione dell'analisi big data v. WP29, *Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU*, 16 settembre 2014, 1 ss..

[2] Sul punto v. RODOTÀ, *La "privacy" tra individuo e collettività*, in *Politica del diritto* 1974,545; T.M. UBERTAZZI, *Il diritto alla privacy, natura e funzione giuridiche*, CEDAM, Padova, 2004, 60 ss..

[3] V. T.M. UBERTAZZI, op. cit., 76 ss.. Per un approfondimento sul passaggio dalla riservatezza alla protezione dei dati personali v. PARDOLESI, *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, in PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Giuffrè, Milano, 2003. Per un ulteriore approfondimento sul diritto alla protezione dei dati personali v. FINOCCHIARO, *Privacy e protezione dei dati personali, Disciplina e strumenti operativi*, Zanichelli, Bologna, 2012, 1 ss..

[4] WARREN and BRANDEIS, *The right of privacy*, in *Harv. L. rev.*, 1890, 4. In Italia per il riconoscimento a livello giurisprudenziale del diritto alla riservatezza si deve attendere il 1975 con Cass., 27 maggio 1975, n. 2129, in *Mass. Giur. It.*, 1975,594.

dell'individuo di controllare il flusso delle informazioni personali che lo riguardano[5]. L'esigenza sempre maggiore di regolare la circolazione dei dati personali e la protezione degli interessati, dettata dall'enorme sviluppo tecnologico degli ultimi vent'anni, ha condotto il legislatore europeo ad innovare ulteriormente la materia con l'adozione del Regolamento europeo n. 679 del 2016, che è diventato effettivamente applicabile a partire dal 25 maggio 2018. L'intento unificatore perseguito tramite l'adozione del regolamento fa sì che alcune norme sebbene innovative nel contesto europeo non lo siano nel contesto italiano, dove il legislatore interno si era già mosso da tempo in tal senso[6]. L'elemento maggiormente significativo, che ha fatto da traino per tutte le novità presenti nel Regolamento europeo consiste nel cambio di approccio del legislatore con l'introduzione del principio di accountability. L'adozione di tale principio all'interno del GDPR impone al titolare del trattamento l'onere di rendicontare tutte le scelte fatte in tema di protezione dei dati personali. Il titolare deve tenere traccia scritta e motivata delle scelte fatte in modo da poter dimostrare il rispetto della normativa a protezione dei dati personali sia all'autorità di controllo che agli interessati. Si vuole responsabilizzare il titolare alleggerendo il carico di notifiche a cui l'autorità di controllo era sottoposta [7]. Di seguito si riportano brevemente le principali novità introdotte dal regolamento europeo che influiscono sulla circolazione dei dati, sulle possibilità dell'analisi big data e sul costo di tale tipo di studio per le imprese[8].

Ambito di applicazione territoriale	A differenza della direttiva il nuovo Regolamento deve essere rispettato anche da quelle imprese che non risiedono nell'Unione Europea, ma offrendo beni o prestando servizi trattano dati personali di soggetti che

[5] FINOCCHIARO, *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, in FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017, 5 ss..

[6] Si pensi ad esempio alle norme del regolamento sul consenso che prevedono che questo sia libero, esplicito e specifico, erano requisiti già previsti dal codice privacy (sul punto v. FINOCCHIARO, *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, cit., 10).

[7] V. WP29, Parere n. 3 del 2010, sul principio di responsabilità, 1 ss..

[8] L'intento dell'inserimento di tale sintesi è quello di facilitare il lettore nella comprensione dell'elaborato evitando che nuovi termini imposti dalla recente normativa possano far trascurare alcuni delicati ed importanti passaggi dell'elaborato.

	risiedono nell'UE[9]. In forza di questa norma, in parte anticipata dalla Corte di Giustizia con la sentenza Schrems[10], anche i grandi colossi del web quale Facebook, Google e Amazon devono rispettare la nuova normativa
L'interesse legittimo	La verifica sulla sussistenza del legittimo interesse non spetta più all'Autorità di controllo, ma proprio in virtù del principio di accountability, al titolare del trattamento. Questa disposizione, come si vedrà meglio nel primo capitolo, sembra non essere stata seguita dal legislatore interno[11].
Ulteriori precisazioni nell'informativa	L'art. 13 e l'art. 14, che dettano il contenuto dell'informativa privacy, hanno un contenuto diverso e ulteriore rispetto a quanto stabilito dal codice privacy. In particolare occorre indicare i dati di contatto del DPO, la base giuridica del trattamento, i destinatari a cui sono comunicati i dati, il periodo di conservazione degli stessi, il diritto di presentare reclamo all'autorità di controllo competente ecc.. Inoltre è previsto che nell'ipotesi in cui si ponga in essere una profilazione nell'informativa deve essere spiegata in modo chiaro e conciso la logica sottesa a tale trattamento[12].
Diritti degli interessati	Il termine per rispondere alle richieste degli interessati è stato esteso fino ad un mese dalla ricezione della richiesta,

[9] V. art. 3 del GDPR.

[10] CGUE, 6 ottobre 2015, C-362/14, Schrems contro Data Protection Commissioner, in www.curia.europa.eu. Per un approfondimento FINOCCHIARO, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*, in RESTA e ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali, dai "Safe Harbour principles" al "Privacy Shields"*, RomaTrE Press, Roma, 2017, passim.

[11] V. infra cap. 1 par. 2. Mentre si scrive si attende la pubblicazione in gazzetta del decreto attuativo del GDPR che potrebbe sovvertire quanto qui di seguito riportato sul legittimo interesse.

[12] Sul punto v. Garante per la protezione dei dati personali, *Guida all'applicazione del Regolamento UE 2016 679*, in www.garanteprivacy.it/regolamentoue/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali, 8 ss.

	e nel caso vi siano particolari complessità il termine è estendibile fino a 3 mesi[13]. Sono stati previsti anche diritti ulteriori e di alcuni ne è stata modificata in modo significativo la portata[14].
Diritto alla cancellazione dei dati	Tale diritto ha una portata più ampia, essendoci l'onere del titolare di informare anche altri titolari della ricezione di tale istanza[15].
Diritto alla portabilità dei dati	È un nuovo istituto che permette all'interessato i cui dati sono oggetto di un trattamento automatizzato dietro suo consenso o per l'esecuzione di un contratto di trasferire i suoi dati personali ad un altro titolare[16]. Tale diritto è stato introdotto innanzitutto con l'intento di permettere all'interessato un maggiore controllo sulla circolazione dei dati personali. Inoltre viene perseguita anche la finalità di favorire la concorrenza tra le imprese e di permettere con maggiore facilità agli utenti di cambiare il fornitore del servizio di cui usufruiscono.
Privacy by design e privacy by default	La privacy by design impone al titolare del trattamento di tenere in considerazione l'aspetto relativo alla protezione dei dati personali fin dall'ideazione e progettazione di un trattamento in modo da garantire che siano trattati solo i dati personali strettamente necessari e siano rispettati i principi posti dalla normativa privacy[17]. La privacy by default impone al titolare la configurazione degli strumenti preposti al trattamento in modo che trattino per impostazione predefinita solo i dati personali necessari per ogni specifica finalità del trattamento[18].

[13] V. Garante per la protezione dei dati personali, *Guida all'applicazione del Regolamento UE 2016 679*, cit., 12.
[14] V. art. 15 e seguenti del GDPR
[15] V. Garante per la protezione dei dati personali, *Guida all'applicazione del Regolamento UE 2016 679*, cit., 16
[16] V. art. 20 del GDPR, v. Garante per la protezione dei dati personali, *Guida all'applicazione del Regolamento UE 2016 679*, cit., 8. Sul punto v. anche infra par. 4 cap. 2 e par. 3 cap. 3.
[17] V. art. 25 par. 1 GDPR.
[18] V. art. 25 par. 2 GDPR

	Entrambi questi strumenti sono stati introdotti per via della notevole inefficacia dell'informativa privacy e dell'eventuale richiesta di consenso. In molti casi l'interessato non è consapevole del trattamento cui sono stati sottoposti i suoi dati, perché non presta piena attenzione al testo dell'informativa o alla richiesta di consenso. Si è deciso così di spostare la tutela ex ante nell'impostazione e prefigurazione dei trattamenti, in considerazione dell'incapacità frequente degli interessati di proteggere da soli il proprio diritto alla protezione dei dati personali[19]. Quest'impostazione è dovuta anche alla sempre maggior diffusione di trattamenti di dati personali a cui ciascuna persona più o meno consapevolmente è sottoposta ogni giorno.
Responsabile del trattamento	L'art. 28 del GDPR prevede che il titolare nell'atto di nomina del responsabile inserisca istruzioni su determinate materie: natura, durata, categorie di dati trattati, misure tecniche e organizzative adeguate per rispettare il GDPR, finalità del trattamento. Inoltre è stata introdotta la figura del sub-responsabile del trattamento, con l'obbligo del responsabile di vincolare il suo sub responsabile al rispetto degli stessi oneri a lui imposti dal titolare. Qualora il sub-responsabile ponga in essere delle violazioni della normativa, nei confronti del titolare ne risponderà il responsabile che potrà rifarsi sul sub-responsabile. Il legislatore vuole imporre al titolare di controllare il flusso dei dati per l'esecuzione dei propri servizi.
Registro del trattamento	Tutti i titolari del trattamento con più di 250 dipendenti o che effettuino trattamenti che comportino un particolare rischio o che trattino dati rientranti negli elenchi di cui agli

[19] Sul punto v. D'ACQUISTO e NALDI, *Big Data e Privacy By Design, Anonimizzazione Pseudonimizzazione Sicurezza*, Giappichelli, Torino, 2017, 33 ss,,

	artt. 9 e 10 del GDPR devono procedere a redigere e a tenere aggiornati degli appositi registri che mappino tutti i trattamenti posti in essere sui dati personali[20].
Misure di sicurezza	Non sono previste misure minime di sicurezza da adottare in ogni caso, ma in ottica di accountability deve essere il titolare ad operare la scelta sulle misure di sicurezza adeguate al rischio posto in essere dal trattamento e motivare la sua scelta. A tal fine l'art. 32 del GDPR contiene una lista di possibili misure da implementare, tale elenco è da considerarsi non esaustivo[21].
Data breach	È prevista un'apposita procedura in caso si verifichi una violazione dei dati personali. In particolare il titolare dovrà notificare all'autorità di controllo, se vi è un rischio per gli interessati, entro 72 ore, l'avvenuta violazione. Tramite tale notifica il titolare rende edotto il Garante delle principali caratteristiche della violazione, dei rimedi che si stanno attuando e dei possibili rischi per gli interessati. Se tale violazione comporta rischi notevoli per gli interessati, il titolare dovrà avvisare anche questi ultimi senza ingiustificato ritardo[22].
Valutazione di impatto	La Valutazione di impatto è un procedimento volto a descrivere il trattamento in modo da valutare al meglio i rischi e decidere come gestirli. Tale procedimento deve essere posto in essere per quei trattamenti particolarmente invasivi e rischiosi per gli interessati quali ad esempio alcuni tipi di profilazione, i monitoraggi regolari e sistematici ecc.. Tale tipo di obbligo che ricorre in modo

[20] Sul punto v. WP29, *Position Paper on the derogations from the obligation to maintain record of processing activities pursuant to Article 30 GDPR*, 1 ss..
[21] V. Garante per la protezione dei dati personali, *Guida all'applicazione del Regolamento UE 2016 679*, cit., 27.
[22] Sul punto v. WP29, *Guidelines on personal data breach notification under Regulation 2016/679*, 6 febbraio 2018, 1 ss..

	frequente laddove si ponga in essere un analisi big data sui dati personali rappresenta un ulteriore onere e costo a carico delle imprese[23].
Responsabile per la protezione dei dati (DPO)	Per alcune imprese che pongono in essere trattamenti particolarmente invasivi è fatto obbligo di nominare un Responsabile per la protezione dei dati (DPO), questa figura ha la funzione di vigilare all'interno della società sul rispetto della normativa a protezione dei dati personali e di fungere da punto di contatto per l'Autorità di controllo e gli interessati[24]. Tale figura può essere adottata anche da imprese, in via facoltativa, che non rientrano nelle ipotesi previste dall'art. 37 del GDPR. È chiaro che l'inserimento di tale figura rappresenta un costo ulteriore per le imprese che trattano dati personali.
Introduzione meccanismi di certificazione	Per dimostrare la conformità al regolamento UE un'impresa potrà aderire anche alle certificazioni posti in essere dagli appositi organismi o a codici di condotta, così vi sarà una presunzione relativa di conformità alla normativa privacy[25].
Trasferimento extra UE dei dati personali	Il trasferimento di dati personali al di fuori dell'Unione Europea può avvenire solo in presenza di una decisione di adeguatezza della Commissione europea, dell'adozione di clausole standard elaborate dalla Commissione, oppure nell'ipotesi di trasferimenti infra-gruppo dell'adozione di norme vincolanti di impresa[26].
Fori competenti	L'interessato ha diritto di presentare reclamo dinnanzi

[23] Per un approfondimento sul punto v. WP29, *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato ai fini del regolamento (UE) 2016/679*, 4 ottobre 2017, 1 ss..
[24] FINOCCHIARO, *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, cit., 18.
[25] V. artt. 42 e 43 GDPR.
[26] Sul punto v. infra par. 4 cap. 2

	all'autorità di controllo in cui risiede, lavora o in cui si è verificato l'illecito[27].
Sanzioni	È stato previsto un severo inasprimento del tetto massimo della sanzione, che non viene determinato più in termini assoluti ma percentuali, fino al 4% del fatturato mondiale annuo della società[28]. Il rispetto della protezione dei dati personali diventa di importanza precipua dato l'enorme impatto che una sanzione potrebbe avere sul bilancio di un'impresa.

Nel primo capitolo, focalizzo inizialmente l'attenzione sull'importanza dei dati nel contesto economico e tecnologico odierno. In particolare mi soffermo brevemente sulle caratteristiche di questo tipo di economia sottolineando l'importanza, per uno sviluppo ottimale della stessa, della circolazione delle informazioni. Le imprese necessitano di studiare dati provenienti non da compartimenti stagni ma da fonti eterogenee. Tuttavia, come in parte già anticipato, nel caso dei dati personali vi sono diversi limiti posti dalla normativa a protezione dei dati personali. Per comprendere che spazio sia lasciato alle imprese in tale ambito mi soffermo sul concetto di dato personale (partendo dalla distinzione tra livello sintattico e semantico) per poi illustrare l'ambito di applicazione materiale della normativa a protezione dei dati personali. Una volta illustrati i limiti imposti dall'ordinamento introduco il concetto di analisi big data evidenziando i vantaggi e gli svantaggi e soffermandomi sul concetto di big data. Per definire il termine big data solitamente si utilizza il paradigma delle quattro V (Volume, Velocità, Varietà, Veridicità). Volume inteso nel senso di quantità di dati generati che è sempre crescente. Velocità nel senso di continuità nella generazione dei dati, i dati vengono continuamente generati raccolti e analizzati in un contesto fortemente dinamico. Varietà intesa nel senso di eterogeneità delle fonti di provenienza degli stessi, caratteristica imprescindibile dell'analisi big data è lo studio di dati generati da fenomeni diversi per trovare correlazioni. Veridicità nel senso di qualità dei dati, molto spesso questo elemento viene meno perché l'incremento dei dati comporta una maggiore imprecisione

[27] V. art. 77 GDPR. Sulle conseguenze possibili di tale flessibilità di competenza territoriale si rimanda infra al par. 3 cap. 1.
[28] V. art. 83 e 84 GDPR

e una minore qualità dei dati[29]. L'analisi big data consiste nell'individuazione di correlazioni tra i descrittori estratti da ogni singolo dato in ottica predittiva. Se vi sono descrittori simili o comuni per dati diversi frequentemente significa che i singoli fenomeni a cui essi rimandano sono in qualche modo collegati[30].

Dopo aver contestualizzato lo scenario dei big data mi soffermo sui diritti fondamentali che, a mio avviso, sono tra di loro in contrasto in tale ambito: il diritto alla protezione dei dati personali e la libertà di impresa. Occorre individuare un equilibrio e per poterlo fare ho ritenuto estremamente utile ripercorre le principali tappe giurisprudenziali seguite in passato dalla Corte di Giustizia nell'effettuare bilanciamenti tra il diritto alla protezione dei dati personali e altri diritti fondamentali, riproponendo, brevemente, l'importante distinzione, elaborata dalla nostra dottrina, tra privacy nel sistema e privacy per il sistema. Alla luce di queste premesse nel secondo paragrafo del primo capitolo individuo i trattamenti (profilazione e trattamento a fini statistici) e le basi giuridiche (consenso e interesse legittimo) che possono essere utilizzate, a mio avviso, per effettuare l'analisi big data. Dopo questa prima individuazione mi soffermo sul trattamento ulteriore e compatibile per fini statistici, chiarendo che tale utilizzo dei dati, come specificato dal WP29, rientra nell'ipotesi in cui l'interesse legittimo è predeterminato per legge. Per verificare se nei fini statistici possa rientrare l'analisi big data realizzata dalle imprese per scopi commerciali mi propongo di indagare tale concetto e chiarire quali sono i soggetti (i.e. se solo pubblici o anche privati) che possono avvalersi della disciplina particolarmente agevole riservata a tale tipo di trattamento, che permette di riutilizzare dati raccolti per una determinata finalità per scopi statistici senza chiedere un ulteriore consenso all'interessato.

Preso atto che né la direttiva né il nuovo regolamento propongono una definizione del termine statistica, cerco di chiarire il significato partendo da una breve ricostruzione storica del concetto per poi agganciarmi ad alcuni riferimenti normativi utili che contengono una definizione di statistica. In particolare il riferimento normativo più

---

[29] Per un approfondimento sul concetto di big data, sull'origini di tale termine si rimanda a: D'ACQUISTO e NALDI, op. cit., 5 ss.; MAGGIOLINO, *I big data e il diritto antitrust*, Egea, Milano, 2018, 23 ss..

[30] Per un approfondimento sulle tecniche d'analisi e sui modi di utilizzo dei dati in una prospettiva big data v. D'ACQUISTO e NALDI, op. cit., 9 ss.; MAGGIOLINO, op. cit., 37 ss.. In tale campo si parla di correlazioni statistiche: più è elevato il numero di descrittori in comune e più sono i dati generati da diversi fenomeni con descrittori in comune e più è probabile che vi sia un collegamento tra due fenomeni. Vi sono diversi metodi per estrarre i descrittori e individuare le correlazioni: machine learning, hashing, trasformata di Fourier, classificazione semantica di un contenuto per parole chiave o mediante indicatori, crowdsourcing (v. D'ACQUISTO e NALDI, op. cit., 15 ss.).

significativo, a mio parere, è costituito dall'art. 1 dell'appendice alla Raccomandazione n. (97) 18 del CDE. Tale articolo pur essendo contenuto in un provvedimento di cd. "soft law" propone una definizione di trattamento a fini statistici che ritengono vincolante per diverse ragioni: i) in primis per il richiamo che l'art. 52 della Carta di Nizza fa del tessuto normativo della CEDU; ii) in secondo luogo perché la stessa nozione è stata riproposta nell'art. 3 del reg. CE n. 223/2009 relativo alle statistiche ufficiali europee. La definizione ricavata alla fine di questo percorso risulta essere sovrapponibile a quella comunemente proposta per l'analisi big data.

L'ultima parte del paragrafo è dedicata ad illustrare le ragioni per le quali ritengo possibile che la disciplina di favore riservata al trattamento ulteriore e compatibile dei dati a fini statistici possa essere riservato non solo ai soggetti pubblici ma anche a quelli privati. Le argomentazioni poste a fondamento di tale tesi sono le seguenti: i) adozione nel reg. CE n. 223/2009 da parte del legislatore di una definizione lessicale e non stipulativa; ii) il fatto che la direttiva e il regolamento sulla protezione dei dati personali effettuano nei considerandi delle specificazioni quando si riferiscono alle statistiche ufficiali, distinguendole dal trattamento statistico in generale; iii) infine il fatto che due Raccomandazioni del CDE dettino espressamente dei principi applicabili al trattamento dei dati personali a fini statistici validi sia per il settore pubblico che per il settore privato. Nel terzo paragrafo mi soffermo sull'evoluzione normativa che ha caratterizzato la disciplina del trattamento dei dati a fini statistici a partire dal primo e unico atto internazionale giuridicamente vincolante che disciplina tale utilizzo dei dati: la Convenzione n. 108 del 1981 adottata dal Consiglio d'Europa, integrata successivamente con due Raccomandazioni una del 1983 e una del 1997. La Convenzione ha gettato le basi per la direttiva del 1995, chiarendo che l'ulteriore trattamento a fini statistici è considerato compatibile solo se vengono prese adeguate garanzie finalizzate ad impedire che tali dati siano utilizzati per decisioni che abbiano effetti nei confronti dell'interessato. Nella seconda parte del paragrafo mi soffermo quindi sulla disciplina all'interno della direttiva e sull'agganciamento del trattamento ulteriore a fini statistici al principio di limitazione delle finalità, chiarendo il concetto di incompatibilità e soffermandomi sulla nozione di separazione funzionale. Il rispetto della separazione funzionale è un requisito imprescindibile per poter garantire la conformità con il principio di limitazione delle finalità. Sul punto il WP29 ha chiarito che per assicurare la separazione funzionale si deve ricorrere alternativamente:

all'anonimizzazione, alla pseudonimizzazione, e quando queste non sono possibili occorre applicare altre misure individuate dai singoli stati membri[31]. Successivamente analizzo la disciplina nel codice privacy evidenziando alcune specificazioni presenti rispetto alla direttiva e che il richiamo sopra detto alle misure individuate dai singoli stati membri è da intendersi all'interno del nostro ordinamento come riferimento all'articolo 31 codice privacy. Successivamente mi soffermo sul rapporto tra uso statistico dei dati e profilazione dimostrando come la prima possa essere strumentale alla seconda. Infine nell'ultima parte del paragrafo mi soffermo sulle novità introdotte dal regolamento europeo, chiarendo che sul punto resta ancora ferma la discrezionalità degli stati membri[32].

La spiegazione della disciplina presente in questo paragrafo è volta ad individuare il bilanciamento che, a mio modo di vedere, il legislatore ha effettuato in tale ambito tra il diritto alla protezione dei dati personali e la libertà di impresa: i dati personali possono essere oggetto di un trattamento ulteriore per fini statistici senza necessità di ricorrere ad un nuovo consenso da parte dell'interessato, da questo trattamento l'impresa può ricavare delle informazioni che, una volta anonimizzate, possono essere utilizzate per costruire un profilo che successivamente verrà applicato ad altri individui che hanno acconsentito alla profilazione. Nell'ultimo paragrafo, dopo aver dimostrato la strumentalità del trattamento ulteriore a fini statistici rispetto alla profilazione, mi soffermo su quest'ultima tipologia di trattamento, partendo dalla raccomandazione del Comitato dei Ministri del 2010 e illustrando poi come tale testo è stato accolto e disciplinato nel codice privacy e nel GDPR. L'obiettivo è stato quello di mostrare come si possa effettuare l'analisi big data avvalendosi della profilazione e quali garanzie sono state previste dal legislatore europeo a tutela delle persone fisiche, evidenziando quindi quale sia l'esito del bilanciamento tra il diritto alla protezione dei dati personali e la libertà di impresa. L'utilizzo dei dati personali per fini di profilazione implica sempre e comunque delle limitazioni pesanti per l'individuo e al contempo comporta un'utilità notevole per le imprese che possono sfruttare metodi quali la clusterizzazione per essere più competitivi, per cui è consentito tale utilizzo dei dati nel rispetto di severi limiti (ad

[31] WP29, Opinion 03/2013 *on purpose limitation.*

[32] Si tenga conto che questa parte è stata scritta quando ancora non era stato pubblicato in gazzetta ufficiale il decreto attuativo del GDPR, adottato l'8 agosto del 2018.

es. valutazione di impatto, notifica preventiva, consenso dell'interessato, obbligo di disclosoure ecc..).

Nel secondo capitolo verifico se all'interno dell'ordinamento vi sono degli strumenti giuridici che permettono di regolare la circolazione dei dati. A tal proposito nella mia ricerca ho individuato quattro possibili istituti già esistenti che contribuiscono a regolare il flusso dei dati e la loro circolazione: la tutela disposta per le banche dati, il segreto industriale, il brevetto e l'autonomia negoziale. Nel proseguo del testo mi soffermo quindi su ciascun singolo istituto stabilendo limiti e portata ai fini della regolazione della circolazione dei dati anche personali. Così nel primo paragrafo analizzo le caratteristiche della normativa relativa alle banche di dati per verificare se possa essere un utile strumento per controllare la circolazione dei dati. L'analisi sulla portata della disciplina relativa alle banche dati è dovuta anche al fatto che tali strumenti, con lo sviluppo digitale sono diventati sempre più importanti all'interno dell'impresa per conservare, archiviare e trasferire dati in modo rapido ed efficace[33]. Anche per questo motivo è di fondamentale importanza approfondire la portata e i limiti della disciplina sulle banche di dati così da comprendere se uno strumento con tale livello di diffusione all'interno delle imprese possa anche essere utile per controllare la circolazione dei dati.

All'inizio del primo paragrafo chiarisco la distinzione tra diritto d'autore sulla banca dati e diritto connesso del costitutore. Da un raffronto tra i due diritti risulta essere maggiormente adeguato, per le finalità sopra dette, quello attribuito al costitutore. La seconda parte del paragrafo è quindi dedicata ad esaminare i tre concetti chiave per comprendere la portata della disciplina sul diritto connesso del costitutore, ossia le nozioni di estrazione, rimpiego e parte sostanziale, arrivando a dimostrare come in ogni caso il singolo dato anche se di enorme valore non può essere tutelato. Infine l'ultima parte del paragrafo è dedicata a spiegare quale sia il vero oggetto di tutela della disciplina delle banche dati partendo dalla ricostruzione della nozione di investimento rilevante, inteso come quell'investimento notevole volto non all'ottenimento degli elementi da inserire all'interno della banca dati, ma alla predisposizione del materiale all'interno della stessa. Alla luce di queste considerazioni la tutela delle banche dati non sembra essere ottimale per regolare il flusso e la circolazione dei dati. Tuttavia nel secondo paragrafo analizzo la diversa situazione in cui le banche dati contengano dati

[33] Per un approfondimento sull'importanza delle banche dati per le imprese nel contesto tecnologico odierno v. MAGGIOLINO e MONTAGNANI, *Marketing e diritto*, Egea, Milano, 2009, 21 ss..

personali, mostrando come in questo caso il diritto alla protezione dei dati personali previsto a favore delle persone fisiche possa indirettamente essere un utile strumento di controllo della circolazione degli stessi da parte delle imprese. Il costitutore di banche di dati sulla base dell'informativa fornita all'interessato e sulla base della relativa richiesta di consenso (o ricorrendo ad altre basi giuridiche ove applicabili) potrà già decidere le strategie di utilizzo dei dati personali così ottenuti, consentendo o impedendo a monte il futuro utilizzo di quelle informazioni ad altri soggetti. Risulta così fondamentale progettare a monte il trattamento che si vuole realizzare per poter stabilire il regime a cui sottoporre i dati personali raccolti. Ovviamente questo è possibile entro certi limiti che analizzo nell'ultima parte del paragrafo. Questi limiti sono costituiti dai principi in materia di protezione dei dati personali e dai diritti dell'interessato. In particolare, a mio parere, in questo ambito rilevano i seguenti limiti: il principio di liceità, il principio di limitazione delle finalità, il principio di conservazione dei dati, il diritto alla portabilità dei dati e il diritto dell'interessato a ritirare in qualsiasi momento il suo consenso. Cosicché la normativa a protezione dei dati personali da limitazione e costo[34] potrebbe essere considerata un vantaggio competitivo per il titolare che adotta una strategia predeterminata al momento della raccolta.

Nel terzo paragrafo analizzo la disciplina riservata al segreto industriale per comprendere fino a che punto possa essere uno strumento utile per controllare la circolazione dei dati. In particolare mi soffermo sulle modifiche introdotte da d.lgs. del 2010 che ha cambiato in modo significativo la disciplina, segnando il passaggio da una tutela assoluta ad una tutela relativa. Ciò comporta diverse conseguenze, la principale e più importante per le caratteristiche del mondo big data è la seguente: se la fonte da cui sono ricavate le informazioni, come spesso avviene nel mondo dell'Internet of things e del digitale in genere, è "pubblica" nel senso che chiunque potenzialmente può accedere a tale fonte, di fatto una tutela relativa troverebbe uno spazio ristretto in tale ambito,

[34] Per un approfondimento sui costi della protezione dei dati personali a carico delle imprese v. MAGLIO, *Il valore economico dei dati personali: spunti per un'analisi economica della data protection*, in MAGLIO POLLINI e TIGLI (a cura di), *Manuale di diritto alla protezione dei dati personali, La privacy dopo il Regolamento UE 2016/679*, Maggioli Editore, Milano, 2017, 88 ss.. L'autore individua i costi sopportati dalle imprese in materia di privacy distinguendo tra costi di prevenzione e correzione. I primi sono volti a prevenire la violazione dei dati personali e comportano: la disposizione di apposite risorse interne che devono essere impiegate per la gestione dei dati personali; la formazione del personale, controlli interni, la predisposizione di istruzioni interne e policy aziendali, il ricorso a consulenze esterne ecc…Mentre per quanto riguarda i costi di correzione sono principalmente quelli legati alle sanzioni, al risarcimento dei danni, ai danni di immagine della società ecc…

anche se come spiego in questo paragrafo il segreto industriale ben si può prestare per tutelare anche singoli dati o informazioni. Tuttavia il segreto industriale risulta essere uno strumento di difficile utilizzo per controllare alcuni dati come quelli ricavabili dall'Internet delle cose. Inoltre all'interno di questo paragrafo constato come il segreto industriale risulti essere di difficile utilizzo per cedere o licenziare ad altri dati personali, perché acquistare o avere in licenza dati personali implica l'adozione in capo al cessionario o al licenziatario una serie di responsabilità che lo pongono nella condizione di dover effettuare una serie di accertamenti per verificare il rispetto da controparte della normativa posta a protezione dei dati personali. Successivamente dedico l'ultima parte del paragrafo all'analisi della normativa sui brevetti, soffermandomi sul brevetto di procedimento e illustrando che la tutela prevista dal legislatore è indiretta e di difficile applicazione per i dati e per questo motivo non può essere considerata la soluzione ottimale di cui avvalersi per regolare la circolazione dei dati.

Nell'ultimo paragrafo del secondo capitolo mi soffermo gli strumenti negoziali a disposizione dei privati per regolare la circolazione dei dati, dedicando una parte significativa del paragrafo agli strumenti a disposizione delle imprese per condividere patrimoni di dati personali e alle misure da adottare nei confronti degli interessati.

Nel terzo capitolo mi interrogo sulla possibilità di configurare un diritto di proprietà sui dati in capo ai loro detentori e un diritto d'accesso ai dati da parte delle imprese concorrenti. In particolare nel primo paragrafo affronto la possibilità di configurare il diritto di proprietà sui dati nel senso civilistico del termine. In questa prima analisi emergono tuttavia aspetti insormontabili tali per cui non risulta possibile tale configurazione. Per questo motivo nella seconda parte del paragrafo mi soffermo, in una prospettiva de iure condendo, sulla possibilità di introdurre un diritto di proprietà intellettuale sui dati. Per poter trattare questo secondo tema riporto una breve analisi economica sul valore dei dati, così da permettere di comprendere se l'introduzione di un diritto di proprietà intellettuale sui dati sia auspicabile dal punto di vista del corretto funzionamento del mercato, rilevando che anche in questo caso vi sono difficoltà notevoli per procedere in tal senso. Dopo aver dimostrato come non sia configurabile o introducibile in una prospettiva de iure condendo un diritto di proprietà sui dati, nel secondo paragrafo mi interrogo sulla esistenza di un regime d'accesso. La premessa fondamentale per poter configurare un regime d'accesso è l'esistenza di una posizione dominante. Per questo motivo analizzo tale ultimo concetto soffermandomi

sull'essential facility doctrine applicata dalla Corte di Giustizia in materia di proprietà intellettuale. L'obiettivo finale è quello di poter applicare il test elaborato dalla Corte di Giustizia ai patrimoni informativi. Successivamente nel terzo paragrafo mi soffermo sulle peculiarità di alcuni settori fortemente caratterizzati dall'utilizzo dei dati, quali quello dell'Internet of things, ed in cui è maggiormente probabile che si verifichino abusi di posizione dominante e in cui si può ricorrere all'essential facility doctrine. Dopo aver analizzato questi settori propongo una possibile soluzione fatta propria da un recente orientamento dottrinale, in parte seguito dalla Commissione Europea nella comunicazione del 10 gennaio 2017, che propone di ricorrere alle condizioni FRAND. Tuttavia nell'ultima parte sottolineo che l'accesso a condizioni FRAND non è sufficiente e vi è un ulteriore onere in capo alle imprese che ricoprono una posizione dominante sul mercato: ossia il dovere di fornire i dati in modo da permettere alle imprese concorrenti l'esercizio effettivo dell'attività economica sul mercato[35].

[35] Per i precedenti giurisprudenziali in tal senso v. infra par. 3 cap. 3.

CAPITOLO PRIMO

GLI STRUMENTI GIURIDICI PER LO STUDIO DEI DATI PERSONALI

Sommario: 1. Premesse: sulla circolazione e lo studio dei dati personali. - 2. Premesse sul rapporto tra analisi big data e statistica. - 3. Il trattamento dati a fini statistici. – 4. La profilazione.

1. Il contesto economico e tecnologico odierno è caratterizzato, grazie anche alla sempre maggiore diffusione dell'Internet delle cose[36], dalla produzione ed utilizzo di quantità sempre maggiori di dati ricavati da macchine o da altri processi tecnologici. L'utilizzo di dati è alla base dell'emersione di nuovi servizi, nuovi prodotti e nuovi processi produttivi, risulta così che gli operatori del mercato sono sempre più attratti dallo studio ed utilizzo di questi per le ampie opportunità offerte dalle loro svariate applicazioni. Si è venuto ad instaurare un circolo virtuoso (o vizioso[37]) per cui le imprese utilizzano i dati, che raccolgono o producono a vario titolo, per produrre innovazioni che a loro volta generano dati che sono strumentali allo sviluppo e alla scoperta di altre tecnologie. In altri termini: «data is the new oil»[38].

L'importanza dei dati nell'economia odierna è dovuta in gran parte alla diffusione del cd. «Internet delle cose» (IoT). Con tale termine si intendono le «cose intelligenti» che monitorano e comunicano con le nostre case, auto, ambienti di lavoro ecc... Più precisamente il concetto di Internet delle cose (IoT) si riferisce ad un'infrastruttura in cui miliardi di sensori incorporati ad oggetti di uso quotidiano registrano, elaborano, memorizzano e trasferiscono dati in tempo reale e, interagiscono con altri dispositivi o

[36] Per un approfondimento sul tema v. MORO VISCONTI, *Internet delle cose networks e plus valore di connettività*, in *IDI* 2016, 536 ss; CODIGLIONE, *I dati personali come corrispettivo della fruizione di un servizio di comunicazione elettronica e la "consumerizzazione" della privacy*, in *Dir. Inf.* 2017, n. 2, 418 ss..

[37] MAGGIOLINO, op. cit., 194.

[38] V. Commissione Europea, 10 gennaio 2017, *Comunicazione: costruire un'economia dei dati europea*, 9; BANTERLE, *Brevi cenni sulla titolarità dei dati comportamentali nei big data tra privacy e proprietà intellettuale*, in *AIDA* 2016, 579; Vice Commissario REDING, "P*ersonal data is the currency of today's digital market*", in *The EU Data Protection Reform* 2012: *Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age* – Innovation Conference Digital, Life, Design, Monaco, 22 gennaio 2012; MENEGHETTI, *Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali*, in FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e la protezione dei dati personali*, Zanichelli, Bologna, 2017, 427.

sistemi che utilizzano le funzionalità di networking[39]. Le imprese che si avvalgono di questa tecnologia mirano così ad offrire nuove applicazioni e servizi. Infatti, attraverso la raccolta e l'ulteriore combinazione di questi dati, esse riescono ad osservare e analizzare le abitudini degli utenti. Tramite i sensori su questi oggetti i dati vengono raccolti e per mezzo di una connessione a internet trasmessi in cloud dove vengono archiviati, una volta raccolti in questi database vengono studiati attraverso tecniche di data mining e processing che permettono di estrapolare informazioni e conoscenze utili alle imprese per le loro strategie aziendali[40].

Per comprendere meglio questo fenomeno si propone una breve descrizione delle tre tipologie di dispositivi che, tra quelle comunemente in uso degli utenti consumatori, sono maggiormente utilizzate in tale ambito: «wearable computing»; «quantified self»; «domotics». La prima tipologia si riferisce a tutti quegli oggetti che sono indossati dai consumatori ogni giorno, come ad esempio gli occhiali o gli orologi. Questi sono spesso dotati di sensori quali microfoni, videocamere e altri sensori che registrano e raccolgono una notevole quantità di dati che trasferiscono su un opportuno database, al quale, grazie a particolari applicazioni, possono accedere anche soggetti terzi. Le cose per la valutazione auto-quantificata sono progettate per essere regolarmente trasportate da persone che vogliono registrare informazioni sulle proprie abitudini e stili di vita. Ad esempio, un individuo può indossare un «sleep tracker» per monitorare il sonno. Altri dispositivi si concentrano sul costante controllo dei movimenti, come contatori di attività fisica che misurano e segnalano tramite indicatori quantitativi le calorie bruciate o le distanze percorse a piedi. Alcuni oggetti misurano il peso, l'impulso e altri indicatori di salute. Il produttore o il fornitore di servizi possono avere accesso ai dati raccolti, che possono così analizzare per inferire informazioni relative alle condizioni di salute dell'individuo e l'eventuale interesse per taluni particolari tipi di sport. Con il termine domotica ci si riferisce a tutti quei dispositivi IoT che possono anche essere collocati in uffici o in case. Così ad esempio si pensi alle lampadine «connesse», ai termostati, agli allarmi di fumo collegati alla caserma dei pompieri, alle stazioni

[39] V. WP29, Opinion 8/2014 on the Recent Developments on the Internet of Things, 3 ss.. I principali ambiti interessati dall'IoT sono: «domotica; robotica; avionica; industria automobilistica; biomedicale; monitoraggio in ambito industriale; intelligenza ambientale; telemetria; reti wireless di sensori; sorveglianza; rilevazioni di eventi avversi; smart grid, smart metering e cyber security; smart home e smart city; sistemi embedded; telematica»(MORO VISCONTI, *Internet delle cose, Networks e plusvalore della connettività*, cit., 536 e 537).

[40] V. MORO VISCONTI, *Internet delle cose, Networks e plus valore della connettività*, cit. , 536 ss..

meteo, oppure si pensi alle lavatrici o ai forni controllabili in remoto su Internet. La maggior parte dei dispositivi di domotica sono costantemente collegati e possono trasmettere i dati al produttore.

Ovviamente la suddivisione in queste tre tipologie è meramente esemplificativa, potendoci essere oggetti che presentino caratteristiche inerenti a più categorie come ad esempio un orologio che registra e monitora i passi e l'attività fisica svolta quotidianamente da un individuo[41].

Affinché sia possibile sfruttare al meglio i dati è necessario che le imprese accedano ad insiemi di dati provenienti da fonti eterogenee. Questi ultimi non devono essere utilizzati e studiati in compartimenti stagni. Per questo motivo è di vitale importanza chiarire quale sia il regime ottimale di circolazione di queste informazioni che, come appena rilevato, sono alla base dell'emersione di questo nuovo tipo di economia[42].

Uno dei principali limiti alla circolazione dei dati è costituito dalla normativa relativa alla protezione dei dati personali che disciplina e limita la commercializzazione degli stessi, introducendo numerosi ostacoli alla possibilità di incrociare i dati provenienti da diverse fonti. La suddetta normativa si applica esclusivamente ai dati personali. Per comprendere e definire il concetto di dato è importante distinguere tra due livelli: quello sintattico e quello semantico. Il primo riguarda la rappresentazione del dato, il secondo il significato. Per poter capire meglio questa distinzione si consideri ad esempio le riprese delle telecamere fisse in una piazza pubblica: il video in se e per se rappresenta il livello sintattico del dato mentre ad esempio l'informazione relativa a quante macchine passano al giorno in quella piazza è il livello semantico[43].

---

[41] Per un approfondimento su tale tema v. WP29, Opinion 8/2014, 3 ss.; MORO VISCONTI, *Internet delle cose, Networks e plusvalore della connettività*, cit., 536 ss..

[42] Per capire a pieno l'utilità e l'importanza dei dati nel contesto economico odierno si riportano alcuni dati presi dalla comunicazione della Commissione Europea del 10 gennaio 2017 sopra citata: «Il valore dell'economia dei dati nell'UE è stato stimato a 257 miliardi di euro nel 2014, pari all'1,85% del PIL dell'UE, passati a 272 miliardi di euro nel 2015, ossia all'1,87% del PIL dell'UE (per un incremento annuo del 5,6%). La stessa stima prevede che, istituendo per tempo un assetto programmatico e giuridico per l'economia dei dati, il suo valore potrà raggiungere i 643 miliardi di euro nel 2020, pari al 3,17% del PIL complessivo dell'UE». Secondo altre fonti: Il mercato dei dati è sempre in continua crescita dal 2014 al 2015 c'è stato un incremento del suo valore di ben 7 miliardi di euro. Secondo le più recenti previsioni tale crescità non sta rallentando e dovrebbe arrivare nel 2020 ad un valore pari a 84 miliardi di euro, con la creazione di ben tre milioni di posti di lavoro (MENEGHETTI,ibidem*; European Data Market Study, Second Interim Report*, Giugno 2016, in *www.datalandscape.eu/study-reports*).

[43] V. DREXL, *Designing competitive markets. For industrial data, between propertisation and access,*in *Max Planck Institute for innovation and competition research paper*, 2016, 12; ZECH, *Data as tradeable commodity*, in *European contract law and the digital single market*, DE FRANCESCHI (a cura di), Intersentia, 2016, 53 ss..

Come chiarito dal WP29 nel parere 4/2007 sul concetto di dato personale il livello a cui fare riferimento per l'applicazione della disciplina posta a protezione dei dati personali è quello semantico, se così non fosse verrebbe meno il requisito della riconducibilità di un'informazione a un determinato individuo, poiché per «dati personali» si intende ogni informazione relativa ad una persona fisica identificata o identificabile[44]. È inevitabile doversi riferire al significato del dato e non alla sua mera rappresentazione, se si guardasse solo al formato in cui circola il dato ossia al suo contenitore, sarebbe impossibile utilizzare questa informazione per identificare anche indirettamente una persona fisica.

Per poter qualificare un dato come personale e quindi per comprendere se un individuo è identificabile devono essere tenuti in considerazione tutti i mezzi ragionevolmente a disposizione del titolare del trattamento o di un eventuale terzo che permettano l'identificazione, diretta o indiretta, della persona fisica. Il termine ragionevolmente deve essere parametrato su elementi oggettivi, come precisato dal considerando 26 della dir. 95/46/CE e del GDPR. I fattori principali a cui occorre far riferimento per stabilire l'identificabilità variano a seconda dell'utilizzo specifico dei dati. In linea generale per stabilire l'applicazione della disciplina in esame si dovrà tenere in considerazione: i costi dell'identificazione, le finalità del trattamento, la durata dello stesso, lo stato dell'arte della tecnologia al momento in cui i dati devono essere trattati e l'eventuale sviluppo tecnologico durante il periodo in cui gli stessi saranno utilizzati[45]. In estrema

---

[44] Cfr. l'art. 4 n. 1 del GDPR: «dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale». V. anche l'art. 2 lett. a) della dir. 95/46/CE. In questo senso v. DREXL, op. cit., 12 ss.; WP29, parere 4/2007 sul concetto di dato personale, 6. Qualsiasi informazione che riconduca indirettamente ad un determinato individuo è considerata dato personale, così rientrano in questa categoria dati che ad un primo impatto potrebbero non sembrare informazioni riconducibili ad una persona fisica o che permettano di identificare un individuo, come ad esempio l'indirizzo IP. In questo esempio l'identificazione non è diretta ma indiretta infatti è necessario avvalersi dei fornitori di accesso alla rete (sul punto v. Garante per la protezione dei dati personali, parere n. 1/2008, 9 ss.; OTTOLIA, *Big data e innovazione computazionale*, Giappichelli, Torino, 2018, 94 nota 6).

[45] Cfr. WP29, parere n. 4/2007 sul concetto di dato personale, 13 ss.. In questo parere il Gruppo di lavoro ex art. 29 analizza la definizione di «dati personali" secondo la direttiva 95/46/CE. La definizione fornita dalla direttiva si articola su 4 principali elementi: «qualsiasi informazione»; «concernente»; «persona fisica», «identificata o identificabile». Il gruppo di lavoro chiarisce che per qualsiasi informazione si può intendere qualsiasi tipo di affermazione su una persona, sia essa oggettiva o soggettiva, non importa se veritiera e quale sia il formato dell'informazione o del supporto. Come ricavabile anche dai precedenti giurisprudenziali,(si veda CEDU, 16 febbraio 2000, causa Amann/Switzerland e CGCE, 6 novembre 2003, C- 101/2001, Lindqvist), la direttiva adotta un approccio di definizione ampio. Per quanto riguarda il secondo elemento chiave il WP29 chiarisce che un dato concerne una persona fisica quando la riguarda,

sintesi, il legislatore, per i motivi evidenziati nel proseguo della trattazione, ha introdotto la normativa sulla protezione dei dati personali per limitare la commercializzazione dei dati personali, impedendo tendenzialmente alle imprese che li raccolgono di comunicarli a terzi senza prima averli aggregati e anonimizzati[46]. Infatti dopo che è stato anonimizzato il dato non è più sottoposto ai limiti della suddetta normativa. Gran parte della dottrina tuttavia avanza diversi dubbi sulla possibilità di anonimizzare efficacemente un dato, perché nell'attuale scenario è facile reperire quantità enormi di dati provenienti da fonti eterogenee, che utilizzati congiuntamente permettono l'identificazione del soggetto a cui l'informazione si riferisce, i dubbi riguardano soprattutto l'utilizzo delle informazioni raccolte in rete[47].

Fatte queste premesse sull'importanza della normativa posta a protezione dei dati personali, occorre indagare l'ambito di applicazione di tale disciplina in modo da poter comprendere a pieno che spazio di utilizzo di tali informazioni sia ad oggi riservato alle imprese.

Resta da precisare che la normativa sulla data protection non costituisce più un limite per i dati che permettano di identificare direttamente o indirettamente una persona giuridica o un ente. Infatti la direttiva 95/46/CE, pur rivolgendosi esclusivamente alle persone fisiche, lasciava agli stati membri la facoltà di estendere la disciplina relativa alla privacy anche alle persone giuridiche. Il legislatore interno, in controtendenza rispetto alla maggior parte degli altri ordinamenti europei, sia nel 1996 che nel 2003 estendeva l'applicazione delle norme in materia di privacy anche alle persone giuridiche. Nel 2011 con il decreto legge n. 201 convertito con legge n. 214/2011 il legislatore italiano limitava la portata di tutte le disposizioni del Codice privacy che riguardavano gli interessati e il trattamento di dati personali alle persone fisiche. In particolare sono stati modificati l'art. 4 relativo alle definizioni, l'art. 5 sull'oggetto e

---

e a tal proposito sono distinguibili tre tipi di relazioni: di contenuto, di finalità, di risultato. Il terzo elemento chiave è determinabile alla luce della situazione specifica in cui è posto in essere il trattamento. Come già chiarito nel testo, per stabilire se una persona è identificabile si dovranno tenere in considerazione tutti i mezzi che possono essere ragionevolmente utilizzati da chiunque per risalire all'identità del soggetto a cui i dati sono riferibili. Tale criterio è declinato dalle circostanze del caso specifico e i principali fattori a cui prestare attenzione sono: il costo dell'identificazione, lo stadio tecnologico raggiunto nel momento in cui il trattamento inizia e l'evoluzione tecnologica probabile nel periodo in cui si continua l'utilizzo dei dati, le finalità del trattamento. Infine l'ultimo elemento chiave a cui il Gruppo di lavoro si riferisce è il concetto di persona fisica: i dati personali sono tali quando si riferiscono a persone viventi identificate o identificabili.

[46] ZECH, op. cit., 2016, 66.

[47] In tal senso v. OHM, *Broken promises of privacy: responding to the surprising failure of anonymization*, in *Ucla Law Review*, 2010, 1701 ss.; BANTERLE, op. cit., 583. V. anche infra par. 3.

l'ambito di applicazione, l'art. 9 riguardante le modalità di esercizio dei diritti dell'interessato e l'art. 43 disciplinante i trasferimenti dei dati verso paesi terzi. A seguito delle modifiche tali articoli si riferiscono esclusivamente alle persone fisiche e non più alle persone giuridiche, enti ed associazioni, resta quindi applicabile agli enti solamente il titolo X del codice, ossia la parte relativa alle comunicazioni elettroniche e al trattamento dei dati dell'abbonato, adottata dal legislatore interno in attuazione della direttiva 2002/58/CE[48]. La scelta di riservare la tutela dei dati personali alle sole persone fisiche è stata nuovamente confermata dal legislatore europeo che con il nuovo regolamento, come è possibile dedurre già dal titolo, si rivolge esclusivamente a tali soggetti[49]. L'intervento abrogante del legislatore interno nel 2011 preclude la possibilità di applicare analogicamente alle persone giuridiche la disciplina stabilita dal codice privacy a protezione delle persone fisiche. Anche a partire dal 25 maggio 2018 quando diventerà applicabile il regolamento europeo sulla protezione dati delle persone fisiche non sarà possibile ricavare in via analogica il diritto alla protezione dei dati agli enti collettivi, infatti è normalmente esclusa la possibilità di interpretare analogicamente un testo di legge dell'Unione Europea dato il carattere settoriale della normativa prodotta da tale ordinamento[50]. I dati degli enti collettivi sembrerebbero così sprovvisti di qualsiasi tutela, ma delle limitazioni al loro utilizzo sono ricavabili da altre norme dell'ordinamento[51]. Tuttavia, come si vedrà meglio più avanti, queste limitazioni non

---

[48] V. Garante per la protezione dei dati personali, Provv. 20 settembre 2012, n. 262 [doc. web n. 2094932]. In questo provvedimento il Garante prende atto delle modifiche apportate dal legislatore al codice privacy e ribadisce l'applicabilità alle persone giuridiche, nel quadro normativo attuale, del solo Titolo X relativo alla fornitura di servizi di comunicazioni elettroniche. Già in passato si era lamentata la difficoltà di applicare la disciplina della privacy alle persone giuridiche, v. ZOPPINI, *I diritti della personalità delle persone giuridiche (e dei gruppi organizzati)*, in *Riv. dir. civ.*, I, 2002, 851 ss.; contra RESTA, *La tutela dei dati personali dopo il "decreto sviluppo"*, in GAROFOLI e TREU, *Il libro dell'anno del diritto 2012*, Enciclopedia Treccani, Roma, 2012, 3 ss.. V. anche WP29, parere n. 4 del 2007, 23-24.

[49] V. anche art. 1 reg. 679/2016/UE e il considerando 14 del medesimo.

[50] Cfr. RUSSO, *L'interpretazione dei testi normativi comunitari*, Giuffrè, Milano, 2008, 235 ss.; v. anche CGCE, 12 dicembre 1985, Krohn c. Balm, C-165/84, in www.curia.eu. Si è fatto riferimento all'applicazione analogica dei diritti personali attribuiti alla persona fisica perché la dottrina e la giurisprudenza maggioritaria riconoscono diritti della personalità in capo agli enti collettivi dotati di soggettività giuridica ricorrendo alternativamente all'analogia legis o all'analogia iuris. (Cfr. PINO, *L'identità personale degli enti collettivi*, in *Libera circolazione e protezione dei dati personali*, (a cura di) PANETTA, vol. I, Giuffrè, Milano, 2006, 296 ss..)

[51]Qualora ricorrano i presupposti per l'applicazione della disciplina della concorrenza sleale, l'art. 2598 n. 2 cod. civ. permette all'impresa di opporsi alla circolazione di informazioni screditanti nei propri confronti. Poiché è ormai consolidato che per poter essere applicata la fattispecie della denigrazione richiede che le notizie screditanti siano false[51] è possibile affermare l'esistenza di un diritto al controllo della veridicità ed alla rettifica delle notizie riguardanti la propria impresa. L'esercizio di questo potere di controllo e rettifica è subordinato all'esistenza di un danno concorrenziale potenziale o effettivo. Inoltre qualora si aderisca all'orientamento ormai consolidato che riconosce in capo agli enti collettivi un diritto di reputazione è possibile ricavare un diritto di controllo della veridicità ed alla rettifica delle

sembrano avere rilevanza alcuna nella prospettiva dell'analisi big data, che si caratterizza per essere finalizzata all'elaborazione di informazioni predittive attraverso l'utilizzo di grandi masse di dati provenienti da fonti eterogenee[52].

Resta da precisare che la normativa adottata a protezione dei dati personali trova applicazione sia nel caso di trattamento automatizzato che non, ma nell'ultima ipotesi solo se i dati sono contenuti o destinati a figurare negli archivi. Presupposto inoltre per l'applicazione e che tali trattamenti non siano effettuati da persone fisiche nello svolgimento di attività a carattere personale o domestico[53].

Dopo aver chiarito l'ambito di applicazione materiale della suddetta normativa occorre soffermarsi sulle caratteristiche dell'analisi big data e sui metodi possibili di studio di grandi quantità di dati personali, in considerazione del fatto che tale tipo di attività può avere alcuni contrasti con i principi giuridici posti alla base della data protection poiché incentiva la raccolta più ampia possibile di dati e la conservazione per il tempo più a lungo possibile al fine di un utilizzo futuro indefinito al momento della raccolta. Inevitabilmente ciò può implicare dei conflitti con principi quali quello di finalità e di minimizzazione dei dati raccolti. Inoltre gli effetti delle applicazioni big data, in considerazione del fatto che si basano esclusivamente su una correlazione di dati, possono essere discriminatori e comportare un rafforzamento di stereotipi già esistenti. Poi, si consideri che l'estrazione di informazioni dalle enormi quantità di dati a disposizione dei colossi del web può comportare un controllo sul comportamento e sulle intenzioni d'acquisto degli individui permettendo così attività di marketing sempre più mirate e invadenti, in taluni casi si rischia di invadere eccessivamente la sfera di autodeterminazione dell'individuo. Tutti questi aspetti negativi possono creare un effetto disincentivante nei confronti della creatività dell'innovazione e della libertà di espressione perché la consapevolezza di essere costantemente sorvegliati potrebbe

---

informazioni riguardanti l'ente anche al di fuori del contesto concorrenziale. Cfr. ZOPPINI, op. cit., 851 ss..; PINO, op. cit., 296 ss..

Le imprese possono sempre opporsi all'utilizzo di proprie informazioni qualora queste siano tutelabili in base alla disciplina sul segreto industriale ricavabile dagli artt. 98, 99 c.p.i. o 2598 e seguenti cod. civ.. Cfr. VANZETTI e DI CATALDO, *Manuale di diritto industriale*, VII ed., Giuffrè, Milano, 2012, 77 ss..

[52]V. infra par. 3.

[53] V. art. 3 dir. 95/46/CE e art. 2 GDPR. Questi articoli contengono anche una serie nutrita di ipotesi che escludono l'applicazione rispettivamente della direttiva e del nuovo regolamento. In considerazione della scarsa importanza e della poca pertinenza di queste con il tema trattato si rimanda ai testi normativi. Inoltre si consideri che le ulteriori ipotesi elencate nella direttiva e nel regolamento non escludono l'adozione da parte del legislatore interno di norme ad hoc, impediscono soltanto al legislatore europeo di occuparsene per un difetto di competenza.

bloccare certi atteggiamenti se, ad esempio, ritenuti riprovevoli in determinati contesti[54]. Nonostante questi possibili effetti negativi l'uso di queste grandi masse di dati porta alcuni vantaggi, si pensi ad esempio alle innovazioni in campo sanitario[55], ai profitti in campo commerciale, al miglioramento dei servizi e all'utilità delle applicazioni big data per combattere le frodi[56]. È opportuno quindi trovare uno spazio affinché tale tipo di attività possa essere svolta, per fare ciò è d'obbligo cercare un bilanciamento tra i contrapposti interessi fondamentali in gioco. In particolar modo si deve contemperare il diritto fondamentale alla protezione dei dati[57], sancito dall'art. 8 della Carta di Nizza, con il diritto fondamentale alla libertà di impresa sancito dall'art 16[58] per poter comprendere a pieno fino a che punto l'analisi big data può essere sfruttata dalle imprese quando coinvolga dati personali. Per ottenere un corretto bilanciamento occorre guardare alle pronunce della Corte di Giustizia, che già in diverse occasioni ha dovuto occuparsi del conflitto tra il diritto alla protezione dei dati e altri diritti fondamentali.

Nel caso Promusicae v. Telefonica la Corte di Giustizia lascia alla discrezionalità degli stati membri il bilanciamento tra il diritto alla privacy, inteso come comprensivo del diritto alla riservatezza e il diritto alla protezione dei dati, i diritti di proprietà intellettuale e il diritto ad un ricorso effettivo. Nel fare ciò richiama un importante principio in base al quale questa discrezionalità deve essere esercitata: il principio di proporzionalità[59]. Per la Corte non vi è una gerarchia tra il diritto fondamentale alla tutela della proprietà intellettuale sancito dall'art. 17 co. 2 della Carta di Nizza e il diritto alla privacy tutelato dagli artt. 7 e 8 nelle sue due accezioni. In questa pronuncia la Corte di Giustizia si conforma ad un suo precedente orientamento espresso nel caso

---

[54] Per un approfondimento sugli aspetti negativi derivanti dall'analisi big data v. EDPS, Opinion 7/2015, *Meeting the challenges of Big data*, 8 e 9; v. anche PAGALLO, *Il diritto nell'età dell'informazione: il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti*, Giappichelli, Torino, 2014, 180 ss..

[55] Si pensi ad esempio al servizio «Google FluTrends».V. BOLLIER, *The promise and peril of big data*, in https://www.emc.com/collateral/analyst-reports/10334-ar-promise-peril-of-big-data.pdf, 2010, 25 ss..

[56]V. SCHWARTZ, *Data protection Law and the ethical use of analytics*, CIPL, in http://www.huntonfiles.com/files/webupload/cipl_ethical_undperinnings_of_analytics_paper.pdf, 2010, 13 ss..

[57]Il diritto alla protezione dei dati può essere definito come il diritto alla libera proiezione delle proprie informazioni personali, con controllo sulla loro libera circolazione e sul loro utilizzo da parte di terzi. V. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, CEDAM, Padova, 2006, 78.

[58] Le imprese tramite l'analisi big data riescono ad essere molto più competitivi ottimizzando le loro catene produttive e la qualità dei loro servizi (v. in tal senso MAGGIOLINO, op. cit., 54).

[59]CGCE, 29 gennaio 2008, C-275/06, in *AIDA* 2008, *1190*. La sentenza Promusicae v. Telefonica è stata molto criticata dalla dottrina poiché si è sostenuto che la CGUE abbia abdicato al suo dovere di contemperamento di interessi contrapposti. Su questo v. L.C. UBERTAZZI, *Proprietà intellettuale e privacy*, in *AIDA* 2014, 443 ss..

Lindqvist che in ipotesi di conflitto tra il diritto alla libertà di espressione e il diritto alla privacy stabilisce che gli Stati membri sono obbligati a garantire la tutela di entrambi, assicurando al contempo un giusto equilibrio fra gli stessi[60]. Alcuni autori nel fare il bilanciamento tra il diritto alla privacy e altri diritti fondamentali distinguono Privacy "nel sistema" e "per il sistema". Nel primo caso il trattamento dei dati avverrebbe tra privati e sarebbe funzionale al mercato e riguarderebbe i conflitti interprivati. Nel secondo il trattamento è strumentale al rispetto delle regole poste dall'ordinamento. In altri termini riguarda i casi in cui è stato perpetrato un illecito ed il diritto alla privacy entrerebbe in contrasto con l'interesse all'accertamento e alla repressione della violazione[61]. È chiaro che nella prospettiva dello studio di grandi quantità di dati, ossia di un utilizzo di dati personali per finalità economiche occorre soffermarsi in particolare sulla privacy "nel sistema" perché, come già precisato, occorre cercare un punto d'equilibrio tra la libertà di impresa e il diritto alla protezione dati. In tali circostanze, come dimostrato nel caso Scarlet v. SABAM[62] e nella pronuncia del 2014 relativa al caso Google Spain SL v. AEPD[63], la Corte non lascia alla discrezionalità degli stati membri il compito di ricercare un giusto equilibrio ma interviene direttamente contemperando gli interessi contrapposti.

2. L'attuale quadro normativo non considera espressamente l'analisi big data[64] tra i trattamenti ai quali è dedicata una disciplina specifica. A tal proposito occorre osservare che tale tipo di analisi viene comunemente intesa come studio di grandi masse di dati finalizzato alla deduzione di informazioni predittive relative ad individui o gruppi[65],e per le sue caratteristiche la disciplina di questa tipologia di studio può essere

---

[60] V. CGCE, 6 novembre 2003, C-101/01, in curia.europa.eu; v. anche OTTOLIA, *Proprietà intellettuale e trattamento dei dati personali: riflessioni su privacy " per il sistema" e "nel sistema"*, in *AIDA* 2010, 319 ss..

[61] V. OTTOLIA, *Big data e innovazione computazionale*, cit.,10 ss.; v anche L.C. UBERTAZZI, *Proprietà intellettuale e privacy*, cit., 435 ss..

[62]CGUE, 24 novembre 2011, C-70/10, in *AIDA* 2012, *1461*.

[63] CGUE, 13 maggio 2014, C-131/12, in curia.europa.eu.

[64] Per una definizione del termine big data v. ENISA(European union agency for network and information security)G. D'ACQUISTO, DOMINGO FERRER, PANAYIOTIS KIKIRAS, VINCENCTORRA, YVES ALEXANDRE DE MONTOJOYE, ATHENA BOURKA, *Privacy by design in big data , an overview of privacy enhancing technologies in the era of big data analytics*, December 2015, in www.enisa.europa.eu, 10: «Business consultants Gartner Inc. define big data as "high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making"». V. anche WP29, Opinion 03/2013 on purpose limitation, 35.

[65]V. BOLLIER, op. cit., 4 e 5; MATTIOLI, *Disclosing Big Data*, Maurer Faculty Paper 2014, 539, disponibile al seguente indirizzo: www.repositorylaw.indiana.edu/facpub/1480.MANTELERO, *Rilevanza e*

ricavata ricorrendo principalmente sia alla profilazione sia, secondo il parere 03/2013 del WP29, nel rispetto di talune condizioni, al trattamento dati a fini statistici[66]. Quindi l'analisi big data può essere fondata alternativamente sul consenso dell'interessato, su di un legittimo interesse ed infine sulla compatibilità del trattamento ulteriore, che è una specificazione fatta dal legislatore, come si vedrà meglio più avanti, del legittimo interesse. Il ricorso alla clausola della compatibilità e quindi, in questo caso, al trattamento a fini statistici può rilevarsi molto utile perché, come verrà spiegato meglio più avanti, l'uso dei dati per tali scopi non necessità in taluni casi dell'ottenimento di un ulteriore assenso, fungendo da base giuridica del trattamento successivo un legittimo interesse[67]. Il legittimo interesse, come chiarito anche dal nuovo regolamento al considerando 47[68] e dal WP29 nel parere n. 6 del 2014[69], da solo non è sufficiente a

---

tutela della dimensione collettiva della protezione dei dati personali, in *Contratto e impresa/Europa*, 2015, 142; MANTELERO, *Personal data for decisional purposes in the age of analytics: from an individual to a collective dimension of data protection*, in *Computer law and security review*, 2016, 239; WP29, Opinion 03/2013 on purpose limitation, 45.

[66] WP29, Opinion 03/2013 on purpose limitation, 29 : «'Statistical purposes' in particular, cover a wide range of processing activities, from commercial purposes (e.g. analytical tools of websites or big data applications aimed at market research) to public interests (e.g. statistical information produced from data collected by hospitals to determine the number of people injured as a result of road accidents).» Per la dottrina v. MAYER SCHOENBERGER and PADOVA, *Regime change? Enabling big data through europe's new data protection regulation*, in *17 Colum. Sci&Tech. L. Rev. 41(2016)*,http://www.stlr.org/cite.cgi?volume=17&article=SchonbergerPadova**,** 318, 323 e 326; contra MANTELERO, *Big data: I rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Dir. inf.* 2012, 138. V. anche BANTERLE, op. cit., 587: l'autore avanza l'ipotesi che l'analisi big data posso essere effettuata utilizzando, in alternativa al trattamento statistico e alla profilazione, quale base giuridica dell'analisi big data anche l'interesse legittimo. V. anche OTTOLIA, *Big data e innovazione computazionale*, cit. 101 ss.., ammette il ricorso a tali basi giuridiche e in particolare anche alla clausola della compatibilità ma non al trattamento dei dati a fini statistici.

[67] V. BANTERLE, op. cit, 587; ICO, *Big data and data protection*, 2014, 29 ss.; WP29, Opinion n. 6/2014, 24 ss..

[68] Per l'interesse legittimo cfr. considerando 47 GDPR: «I legittimi interessi di un titolare del trattamento, compresi quelli di un titolare del trattamento a cui i dati personali possono essere comunicati, o di terzi possono costituire una base giuridica del trattamento, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento. Ad esempio, potrebbero sussistere tali legittimi interessi quando esista una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento, ad esempio quando l'interessato è un cliente o è alle dipendenze del titolare del trattamento. In ogni caso, l'esistenza di legittimi interessi richiede un'attenta valutazione anche in merito all'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine. Gli interessi e i diritti fondamentali dell'interessato potrebbero in particolare prevalere sugli interessi del titolare del trattamento qualora i dati personali siano trattati in circostanze in cui gli interessati non possano ragionevolmente attendersi un ulteriore trattamento dei dati personali. Posto che spetta al legislatore prevedere per legge la base giuridica che autorizza le autorità pubbliche a trattare i dati personali, la base giuridica per un legittimo interesse del titolare del trattamento non dovrebbe valere per il trattamento effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti. Costituisce parimenti legittimo interesse del titolare del trattamento interessato trattare dati personali strettamente necessari a fini di prevenzione delle frodi. Può essere considerato legittimo interesse trattare dati personali per finalità di marketing diretto. »

giustificare un trattamento di dati personali è necessario che su di esso non prevalgano i diritti e le libertà fondamentali dell'interessato i cui dati sono sottoposti a trattamento. Il Gruppo europeo dei Garanti nel suo parere del 2014 ha identificato alcuni criteri guida da seguire per effettuare questo bilanciamento: i) analizzare e pesare l'importanza degli interessi in conflitto, il diritto fatto valere dal terzo o dal titolare deve essere previsto dalla Carta di Nizza o dalla CEDU; ii) l'utilizzo di misure di sicurezza che possano ridurre l'impatto del trattamento sui diritti e libertà fondamentali dell'interessato; iii) prendere in considerazione l'impatto del trattamento sull'interessato, che ovviamente cambierà al variare della natura dei dati personali presi in esame e del modo in cui saranno processati; iv) la piena conformità del trattamento alla normativa vigente a protezione dei dati personali, acconsentendo ad esempio a facili meccanismi di opt-out[70]. Parte della dottrina ritiene possibile ricorrere al legittimo interesse solo quando non è possibile perseguire con il trattamento una determinata finalità avvalendosi delle altre basi giuridiche elencate nell'art. 6 del Reg. UE 679/2016[71].

Per verificare la sussistenza di un legittimo interesse il Titolare del trattamento dovrà procedere ad effettuare una valutazione interna sulla sussistenza del legittimo interesse, questa valutazione dovrà essere resa in forma scritta per fini probatori e dovrà essere conservata ed esibita dietro richiesta dell'Autorità di Controllo.

La disciplina qui descritta è quella che si ricava dall'interpretazione delle disposizioni del Regolamento, dal parere del Gruppo di lavoro del 2014 e dal principio di accountability immanente a tutto il tessuto normativo del GDPR. Resta da precisare che l'Italia sembra muoversi in altra direzione in evidente contrasto con tale disciplina. Il Codice Privacy con riferimento al legittimo interesse del titolare, all'articolo 24, comma 1, lett. g), stabiliva che esso si applicasse, con esclusione della diffusione, nei casi individuati dal Garante, qualora il trattamento fosse necessario per perseguire un legittimo interesse del titolare o di un terzo destinarlo dei dati, qualora non prevalessero i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato. Con

---

[69] V. WP29 n. 6/2014, 24 ss.. In queste pagine il Gruppo di lavoro fornisce un elencazione esemplificativa di possibili ipotesi in cui si possa riscontrare l'esistenza di un legittimo interesse: esercizio del diritto di libertà di espressione o informazione; pubblicità commerciale tramite marketing diretto ed altre forme; messaggi non commerciali per campagne politiche o raccolta fondi; prevenzioni di frodi, trattamento per fini di ricerca, inclusa l'ipotesi di ricerca di mercato ecc… Nel parere del WP29 viene anche sottolineato che un interesse per essere considerato legittimo deve in ogni caso riguardare un'attività consentita dalla legge.

[70] Per un approfondimento v. WP29, Opinion n. 6/2014, 31 ss..

[71] In questo senso v. PIZZETTI, *Lezione al Politecnico di Torino del 24 novembre 2017*, 12. Questo autorevole orientamento sembra in contrasto con quanto espresso dal WP29 nell'Opinion n. 6/2014.

la legge di bilancio 2018 è stata poi introdotta una procedura *ad hoc* per i Titolari del trattamento per avvalersi del legittimo interesse quale base giuridica di un trattamento: i)invio al Garante per la protezione dei dati personali di un'informativa che illustri le caratteristiche fondamentali del trattamento; ii)decorsi 15 giorni dall'invio, il Titolare anche se non ha ancora ricevuto una risposta può intraprendere il trattamento, salva la possibilità per il Garante di effettuare un'istruttoria; iii) il Garante può sospendere o vietare il trattamento, se l'esito dell'istruttoria è una valutazione negativa circa la sussistenza del legittimo interesse[72].

Si consideri, infine, che l'attuale schema di decreto di adeguamento della normativa nazionale al GDPR, ancora in fase di approvazione mentre si scrive il presente elaborato, fa salva la procedura sopra descritta.

Se questa disciplina normativa fosse confermata è evidente il contrasto che si verrebbe a creare tra normativa interna e normativa europea direttamente applicabile[73]. La procedura sopra descritta è in evidente contrasto con quanto previsto dal GDPR, per questo motivo, qualora in Italia la disciplina posta dal Decreto attuativo dovesse confermare la procedura, a parere di chi scrive, si dovrà ugualmente considerare inapplicabile perché in contrasto con norme europee direttamente applicabili e di rango superiore.

La contraddizione è maggiore se si considera che lo stesso Garante per la protezione dei dati personali sembra riconoscere l'applicabilità della disciplina sul legittimo interesse stabilità dal Regolamento, come si può notare leggendo le linee guida sul Regolamento

[72] Legge di bilancio 2018, art. 1 commi 1022 e 1023: «1022. Il titolare di dati personali, individuato ai sensi dell'articolo 4, numero 7), del regolamento RGPD, ove effettui un trattamento fondato sull'interesse legittimo che prevede l'uso di nuove tecnologie o di strumenti automatizzati, deve darne tempestiva comunicazione al Garante per la protezione dei dati personali. A tale fine, prima di procedere al trattamento, il titolare dei dati invia al Garante un'informativa relativa all'oggetto, alle finalità e al contesto del trattamento, utilizzando il modello di cui al comma 1021, lettera c). Trascorsi quindici giorni lavorativi dall'invio dell'informativa, in assenza di risposta da parte del Garante, il titolare può procedere al trattamento. 1023. Il Garante per la protezione dei dati personali effettua un'istruttoria sulla base dell'informativa ricevuta dal titolare ai sensi del comma 1022 e, ove ravvisi il rischio che dal trattamento derivi una lesione dei diritti e delle libertà dei soggetti interessati, dispone la moratoria del trattamento per un periodo massimo di trenta giorni. In tale periodo, il Garante può chiedere al titolare ulteriori informazioni e integrazioni, da rendere tempestivamente, e, qualora ritenga che dal trattamento derivi comunque una lesione dei diritti e delle libertà del soggetto interessato, dispone l'inibitoria all'utilizzo dei dati. »

[73] In questo senso v. SENOR, *La reticenza italiana sul legittimo interesse del titolare quale base giuridica del trattamento di dati personali*, in www.filodiritto.com, 2018, 1 ss.

pubblicate sul sito ufficiale[74]. Una soluzione diversa d'altronde rischierebbe di mettere in serie difficoltà le imprese multinazionali e vanificherebbe l'intento del Regolamento di unificare la disciplina all'interno dell'Unione europea[75].

Qui di seguito si propone un esempio di standard per effettuare il test di bilanciamento, il presente standard è stato elaborato basandosi in larga parte sul principio di accountability immanente al Regolamento Europeo per la protezione dei dati, sul considerando 47 del Regolamento e sul Parere n. 6 del 2014 del WP29[76].

Breve descrizione del trattamento e del legittimo interesse che si intende perseguire			
Finalità e modalità del trattamento	**Natura dei dati oggetto del trattamento**	**Classificazione dell'interesse del Titolare**	**Breve descrizione del legittimo interesse del Titolare**
In questa sezione occorre fornire una breve descrizione del trattamento che si intende realizzare precisando le finalità e il modo in cui i dati sono trattati. In particolare, occorre specificare	*In questa sezione occorre specificare se verranno trattati dati sensibili, per tali intendendo i dati rientranti nelle categorie di cui all'art. 9 del Regolamento europeo per la protezione dei dati.*	*In questa sezione occorre completare con una (X) l'ipotesi corrispondente:* ( ) a) Esercizio di un diritto fondamentale del Titolare o di terzi (1) ( ) b) Interesse pubblico o interesse	*In queste sezione occorre inserire una descrizione del legittimo interesse che il Titolare intende perseguire, precisando anche perché si vuole ricorre a questa determinata base giuridica. Se è possibile fare*

[74] Garante per la protezione dei dati personali, *Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali*, www.garanteprivacy.it. In questo senso v. BOCCHI, *Privacy: sotto natale siamo tutti più buoni…o contatti no?*, in www.lcalex.it, 2017.

[75] In questo senso v. SENOR, op. cit., 4.

[76] Uno strumento utile per completare le singole sezioni delle tabelle dello standard è costituito da ICO, *"Gdpr guidance legitimate interests sample lia template*". In tale documento sono presenti una serie di domande le cui risposte possono essere utilizzate per completare e approfondire le schede del modello qui proposto. V. anche ICO, *Legitimate interests guidance*, in https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/.

se il trattamento è manuale o automatizzato		più ampio della collettività(2): ( )c) Altri legittimi interessi (3) ( ) d) Riconoscimento legale e culturale/ sociale della legittimità degli interessi (4)	*riferimento anche a provvedimenti o documenti ufficiali in cui l'Autorità di controllo o il WP29 ha preso in considerazione tale interesse o interessi simili*

(1) es. Analisi sull'affidabilità economica del fornitore persona fisica. Quando si fa riferimento all'esercizio di un diritto fondamentale dell'interessato o di un terzo occorre indicare in modo specifico il fondamento normativo. Così l'esempio appena riportato potrebbe trovare fondamento nell'art. 41 cost. o nell'art 16 della Carta di Nizza.

(2) es. Ente no profit che utilizza i dati raccolti per profilare i donatori in modo da incrementare le donazioni, oppure trattamenti posti in essere per ostacolare la corruzione tra privati (cd. whistleblowing)

(3) In questi casi il legittimo interesse serve per effettuare un trattamento che trova un parziale fondamento in un'altra base giuridica. Così ad esempio in alcuni casi un determinato trattamento potrebbe non essere strettamente necessario per dare esecuzione ad un contratto oppure la legge lo permette almeno in parte ma non lo ritiene in alcun modo obbligatorio.

(4) Specificare se c'è un fondamento culturale o legale da cui è possibile ricavare la legittimità del trattamento. Ad esempio: il trattamento ulteriore per fini di ricerca scientifica in campo sanitario. Se vi sono fondamenti normativi di cui si può parzialmente avvalersi occorre indicare anche le disposizioni normative[77].

Relazione tra il Titolare e l'interessato		
Rapporti tra Titolare e interessato	**Aspettative ragionevoli per l'interessato**	**Valutazione dell'impatto: conseguenze negative e**

[77] V. infra in questo paragrafo dove si parla del trattamento ulteriore per fini statistici

		positive del trattamento (POSITIVO-NEGATIVO)
In questa sezione occorre precisare che relazione intercorre tra l'interessato e il Titolare (5). *Inoltre è doveroso soffermarsi sullo status del Titolare o dell'interessato* (6).	*In questa sezione occorre specificare se l'interessato si aspetta un tale tipo di trattamento, o comunque è in grado di prevederlo in ragione della particolare relazione che intercorre tra egli e il Titolare. Non è sufficiente il fatto che all'interessato sia stata fornita un'informativa a riguardo. È necessario che vi sia una relazione pertinente.*	*In questa sezione occorre elencare per punti le conseguenze possibili del trattamento dei dati nei confronti dell'interessato. Per ogni singola voce occorre inserire il giudizio sopra riportato (**POSITIVO** o **NEGATIVO**)* (7)

(5) È importante evidenziare se tra Titolare e interessato vi è una relazione in qualche modo qualificata, ad esempio: datore di lavoro – dipendente, oppure vi è un rapporto di clientela. L'esistenza di una relazione qualificata incide in maniera evidente sulle aspettative ragionevoli dell'interessato.

(6) Occorre soffermarsi sullo status del Titolare e dell'interessato. Così se il Titolare è un'impresa in posizione dominante che offre un determinato servizio e l'interessato non ha alternative che rivolgersi a tale impresa per ottenere un determinato servizio sarà più difficile riconoscere un legittimo interesse in capo al Titolare, proprio perché l'interessato non ha la possibilità di sottrarsi a quel determinato trattamento che si vuole fondare su di un legittimo interesse.

Esito provvisorio del test e garanzie supplementari		
Impatti privacy sull'interessato	**Bilanciamento provvisorio**	**Garanzie supplementari per ridurre gli impatti privacy sull'interessato**
In questa sezione occorre	*In questa sezione occorre*	*In questa sezione occorre*

specificare i possibili impatti privacy sull'interessato. In particolare si dovrà ragionare sull'eventuale conseguenza di un data breach e sulle misure che si intende adottare per evitare che tale violazione si verifichi.	*indicare se alla luce degli elementi analizzati fin ora si possa ritenere sussistente un legittimo interesse oppure no, oppure parzialmente sussistente. È particolarmente importante, nell'esprimere questo giudizio provvisorio, tenere in considerazione gli impatti nei confronti dell'interessato. Quanto indicato in questa sezione influenza in modo significativo la colonna successiva relativa alle garanzie supplementari. Infatti, più il bilanciamento provvisorio è sfavorevole, maggiori dovranno essere le garanzie supplementari che si intende implementare.*	*completare con una (X) l'ipotesi corrispondente, più ipotesi sono selezionate e maggiore sarà la possibilità di ritenere lecito il trattamento fondato sul legittimo interesse perché si riduce l'impatto nei confronti dei diritti e delle libertà fondamentali dell'interessato*: ( ) a) Misure di sicurezza (es. anonimizzazione o pseudonimizzazione) (8) ( ) b) Valutazione di impatto (9) ( ) c) Disclosoure delle logiche di trattamento e più in generale completezza delle informazioni sul trattamento dell'interessato(10) ( ) d) diritto generale di opt-out (11) ( ) e) diritto alla portabilità dei dati e relative misure per accrescere il potere degli interessati (12)

Esito del TEST	*In questa sezione occorre specificare se si ritiene sussistente il legittimo interesse del Titolare. Qualora non si ritenesse*

	sussistente il legittimo interesse occorre individuare un'altra base giuridica per procedere a tale trattamento e se non fosse possibile ricorrere ad un'altra base giuridica il trattamento non potrà essere effettuato

(7) In particolare in questa sezione occorre interrogarsi se c'è qualche rischio di discriminazione, oppure ci possono essere impatti emotivi per l'interessato (es. irritazione, stress ecc..), o si va in qualche modo a ledere l'autonomia privata dello stesso. Allo stesso tempo occorre ipotizzare se vi possono essere dei benefici per l'interessato.

(8) Se sono state adottate misure di sicurezza occorre specificare quali, a tal proposito si può far riferimento all'art. 32 del Regolamento europeo in materia di protezione dei dati personali.

(9) Occorre indicare se si è proceduto a fare una valutazione di impatto, qualora la risposta fosse positiva occorre allegare al presente modello la stessa valutazione riportando in sintesi in questa sezione l'esito della valutazione.

(10) In questo caso occorre specificare eventualmente con un allegato le informazioni che si intende dare all'interessato per illustrargli il trattamento.

(11) Tramite il meccanismo di opt-out l'interessato ha sempre la possibilità di sottrarsi al trattamento. Occorre specificare anche come si intende permettere all'interessato di avvalersi di tale meccanismo. Se si tratta di un diritto generale e incondizionato oppure è subordinato al ricorrere di determinate circostanze.

(12) Occorre specificare se oltre al diritto di portabilità sono state riconosciute altre misure, avendo cura di riportare anche i modi in cui per l'interessato è possibile avvalersi di tali misure.[78]

In alcuni casi è direttamente la legge ad effettuare parte del bilanciamento tra i contrapposti interessi come nel caso del trattamento ulteriore per fini statistici[79], che

[78] La presente tabella è stata costruita basandosi in gran parte su WP29, Opinion n. 6/2014, 30 ss..
[79] V. infra par. 3

corrisponde ad un'ipotesi specifica di legittimo interesse[80], come si può ricavare dallo stesso parere del WP29 che nel fornire un'elencazione esemplificativa di ipotesi in cui ricorre un legittimo interesse include tale tipo di finalità. A differenza di altre ipotesi di legittimo interesse in questo caso essendoci una previsione specifica del legislatore non è necessario, come in altri casi, verificare se tale interesse sia consentito dalla legge. Quindi si può passare direttamente allo step successivo, ossia quello del bilanciamento con interessi inerenti a diritti e libertà fondamentali del titolare dei dati personali oggetto di trattamento. In questo caso un sicuro strumento utile è costituito da quanto già detto sopra sul bilanciamento tra legittimo interesse e diritti e libertà fondamentali del titolare dei dati. A questa guida si dovrà aggiungere, come si avrà modo di approfondire più avanti, lo studio del concetto di compatibilità[81]. Infatti a differenza di altre ipotesi nel caso di trattamento ulteriore per fini statistici è la stessa normativa posta protezione dei dati personali a dettare più specificatamente le condizioni in presenza delle quali si possa ricorrere a tale tipologia di studio, subordinando la fruibilità di tale particolare tipo di trattamento al concetto sopra menzionato.

Per comprendere a pieno cosa comporti il ricorso alla disciplina dei trattamenti ulteriori per finalità statistiche è necessario indagare il concetto e considerare le condizioni in presenza delle quali si possa effettuare l'analisi big data senza dover richiedere alcun preventivo assenso da parte dei titolari dei dati[82]. In considerazione del fatto che la possibilità di effettuare un trattamento di dati personali senza richiedere alcun consenso nella prospettiva big data è un tema particolarmente delicato perché caratteristica fondamentale di questa tipologia di analisi è proprio l'imprevedibilità, al momento in cui viene richiesto il consenso, delle informazioni che si potranno ricavare dalla combinazione dei dati trattati, e più in generale l'imprevedibilità dell'utilizzo dei dati raccolti[83].

---

[80] WP29, Opinion n. 6/2014, 25 e 28. Cfr. BANTERLE, op. cit., 588. L'autore ritiene che l'interesse legittimo possa essere alla base dell'analisi big data ma non della profilazione.

[81] V. infra par. 3.

[82]La riconduzione alla profilazione o al trattamento dati a fini statistici, come si vedrà nel prosieguo del testo, avviene in conseguenza del fatto che l'analisi big data comporta un trattamento automatizzato di dati tipico di queste modalità di utilizzo dei dati. La differenza principale che verrà posta in luce verterà sul fatto che nella profilazione il titolare dei dati (i.e. l'interessato) acconsente a che il trattamento possa avere come fine delle misure nei suoi confronti, cosa che invece non può avvenire nel trattamento dati a fini statistici. La vicinanza tra il trattamento a fini statistici e la profilazione è evidenziata anche del regolamento, come si vedrà meglio nell'apposito paragrafo, che al considerando 71 fa riferimento a procedure matematiche e statistiche strumentali all'ottenimento del profilo del titolare dei dati.

[83] Sulla difficoltà di ricorrere al consenso per l'analisi big data v. CATE and MAYER SCHONBERGER, *Tomorrow 's privacy notice and consent in a world of big data*, in *international data privacy law review*,

Posto che per trattamento dati, in base al regolamento UE n. 679 del 2016[84], si intende « …qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali…»[85]. Occorre interrogarsi sul significato del termine fini statistici, del quale non abbiamo alcuna definizione normativa né nel nuovo regolamento né nella direttiva del 1995.

Lo studio statistico nasce verso la fine del settecento e l'inizio dell'ottocento. Inizialmente la nozione di statistica viene intesa come scienza dello stato, più precisamente, riproponendo una definizione del 1770, la statistica è definita come quella scienza che studia l'assetto politico degli stati moderni. Successivamente la statistica incomincia ad essere riferita alla società per poi essere concepita, già a partire dalla prima metà del ventesimo secolo, come lo studio di fenomeni collettivi[86]. A livello normativo per colmare la lacuna si può far ricorso alla definizione contenuta nell'art. 1 dell'Appendice alla Raccomandazione N.R(97)18 del CDE: «… "per scopi statistici" si riferisce a qualsiasi operazione di raccolta e trattamento di dati personali necessari per indagini statistiche o per la produzione di risultati statistici. Tali operazioni escludono qualsiasi utilizzo delle informazioni ottenute per prendere decisioni o provvedimenti relativi ad un determinato individuo; per "risultati statistici" si intendono informazioni ottenute attraverso il trattamento di dati personali per caratterizzare un fenomeno collettivo in rapporto ad una popolazione presa in esame». Questa definizione è fornita da un atto non vincolante dal punto di vista giuridico ma che sicuramente possiede un valore esortativo e rilevatore di una prassi[87] presente negli stati membri del Consiglio d'Europa di cui fanno parte tutti i Paesi aderenti all'UE e ai quali si applica quindi la direttiva ed il regolamento sulla protezione dei dati personali. Inoltre si deve tenere in

---

2013, 67 e 68;TENE&POLONETSKY, *Big Data for All: Privacy and User Control in the Age of Analytics*, in *Northwestern Journal of Technology and Intellectual Property*, 2013, 260 e 261; MANTELERO e VACIAGO, *The "Dark side" of Big Data, Private and Public Interaction in Social Surveillance*, in *Cri 6/2013*, 162 e 163.

[84] Definizione simile la troviamo anche nella direttiva 95/46/CE all'art. 2 lett. a) e nel codice privacy all'art. 4 lett. a).

[85]V. art. 4 n. 2 reg. UE n. 679/2016.

[86] V. WILLICOX, *Definitions of statitics*, in *Review of the international statistical institute*, vol. 3, no. 4 (1936), 388 ss.; v. (voce)Statistica, in Vocabolario Treccani online.

[87]Sul valore delle raccomandazioni v. CONFORTI, *Diritto internazionale*, VIII ed., ES, Napoli, 2010, 176. Sul valore che ha avuto questa raccomandazione nell'ordinamento italiano v. D.lgs. 281/1999 «Disposizioni in materia di trattamento dei dati personali per finalità storiche, statistiche e di ricerca scientifica», in particolare v. art. 1 co. 1. V. anche il «codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici» che all'art. 1 co. 1 contiene una definizione analoga di risultato statistico: «l'informazione ottenuta con il trattamento di dati personali per quantificare aspetti di un fenomeno collettivo».

considerazione l'art. 52 della Carta di Nizza: «Laddove la presente Carta contenga diritti corrispondenti a quelli garantiti dalla Convenzione Europea per la salvaguardia dei diritti dell'uomo e per le libertà fondamentali, il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta convenzione. La presente disposizione non esclude che il diritto dell'Unione conceda una protezione più estesa.» Per quanto qui interessa da questo articolo si può ricavare la vincolatività per tutti gli stati membri dell'UE del corpus normativo della CEDU[88].

Questo modo di intendere la nozione di statistica sembra inoltre essere stato recepito dal legislatore europeo nell'art. 3 del reg. CE 223/09 relativo alle statistiche ufficiali europee: «…«statistiche»: le informazioni quantitative e qualitative, aggregate e rappresentative che caratterizzano un fenomeno collettivo in una determinata popolazione». La definizione offerta da questo regolamento risulterebbe essere applicabile solo ed esclusivamente per le statistiche europee, ossia le statistiche necessarie per lo svolgimento delle attività dell'UE. Occorre chiedersi se si possa applicare anche agli altri tipi di statistiche data la presenza di una lacuna normativa, posto che, come già detto sopra, vi è un chiaro indice rilevatore nell'art. 1 dell'Allegato alla Raccomandazione N.R(97)18 del CDE della volontà degli stati membri del Consiglio d'Europa, tra cui figurano anche quelli appartenenti all'UE, di intendere in tal modo la nozione di statistica e tenuto conto dell'importanza del corpus normativo della CEDU per l'Unione Europea. Se si considera che la definizione fornita dall'art. 3 del reg. 223/09/CE è una definizione lessicale, intendendo in tale senso tutte le definizioni che rispecchiano il significato che un determinato termine è venuto ad assumere nel linguaggio comune, come dimostrato dalla corrispondenza della nozione di statistica fornita dal regolamento a quella offerta da diversi dizionari[89]. In altri termini il legislatore non offre alcuna ridefinizione di statistica, mostrando la volontà di adottare per la normativa relativa alle statistiche ufficiali la nozione diffusa del termine[90]. In mancanza di una definizione del termine nella normativa relativa alla protezione dati e in considerazione del fatto che il legislatore comunitario laddove ha definito la nozione di statistica si è attenuto alla definizione lessicale del termine si può parlare di

---

[88] Sul punto v. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali, dalla direttiva 95/46 al nuovo regolamento europeo*, Giappichelli, Torino, 2016, 141 e 142.

[89] V. (voce)Statistica, in Vocabolario Treccani online; (voce) Statistica, in Vocabolario Garzanti online.

[90] Sulla valenza e il significato delle definizioni lessicali e delle ridefinizioni v. BELVEDERE, *Aspetti ideologici delle definizioni nel linguaggio del legislatore e dei giuristi*, in *Definizioni giuridiche e ideologiche*, (a cura di) BELVEDERE, JORI e LANTELLA, Giuffrè, Milano, 1979, 349 ss..

trattamento dati a fini statistici quando i dati personali vengono utilizzati per lo studio di un fenomeno collettivo relativo ad una determinata popolazione, attraverso l'estrazione da questo di informazioni quantitative o qualitative. Dalla nozione qui accolta sembrerebbe potersi ricavare che la disciplina riservata per il trattamento dati a fini statistici possa applicarsi sia ai soggetti privati(imprese) che effettuano tale trattamento sia agli enti pubblici[91]. La presente definizione non fa alcun riferimento al soggetto che compie l'attività statistica. Ad ulteriore conferma di ciò si consideri il fatto che la direttiva 95/46/CE al considerando 34 effettua un riferimento esplicito alle statistiche pubbliche, mostrando la consapevolezza del legislatore di ricondurre nella disciplina del trattamento statistico generale anche quello effettuato da soggetti privati, riservando alle statistiche pubbliche un quadro normativo più dettagliato. A sua volta il nuovo regolamento sulla protezione dei dati effettua una distinzione analoga al considerando 163, che contiene delle statuizioni riferite solamente alle statistiche ufficiali europee e nazionali. Si consideri anche che il legislatore europeo quando è voluto intervenire per disciplinare le statistiche ufficiali lo ha fatto con un apposito strumento, quale il reg. 223/2009 che si riferisce specificatamente ad esse e non a quelle di matrice privata. Infine il fatto che l'allegato alla Raccomandazione N.R. (83) 10 del CDE detti principi applicabili al trattamento dati a fini statistici nel settore pubblico e nel settore privato e che la Raccomandazione N.R. (97) 18 del CDE nel suo incipit consideri il trattamento dati a fini statistici come un utile strumento per l'analisi e la conoscenza della società contemporanea sia nel settore privato che pubblico è indice di una prassi diffusa a livello internazionale di considerare tale tipo di trattamento un'attività che possa essere effettuata sia da operatori privati che pubblici. Si può quindi affermare che in assenza di specificazioni quando si fa riferimento a tale tipologia di utilizzo dei dati personali non si tenga minimamente in considerazione la natura pubblicistica o privatistica del titolare[92]. Più precisamente, salvo rare ipotesi in cui vi è una disciplina specifica per

[91]Per soggetti pubblici si vuole indicare tutti quei soggetti istituzionali a cui è affidato il compito di redigere statistiche ufficiali. Per la possibilità di applicare la disciplina del trattamento dati a fini statistici anche ai soggetti privati v. MAYER-SCHOENBERGER&PADOVA , op. cit., 326 ss..

[92]Anche nell'ordinamento italiano il legislatore interno quando intende riferirsi al sistema statistico nazionale fa un riferimento espresso, v. ad esempio: Dlgs. n. 322/1989; L. n. 59/1997 art. 1. Mentre nel codice privacy quando parla di trattamento di dati personali a fini statistici (art. 97 ss.) il legislatore non fa alcuna distinzione sul soggetto preposto al trattamento di tali informazioni. Contra la possibilità per i soggetti privati di avvalersi della disciplina di favore riservata al trattamento statico v. OTTOLIA, *Big data e innovazione computazionale*, cit., 97 ss.. L'autore, contrariamente a quanto qui sostenuto, individua diversi indici da cui desumere che tale tipo di trattamento sia volto unicamente a perseguire fini in senso lato pubblici: i) collocazione sistematica all'interno del regolamento europeo della disciplina riservata al

determinati ambiti del settore pubblico (es. reg. 223/2009), di norma l'utilizzo di dati personali per effettuare analisi statistica non è precluso ai privati e si applicano a tali soggetti le medesime norme previste per i soggetti pubblici. Indubbiamente ciò conferma l'enorme utilità del trattamento a fini statistici per le imprese che vogliano elaborare e studiare enormi quantità di dati.

3. Una volta superati i problemi definitori e chiarito quali sono i destinatari della normativa occorre soffermarsi sul contenuto della disciplina riservata al trattamento dei dati a fini statistici dalla normativa europea e interna. Il primo riferimento a tale tipo di trattamento risale alla Convenzione n. 108 del 1981, adottata a Strasburgo dal Consiglio d'Europa, che si occupa della «protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale» e rappresenta tuttora l'unico atto internazionale giuridicamente vincolante in questa materia[93]. Come in parte già anticipato, analizzare tale convenzione è molto importante in considerazione dell'influenza della CEDU sull'ordinamento comunitario[94].

In questa convenzione vengono enunciate una serie di regole generali che saranno alla base della protezione dei dati personali negli anni a seguire. Si pensi ad esempio all'art. 5 che nel disciplinare la qualità dei dati fissa diversi principi, come quello di liceità, di esattezza, di finalità, di proporzionalità, di minimizzazione; oppure ai diritti previsti all'art. 8 a favore dell'interessato: diritto di accesso, diritto alla rettifica, alla cancellazione e al ricorso in caso di elaborazione automatizzata dei dati realizzata in violazione delle norme dettate dalla convenzione.

Il riferimento al trattamento dei dati a fini statistici è contenuto nell'art. 9 co. 3 della Convenzione. In questo articolo il Consiglio d'Europa stabilisce dell'eccezioni e restrizioni all'esercizio dei diritti da parte del titolare dei dati trattati, tra queste vi è la facoltà degli stati di prevedere in via legislativa delle restrizioni all'esercizio di alcuni diritti stabiliti dall'articolo 8 per «i casellari automatizzati di dati di carattere personale impiegati a fini statistici o di ricerca scientifica», purché non vi sia un rischio manifesto

---

trattamento dati a fini statistici nell'ambito di trattamenti che perseguono interessi pubblici (e.g. per fini di archiviazione, di ricerca scientifica o storica); ii) continui riferimenti ai principi cardine della normativa relativa alle statistiche ufficiali all'interno delle disposizioni che disciplinano tale tipologia di utilizzo di dati personali.

[93]Per un approfondimento sulla convenzione v. FRA, CED e COE, *Manuale sul diritto europeo in materia di protezione dei dati*, Belgio, 2014, 15.

[94] PIZZETTI, ibidem.

di violazione della vita privata delle persone interessate. Più precisamente al legislatore ordinario dei singoli stati membri è concessa la possibilità di derogare al diritto di rettifica di cancellazione e al diritto di ricorso, ma non al diritto di accesso stabilito all'art. 8 lett. a)[95], rispettando il limite di non invasione eccessiva della sfera privata del cittadino titolare dei dati trattati. A tal proposito il rapporto esplicativo che accompagna la convenzione afferma che non vi è un'eccessiva invasione della sfera privata del cittadino quando l'utilizzo a fini statistici dei dati avvenga in forma aggregata e questi siano spogliati dei loro identificatori, consigliando così ove possibile che il trattamento avvenga con dati anonimi. Questa soluzione viene confermata anche nell'Allegato alla Raccomandazione N.R. (83) 10 del CDE che, dopo aver ricondotto il trattamento dati a fini statistici nella più ampia categoria del trattamento dati a fini di ricerca, nell'art. 2 co. 2 indica la necessità di valutare in via prioritaria la possibilità di ricorrere all'anonimizzazione nell'utilizzazione di dati per fini di ricerca[96]. Successivamente a questa raccomandazione, come già accennato, nel 1997 viene adottata un'altra raccomandazione relativa al trattamento dei dati a fini statistici, che individua una disciplina più puntuale da riservare a tale tipo di utilizzazione dei dati. La raccomandazione infatti ha introdotto alcuni principi, che coincidono con quanto sancito dalla direttiva 95/46/CE, e norme più dettagliate che, rispettando e applicando tali principi, vanno a costituire una linea guida più dettagliata per il trattamento dei dati a fini statistici. In questo testo è stabilito che i dati raccolti da un titolare del trattamento a fini statistici non possano essere usati per nessun altro scopo, e quelli trattati per scopi non statistici siano utilizzabili ulteriormente a fini statistici. L'ulteriore trattamento a fini statistici è considerato compatibile solo se vengono prese adeguate garanzie finalizzate soprattutto ad impedire che tali dati siano utilizzati per decisioni che abbiano effetti nei confronti dell'interessato. In considerazione del fatto che il trattamento ulteriore può prescindere dal consenso dell'interessato è necessario che la legislazione nazionale introduca garanzie ulteriori in modo da ridurre al minimo qualsiasi rischio di abuso sui dati personali così trattati. In via esemplificativa la raccomandazione individua, quali strumenti utili per la protezione dei dati nel trattamento a fini statistici, l'utilizzo di due

[95]Il diritto di «conoscere l'esistenza di un casellario automatizzato di dati a carattere personale, i suoi fini principali, nonché l'identità e la residenza abituale, ovvero la sede amministrativa, del responsabile del casellario»,

[96]Art. 2 co. 2 Raccomandazione N.R. (83) 10 del CDE: «Nella misura del possibile, la ricerca deve utilizzare dati anonimi».

misure. Quando è possibile si deve usare la tecnica dell'anonimizzazione, se questa non è utilizzabile occorre ricorrere alla pseudonimizzazione. Inoltre è stabilito che, qualora il trattamento a fini statistici richieda l'uso di dati personali, non appena raggiunto lo scopo dello studio i dati devono essere privati dei loro elementi identificativi. La raccomandazione introduce anche delle indicazioni per chi effettua attività di ricerca statistica in via professionale invitando i singoli ordinamenti nazionali a prevedere per tali soggetti degli obblighi di segreto professionale. Essa ammette la comunicazione dei dati a terzi solo se ciò avvenga per fini statistici e le parti abbiano concordato per iscritto la portata dell'utilizzo dei dati da parte del terzo. Ogni trattamento dei dati a fini statistici che non sia prescritto dalla legge deve essere pubblicizzato come tale e deve essere effettuato in modo da consentire agli interessati di prestare il loro consenso od opporsi all'utilizzo dei loro dati. È previsto un regime più rigido per i dati sensibili che non devono essere raccolti in modo da consentire l'identificazione della persona interessata sempreché non vi siano deroghe in tal senso da parte dei singoli ordinamenti nazionali[97]. Infine è previsto che i risultati statistici non dovrebbero acconsentire all'identificazione di nessuno degli interessati a cui si riferiscono i dati oggetto di trattamento a meno che ciò non presenti alcun rischio manifesto[98].

Successivamente alla Convenzione n. 108 del 1981 vi è stato un intervento del legislatore comunitario che il 24 ottobre del 1995 adotta la direttiva «relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati», disciplinando per la prima volta a livello comunitario il diritto alla protezione dei dati sia nel settore privato che pubblico. Nella predisposizione di questo testo il legislatore tiene inevitabilmente conto degli strumenti internazionali sulla protezione dei dati allora esistenti. L'obiettivo della normativa infatti è stato quello di armonizzare la disciplina fra i diversi stati membri in modo da semplificare la libera circolazione dei dati nello spazio economico europeo garantendo al contempo la protezione dei diritti e delle libertà fondamentali. Per fare ciò inevitabilmente si è dovuti partire dal livello di protezione offerto dai singoli stati membri e dagli strumenti internazionali in modo da esaltare i punti in comune e riavvicinare le varie discipline[99].

---

[97] Anche se a proposito di utilizzo dei dati sensibili la discrezionalità dei singoli ordinamenti firmatari della CEDU è estremamente ridotta. Per un approfondimento v. PAGALLO, *La tutela della privacy negli Stati Uniti d'America e in Europa*, Giuffrè, Milano, 2008, 51.

[98] V. FRA, CED e COE, op. cit., 188 e 189

[99] V.WP29 Opinion 03/2013 on purpose limitation, 9; Commissione Europea, Evaluation of the implementation of the data protection directive, 2012, 2.

Il testo è stato adottato in un'epoca dove internet non era ancora sviluppato ed era imprevedibile il progresso tecnologico attuale, in particolare era impensabile un incremento così rilevante della circolazione delle informazioni personali. La direttiva interviene in un momento dove la raccolta e il relativo trattamento di dati personali richiede il dispiego di diverse risorse e quindi viene intrapreso con una certa parsimonia[100] per cui inevitabilmente il testo non regola attività e prassi che si sono affermate successivamente per via dello sviluppo tecnologico, tuttavia grazie alla flessibilità delle sue clausole e dei suoi principi è stato possibile, tramite gli organi a ciò predisposti[101], intervenire con un interpretazione in chiave evolutiva che mantenesse attuale il testo e sopperisse alla lentezza del legislatore europeo, cosicché si è riusciti ad adeguare il tessuto normativo ai cambiamenti determinati dall'evoluzione tecnologica. Infatti, la direttiva si caratterizza per essere tecnologicamente neutrale con principi e norme sufficientemente generiche da consentire un continuo adeguamento alle nuove situazioni che si vengono a creare con lo sviluppo tecnologico[102]. Per questo motivo è molto importante nell'analisi del testo normativo far riferimento alle guide e alle prassi affermate dagli organi che hanno svolto un ruolo chiave nell'attualizzazione del dettato normativo[103].

In base alla direttiva il trattamento dati a fini statistici può avvenire in due differenti modalità: o si ricorre ad un'apposita base giuridica[104], quale ad esempio il consenso dell'interessato; o si rispetta il principio di finalità, ossia il trattamento ulteriore dei dati a fini statistici non richiede una nuova base giuridica, purché esso non sia incompatibile con le finalità iniziali su cui si è basata la raccolta dei dati. In particolar modo dall'art. 6 e dal considerando 29 si ricava che i dati inizialmente raccolti per fini determinati espliciti e legittimi possono essere sottoposti ad ulteriori trattamenti che non siano incompatibili con le finalità inziali e che il trattamento per scopi statistici non è generalmente considerato incompatibile, purché gli stati membri introducano adeguate

[100] MAYER SCHOENBERGER e PADOVA, op. cit., 321.

[101] Si fa riferimento alle attività interpretative del WP29, della CGUE e delle singole autorità nazionali.

[102] V. PAGALLO, *Il diritto nell'età dell'informazione: il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti*, cit., 285; Comissione Europea, Evaluation of the implementation of the data protection directive, 2012, 2.

[103] Si fa riferimento in particolare alla Corte di Giustizia della CE(poi UE), al Gruppo di lavoro ex art. 29 (WP29), e al Garante per la protezione dei dati personali, nonché alle altre Autorità di controllo degli stati membri.

[104] V. art. 7 dir. 95/46/CE. Il trattamento dati normalmente per essere effettuato necessità di un'apposita base giuridica che può essere costituita dal consenso dell'interessato oppure dall'obbligo legale del responsabile oppure, ad esempio per le statistiche pubbliche, dall'esecuzione di un compito di interesse pubblico ecc...

garanzie volte ad evitare soprattutto che l'uso dei dati sia posto in essere per adottare misure o decisioni nei confronti di singole persone o individui. Questa possibilità offerta dalla direttiva è molto importante per l'analisi big data perché molto spesso il valore dei dati non è comprensibile al momento della raccolta, esso viene compreso in fasi successive attraverso la combinazione con altre fonti di dati[105]. Tuttavia l'agganciamento espresso al principio di finalità, implica dei limiti nel riutilizzo dei dati perché, come chiarito dal WP29, l'ulteriore trattamento dei dati a fini statistici non richiede una nuova base giuridica solo se è dimostrata la sua compatibilità con il trattamento dati realizzato anteriormente. Ciò in considerazione del fatto che non si tratta di una presunzione assoluta, d'altronde sul punto il considerando 29 della direttiva è molto chiaro laddove statuisce che il trattamento dati per fini statistici non è generalmente considerato incompatibile[106].

Occorre quindi analizzare il principio di finalità e più specificatamente il concetto di incompatibilità per poter chiarire al meglio quando il trattamento a fini statistici possa avvenire senza il consenso dell'interessato o senza altra base giuridica.

Il principio di limitazione delle finalità statuisce, come è possibile ricavare dall'art. 6 della direttiva, che i dati personali possono essere trattati solo sulla base di una finalità concretamente individuata al momento della raccolta e quando tale scopo è stato soddisfatto i dati devono essere eliminati. Trattare i dati per un ulteriore e nuovo proposito è proibito a meno che non sia un trattamento non incompatibile. Risulta evidente che detto principio è formato da due componenti: la prima riguarda le finalità del trattamento che devono essere determinate esplicite e legittime; la seconda, che è quella su cui si focalizzerà principalmente il discorso, è costituita dal concetto di compatibilità. Nel loro insieme le due componenti del principio garantiscono che il trattamento dei dati sia trasparente, avvenga in un contesto di certezza legale e prevedibilità, assicurando al contempo un certo grado di flessibilità. Infatti, il fatto che le finalità debbano essere determinate esplicite e legittime chiarisce subito le possibilità

---

[105]V. MAYER SCHOENBERGER e PADOVA, op. cit., 319 e 320;v. supra nota 4. Sull'utilizzo di fonti eterogenee per l'analisi big data v. MORO VISCONTI, *Valutazione dei big data e impatto su innovazione e digital branding*, in *IDI* 2016, 46 ss..

[106] Come chiarito dalla direttiva 95/46/CE al considerando 29 l'ulteriore trattamento per fini statistici non è generalmente considerato incompatibile, ciò è stato interpretato dal WP29 nell'Opinion 03/2013 come una specificazione dei casi in cui il trattamento può essere compatibile. In altri termini oltre all'ulteriore trattamento per fini statistici scientifici e storici vi possono essere altri trattamenti che se rispettano i criteri della compatibilità possono essere effettuati senza ricorrere ad un'altra base giuridica. WP29, ibidem, 39.

di utilizzo dei dati da parte del titolare del trattamento, mentre il concetto di uso compatibile, come correntemente interpretato dal WP29, permette che gli stessi siano trattati per fini ulteriori a quelli specificati al momento della raccolta. In molti casi infatti, come nella prospettiva dell'analisi big data, può accadere che il rapido sviluppo tecnologico renda possibile utilizzare più proficuamente i dati raccolti raggiungendo finalità ulteriori rispetto a quelle per le quali si era iniziato il trattamento[107]. Per quanto riguarda la prima componente del principio, come già detto, la finalità deve essere determinata ciò significa che occorre predeterminare prima di procedere alla raccolta gli scopi che si intende perseguire con il trattamento. La finalità deve essere anche esplicita, ossia deve essere chiara in modo da poter essere compresa da qualsiasi persona allo stesso modo a prescindere dal suo livello culturale e inoltre deve essere espressa nella lingua madre di ciascun soggetto destinatario del trattamento e non deve in alcun modo contenere termini ambigui[108]. Infine la finalità deve essere legittima e sul punto, come chiarisce il WP29, la legittimità dello scopo non va valutata solo con riferimento all'art. 7 che regola le basi giuridiche del trattamento ma occorre tenere in considerazione anche i vari divieti imposti da altri settori della legge, a tal fine occorre procedere a verificare la legittimità guardando con particolare attenzione al contesto del trattamento[109].

La seconda componete del principio di limitazione delle finalità, come detto sopra, richiede la verifica della ammissibilità dei fini ulteriori che, a parere del WP29, deve essere un controllo sostanziale e non solo formale, ossia non è sufficiente un semplice confronto tra i propositi iniziali e gli usi successivi per verificare se le finalità ulteriori sono coperte implicitamente o esplicitamente dagli scopi per i quali è stato iniziato il trattamento. È necessario tenere in considerazione diversi fattori, quali ad esempio il contesto, il modo in cui avviene il trattamento, se la finalità poteva essere prevista ecc.. Un controllo sostanziale consente una maggior flessibilità ed è più effettivo perché permette di adattarsi agli sviluppi tecnologici continuando a garantire la protezione dei

---

[107] WP29, Opinion 03/2013 on purpose limitation, 1, 11 e 21.V. supra par. 1; v. anche MANTELERO, *Rilevanza e tutela della dimensione collettiva della protezione dei dati personali*, cit., 142: «L'analisi dei big data rende possibile dedurre informazioni predittive da grandi masse di dati, al fine di conoscere ulteriori aspetti relativi a individui e gruppi, che possono anche non essere correlate alle finalità iniziali di raccolta dei dati».

[108] La finalità viene esplicitata all'interessato attraverso un apposito strumento: l'informativa, v. art. 13 del Codice Privacy e art. 13 del Regolamento Europeo sulla protezione dei dati personali.

[109] V. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali, dalla direttiva 95/46 al nuovo regolamento europeo*, cit., 251; WP29 Opinion 3/2013, 11 ss..

dati personali[110]. È stato poi compito degli stati membri individuare i canoni in base ai quali valutare la compatibilità e sul punto occorre rilevare che vari paesi membri dell'Unione Europea hanno inteso tale concetto in modo non univoco[111].

Il WP29 nel suo parere sul principio di finalità individua quattro fattori chiave che devono essere considerati quando si effettua la valutazione della compatibilità del trattamento ulteriore. Il primo fattore chiave tiene in considerazione la relazione tra la finalità iniziale per cui si è proceduto alla raccolta dei dati e la finalità per la quale si vuole procedere all'ulteriore trattamento. La relazione gioca un ruolo fondamentale perché la compatibilità è certa se da un confronto non solo testuale ma sostanziale risulta che la prima finalità ricomprende la seconda, o comunque l'ulteriore trattamento è il logico passo successivo al raggiungimento delle finalità del primo. Più è ampia la distanza fra le due finalità più è difficile attestare la compatibilità. Per valutare la relazione intercorrente tra i due diversi trattamenti occorre tenere in considerazione anche il contesto in cui avviene il trattamento e come certe finalità vengano comprese dai soggetti coinvolti e, proprio su questo punto, entra in gioco il secondo fattore che impone di tenere in considerazione il contesto in cui si è proceduto alla raccolta dei dati e la ragionevole aspettativa dei titolari dei dati sul loro uso ulteriore. In questo caso sarà fondamentale valutare la natura della relazione fra il titolare del trattamento e gli interessati. Non solo per determinare i limiti legali a cui il titolare è sottoposto nel trattamento dei dati raccolti, ma anche per porre in evidenza quali sono le consuetudini e le prassi sull'ulteriore trattamento in un determinato tipo di relazione. In altri termini la relazione tra le parti ha un ruolo cruciale per poter porre in luce per che cosa è ragionevole aspettarsi che i dati vengano trattati, se la relazione è di tipo commerciale oppure è di tipo lavorativo l'aspettativa dell'interessato sull'uso dei suoi dati sarà diversa. Nel valutare tale tipo di legame non si può non tenere in considerazione se il soggetto titolare dei dati sia obbligato ad avere tale tipo di relazione con il controller[112] oppure sia vincolato contrattualmente a tale trattamento e se abbia o meno la possibilità di cambiare titolare del trattamento senza alcuna difficoltà. Infatti più sarà vincolante la relazione più sarà limitato l'uso ulteriore dei dati perché è ragionevole che l'interessato consideri maggiormente confidenziali le informazioni trasmesse se non ha alcuna

[110]WP29, Opinion 3/2013, 21 e 22.

[111]V. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali, dalla direttiva 95/46 al nuovo regolamento europeo*, cit., 249.

[112] Il termine controller è il termine inglese utilizzato per indicare il titolare del trattamento.

possibilità di scelta, o comunque è ristretta la sua possibilità di scelta. Il terzo fattore chiave tiene in considerazione unitamente due aspetti: la natura dei dati e l'impatto che un ulteriore trattamento potrebbe avere sugli interessati. Il primo aspetto può considerarsi ricompreso nel secondo, infatti più i dati sono sensibili più sarà limitata la possibilità di un riutilizzo degli stessi perché è più probabile che vi sia un impatto negativo nei confronti dei soggetti interessati proprio per le caratteristiche particolari dei dati trattati. Nel valutare l'impatto di un ulteriore trattamento occorrerà tenere in considerazione sia le conseguenze positive e negative. Sarà necessario verificare ad esempio se con il successivo utilizzo dei dati vi è il rischio di una discriminazione oppure se l'uso non essendo pienamente prevedibile possa comportare una situazione di diffidenza dei soggetti interessati nel porre in circolazione i propri dati. Nell'analizzare le eventuali conseguenze negative e positive è importante tenere in considerazione anche il modo in cui i dati sono ulteriormente trattati, perché si potrebbero verificare delle tensioni col rispetto della compatibilità se il modo di trattarli non permettesse di valutare preventivamente l'impatto del trattamento ulteriore, così se ad esempio i dati fossero trattati da diversi titolari in altri contesti, oppure se questi fossero combinati con altri dati, oppure se fossero resi pubblici o accessibili ad un largo numero di persone, non sarà sempre prevedibile quali conseguenze vi potranno essere nei confronti dei titolari dei dati (cd. interessati). Infine l'ultimo fattore chiave preso in considerazione dal WP29 concerne le misure di sicurezza applicate dal titolare per assicurare un trattamento corretto e per prevenire qualsiasi impatto eccessivo per le persone interessate. Il non pieno rispetto di alcuni requisiti può essere compensato dall'applicazione di idonee misure di salvaguardia, come ad esempio l'anonimizzazione la pseudonimizzazione, oppure l'incremento della trasparenza o la richiesta di un successivo consenso da parte del titolare dei dati per procedere al trattamento ulteriore. La valutazione della compatibilità avviene tramite un giudizio di bilanciamento tra i diversi fattori determinati dal contesto e l'elevato livello di sicurezza del trattamento può ridurre la necessità che altri criteri siano pienamente rispettati[113].

Il trattamento dei dati a fini statistici, come quello per finalità storiche o di ricerca scientifica, può essere generalmente considerato come un trattamento ulteriore compatibile, come precisato dal WP29 si tratta di una specificazione[114], se rispetta i

[113] WP29, Opinion n. 3/2013, 23 ss..
[114] V. supra nota 36.

criteri sopra esposti, in particolar modo, come già accennato, la direttiva si sofferma in particolare sulla necessità che per queste tipologie di trattamenti ulteriori gli stati membri prendano adeguate misure di sicurezza volte ad impedire che i dati possano essere utilizzati per supportare misure o decisioni riferibili ai singoli individui[115], ossia occorre che sia assicurata la separazione funzionale.

Per assicurare la separazione funzionale il WP29 individua tre differenti tecniche d'applicare alternativamente a seconda del contesto e del fine concreto perseguito: l'anonimizzazione[116]completa,o parziale, la pseudonimizzazione[117] e solo quando queste misure rischiano di far sfumare il fine del trattamento possono essere utilizzati dati personali direttamente riconducibili ai loro titolari (cd. interessati) purché si siano adottate altre misure di sicurezza, come quelle elencate in precedenza, volte ad assicurare la separazione funzionale[118]. L'ordine con cui valutare quale strumento

---

[115] È evidente sul punto il richiamo all'art. 9 co. 3 della convenzione 108 del 1981 che come evidenziato sopra statuisce che: «Restrizioni all'esercizio dei diritti di cui ai paragrafi b), c) e d) dell'art. 8 possono essere previste dalla legge per i casellari automatizzati di dati di carattere personale impiegati a fini statistici o per ricerche scientifiche, laddove non esista manifestamente il rischio di violare la vita privata delle persone interessate». V. supra par. 3.

[116] Una volta reso anonimo al dato non si deve più applicare la normativa sulla protezione dati, se, come si ricava dal considerando 26 della direttiva 95/46/CE e dall'art. 3 del codice privacy, il trattamento è irreversibile e l'interessato a cui si riferisce il dato non è più identificabile mediante i mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri. Come chiarito dal WP29 nel parere n. 5 del 2014, il processo di anonimizzazione dei dati è un trattamento ulteriore di dati, quindi per poter essere effettuato deve essere rispettata la compatibilità con il trattamento precedente seguendo i canoni illustrati nel parere n. 3 del 2013 del WP29. La dottrina è divisa sull'utilità dell'anonimizzazione nel contesto tecnologico attuale. Da una parte vi è chi sostiene l'inutilità dell'anonimizzazione in considerazione del crescente sviluppo tecnologico che permette sempre più di risalire all'interessato incrociando dati provenienti da diverse fonti(per tutti v. OHM, op. cit., 2010, 1701 ss..). Poi vi è quella parte della dottrina che considera l'anonimizzazione, nonostante i suoi limiti, una misura di sicurezza molto utile, soprattutto nel caso in cui il soggetto che viene a contatto con i dati anonimizzati non ha la motivazione, la capacità tecnologica o le risorse necessarie per riuscire a re-identificare l'interessato (per tutti v. CAVOUKIAN and ELEMAM, *Dispelling the myths surrounding de-identification: Anonymization remains a strong tool for protecting privacy*, IPC, June 2011, 1 ss.: molto efficace la similitudine con la porta di casa, utilizzata in questo articolo, per dimostrare la necessità di ricorrere comunque all'anonimizzazione nonostante questa tecnica possa, come una porta, non essere sufficiente a proteggere gli interessi tutelati costituisce pur sempre un ottimo disincentivo nei confronti dei terzi). V. anche FINOCCHIARO, *Il contratto nell'era dell'intelligenza artificiale*, in *Riv. trim. dir e proc. civ*. 2018, 441.

[117] Come precisato dal WP29 nel parere n. 5 del 2014,la pseudonimizzazione non è una tecnica di anonimizzazione ma bensì una misura di sicurezza diretta a ridurre la correlabilità di un determinato dato ad una determinata persona. Essa «…consiste nel sostituire un attributo (solitamente un attributo univoco) di un dato con un altro. La persona fisica potrebbe pertanto essere ancora identificata in maniera indiretta…» (v. WP29, parere 05/2014, 21 ss.). In altri termini gli identificatori diretti vengono sostituiti con codici o numeri, cosicché si possa nel prosieguo del trattamento raccogliere dati ulteriori senza la necessità di conoscere l'identità degli individui sottoposti al trattamento. V. BANTERLE, op. cit., 584; POLONETSKY, TENE, KELSEY, *Shades of Gray: Seeing the full spectrum of pratical data deidentification*, in *Santa Clara law review* 2016, 593.

[118]WP29, Opinion n. 3/2013, 28 ss.. L'assunto interpretativo del WP29, come si è visto nel paragrafo precedente, è stato anticipato dalla raccomandazione del 1997 del Consiglio d'Europa che si riferisce espressamente all'anonimizzazione e alla pseudonimizzazione. Per un ulteriore approfondimento

applicare è imposto dal principio di adeguatezza pertinenza e non eccedenza come sancito dalla lett. c) dell'art. 6 della direttiva, il quale stabilisce che i dati trattati devono essere «adeguati e pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o successivamente trattati»[119]. Il principio di minimizzazione dei dati apparentemente si pone in contrasto con l'analisi big data che incentiva la raccolta e la conservazione più ampia possibile di dati. Per tale motivo è necessario trovare un punto di equilibrio tra le utilità derivanti dall'analisi big data e i rischi per la privacy. Ciò è possibile imponendo che: (i) i dati vengano utilizzati, ove possibile, in forma anonima; (ii) siano implementate opportune misure di sicurezza e (iii) sia limitato l'uso dei dati alla luce non solo dell'utilizzo accettabile dal singolo individuo ma anche da una valutazione sull'accettabilità dell'uso in una prospettiva sociale[120].

In base all'art. 99 del codice privacy i trattamenti ulteriori a fini statistici possono essere effettuati anche oltre il periodo di tempo previsto per il raggiungimento degli scopi per i quali i dati sono stati inizialmente raccolti e trattati. Inoltre gli stessi dati quando è cessato il loro trattamento iniziale possono essere ceduti ad altro titolare o conservati ulteriormente per scopi statistici. Per quanto concerne l'informativa si applica l'art. 13 e lo scopo statistico deve essere chiaramente determinato e reso noto all'interessato, a meno che il trattamento a fini statistici avvenga come trattamento ulteriore in tal caso l'informativa non è necessaria quando richiede uno sforzo sproporzionato rispetto al diritto tutelato. Occorrerà pur sempre rispettare le forme di pubblicità individuate dai codici di deontologia, in particolare si deve far riferimento, in forza dell'art. 105 co. 4, all'art. 6 co. 4 del Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici che prescrive le forme di pubblicità da adottarsi[121].

---

sull'anonimizzazione e la pseudonimizzazione v. PAGALLO, *Il diritto nell'età dell'informazione: il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti*, cit., 244-245; PAGALLO and BASSI, *Open data protection: Challenges, perspectives, and tools, in Digital enlightenment year book 2013: the value of personal data*, a cura di HILDEBRANDT, O'HARA, WAIDNER, IOS press, Amsterdam, 2013, 183 e 185 ss..

[119] V. anche art. 3 cod. privacy. Cfr. MORELATO, *Anonimato e protezione dei dati personali*, in *Diritto all'anonimato*, (a cura di) FINOCCHIARO, CEDAM, Padova, 2008, 209 ss..

[120] V. TENE & POLONETSKY, op. cit., 259 e 260; PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali, dalla direttiva 95/46 al nuovo regolamento europeo*, cit., 255 ss..

[121] Art. 6 co. 4 cod. deont. trattamento per scopi statistici e scientifici: «Quando i dati sono raccolti presso terzi, ovvero il trattamento effettuato per scopi statistici o scientifici riguarda dati raccolti per altri scopi, e l'informativa comporta uno sforzo sproporzionato rispetto al diritto tutelato, il titolare adotta forme di pubblicità con le seguenti modalità: per trattamenti riguardanti insiemi numerosi di soggetti distribuiti sull'intero territorio nazionale, inserzione su almeno un quotidiano di larga diffusione nazionale o annuncio presso un'emittente radiotelevisiva a diffusione nazionale;

Nella direttiva il legislatore europeo lascia agli stati membri l'individuazione dei criteri per la determinazione della compatibilità dell'ulteriore trattamento. Sul punto il codice privacy all'art. 99 co. 1 dichiara la compatibilità del trattamento ulteriore fatto per fini statistici con i diversi scopi per i quali si è proceduto a raccogliere e trattare i dati in precedenza, stabilendo che tale trattamento possa essere effettuato oltre il periodo di tempo necessario per il raggiungimento dei fini per i quali si è avuta la raccolta dei dati. Inoltre è previsto che qualora sia cessato il trattamento i dati trattati per scopi statistici possano essere conservati o ceduti ad un altro titolare. L'art. 105 del codice poi stabilisce che i dati personali trattati per scopi statistici non possano essere utilizzati per assumere decisioni o provvedimenti nei confronti dell'interessato, né possano essere utilizzati successivamente per ulteriori trattamenti. In apparenza il codice non prevede alcunché per quanto riguarda le misure d'adottare per assicurare la separazione funzionale, ma a tal proposito, a parere di chi scrive, si può ricorrere all'art. 31. Infatti se non viene assicurata la separazione funzionale l'ulteriore trattamento dati per fini statistici è un trattamento non consentito e l'articolo, appena menzionato, prescrive l'obbligo di adottare idonee misure di sicurezza volte ad evitare che un trattamento diventi non consentito. Tali misure sono determinate in relazione alle conoscenze acquisite in base al progresso tecnico e alle specifiche caratteristiche del trattamento[122]. In definitiva sembrerebbe che la separazione funzionale debba essere assicurata dalle buone prassi diffuse in tale ambito, un sicuro strumento utile sono i pareri del WP29 riguardanti l'anonimizzazione e la pseudonimizzazione.

Occorre soffermarsi su come concretamente operi la separazione funzionale e cosa comporti. Sul punto, come già detto, il codice privacy in modo più puntuale rispetto alla direttiva riferisce il rispetto della separazione funzionale all'interessato i cui dati personali sono stati oggetto di trattamento. La direttiva prevede solo che i dati personali oggetto del trattamento statistico non siano utilizzati per supportare decisioni nei confronti di singole persone fisiche senza alcuna specificazione. Posto che vi è una

---

per trattamenti riguardanti insiemi numerosi di soggetti distribuiti su un'area regionale (o provinciale), inserzione su un quotidiano di larga diffusione regionale (o provinciale) o annuncio presso un'emittente radiotelevisiva a diffusione regionale(o provinciale) ;per trattamenti riguardanti insiemi di specifiche categorie di soggetti, identificate da particolari caratteristiche demografiche e/o da particolari condizioni formative o occupazionali o analoghe, inserzione in strumenti informativi di cui gli interessati sono normalmente destinatari.»

[122]Per un approfondimento sulle misure di sicurezza v. PAGALLO, *Il diritto nell'età dell'informazione: il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti*, cit., 238 ss.;

specificazione nel codice occorre riferirsi ad esso su questo punto, per cui lo scopo della separazione funzionale, come declinato nell'ordinamento italiano, a parere di chi scrive, è quello di evitare che vengano prese decisioni o misure nei confronti dell'interessato i cui dati sono stati oggetto di trattamento statistico. È necessario quindi indagare in che modo il legislatore ha inteso il concetto di decisione e misure così da chiarire quando si possa ricorrere al trattamento ulteriore e compatibile a fini statistici. È evidente che un supporto per capire il modo di intendere tali concetti può essere ricavato dalla definizione qui accolta di statistica[123] e dalla disciplina riservata alla profilazione, ossia al trattamento dati automatizzato finalizzato a prendere una decisione o una misura nei confronti del soggetto che, prestando il suo consenso, ha accettato di essere profilato o che, sulla base di un legittimo interesse è stato profilato. L'allegato alla raccomandazione n. 13 del 2010 del Comitato dei Ministri del Consiglio d'Europa fornisce la nozione di profilazione all'art. 1: essa è considerata una «tecnica di trattamento automatico consistente nell'applicazione di un profilo ad una persona fisica determinata, in particolare al fine di prendere decisioni relative a tale persona oppure ai fini dell'analisi o della previsione delle sue preferenze, dei suoi comportamenti e delle sue propensioni personali» e profilo: «insieme di dati caratterizzanti una categoria di persone fisiche che si intende applicare ad una persona fisica determinata»[124]. Da queste prime due definizioni, a parere di chi scrive, si ricava che non può rientrare nel trattamento dati a fini statistici la riconduzione di uno specifico soggetto ad una determinata categoria o gruppo di persone. Dal comma 1 dell'art. 15 della direttiva si ricava che per decisioni il legislatore non intende solo quelle produttive di effetti giuridici ma anche qualsiasi misura produttiva di effetti significativi nei confronti dell'interessato. Più specificamente poi il codice privacy all'art. 14 fa rientrare nella disciplina della profilazione qualsiasi tipo di determinazione nei confronti dell'interessato che avvenga tramite un trattamento automatizzato. Da queste norme si ricava che le nozioni di decisioni e misure adottate dal legislatore comunitario e soprattutto da quello interno risultano estremamente ampie. Ciò è confermato anche dalla definizione di statistica posta in luce nel presente lavoro. Infatti se per statistica si intende lo studio da un punto di vista qualitativo o quantitativo di un fenomeno collettivo è evidente che il trattamento dati a fini statistici è lo strumento per ottenere

[123]V. supra par. 2.
[124]Sul valore delle definizioni contenute nelle raccomandazione del Consiglio d'Europa v. supra par. 2.

determinate informazioni e non per prendere alcun provvedimento o misura, quale ne sia la portata, nei confronti del soggetto. Da tutto ciò si ricava che, nel rispetto del principio di finalità e di minimizzazione, i dati personali possano essere oggetto di un trattamento ulteriore per fini statistici, volto ad estrapolare un'informazione da quei dati. L'informazione una volta resa anonima potrà essere applicata ad un terzo soggetto nel rispetto della disciplina stabilita per la profilazione, per cui occorrerà avere una nuova base giuridica, sia essa il consenso dell'interessato o un legittimo interesse del titolare del trattamento[125]. I dati personali oggetto del trattamento a fini statistici possono essere utilizzati per costruire un profilo che successivamente verrà applicato a persone terze che hanno acconsentito alla profilazione[126]. D'altronde questa soluzione, a parere di chi scrive, non stupisce se si considera l'orientamento della Corte di Giustizia emerso nelle decisioni relative alla "privacy nel sistema"[127]. Infatti si deve trovare un equilibrio tra la libertà di impresa e il diritto alla protezione dei dati in modo che entrambi abbiano uno spazio e non vengano svuotati del loro contenuto[128]. L'impresa è libera di utilizzare ulteriormente i dati personali a fini statistici per ottenere nuove conoscenze, ma per poterle applicare nei confronti di determinati soggetti si deve tenere in considerazione il diritto alla protezione dei dati personali di tali persone e quindi occorre passare attraverso la disciplina della profilazione, avendo quindi cura di rispettare tutti gli adempimenti che saranno evidenziati meglio nel successivo paragrafo. D'altronde in un'ottica di bilanciamento dei due contrapposti diritti fondamentali (i.e. la libertà di impresa e il diritto alla protezione dei dati personali) se la comprensione del diritto del titolare dei dati personali è minima e l'impresa ha interesse ad utilizzare i dati solamente per trovare delle correlazioni e ciò avviene in un contesto in cui sono state adottate notevoli cautele ed è stato seguito il procedimento qui descritto, risulta pienamente

---

[125] V. supra par. 2

[126] V. HILDEBRANDT and GUTWIRTH, *Profiling the European Citizen, Cross-Disciplinary Perspectives*, Springer, 2008, 245.

[127]V. supra par. 2.

[128]V. CGCE, C-200/96, MetronomeMusik v. Music point Hokamp, punto 21 ss., in CGUE, C-131/12, Google v. Agencia Espanola de Protecciòn de Datos ECLI, in curia.europa.eu; in questa sentenza la Corte richiamando un orientamento costante in giurisprudenza ribadisce che la libertà di impresa non si deve considerare un diritto assoluto e quindi può subire delle restrizioni giustificate da altri interessi generali, purché tale libertà non venga lesa nella sua sostanza da tali altri diritti fondamentali. Per converso v. CGUE, C-131/12, Google v. Agencia Espanola de Protecciòn de Datos ECLI, cit., punto 68 ss.; la Corte richiamando un orientamento consolidato afferma che il diritto fondamentale alla protezione dei dati personali deve essere interpretato alla luce degli altri diritti fondamentali presenti nella Carta di Nizza e che concorrono a formare i principi generali del diritto. la cui osservanza deve essere garantita dalla Corte.

rispettato il principio di proporzionalità richiamato dagli articoli 52 della Carta di Nizza e 10 co. 2 della CEDU[129].

Il regolamento UE 679 sulla protezione dei dati è uno dei diversi strumenti adottati dal legislatore europeo per l'unificazione del mercato unico digitale. Il testo è entrato in vigore nel mese di maggio del 2016 e sarà effettivamente applicato a partire dal 25 maggio 2018. Con il nuovo regolamento si vuole aggiornare e rendere più attuale la disciplina sulla protezione dei dati tenendo conto dell'enorme evoluzione tecnologica avuta negli ultimi vent'anni, rimediando così all'anacronismo venutosi a creare con la direttiva che veniva applicata per risolvere questioni imprevedibili al momento in cui fu adottata. Inoltre l'intento del regolamento è quello di unificare nel modo più ampio possibile la normativa sulla privacy in modo da emarginare il fenomeno del forum shopping conseguenza dell'attuazione e implementazione delle discrezionalità lasciate ai legislatori nazionali dalla direttiva[130]. Un ruolo chiave nella determinazione di aspetti innovativi del regolamento è stato svolto dal WP29, come si è già in parte visto e si vedrà meglio nel proseguo del testo per il trattamento a fini statistici, e dalla Corte di Giustizia. Molte norme chiave del regolamento, infatti, recepiscono orientamenti interpretativi posti in essere da tali organi[131].

Alla luce del nuovo regolamento il trattamento ulteriore a fini statistici diventa uno strumento ancora più importante rispetto al passato perché sono aumentati i requisiti che il consenso del titolare dei dati (cd. interessato), il legittimo interesse del titolare e l'informativa devono avere, venendo così ad essere più complicato studiare grandi masse di dati personali[132].

Sempre per quanto concerne il trattamento a fini statistici il regolamento nel suo corpus normativo recepisce le innovazioni proposte dal WP29 nell'interpretazione della direttiva. Anche nel regolamento per il trattamento ulteriore dei dati personali a fini statistici non si può sempre far ricorso all'esenzioni offerte dal principio di limitazione delle finalità. Occorre che sia rispettata la compatibilità garantendo la separazione

---

[129] In tal senso v. OTTOLIA, *Big data e innovazione computazionale*, cit. 198.

[130]MAYER- SCHOENBERGER and PADOVA, op. cit., 323 e 324. Per un ulteriore approfondimento dei motivi che hanno portato all'adozione del GDPR(General Data Protection Rules) v. PAGALLO, *Il diritto nell'età dell'informazione: il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti*, cit., 190 ss..

[131]Per il ruolo chiave svolto dalla CGUE v. ad esempio: CGUE, C-131/12, Google v. Agencia Espanola de Protecciòn de Datos ECLI, cit.. In questa sentenza la Corte di Giustizia anticipa, tra le altre cose, l'ampliamento dell'ambito di applicazione territoriale fatto proprio dal regolamento all'art. 3 e il diritto all'oblio recepito nell'art. 17 della nuova disciplina.

[132]V. art. 7 reg. 679/2016.

funzionale nei confronti di persone fisiche specifiche[133]. Su questo punto il considerando 162 del regolamento delinea più precisamente rispetto alla direttiva e all'attuale codice privacy i limiti del trattamento di dati personali a fini statistici. Infatti dal codice privacy e dalla direttiva si ricava che i dati personali trattati a fini statistici non possono essere alla base di provvedimenti o decisioni nei confronti del singolo interessato[134]. Mentre dal regolamento si ricava esplicitamente l'impossibilità di ricorrere anche ai risultati statistici, che devono essere rappresentati in dati aggregati e non personali, per prendere misure o decisioni riguardanti persone fisiche specifiche. Attraverso il ricorso ai considerandi 26 e 162 del regolamento, a parere di chi scrive, è possibile osservare una conferma parziale della soluzione ricavabile in via interpretativa dalla direttiva e dal codice privacy e ottenere la disciplina applicabile ai risultati statistici. Il considerando 26 nella parte finale stabilisce che ai dati anonimizzati non si applica la disciplina del presente regolamento anche qualora questi vengano trattati per finalità statistiche. Il considerando 162 afferma, come in parte anticipato, che i risultati statistici ottenuti tramite il trattamento di dati personali per finalità statistiche non possano in alcun modo essere utilizzati a sostegno di misure o decisioni nei confronti di persone fisiche. Sembra quindi possibile affermare l'esistenza di una duplice disciplina a seconda che i risultati statistici siano stati ottenuti tramite dati personali o per mezzo di dati anonimi. Infatti nell'ipotesi in cui si tratti di risultati statistici ottenuti tramite il trattamento di dati personali scatteranno le limitazioni anzidette, per cui non sarà possibile in alcun modo utilizzarli a sostegno di decisioni o misure nei confronti di persone fisiche specifiche. Il trattamento che utilizza dati personali per finalità statistiche viene quindi relegato esclusivamente allo studio di fenomeni collettivi e disciplinato come un procedimento di elaborazione dati finalizzato alla produzione di conoscenza. Mentre qualora il trattamento a fini statistici avvenga con dati anonimi i risultati statistici così ottenuti potranno essere utilizzati senza incorrere nelle limitazioni del considerando 162, si potrà utilizzare tali risultati a sostegno di misure o decisioni nei confronti delle persone fisiche specifiche passando pur sempre per la disciplina della profilazione.

---

[133] V. considerando n. 162: «…La finalità statistica implica che il risultato del trattamento per finalità statistiche non siano dati personali, ma dati aggregati, e che tale risultato o i dati personali non siano utilizzati a sostegno di misure o decisioni riguardanti persone fisiche specifiche...».
[134]V. supra par. 4.

Una conferma della strumentalità del trattamento di dati anonimi per fini statistici rispetto a quello profilatorio è ricavabile dal considerando 71 laddove si fa riferimento all'utilizzo di procedure statistiche e matematiche per la profilazione[135]. In definitiva sembrerebbe che il regolamento a differenza della direttiva e del codice privacy prediligendo la protezione dei dati personali lasci di conseguenza meno spazio alla libertà di impresa[136]. D'altronde il legislatore comunitario e poi il legislatore interno nel 2003 si sono preoccupati di stabilire una disciplina del trattamento di dati personali per fini statistici protettiva solo nei confronti dell'interessato e non, come nel regolamento, di qualsiasi persona fisica specifica ed inoltre i primi non hanno disciplinato l'utilizzazione dei risultati statistici.

Per quanto riguarda il rispetto della compatibilità, in modo diverso dalla direttiva, i criteri per valutarla sono direttamente disciplinati dal regolamento e non lasciati alla discrezionalità dei singoli stati membri. Alcuni sono disciplinati dal comma 4 dell'art. 5 mentre per quanto riguarda il trattamento ulteriore a fini statistici la compatibilità è assicurata dal rispetto dell'art. 89, come si ricava dall'art. 5 lett. b): «… un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'art. 89, paragrafo 1, considerato incompatibile con le finalità iniziali».

Per il rispetto della separazione funzionale il regolamento a differenza della direttiva impone espressamente di utilizzare: l'anonimizzazione[137] e se questa non fosse possibile occorre ricorrere alla tecnica della pseudonimizzazione[138] e qualora il trattamento non

---

[135]Il regolamento sembra adottare una nozione più ristretta di decisione e misura rispetto a quella evidenziata nel codice privacy.

[136]La soluzione offerta è in linea con altri dettami del regolamento come l'introduzione della valutazione di impatto e della privacy by design che confermano l'intenzione del legislatore europeo di introdurre una disciplina più severa e più gravosa per le imprese che utilizzino dati personali.

[137]Il regolamento al considerando 26 afferma la non applicabilità dei dati resi anonimi ed in modo più analitico stabilisce quando un informazione può considerarsi anonima ed è esente dall'applicazione della normativa sulla protezione dei dati: «… 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. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici. I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca.»

[138]Il regolamento disciplina in modo più analitico, rispetto all'anonimizzazione, la pseudonimizzazione riferendosi ad essa in diversi passaggi del testo normativo. Innanzitutto al considerando 26 e 28 distingue

può avvenire senza l'identificazione degli interessati sarà necessario adottare altre misure tecniche ed organizzative per garantire che il trattamento dei dati a fini statistici non avvenga per supportare decisioni nei confronti degli interessati[139]. Nell'ultimo caso il regolamento lascia agli stati membri l'onere di scegliere quali misure e garanzie adottare in via residuale. Quindi, come nella direttiva, sarà necessario valutare prima la possibilità di ricorre all'anonimizzazione o alla pseudonimizzazione e solamente quando non è possibile utilizzare gli strumenti previsti dagli stati membri, o, come chiarito dal considerando 28, quando la pseudonimizzazione da sola non è sufficiente, si potrà accedere alle ulteriori garanzie adottate dai singoli paesi. Questo ordine di adozione degli strumenti è imposto dal richiamo fatto dal regolamento in più punti al principio della minimizzazione dei dati ed è chiarito dal medesimo al considerando 156 e all'articolo 89[140]. Infatti il principio di minimizzazione dei dati impone che l'utilizzo dei dati personali sia adeguato pertinente e limitato rispetto alle finalità perseguite con il trattamento[141].

Il rispetto delle garanzie e delle misure previste dall'art. 89 può consentire agli stati membri e al diritto europeo di derogare a taluni obblighi e diritti, quali ad esempio: l'obbligo di informativa, il diritto di accesso, di rettifica e di cancellazione dei dati.

Come risulta evidente da queste disposizioni il regolamento lascia ancora una notevole discrezionalità agli stati membri sulle misure e sulle garanzie d'assicurare per garantire la separazione funzionale e derogare ai diritti sopra menzionati[142]. Su questo punto la

---

tale tecnica rispetto all'anonimizzazione avendo cura di precisare l'applicabilità della normativa del regolamento per i dati pseudonimizzati poiché si tratta di una misura di sicurezza che riduce e non elimina il rischio di identificazione. L'art. 4 num. 5) definisce la pseudonimizzazione: «il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.»

[139]V. art. 89. Da un confronto dell'art. 89 con il considerando 162 è possibile notare che in misura più restrittiva il testo dell'articolo prevede l'adozione di garanzie per assicurare protezione ai diritti e alle libertà del solo interessato mentre il considerando 162 in modo più restrittivo, come già detto, preclude la possibilità di prendere decisioni nei confronti di qualsiasi persona fisica ricorrendo ai risultati a fini statistici.

[140]V. considerando n. 156 e art. 89 par. 1 che richiamando il principio della minimizzazione dei dati impongono di seguire il seguente ordine. Art. 89 par. 1 :«… Tali misure possono includere la pseudonimizzazione, purché le finalità in questione possano essere conseguite in tal modo. Qualora possano essere conseguite attraverso il trattamento ulteriore che non consenta o non consenta più di identificare l'interessato, tali finalità devono essere conseguite in tal modo.»

[141]V. art. 5 lett. c).

[142] Anche se è nello spirito del nuovo testo normativo una maggior rigidità per quanto concerne l'adozione di misure di sicurezza. Si pensi ad esempio alla privacy by design o by default. Per un approfondimento sul punto v. PAGALLO, *Il diritto nell'età dell'informazione: il riposizionamento*

nuova normativa non ha raggiunto il suo obiettivo di unificazione della disciplina relativa alla protezione dei dati, infatti grazie a queste discrezionalità alcuni stati saranno più permissivi di altri sulla possibilità di ricorrere all'analisi big data tramite il trattamento dati a fini statistici, ciò comporterà sicuramente delle difficoltà alle imprese che operano sul territorio di diversi stati membri[143]. A maggior ragione vi saranno degli ostacoli da questo punto di vista se si prende in considerazione questo dato unitamente alle nuove norme che determinano la competenza territoriale in modo più flessibile rispetto a quanto previsto dalla direttiva. Infatti ai sensi dell'art. 77 l'interessato ha diritto di proporre reclamo dinnanzi all'autorità dello stato membro in cui risiede abitualmente, in cui lavora o in cui si è verificato l'illecito[144].

In definitiva, in considerazione anche dell'enorme discrezionalità ancora lasciata ai singoli stati membri, risulta applicabile lo stesso tipo di bilanciamento che è stato proposto poc'anzi analizzando la disciplina introdotta con la direttiva nel 1995 per cui le imprese possono utilizzare i dati personali per ottenere delle correlazioni se rispettano i limiti qui sopra illustrati, avendo cura di passare attraverso le più strette maglie della profilazione qualora vogliano utilizzare i risultati delle loro analisi big data per prendere decisioni nei confronti delle persone fisiche. Quindi, come anche si vedrà in modo più approfondito nel successivo paragrafo, si dovrà procedere prima a valutare la presenza della compatibilità e poi successivamente se si vuole ricorrere alla profilazione occorrerà, nel rispetto di eventuali ulteriori limiti, individuare la base giuridica. Se la base giuridica è un legittimo interesse si potrà utilizzare il metodo di bilanciamento proposto sopra nel secondo paragrafo.

4. Il trattamento ulteriore a fini statistici, come mostrato nel precedente paragrafo, può essere considerato strumentale alla profilazione, che risulta quindi essere un utile strumento per lo sfruttamento economico di enormi quantità di dati personali. Rispetto allo studio statistico risulta essere molto più pervasiva e per questo motivo il

---

tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti, cit., 238 ss..

[143] V. MAYER SCHOENBERGER&PADOVA, op. cit., 327 e 328. Si consideri anche il considerando 162 del regolamento lascia alla discrezionalità degli stati membri la disciplina delle «specifiche per il trattamento dei dati per finalità statistiche».

[144] Questo problema è poi particolarmente presente per tutti quei trattamenti realizzati online dai colossi del web.

legislatore ha previsto l'utilizzo di maglie più strette[145]. Difatti tale tecnica di trattamento è in grado di determinare la riconduzione delle persone interessate in clusters predefiniti, senza che queste ne abbiano una piena consapevolezza[146]. Inoltre più dati personali vengono prodotti dall'interessato e più il profilo diventa intrusivo, si viene così a creare un profilo che rischia di discriminare l'individuo, viene meno il potere di controllo dello stesso sulla sua identità personale e sul suo potere di autodeterminarsi[147]. Lo scopo principale di questa tipologia di trattamento automatizzato è quello di riuscire a fornire servizi che siano sempre più adeguati all'esigenze dell'interessato, effettuare messaggi pubblicitari mirati ed infine poter utilizzare commercialmente i profili ottenuti per la loro capacità di indicare le abitudini di consumo di alcuni soggetti[148]. La possibilità di ricorrere a questa tecnica nel contesto big data è pacificamente ricavabile sia guardando all'ultimo scopo appena menzionato sia da un confronto tra le nozioni comunemente attribuiti a questi due termini. Infatti se l'analisi big data viene normalmente intesa quale studio di grandi quantità di dati con la finalità di ottenere informazioni predittive su determinati individui o gruppi[149], la profilazione è considerata: «una tecnica di trattamento automatico consistente nell'applicazione di un profilo ad una persona fisica determinata, in particolare al fine di prendere decisioni relative a tale persona oppure ai fini dell'analisi o della previsione delle sue preferenze, dei suoi comportamenti e delle sue propensioni personali», con il termine profilo si vuole fare riferimento «ad un insieme di dati caratterizzanti una categoria di persone fisiche che si intende applicare ad una persona fisica determinata»[150]. In considerazione dei potenziali rischi che essa rappresenta le basi

---

[145] V. supra par. 2.

[146] V. v. WP29, *Guidelines on Automated individual decision – making and Profiling for the purposes of Regulation 2016/679*, 3 ottobre 2017,5.

[147] Sui rischi connessi alla profilazione v. CM/Rec(2010)13; DE MEO, *Autodeterminazione e consenso nella profilazione dei dati personali*, in *Dir. Inf.* 2013, n. 3, 587 ss.; HILDEBRANDT and GUTWIRTH, *Profiling the European Citizen, Cross-Disciplinary Perspectives*, cit., 241.

[148] V. Garante per la protezione dei dati personali, Linee guida in materia di trattamento di dati personali per profilazione on line, 19 marzo 2015, doc. web n. 3881513, in www.garanteprivacy.it.

[149] V. supra par. 2.

[150] V. Art. 1 rispettivamente lett. e) e lett. d) allegato a Comitato dei ministri, 23 novembre 2010, Raccomandazione sulla protezione delle persone fisiche con riguardo al trattamento automatizzato di dati personali nel contesto dell'attività di profilazione(d'ora in avanti abbreviata: CM/Rec(2010)13. Cfr. considerando 71 e art. 4 n. 4 GDPR: «"profilazione": qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica». Sul punto v. anche Garante per la protezione dei

giuridiche che legittimano tale tipo di trattamento sono: i) il consenso; ii) esplicita previsione di legge; iii) necessità di procedere alla profilazione per conclusione od esecuzione di un contratto; iv) il legittimo interesse del titolare [151].

Le caratteristiche qui evidenziate sono state sottolineate dalla raccomandazione del Consiglio d'Europa: CM/Rec(2010)13, con la quale vengono suggerite agli stati membri l'adozione di norme minime di riferimento per la regolamentazione delle attività di profilazione in modo da rispettare i diritti fondamentali posti a tutela della persona. Questo testo normativo è il primo del suo genere a livello internazionale con l'obiettivo di proporre una disciplina minima per il trattamento automatizzato con finalità di profilazione che sia rispettoso della vita privata degli individui. La scelta del Comitato dei ministri di intervenire con un provvedimento di soft law e non adottare un'apposita convenzione probabilmente si giustifica per il fatto che l'attività di profilazione, potendo entrare in contrasto con diversi diritti fondamentali e al contempo potendo apportare notevoli utilità, necessita di un opportuno bilanciamento da parte degli stati membri. Significativo a tal proposito la previsione contenuta nell'art. 6, che rimette agli stati la facoltà di derogare per ragioni inerenti alla sicurezza pubblica o alla repressione di reati gran parte della disciplina dettata dalla raccomandazione. In particolare con un'apposita previsione di legge è possibile derogare alle norme inerenti alle condizioni del trattamento, all'informativa ed al diritto degli interessati [152]. Proprio in considerazione della natura giuridica di tale provvedimento occorre analizzare le declinazione che la raccomandazione del Comitato dei ministri ha avuto rispettivamente nel codice privacy e nel nuovo regolamento, partendo dalla premessa che, come ogni trattamento, anche per la profilazione, l'art. 3 della CM/Rec(2010)13 nel fissare le condizioni minimi applicabili richiama i principi alla base della protezione dati quali: il principio di correttezza, quello di liceità, di finalità, di adeguatezza, pertinenza, non

---

dati personali, Linee guida in materia di trattamento di dati personali per profilazione on line, cit.; DE MEO, op. cit., 587 ss..

[151] Cfr. artt. 22 GDPR, co. 3-4 CM/Rec(2010)13, art. 15 dir. 95/46/CE, art. 14 cod. privacy. Sul legittimo interesse sono state introdotte delle novità importanti nella legge di bilancio del 2018 al comma 1022: « Il titolare di dati personali, individuato ai sensi dell'articolo 4, numero 7), del regolamento RGPD, ove effettui un trattamento fondato sull'interesse legittimo che prevede l'uso di nuove tecnologie o di strumenti automatizzati, deve darne tempestiva comunicazione al Garante per la protezione dei dati personali. A tale fine, prima di procedere al trattamento, il titolare dei dati invia al Garante un'informativa relativa all'oggetto, alle finalità e al contesto del trattamento, utilizzando il modello di cui al comma 1021, lettera c). Trascorsi quindici giorni lavorativi dall'invio dell'informativa, in assenza di risposta da parte del Garante, il titolare può procedere al trattamento.»

[152] Sull'importanza e il ruolo della raccomandazione adottata dal Comitato dei ministri il 23 novembre 2010 v. DE MEO, op. cit., 587 ss..

eccedenza, di esattezza dei dati, ed infine quello relativo alla conservazione dei dati. Il riferimento a questi principi è molto importante perché sottopone la profilazione al rispetto, in mancanza di deroghe espresse, di tutte le norme stabilite in via generale per qualsiasi tipo di trattamento[153].

Nel codice privacy gli articoli dai quali poter ricavare la disciplina della profilazione sono gli artt. 7,14, 17 e 37. L'art. 14 nel disciplinare i limiti statuisce che l'interessato non può essere oggetto di un provvedimento amministrativo o giudiziario che si basi esclusivamente su un trattamento automatizzato di dati personali finalizzato alla creazione di un profilo dello stesso. Il titolare dei dati potrà subire decisioni che si basano sull'attività di profilazione, salvo sempre il diritto di opporsi qualora ai sensi dell'art. 7 comma 4 lett. a) vi siano dei motivi legittimi che lo riguardano[154]. Quest'ultima norma non è applicabile nel caso in cui la decisione adottata all'esito del trattamento automatizzato sia stata presa in occasione della conclusione o dell'esecuzione di un contratto[155]. Resta infine l'art. 37 che al comma 1 lett. d) annovera la profilazione tra i trattamenti che necessitano una notificazione preventiva all'autorità garante[156]. Questa norma è da leggersi unitamente all'art. 17 comma 2 che per i trattamenti che presentano rischi specifici per i diritti e le libertà fondamentali impone al Garante la prescrizione al titolare del trattamento, nell'ambito di una verifica preliminare, di misure e accorgimenti a garanzia dell'interessato. Da queste norme del codice risulta essere evidente l'importante ruolo svolto dal Garante per la protezione dei dati personali, il quale riceve la notifica preventiva di tutte le attività di profilazione ed effettua un'analisi preventiva prescrivendo tutte le misure che ritiene più opportune a favore dell'interessato. Nei provvedimenti autorizzativi il Garante ha sempre adottato

---

[153] Cfr. con considerando 72 GDPR: «La profilazione è soggetta alle norme del presente regolamento che disciplinano il trattamento dei dati personali, quali le basi giuridiche del trattamento o i principi di protezione dei dati…».

[154] Cfr. art. 5 co. 3 CM/Rec(2010)13, in questo comma il Comitato specifica che nel caso in cui l'opposizione riguardi ipotesi di marketing diretto l'interessato si può astenere da dare qualsiasi giustificazione.

[155] Così anche l'art. 5 comma 5 CM/Rec(2010)13.

[156] Così anche l'art. 9 comma 2 CM/Rec(2010)13: in questo articolo gli stati membri sono invitati ad introdurre un obbligo di notificazione preventiva per la profilazione. Tale obbligo è destinato ad essere limitato o a sparire a partire dal 25 maggio 2018. Infatti il nuovo regolamento europeo in materia di protezione dei dati personali impone di prestare maggiore attenzione alla costruzione e alla progettazione del trattamento e solamente quando ricorra un rischio specifico non superabile adottando semplici accorgimenti sarà necessario e opportuno rivolgersi all'autorità garante competente(v. art. 35 GDPR e WP29, *Linee guida in materia di valutazione di impatto sulla protezione dei dati e determinazione della possibilità che il trattamento possa presentare un rischio elevato ai fini del regolamento* (UE) 2016/679, 4 ottobre 2017).

un approccio generale, cercando così di esprimere principi valevoli in diversi contesti. In particolare, oltre a richiamare il principio di minimizzazione[157], si è concentrato sul consenso necessario per poter effettuare la profilazione[158].

Il consenso[159] necessario per poter effettuare attività di profilazione deve rispettare principalmente tre requisiti: la pienezza, la libertà e la specificità[160]. Un consenso è pieno o informato quando l'interessato ha la precisa consapevolezza che vi sarà un'attività di profilazione; in altri termini l'interessato deve essere pienamente consapevole che dalle informazioni fornite sarà ricavato, tramite un trattamento automatico, un profilo che gli verrà attribuito. In particolare, l'individuo prima di accettare dovrà essere edotto circa la logica alla base della profilazione e le conseguenze della medesima. In altri termini, alla luce anche di quanto ribadito dalla raccomandazione del Comitato dei ministri, a parere di chi scrive, vi è un vero e proprio obbligo di disclosure dei metodi mediante i quali verrà ricavato il profilo[161]. Affinché vi sia una piena consapevolezza da parte dell'interessato occorre prestare molta attenzione all'informativa fornita all'interessato. Questa deve essere intellegibile in ogni sua parte, ossia deve essere il più chiara e trasparente possibile di modo che sia garantita all'interessato l'esatta conoscenza dell'intenzione profilatoria di chi raccoglie i dati e delle finalità che si intendono perseguire attraverso la profilazione. Ciò implica un'attenzione particolare volta ad evitare che tale informativa si traduca in una semplice comunicazione diluita all'interno dell'informativa generale fornita al titolare dei dati (cd. interessato)[162]. Il consenso inoltre deve essere libero, ossia non deve essere

---

[157] Per un approfondimento su tale principio v. supra par. 3.

[158] Sull'importante ruolo dei provvedimenti del Garante v. DE MEO, op. cit., 587 ss..

[159] Art. 2 lett. h) dir. 95/46/CE: per consenso si intende «qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento».

[160] V. DE MEO, op. cit., 587 ss..

[161] Cfr. artt. 4.1 lett. f) e 5.1 lett. b) CM/Rec(2010)13. V. anche considerando 63 GDPR che conferma questa soluzione anche per la nuova regolamentazione della protezione dati.

[162] V. Garante per la protezione dei dati personali, Provv. 24 febbraio 2005, Fidelity card e garanzie per i consumatori, doc. web n. 1103045, in www.garanteprivacy.it; WP29, parere n. 15/2011, sulla definizione di consenso, 40. Sulle modalità in cui deve essere fornita l'informativa nella profilazione on line v. Garante per la protezione dei dati personali, Linee guida in materia di trattamento di dati personali per profilazione on line, cit., par. 3. Il garante nel provvedimento qui indicato affronta il tema delle carte fedeltà quelle tessere che vengono date ai clienti per poter usufruire di sconti sulla spesa in proporzione all'entità dei beni e dei servizi acquistati dagli stessi. L'utilizzo di queste carte comporta il trattamento di dati personali, però molto spesso, come rileva il garante, vengono raccolte anche informazioni ulteriori e non necessarie ai fini dell'erogazione del servizio in questione e l'informativa che precede il trattamento e molto generica e poco puntuale. Il garante sul punto rileva che è necessario predisporre un'informativa che permetta all'interessato di esprimere un consenso pienamente consapevole. A tal fine l'informativa deve essere in un linguaggio chiaro e non deve dare adito a dubbi interpretativi, non deve rimandare ad

strutturato in modo da costituire una precondizione necessaria per l'accesso a servizi o benefits ed inoltre non deve esserci il rischio che esso sia stato ottenuto tramite raggiri o coercizioni di alcun tipo[163]. In altri termini la libertà è garantita quando l'interessato è in grado di operare una scelta in piena coscienza delle conseguenze dettate dalla sua decisione[164]. Infine il consenso deve essere specifico, i form del consenso ai fini della profilazione devono essere distinti in modo chiaro dai moduli utilizzati per l'accettazione delle condizioni generali di contratto necessari per raccogliere le informazioni dell'utente che il professionista deve adoperare per l'esecuzione del contratto[165]. Come chiarito dalla CGUE nella sentenza sul caso Deutsche Telekom AG c. Germania[166] del 5 maggio 2011 la specificità del consenso è da riferirsi alla finalità perseguita col trattamento e alle modalità dello stesso, cosicché più finalità si perseguiranno più consensi si dovranno ottenere e qualora il titolare volesse cambiare le finalità dovrà ottenere una nuova base giuridica. Non è in alcun modo pensabile un consenso autorizzativo di diverse tipologie di trattamento con finalità non puntualmente delineate[167].

---

altri regolamenti o testi di legge, inoltre deve essere tenuta distinta dalla restante parte relative alle condizioni generale. Infine qualora si decida di profilare il soggetto la volontà di procedere in tal senso deve essere inserito nell'informativa in una parte distinta, di modo che la presente intenzione possa essere evidente rispetto alle altre parti e risulti chiaro che la mancata accettazione della profilazione non ha conseguenze sul trattamento relativo alla fidelizzazione.

[163] V. Garante per la protezione dei dati personali, Provv. 15 novembre 2007, Trattamento dei dati personali e fidelizzazione della clientela, doc. web n. 1466898 in www.garanteprivacy.it; Garante per la protezione dei dati personali, Provv. 3 febbraio 2005, Tv interattiva, doc. web n. 1109503, in www.garanteprivacy.it: «Se si pone in essere un'eventuale monitoraggio o profilazione, o si intende cedere dati personali a terzi specificamente individuati, queste circostanze e le relative finalità devono essere indicate puntualmente e con evidenza sia all'atto della costituzione del rapporto, sia prima di evadere le singole richieste di servizio o sollecitare le risposte degli utenti. Deve risultare chiara la circostanza che per questi scopi (come pure per la partecipazione a sondaggi che devono avere fini chiaramente determinati e legittimi), il conferimento dei dati e il consenso sono liberi e facoltativi rispetto all'ordinaria prestazione dei servizi, e non possono ottenersi sulla base di pressioni o condizionamenti.»

[164] WP29, Parere n. 15/2011, sulla definizione di consenso, 14. V. anche FRA, CED e COE, op. cit., 60 e 61. Il parere contiene alcuni esempi utili a comprendere quando il consenso possa dirsi libero.

[165] V. Garante per la protezione dei dati personali, Provv. 15 luglio 2010, Raccolta di dati via internet per finalità promozionali, doc. web 1741998, in www.garanteprivacy.it.

[166] CGUE, 5 maggio 2011, Deutsche Telekom AG c. Germania, C-543/09, in curia.europa.eu. V. anche WP29, parere n. 15/2011, cit., 41.

[167] V. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali, dalla direttiva 95/46 al nuovo regolamento europeo*, cit., 217 e 218. Tale concetto è stato ribadito di recente anche dal WP29 che in questo caso parla di granularità del consenso. Nelle linee guida il Gruppo europeo dei Garanti, seguendo l'orientamento della CGUE, estende il concetto di granularità del consenso, dapprima elaborato esclusivamente per le applicazioni (v. WP29, Opinion 02/2013, on apps on smart devices, passim), a qualsiasi tipo di trattamento imponendo quindi di distinguere le richieste di consenso a seconda delle finalità del trattamento. Questo rileva indirettamente anche per la profilazione in quanto non potrà essere richiesto un consenso generale ma il titolare dovrà richiederne uno specifico per tale tipo di trattamento, così non è possibile richiedere un unico consenso per il marketing diretto e la profilazione ma occorrerà distinguere (v. WP29, Guidelines on consent, 28 novembre 2017).

Resta da precisare che il consenso deve essere documentato per iscritto e deve essere preventivo rispetto al trattamento e dato in modo inequivocabile, non importa se esplicitamente o implicitamente. Poiché l'art. 2 lett. h) della dir. 95/46/CE definisce il consenso come qualsiasi manifestazione di volontà con la quale l'interessato accetta il trattamento, si può ritenere che, questo nel rispetto dei requisiti sopra menzionati, possa essere prestato anche con un comportamento che indichi chiaramente la volontà dell'interessato. Tuttavia è escluso che l'assenso ad un trattamento di dati personali possa essere ricavato da un comportamento passivo, è pur sempre necessaria un'azione positiva[168].

Posto che quanto detto per il consenso[169] è valido anche per il nuovo regolamento, che su questi punti non ha innovato in modo particolarmente significativo[170], occorre soffermarsi sulle novità introdotte dal GDPR in tema di profilazione. Si fa riferimento agli artt. 35 e 36 del regolamento. Il primo sancisce l'obbligo per il titolare del trattamento che intenda procedere a profilazione di effettuare una valutazione di impatto[171]. L'art. 36 stabilisce l'obbligo di consultazione preventiva del Garante qualora

---

[168] V. FRA, CED e COE, op. cit., 58 ss.; WP29, parere n. 15/2011, 11 ss.; Garante per la protezione dei dati personali, *Linee guida in materia di trattamento di dati personali per profilazione on line*, 19 marzo 2015, cit.. V. anche art. 7 lett. a) dir. 95/46/CE. Sulla necessità di un'azione positiva è molto chiaro il GDPR che all'art. 4 num. 11) sancisce espressamente che il consenso possa essere dato alternativamente o con una dichiarazione oppure con un azione positiva. Un chiaro esempio di come è stato intenso il consenso nel contesto dei cookie dal Garante per la protezione dei dati personali in materia di profilazione online è contenuto nel provvedimento dell'8 maggio 2014. In questo atto il Garante chiarisce che il consenso per essere profilati tramite cookie può essere desunto da un'azione positiva dell'utente che, dopo aver visualizzato un banner che in qualche modo si stacca dalla pagina di navigazione e informa sull'uso di tali tipologie di cookie, prosegue con qualsiasi azione nella navigazione del sito web(v Garante per la protezione dei dati personali, *Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie*, 8 maggio 2014, doc. web. n. 3118884.

[169] Per il consenso v. art. 4 n. 11) e considerando 32 reg. 679/2016/UE: «Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso.»

[170] Una lettura completa delle norme del regolamento relative al consenso, ma non estremamente rilevante ai fini della trattazione, è rinvenibile nelle linee guida del WP29 sul consenso del GDPR (WP29, Guidelines on consent, cit.).

[171] Per un approfondimento sulla valutazione di impatto v. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali, dalla direttiva 95/46 al nuovo regolamento europeo*, cit., 294 ss.; MANCINI, *La protezione dei dati personali*, in MEGALE, *ICT e diritto nella società dell'informazione*, Giappichelli, Torino, 2017, 132 ss..

dalla valutazione di impatto risulti evidente che vi siano dei rischi se non verranno prese adeguate misure di sicurezza per effettuare il trattamento. Apparentemente rispetto al codice privacy non sembra più obbligatorio procedere alla consultazione preventiva se non risultano rischi dalla valutazione di impatto. La consultazione dell'Autorità di controllo, come chiarito anche recentemente dalle linee guida del Gruppo europeo dei Garanti, resta ferma esclusivamente nel caso il cui pur avendo preso adeguate contromisure, il trattamento comporta ancora un rischio specifico per gli interessati, è compito poi del titolare del trattamento documentare adeguatamente tale tipo di scelta motivando in un apposito atto (contenente la valutazione di impatto) su quali basi non ha effettuato alcuna notificazione al Garante per la protezione dei dati personali[172]. Queste disposizioni sono molto importanti perché sono indice di una nuova consapevolezza del legislatore europeo. Difatti, a parere di chi scrive, il legislatore sembra consapevole che il consenso in alcuni contesti è una base giuridica non sufficiente perché molto spesso è difficile che vengano rispettati i suoi tre requisiti, soprattutto per quanto riguarda la libertà e la consapevolezza[173]. In un contesto dinamico, diverse attività compiute quotidianamente da un individuo implicano lo scambio di dati personali e la relativa profilazione da parte di diversi operatori economici. Il consenso molto spesso è prestato con poca attenzione e anche qualora l'utente voglia soffermarsi attentamente sull'informativa molto spesso questa è complicata e non è pienamente comprensibile. Basti pensare alle informative di alcuni social network che sono testi molto lunghi e complessi, anche per addetti al mestiere

[172] Sul punto v. WP29, Linee guida in materia di valutazione di impatto, 4 ottobre 2017, passim. In queste linee guida il Gruppo europeo dei Garanti chiarisce le circostanze in presenza delle quali è opportuno effettuare una valutazione di impatto, spiegando che l'elencazione contenuta al terzo comma dell'art. 35 del GDPR non è da considerarsi tassativa. A tal proposito individua dieci criteri, tra di loro alternativi, in presenza dei quali è opportuno interrogarsi sulla necessità di una valutazione di impatto. Più precisamente in presenza di almeno due di questi criteri il titolare del trattamento deve porsi il problema della valutazione di impatto e documentare la sua scelta. L'elencazione dei criteri individuati dal WP29 non è rilevante perché il terzo comma dell'articolo 35 non lascia dubbi sulla necessità di effettuare una valutazione di impatto nel caso della profilazione laddove prevede che: «La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti: a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati; o c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.» Come si ricava dal regolamento e dalle linee guida, il legislatore ha adottato un nuovo approccio volto a documentalizzare le scelte effettuate, creando così per il titolare diverse occasioni di riflessioni sul tipo di trattamento posto in essere e sui suoi eventuali impatti.

[173] Cfr. considerando 43 GDPR.

diventa difficile comprendere a pieno la portata del trattamento[174]. Per questi motivi il legislatore europeo nel nuovo regolamento spinge su due fronti da una parte puntualizza e precisa meglio i requisiti richiesti per il consenso e impone che l'informativa sia il più chiara possibile e comprensibile da chiunque[175]. Dall'altra parte introduce strumenti che assicurino l'adozione di misure di sicurezza idonee a tutelare in ogni caso i diritti e le libertà fondamentali delle persone fisiche, si pensi ad esempio: alla privacy by design, alla valutazione di impatto e alla pseudonimizzazione[176]. In questo modo sarà possibile effettuare trattamenti particolarmente pervasivi come l'analisi big data effettuata non semplicemente per studiare le correlazioni ma per prendere decisioni nei confronti di determinati individui che, per usare il linguaggio dell'articolo 22 del regolamento, producano effetti giuridici o incidano in modo analogo sulla loro posizione[177]. La profilazione, come già anticipato, è un tipo di trattamento che si avvale della statistica, implicando una serie di deduzioni di tale tipo, per ricavare informazioni riguardanti un individuo basandosi sulle qualità e sulle scelte effettuati da altri a lui simili o che si siano trovati nella sua stessa situazione[178].

È proprio l'elemento decisionale e il fatto che produca effetti giuridici o simili sugli individui che distingue la profilazione dal trattamento statistico e che impone l'adozione di tutte queste cautele. In quest'ipotesi è evidente che il legislatore effettua un bilanciamento tra i due diritti fondamentali, sopra considerati, il diritto alla protezione dei dati personali e la libertà di impresa. Un utilizzo dei dati per finalità statistiche ulteriori rispetto a quelle dichiarate non comporta un enorme sacrificio per l'individuo se condotto nel rispetto della normativa sopra illustrata. Mentre un utilizzo per fini di profilazione implica sempre e comunque delle limitazioni pesanti per l'individuo e al

---

[174] In questo senso v. PAGALLO, *Il diritto nell'età dell'informazione: il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti*, cit., passim.

[175] Cfr. considerando 39 GDPR.

[176] Per la privacy by design cfr. art. 25 GDPR. Per la valutazione di impatto cfr. considerando 90 e art. 35 GDPR. Per la pseudonimizzazione v. supra par. 3.

[177] Un esempio emblematico di profilazione che permette di comprendere a pieno gli effetti significativi che l'analisi big data può avere nei confronti dell'interessato è costituito dal cd. look alike. L'individuo in base alle sue scelte di acquisto, che possono essere state effettuate sia online che "offline" utilizzando carte fedeltà, viene tracciato e ricondotto ad un cluster ed in base al cluster di appartenenza gli vengono sottoposti in svariati contesti offerte di servizi o prodotti che hanno incontrato l'interesse di altri soggetti appartenenti al medesimo cluster. Come sottolineato dal Gruppo Europeo dei Garanti questo può in qualche modo compromettere la sua libertà di scelta e risultare particolarmente pervasivo se non viene effettuato adottando le opportune cautele evidenziate all'interno del presente paragrafo. (v. WP29, *Guidelines on Automated individual decision – making and Profiling for the purposes of Regulation 2016/679*, cit.,5).

[178] V. WP29, *Guidelines on Automated individual decision – making and Profiling for the purposes of Regulation 2016/679*, cit.,7.

contempo comporta un'utilità notevole per le imprese che possono sfruttare la clusterizzazione per essere più competitivi. Per questo è opportuno consentire tale utilizzo dei dati ponendo dei severi paletti, e permettendo alla persona fisica, che subisce una scelta quale esito di un processo di trattamento automatizzato dei suoi dati personali, di richiedere l'intervento umano o di esprimere la sua opinione e di contestare tale decisione[179].

[179] V. art. 22 co. 3 GDPR. In questo paragrafo si è soffermati sul consenso e sui requisiti tralasciando l'analisi del legittimo interesse che è stata affrontata nel paragrafo 2 del presente capitolo a cui si rimanda.

Capitolo Secondo

Gli strumenti giuridici volti a regolare la circolazione dei dati.

Sommario 1. La duplice tutela delle banche di dati - 2. Banche dati e privacy – 3. Il segreto industriale e il brevetto – 4. Altre tecniche per regolare la circolazione dei dati.

1. Attualmente non vi è alcun strumento giuridico specifico volto a riconoscere in capo ad un soggetto la titolarità dei dati che produce o raccoglie a vario titolo tramite l'utilizzo di dispositivi o programmi che gli appartengono o di cui si avvale in virtù di appositi contratti.

Occorre soffermarsi sul ruolo in tale ambito della disciplina della proprietà intellettuale, alla quale il legislatore ha assegnato la funzione di incentivare la circolazione delle informazioni, attribuendo in determinati casi la possibilità di appropriarsi dei dati se questo può in qualche modo incidere positivamente sulla produzione di informazioni ulteriori[180].

In particolare, nel presente capitolo si esploreranno alcuni regimi legali che possono offrire una protezione sui dati raccolti dalle imprese o per lo meno incidere in modo significativo sulla loro circolazione. Questi strumenti sono il diritto del costitutore sulle banche dati e il segreto industriale. In certi casi inoltre ci si può interrogare sulla possibilità di estendere la protezione del brevetto sui dati che sono generati attraverso l'attuazione di brevetti di procedimento. Nella parte che segue si osserverà la normativa sui database per comprendere fino a che punto il diritto del costitutore può imporsi sulla circolazione dei dati.

La definizione di banca dati è contenuta nella direttiva 96/9/CE all'art. 1.2 che la definisce: «una raccolta di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili grazie ai mezzi elettronici o in altro modo», la presente nozione è stata poi recepita dal legislatore interno con il d.lgs. 169/1999, che è intervenuto sull'art. 2 l.a. inserendola al nono posto nell'elencazione, ivi contenuta, relativa alle tipologie di opere espressamente tutelate dal diritto d'autore.

Una veloce analisi della nozione pone in evidenza tre elementi strutturali senza i quali non è possibile parlare di banca dati: i) la presenza di più elementi tra loro indipendenti

[180] Cfr. BERTANI, *Proprietà intellettuale e nuove tecniche di appropriazione delle informazioni*, in *Studi in onore di Gerhard Schricker*, Giuffrè, Milano, 2005, 22.

e autonomi; ii) la disposizione sistematica o metodica degli stessi iii) la possibilità di accedere, grazie alla disposizione sistematica o metodica, direttamente ad ogni singolo elemento, di cui è composta l'opera, in modo completamente separato dagli altri[181]. Il primo punto permette di distinguere le banche di dati da altri tipi di opere composte quali quelle: audiovisive, cinematografiche, letterarie o musicali. Infatti, gli elementi devono essere tra loro separabili senza che il loro valore, sia esso letterario o artistico o informativo o di qualsiasi altro genere, venga meno[182]. Infine la disposizione sistematica o metodica e l'accessibilità individuale di ogni singolo elemento comporta che «[…] la raccolta figuri su un supporto fisso di qualsiasi natura, e contenga un mezzo tecnico quale un processo di tipo elettronico, elettromagnetico o elettrottico, in base al tredicesimo considerando della stessa direttiva, o un altro mezzo, quale un sommario, un indice delle materie, un piano o un metodo di classificazione particolare, che consente la localizzazione di ogni elemento indipendente contenuto nel suo ambito»[183]. Grazie a queste due caratteri costitutivi è possibili distinguere la banca dati «[…] da un insieme di elementi che fornisce informazioni che è privo di qualsiasi mezzo di elaborazione dei singoli elementi che lo compongono»[184].

I singoli elementi che vanno a comporre la banca dati, come si ricava dal considerando 17, possono consistere in: «[…] opere, siano esse letterarie, artistiche o musicali o di altro genere, oppure di materiale quali testi, suoni, immagini, numeri, fatti e dati.» Infine, dall'art. 1 co. 1 e dal considerando 14 della dir. 96/9/CE si ricava che la tutela giuridica, ivi concessa, si applica a prescindere dalla natura elettronica della banca dati[185]. La novità più importante introdotta dalla direttiva riguarda la tutela, tramite un diritto sui generis, delle banche dati che non denotino carattere creativo per la predisposizione e l'organizzazione del materiale, ma che tuttavia abbiano richiesto per la loro realizzazione investimenti rilevanti[186]. Infatti, in passato, già prima che il

---

[181] Cfr. CARDARELLI, *Le banche dati pubbliche: una definizione*, in *Dir. inf.* 2002, 324 e 325.; CGCE, Fixture Marketing, 9 novembre 2004, C-444/02, in www.curia.europa.eu. In realtà quest'ultima non propone una tripartizione degli elementi costitutivi ma una bipartizione, considerando come un solo elemento la predisposizione sistematica e metodica e la possibilità di accedere individualmente a ciascun singolo elemento.

[182] V. CGCE, Fixture Marketing, 9 novembre 2004, cit., punto 29; v. anche Trib. Milano, 8 settembre 2014, in *AIDA* 2015, *1691*.

[183] CGCE, Fixture Marketing, 9 novembre 2004, cit., punto 30.

[184] CGCE, Fixture Marketing, 9 novembre 2004, cit., punto 31.

[185] Art. 1 co. 1: « La presente direttiva riguarda la tutela giuridica delle banche di dati, qualunque ne sia la forma» . Considerando 14: «occorre estendere la tutela concessa dalla presente direttiva alle banche di dati non elettroniche».

[186] V. art. 7 dir. 96/9/CE.

legislatore comunitario e poi quello interno intervenissero annoverando specificatamente nell'elencazione dell'art. 2 l.a. le banche dati, era pacifica la possibilità di ricorrere alla tutela autorale per tale tipo di opere che venivano ricondotte nel genere letterario[187]. La CUB[188], già nella sua prima versione del 9 settembre 1886, stabilisce all'art. 2 co. 5 che: «le raccolte di opere letterarie o artistiche come le enciclopedie e le antologie che, per la scelta o la disposizione della materia, abbiano carattere di creazioni intellettuali sono protette come tali, senza pregiudizio del diritto d'autore su ciascuna delle opere che fanno parte delle raccolte stesse». Per cui già sul finire del diciannovesimo secolo era riconosciuta tutela alle banche dati composte da opere dell'ingegno. Non vi era alcun riferimento invece alle banche dati formate da materiali diversi. Tuttavia, sotto la previgente legge d'autore del 1925, poiché l'art. 1[189] attribuiva protezione alle opere dell'ingegno a prescindere dal merito e dalla destinazione, non vi era dubbio che potesse applicarsi la tutela autorale alle banche di dati purché queste avessero elementi distintivi rispetto al patrimonio culturale comune[190]. Con la nuova legge del 1942 viene meno il riferimento al merito e alla destinazione e si aggiunge quello alla creatività[191]. Dottrina e giurisprudenza prevalente, una volta definito tale requisito, dimostrato che possa essere presente anche nelle creazioni utili, in considerazione del carattere esemplificativo dell'elencazioni contenute negli artt. 2 CUB e 2 l.a., hanno ritenuto possibile applicare il diritto d'autore per tutelare le banche dati creative[192]. Successivamente la direttiva 1996/9/CE e la legge sul diritto d'autore hanno espressamente introdotto una duplice tutela a favore delle banche dati. Per essere

---

[187] In tal senso v. L. C. UBERTAZZI, *Raccolte elettroniche di dati e diritto d'autore: prime riflessioni*, in *Foro it.* 1984, V, 23; INTROVIGNE, *Computer data bases e proprietà intellettuale in diritto comparato*, in ALPA, *La tutela giuridica del software* , Giuffrè, Milano, 1984, 67 ss.; PARDOLESI. *Banche dati al guado*, in *Foro it.* 1987, IV, 357; FRASSI, *Creazioni utili e diritto d'autore*, Giuffrè, Milano, 1997, 168. Per la giurisprudenza v. Cass. 2 dicembre 1993, n. 11953, in *Riv. dir. ind.* 1994, II, 157 ss.; Cass., 14 dicembre 1959, n. 3544, in *Foro it.* 1960, I, 54; Pret. Roma, 14 dicembre 1989, in *Dir. inf.* 1990, 219; Pret. Roma, 22 febbraio 1952, in *Rep. Foro it*. 1952, v. *Diritto d'autore*, n. 94.

[188] Convezione dell'Unione di Berna per la protezione delle opere letterarie ed artistiche del 1886.

[189] Art. 1 co. 1 r.d.l. n. 1950/1925: «Sono protette dal presente decreto, qualunque ne sia il merito e la destinazione, tutte le opere dell'ingegno. scientifiche, letterarie, artistiche e didattiche.»

[190] Sul punto v. STOLFI, *Il diritto d'autore,* vol. I, SEL, Milano, 1932, 190 ss. per come trattato da FRASSI, op. cit., 184 e 185. Per la giurisprudenza cfr. App. Venezia, 24 febbraio 1933, in *IDA* 1933, 339 ss.;

[191] V. art. 1 co. 1 l.a. : «Sono protette ai sensi di questa legge le opere dell'ingegno di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma di espressione».

[192] Sul punto v. ARE, *L'oggetto del diritto d'autore*, Giuffrè, Milano, 1963, 361 ss.; GRECO e VERCELLONE, *I diritti sulle opere dell'ingegno*, UTET, Torino, 1974, 58; L. C. UBERTAZZI, *Raccolte di dati e diritto d'autore*, cit., 23 ss.; CHIAROLLA, *Diritto d'autore: La prima volta delle banche dati in Italia*, in *Foro it*. 1990, I, 2674; FRASSI, op. cit.,185. Per la giurisprudenza v. Cass., 19 luglio 1990, n. 7397, in *Giur. it. Mass.* 1990, 867; Cass., 14 dicembre 1959, cit.; Pret. Roma, 14 dicembre 1989, cit.; Trib. Bari, 17 giugno 1974, in *IDA* 1975, 93; App. Torino, 16 maggio 1944, in *Giur. tor.* 1944, 171.

protette dal diritto d'autore puro le banche dati devono essere strutturate secondo criteri che denotino carattere creativo. Qualora l'organizzazione e la predisposizione del materiale contenuto nell'opera non mostri tale requisito non si potrà accedere alla tutela autorale. Tuttavia se per la creazione della stessa sono stati impiegati investimenti rilevanti il costitutore avrà un diritto connesso sulla banca dati ex art. 102 bis l.a.[193].

Occorre ora soffermarsi sul requisito di creatività per comprendere a pieno quando è possibile accedere alla tutela autorale. Parte della dottrina italiana, in armonia con alcuni orientamenti di matrice continentale, definisce la creatività come l'impronta della personalità dell'autore nell'opera[194]. Tale requisito renderebbe l'opera dell'ingegno infungibile, poiché il lavoro creativo offre una fotografia della personalità dell'autore nel momento della sua realizzazione. Se l'opera non contiene l'impronta della personalità del suo autore non può essere considerata una creazione ma l'attività sarà meramente intellettuale: come ad esempio avviene nei contributi solamente informativi ed in quelli tecnici[195]. Quest'indirizzo dottrinale presenta il difetto di basarsi su criteri estremamente soggettivi, per questo motivo parte della giurisprudenza interna ha cercato di ancorare la ricerca del valore della creatività a parametri più oggettivi. Inizialmente lo ha fatto nelle diverse occasioni in cui è stata chiamata a decidere se una fotografia avesse o meno carattere creativo[196]. La soluzione offerta, estesa poi ai diversi tipi di opere dell'ingegno, individua il requisito della creatività nelle scelte creative fatte dall'autore dell'opera[197]. L'impronta personale impressa nella creazione deve essere il risultato di scelte discrezionali di carattere estetico che hanno portato ad ottenere quel determinato risultato. Quindi non si guarda più solamente all'opera finale ma anche al percorso necessario per la sua realizzazione. Diventa fondamentale ricostruire il

---

[193] Sul punto v. V.M. De Sanctis, *Il diritto d'autore*, Giuffrè, Milano, 2012, 51 ss. e 202 ss..

[194] V. VAL DE SANCTIS, *Il contratto di edizione*, Giuffrè, Milano, 1965, 8; V.M. DE SANCTIS, *Il carattere creativo delle opere dell'ingegno*, Giuffrè, Milano, 1971, 41.

[195] In tale senso parte della dottrina tedesca propone la distinzione tra creazione e prestazione. Nella creazione l'intelletto individuale si traduce in una forma espressiva soggettivamente individuale che costituisce un nuovo oggetto intellettuale, mentre la prestazione implicherebbe un'attività individuale dando origine ad un prodotto solo oggettivamente caratteristico che non comporta alcun impiego dell'intelletto individuale. Quindi nella prestazione se cambia la persona tendenzialmente il risultato finale non cambia, mentre nella creazione la persona dell'autore non può essere sostituita V. HUBMANN, *Urheber-und Verlagsrecht: ein studienbuch*, Munchen Juristische Kurz-Lehrbücher, 1959, riletto da ARE, op. cit., 170 e 171.

[196] Ex multae cfr. Trib. Catania, 24 novembre 2004, in *AIDA* 2006, *1077*; Trib. Catania, 27 agosto 2001, in *IDI* 2002, 97 ss.; Trib. Firenze, 16 febbraio 1994, in *AIDA* 1995, *318*. Sul punto cfr. anche BERTANI, *Diritto d'autore e connessi*, in *La proprietà intellettuale*, (a cura di) L. C. UBERTAZZI, Giappichelli, Torino, 2011, 287.

[197] V. Trib. Bologna ord. 17 gennaio 2006, in *AIDA* 2008, *1205*; Trib. Monza ord. 15 maggio 2000, in *AIDA* 2001, *765*.

processo creativo dell'opera. Così ad esempio: la creatività in una fotografia emerge dalla scelta dell'inquadratura, delle condizioni di luce, del momento dello scatto e da altri criteri elaborati caso per caso dalla giurisprudenza[198]. Questo orientamento portato avanti dalla giurisprudenza e anche da parte della dottrina ritiene necessario che l'opera dell'ingegno costituisca un quid novi, cioè un contributo innovativo dell'autore al preesistente patrimonio culturale della collettività[199]. In altri termini l'opera deve essere oggettivamente nuova, a tal fine la giurisprudenza preponderante utilizza il test della non banalità[200]. Esso consiste nel verificare: sia che l'opera non sia successiva ad altra identica negli elementi caratteristici del genere a cui appartiene; sia che la forma espressiva dell'opera non sia banale a tal punto da poter essere ricavata senza alcuno sforzo dal patrimonio culturale. Tale giudizio di non banalità dovrà essere condotto tenendo in considerazione le diverse peculiarità che sono proprie dei singoli generi creativi e avendo come parametro di valutazione l'esperto conoscitore del genere di appartenenza dell'opera esaminata[201]. Da tutta questa analisi risulta evidente che il requisito di creatività non è quindi un valore assoluto ma varia a seconda del genere di provenienza dell'opera[202]. Più il genere contiene varianti creative e possibilità di scelta più il gradiente di creatività richiesto sarà elevato. Così per le opere letterarie e di fantasia il livello di novità richiesto sarà molto elevato poiché vi è un ampia possibilità di scelta mentre per le creazioni utili il minimo di creatività richiesto è molto basso, dato che esse devono possedere senz'altro alcuni elementi chiave contenuti in altre opere per adempiere alle loro funzioni. Quindi per tutti questi particolari tipi di creazioni, quali le banche di dati, la libertà creativa dell'autore risulta molto limitata[203].

---

[198] V. SPEDICATO, *Gradiente creativo dell'opera dell'ingegno e proporzionalità della tutela*, in *IDA* 2012, 382 e 383. Per la giurisprudenza v. ad esempio: Trib. Milano, 28 giugno 1993, in *Foro it. online*. Il tribunale di Milano nella sentenza chiarisce che affinché sia riconosciuto il requisito della creatività il fotografo non può limitarsi a riprodurre la realtà ma attraverso la scelta di luci, scorci inquadrature e simili, l'autore dovrà aggiungere alla riproduzione meccanica la sua fantasia, il suo gusto e la sua sensibilità in modo che l'opera diventi mezzo di comunicazione dell'emozioni del suo autore. Per utilizzare un'espressione propria del sistema di common law l'opera deve testimoniare «skill, judgment, labour,»(v. W.R. CORNISH e D. LLEWELYN, *Intellectual property*, 6 ed., Sweet & Maxwell, Londra, 2007, passim).

[199] V. ARE, op. cit., 49.; GRECO e VERCELLONE, op. cit., 48 s.; BERTANI, *Diritto d'autore e connessi*, cit., 288 ss..

[200] Ex multae Cass., 13 dicembre 1999, in *AIDA* 2000, *659*; Trib. Venezia, 19 ottobre 2007, in *AIDA* 2009, *1270*; Trib. Milano, 29 gennaio 1997, in AIDA 1997, *489*; Pret. Monza, 4 dicembre 1991, in AIDA 1992, *77*.

[201] BERTANI, *Diritto d'autore e connessi*, cit., 288 ss..

[202] Sul punto v. DI CATALDO, *Banche dati e diritto sui generis: la fattispecie costitutiva*, in *AIDA* 1997, 21; BERTANI, Ibidem.

[203] In questo senso v. BERTANI, *Diritto d'autore e connessi*, cit., 289 ss.; FRASSI, op. cit., 173.

Il punto di partenza per valutare la creatività di tali opere è costituito dall'art. 3 co. 1 della dir. 96/9/CE che precisa quali elementi occorre prendere in considerazione per la verifica laddove si riferisce esclusivamente alla scelta e alla disposizione del materiale[204]. Per accertare la presenza di questo requisito, seguendo l'orientamento prevalente, occorre applicare il test di non banalità esclusivamente ai criteri di scelta e organizzazione del materiale. In altri termini è necessario che i metodi utilizzati siano nuovi e non siano banali[205]. Inoltre, come precisato dalla Corte di Giustizia nella causa C-604/10 la tutela autorale di una banca dati è esclusa quando il suo creatore è vincolato a seguire regole tecniche che non lascino alcun margine di libertà[206]. La vera difficoltà per poter verificare l'applicazione della disciplina autorale è riferita al livello minimo di novità che devono possedere questi criteri. Come già osservato, nel campo delle creazioni utili la possibilità di scelta è molto limitata e varia molto a seconda del tipo di banca di dati[207].

Il diritto d'autore tutela ciò su cui insiste il requisito della creatività quindi nel caso delle banche di dati oggetto di protezione saranno i criteri di scelta e predisposizione del materiale ivi contenuto. Infatti, come precisato dall'art. 3 della dir. 96/9/CE la tutela autorale non si estende agli elementi presenti nell'opera. Per questi motivi la protezione offerta dal diritto d'autore non può essere uno strumento utile per regolare la circolazione e l'appartenenza dei dati ivi contenuti. Sul punto molto chiaramente la Corte di Giustizia ha sostenuto che, come è possibile ricavare dai considerandi 9 10 e 12, la finalità principale della direttiva è quella di incentivare la creazione di database al fine di contribuire allo sviluppo del mercato delle informazioni e non persegue l'obiettivo di proteggere gli elementi che possono essere raccolti all'interno della banca

---

[204] Art. 3 co. 1 dir. 96/9/CE: «A norma della presente direttiva, le banche di dati che per la scelta o la disposizione del materiale costituiscono una creazione dell'ingegno propria del loro autore sono tutelate in quanto tali dal diritto d'autore. Per stabilire se alle banche dati possa essere riconosciuta tale tutela non si applicano altri criteri.» V. DI CATALDO, op. cit., 21; SAPPA, *nota a Trib. Roma, ord. 5 giugno 2008*, in *AIDA* 2010, 692. Già prima dell'adozione della direttiva parte della dottrina e della giurisprudenza riferivano il concetto di creatività delle banche dati alla scelta e disposizione del materiale cfr. L.C. UBERTAZZI, *Raccolte e elettroniche di dati e diritto d'autore,* cit., 23; Cass., 14 dicembre 1959, cit. contra per le banche dati non elettroniche Cass., 2 dicembre 1993, in *Riv. dir. ind.* 1994, II, 157 ss. V. anche art. 10 par. 2 Accordi Trips: «Le compilazioni di dati o altro materiale, in forma leggibile da una macchina o in altra forma, che a causa della selezione o della disposizione del loro contenuto costituiscono creazioni intellettuali sono protette come tali.[…]»

[205] Questo orientamento è stato seguito anche dalla Corte di Giustizia laddove parla di originalità nella scelta e organizzazione del materiale all'interno della banca di dati. V. CGUE, 16 luglio 2009, C-5/2008, in *AIDA* 2009, *1261*. V. anche Trib. Milano, 16 febbraio 2012, in *AIDA* 2013, Rep. I. 13bis.

[206] V. CGUE, 1 marzo 2012, C-604/10, in www.curia.europa.eu, punto 39.

[207] Per uno studio approfondito sui requisiti di protezione nei vari tipi di banca dati si rimanda a FRASSI, op. cit., 187 ss..

dati[208]. D'altronde l'art. 3 co. 2, laddove precisa che la tutela autorale sulle banche dati non si estende al contenuto e lascia impregiudicati gli eventuali diritti esistenti su di esso, conferma pienamente l'interpretazione della Corte di Giustizia.

Occorre analizzare le caratteristiche del diritto sui generis introdotto dalla dir. 96/9/CE per verificare se tale tipo di potere attribuito al costitutore possa permettergli di controllare la circolazione dei dati.

In base ad una lettura congiunta dell'art. 7 con l'art. 10 co. 3 della dir. 96/9/CE per accedere alla tutela del diritto sui generis è necessario che la costituzione della banca dati abbia comportato un investimento sostanziale, rilevante sotto il profilo qualitativo e quantitativo[209]. L'investimento valutato ai fini dell'accesso alla tutela deve avere ad oggetto, come chiarito dall'orientamento prevalente confermato dalla stessa Corte di Giustizia, tutti i mezzi necessari per la ricerca di elementi indipendenti e il loro inserimento all'interno della banca di dati. Non rilevano in alcun modo gli investimenti utilizzati al fine della produzione dei dati ivi raccolti[210]. L'impiego di risorse deve essere rilevante sia sotto il profilo quantitativo che sotto il profilo qualitativo. Per il primo aspetto si guarda esclusivamente ai mezzi finanziari impiegati[211]. Per il livello qualitativo un orientamento propone di parametrare la spesa sostenuta con il livello medio di investimento necessario per creare una banca di dati nel settore di riferimento[212]. Una seconda tesi invece guarda all'originalità del metodo di sistemazione dei dati o al livello culturale dell'opera[213]. Poiché il diritto sui generis pare

---

[208] V. CGUE, 1 marzo 2012, C-604/10, cit., punto 34; CGCE, 9 novembre 2004, Fixture Marketing, C-444/02, cit., punto 39; CGCE, 9 novembre 2004, C-203/02, in www.curia.europa.eu, punto 30.

[209] V. DI CATALDO, op. cit., 24 ss.; MELI, *Le utilizzazioni libere nella direttiva 96/9/CEE sulla protezione giuridica delle banche dati*, in *AIDA* 1997, 102; BERTANI, *Proprietà intellettuale e nuove tecniche di appropriazione delle informazioni*, cit., 24. Art 7 co. 1 dir. 96/9/CE: «Gli stati membri attribuiscono al costitutore di una banca di dati il diritto di vietare operazioni di estrazione e/o reimpiego della totalità o di una parte sostanziale del contenuto della stessa, valutata in termini qualitativi o quantitativi, qualora il conseguimento, la verifica e la presentazione di tale contenuto attestino un investimento rilevante sotto il profilo qualitativo o quantitativo». Art. 10 co. 3: «Ogni modifica sostanziale, valutata in termini qualitativi o quantitativi, del contenuto di unna banca dati, ed in particolare ogni modifica sostanziale risultante dell'accumulo di aggiunte, stralci o modifiche successivi che permetta di ritenere che si tratti di un nuovo investimento sostanziale, valutato in termini qualitativi o quantitativi, consente di attribuire alla banca derivante da tale investimento una propria specifica durata di protezione.»

[210] In questo senso v. CGCE, 9 novembre 2004, C-444/02, in *AIDA* 2005, *1016*; COGO, nota a CGCE, 9 novembre 2004, in *AIDA* 2005, 415 ss.

[211] DI CATALDO, op. cit., 24.

[212] DI CATALDO, Ibidem.

[213] BERTANI, *nota a Trib. Torino 17 luglio 1997*, in *AIDA* 1998, 616; LEISTNER, *The legal protection of telephone directories relating to the new database maker's right*, in *IIC* 2000 ,957 ss.; DAVISON, *The legal protection of Databases*, Cambridge University Press, Londra, 2003, 84. In tale senso anche le conclusioni dell'avvocato generale Stix Hackl che accompagnano la decisione della Corte di Giustizia

volto a tutelare ciò che non è proteggibile dal diritto d'autore sembrerebbe più coerente, a parere di chi scrive, seguire il primo orientamento. Altrimenti tale strumento si tradurrebbe in un semplice allargamento del diritto d'autore sulla banca dati che sarebbe stato ottenibile dal legislatore comunitario intervenendo direttamente sulla disciplina autorale e senza l'introduzione di un nuovo istituto.

Il diritto sui generis del costitutore consta principalmente di una facoltà. Come stabilito dall'art. 7 co. 1 della direttiva 96/9/CE al titolare spetta: «il diritto di vietare operazioni di estrazioni e/o reimpiego della totalità o di una parte sostanziale della stessa, valutata in termini qualitativi e quantitativi, qualora il conseguimento, la verifica e la presentazione di tale contenuto attestino un investimento rilevante sotto il profilo qualitativo o quantitativo». Per evitare che tale potere di controllo venga aggirato tramite estrazioni e rimpieghi che solo unitamente considerati intacchino la parte sostanziale dell'opera il comma 5 dell'art. 7 precisa che: «Non sono consentiti l'estrazione e/o il reimpiego ripetuti e sistematici di parti non sostanziali del contenuto della banca di dati che presuppongano operazioni contrarie alla normale gestione della banca dati o che arrechino un pregiudizio ingiustificato ai legittimi interessi del costitutore della banca di dati»[214]. I concetti chiave che occorre interpretare e riempire di significato per poter comprendere a pieno la portata del diritto sui generis sono tre. È necessario infatti soffermarsi sulla nozione di estrazione, reimpiego e parte sostanziale.

Per estrazione si intende il trasferimento di tutto o parte del contenuto di una banca dati da un supporto ad un altro. Non rileva in alcun modo la temporaneità o la definitività del trasferimento[215]. L'estrazione è illecita quando, anche in più riprese, abbia riguardato una parte sostanziale dell'opera, a meno che non sia avvenuta per finalità consentite, ossia per scopi didattici, di ricerca o per fini privati, o per esigenze di pubblica sicurezza o per procedura amministrativa o giurisdizionale[216]. Per reimpiego si intende: «qualsivoglia forma di messa a disposizione del pubblico della totalità o di una parte sostanziale del contenuto della banca dati mediante distribuzione di copie, noleggio, trasmissione effettuata con qualsiasi mezzo e in qualsiasi forma. L'attività di

---

relativa al caso British Horseracing Board(CGCE, 8 giugno 2004, C-444/02, concl. Avv. Gen. STIX HACKL, in www.curia.eu).

[214] Cfr. SPOLIDORO, *Il contenuto del diritto connesso sulle banche di dati*, in *AIDA* 1997, 45 ss.

[215] Per la nozione di estrazione cfr. SPOLIDORO, ibidem; CGUE, 5 marzo 2009, C-545/07, in *www.curia.eu*; CGUE, 9 ottobre 2008, C- 304/07, in *www.curia.eu;* CGCE, 8 giugno 2004, C- 444/02, in www.curia.europa.eu..

[216] V. art. 9 dir. 96/9/CEE.

prestito dei soggetti di cui all'art. 69 comma 1 non costituisce atto di reimpiego»[217]. In altri termini si ha reimpiego quando si effettua una qualsiasi operazione non autorizzata con la quale si mette a disposizione del pubblico tutto o una parte sostanziale del contenuto di una banca dati[218].

La nozione di parte sostanziale divide gli interpreti: l'orientamento più diffuso ricostruisce la nozione partendo dal concetto di investimento rilevante. Così ritiene che l'estrazione o il reimpiego abbia riguardato una parte sostanziale quando il contenuto estratto/reimpiegato se sistematizzato andrebbe a costituire una banca dati meritevole di tutela da parte dell'ordinamento[219]. Così anche parti quantitativamente irrilevanti potrebbero essere oggetto di protezione se il loro valore è tale da comportare investimenti rilevanti. Tale orientamento è stato criticato da parte della dottrina perché si porrebbe in contrasto con il principio guida di tale materia che esclude la protezione del singolo dato, anche nel caso in cui questo ha comportato l'impiego di risorse notevoli[220]. Un autore identifica la parte sostanziale dell'opera partendo dai fini perseguiti dal titolare con la creazione della stessa, senza prestare alcuna considerazione a quelli perseguiti dall'utilizzatore. Così se un utilizzatore attraverso un apposito software riuscisse ad estrarre un valore computazionale notevole da dati che sono considerati marginali rispetto agli altri elementi di cui è composta la banca dati non porrebbe in essere alcuna attività contraffattiva[221]. Questo orientamento, nonostante abbia il pregio di favorire la circolazione delle informazioni e le innovazioni nello studio dei dati, non tiene conto di un principio immanente al diritto d'autore: il titolare ha diritto a ricevere un compenso per ogni utilizzazione commerciale della sua creazione. Una deviazione da tale principio si porrebbe come norma eccezionale e dovrebbe essere espressamente sancita dal legislatore e non solo ricavabile in via interpretativa dall'art. 8 par. 1 che permette all'utente legittimo di estrarre e reimpiegare parti non sostanziali della banca dati. Una soluzione che porterebbe a risultati analoghi potrebbe essere quella di qualificare parte sostanziale della banca dati quella parte in assenza della quale essa non avrebbe più valore.

---

[217] Art. 102bis co. 1 lett. c).

[218] Cfr. CGUE, 19 dicembre 2012, C- 202/12, in *Diritto comunitario online* 2014; CGUE, 5 marzo 2009, cit..

[219] In questo senso v. BERTANI, *Impresa culturale e diritti esclusivi*, Giuffrè, Milano, 2000, 342; per la giurisprudenza v. CGUE, 5 marzo 2009, cit..

[220] BERTANI, *Big data, Proprietà intellettuale e mercati finanziari*, in *AIDA* 2017, 540 ss.; OTTOLIA, *Big data e innovazione computazionale*, cit., 86.

[221] OTTOLIA, *Big data e innovazione computazionale*, cit., 86 ss..

In conclusione sembrerebbe, anche alla luce delle nozioni sopra illustrate, che la duplice tutela prevista per le banche dati, diritto d'autore per quelle creative e diritto sui generis per quelle che abbiano richiesto un investimento rilevante, non sia sufficiente per controllare l'accesso ai dati ed impedire il loro utilizzo. Infatti, come si è potuto osservare, la direttiva 96/9/CE protegge il metodo di predisposizione del contenuto e impedisce l'estrazione ed il rimpiego della totalità o di una parte sostanziale di ciò che è racchiuso nella banca dati, ma come si ricava dall'articolo 3 comma 2 e 7 comma 4: «La tutela delle banche di dati in base al diritto d'autore prevista dalla presente direttiva non si estende al loro contenuto e lascia impregiudicati i diritti esistenti su tale contenuto». Inoltre, si consideri che la Corte di giustizia ha interpretato in maniera restrittiva l'investimento rilevante necessario per accedere alla tutela offerta dal diritto sui generis sulle banche dati. L'investimento valutato ai fini della verifica circa la sussistenza del diritto è quello relativo alla ricerca di materiale indipendente già esistente e quello necessario alla sua raccolta e predisposizione in un database, mentre non rileva in alcun modo le risorse impiegate per la creazione di questo materiale[222]. Cosicché, per quanto qui ci riguarda, non devono e non possono essere in alcun modo presi in considerazione gli investimenti impiegati per effettuare l'analisi big data[223]. Le ragioni della non rilevanza dell'attività di produzione dei dati possono essere spiegate individuando gli obiettivi che si è posto il legislatore comunitario con l'adozione della direttiva 96/9/CE. In primo luogo, il legislatore nel considerando 9 della direttiva citata prende atto che le banche dati sono uno strumento importante per lo sviluppo del mercato dell'informazione. Posta questa loro importanza è fondamentale che siano fruibili nel migliore dei modi e quindi è imprescindibile incentivare l'investimento relativo alla sistemazione più efficiente e non quello iniziale relativo alla produzione[224]. L'investimento rilevante è quindi solo quello volto all'organizzazione del materiale ottenuto, per applicare la tutela sui generis i dati ottenuti dovranno essere sistemati

[222] V. CGCE, 9 novembre 2004, cit.. In questo senso per la dottrina v. GIOV. GUGLIELMETTI, *La tutela delle banche dati con diritto sui generis nella direttiva 96/9/CE*, in *Contratto e impresa Europa* 1997, 184; GIOV. GUGLIELMETTI, *Commento all'art. 5, in Aa.Vv*., *Attuazione della direttiva 96/9/CE relativa alla tutela giuridica delle banche dati*, a cura di AUTERI, in *NLCC* 2003, 1241; BERTANI, *Proprietà intellettuale e nuove tecniche di appropriazione delle informazioni*, cit., 25 e 26. Per la giurisprudenza di merito v. Trib. Torino, ord. 16 dicembre 1997, in *AIDA* 1998, 550; Trib. Pavia, ord. 22 marzo 1997, in *AIDA* 1998, 526.
[223] ZECH, op.cit., passim; DREXL, op. cit., passim, 2016.
[224] V. OTTOLIA, *Big data e innovazione computazionale*, cit., 78 ss..

secondo un criterio organizzativo volto a permettere l'analisi e lo studio degli stessi e questa sistemazione dovrà comportare un investimento rilevante[225].

In più si consideri che le nozioni di estrazione e di rimpiego non sono applicabili ai dati del database utilizzati per l'analisi big data, infatti questa operazione non comporta alcun trasferimento permanente o temporaneo della totalità o di una parte sostanziale del contenuto del database su un altro supporto.

In definitiva quindi è possibile affermare, a parere di chi scrive, che se sul singolo dato non insiste alcun diritto autonomo, come può essere il diritto d'autore su un'opera contenuta nel database, questo non è tutelato e non si può impedire all'utente legittimo di utilizzarlo.

Questa conclusione è ulteriormente supportata da una recente comunicazione della Commissione Europea. Nel comunicato del 10 gennaio 2017 la Commissione a proposito di questo tema ha affermato l'impegno ad avviare una valutazione della direttiva sulle banche dati che tenga conto del mutato contesto tecnologico e dell'importanza per l'economia odierna dell'analisi big data. La Commissione rileva quindi l'inadeguatezza dell'attuale testo normativo e l'impossibilità di considerare le banche dati uno strumento utile per avere una padronanza del contenuto ed escludere ai terzi la possibilità di effettuare analisi big data.

Resta comunque da precisare che, come sostiene un importante autore, qualora si ritenesse che il soggetto che compie l'analisi big data sui dati contenuti sul database effettui attività di estrazione e reimpiego, lo strumento delle banche dati sarebbe sicuramente utile per proteggere il contenuto, almeno in parte, poiché il diritto del costitutore della banca dati può essere fatto valere quando l'analista, che utilizza i dati contenuti nel database, compie estrazioni e/o riutilizzazione che singolarmente considerate non sono rilevanti perché non riguardano una parte sostanziale del database ma nel loro insieme costituiscono estrazione e reimpiego di una parte considerevole della banca dati e si pongono in contrasto con il diritto del costitutore qualora avvengano senza il consenso di questi[226].

---

[225] Ibidem.

[226] In questo senso v. ZECH, op. cit., 66 ss.. Nel senso di considerare rilevanti le azioni di utilizzo dei dati a prescindere da una materiale riproduzione o trasferimento degli stessi su un altro supporto v. Ottolia, Big data e innovazione computazionale, cit., 90.

2. Come appena dimostrato nel precedente paragrafo: la duplice tutela prevista per le banche dati, diritto d'autore per quelle creative e diritto sui generis per quelle che abbiano richiesto un investimento rilevante, non è sufficiente per controllare l'accesso ai dati ed impedire il loro utilizzo. Tuttavia, le cose cambiano se si tratta di dati personali, in questo caso, grazie alle limitazioni poste a tutela dell'interessato, il costitutore della banca dati può controllare la loro circolazione e il loro impiego pre-impostando in un determinato modo la strategia di raccolta di tali dati e il loro successivo utilizzo. Per comprendere al meglio come il titolare del trattamento possa utilizzare ai fini di analisi big data i dati personali raccolti si farà riferimento in alcuni passaggi all'ipotesi più rilevante in tale ambito, ossia quella di una banca dati contente dati personali raccolti e trattati per finalità di profilazione commerciale.

La disciplina relativa alla protezione dei dati sembra essere stata concepita in completa opposizione con la normativa sulle banche dati. Infatti, nel primo caso l'intento del legislatore è quello di limitare la raccolta di dati personali. Nella seconda ipotesi invece, l'ordinamento vuole incentivare la costituzione di patrimoni informativi che le imprese possono utilizzare sia come prodotto funzionale alla realizzazione di altre attività di impresa, sia come prodotto e servizio da offrire direttamente sul mercato, infatti tutelando con un diritto esclusivo coloro che effettuano investimenti rilevanti per raccogliere e accumulare dati l'ordinamento pone innegabilmente in una posizione di vantaggio chi effettua tale tipo di investimento[227]. Il contrasto tra queste normative non deve stupire se comunque si ragiona sul fatto che esse hanno una notevole vicinanza temporale dato che è del 1995 la direttiva privacy e del 1996 la direttiva sulle banche dati che ha introdotto il diritto connesso, sopra esaminato. Il legislatore comunitario di quegli anni ha voluto introdurre un equilibrio sul mercato per l'utilizzo di informazioni personali, acconsentendo alle imprese l'uso di tali dati ma limitandolo con una serie di regole e principi. In particolare, in questo ambito rileva innanzitutto il principio di liceità. Ciò significa che l'utilizzo dei dati personali all'interno delle banche di dati è consentito solamente nel pieno rispetto di questo principio. L' equilibrio scelto dall'ordinamento europeo, confermato anche dal nuovo Regolamento europeo sulla protezione dei dati personali, ha così introdotto una tutela molto forte nei confronti degli interessati avvantaggiando indirettamente le stesse imprese che si avvalgono di tali dati nei confronti della concorrenza. Infatti, come si vedrà meglio nel proseguo, nel caso si

[227] Cfr. L.C. UBERTAZZI, *Banche dati e privacy*, in *Riv. dir. ind*. 2002, 632.

tratti di banche di dati composti da dati personali le imprese concorrenti del costitutore sono soggetti a limiti ulteriori rispetto a quelli normalmente previsti per l'utilizzo di database altrui[228].

Il principio di liceità, così come formulato nel regolamento europeo, impone che il trattamento dei dati personali avvenga in modo lecito, corretto e trasparente. Il riferimento alla correttezza e alla trasparenza è un richiamo al generico dovere di fornire all'interessato un'informativa appropriata e completa alla luce di quanto previsto dall'art. 13 e 14 GDPR. Mentre il richiamo alla liceità ha un significato più pregnante imponendo che esso possa avvenire solo nel caso in cui vi sia un'idonea base giuridica[229]. Il punto di partenza per comprendere a pieno il significato di questo termine nel contesto attuale del diritto europeo per la protezione dei dati personali è costituito dall'art. 52 par. 1 della Carta di Nizza, in virtù del quale limitazioni ai diritti e libertà fondamentali dell'individuo vi possono essere unicamente nel rispetto del principio di proporzionalità e quando siano volte a realizzare finalità altrui di interesse generale riconosciute dall'Unione o volte ad esigenze di protezione di altrui diritti e libertà fondamentali. A tal proposito rileva quindi l'art 8 della citata convenzione che acconsente a limitazioni al diritto alla protezione dei dati personali nel limite in cui questo avvenga col consenso dell'interessato o sulla base di un altro fondamento giuridico previsto dalla legge. Dal combinato disposto di questi articoli si ricavano due premesse fondamentali: i) in materia vi è una riserva assoluta di legge, per cui non si può procedere a trattare i dati su fondamenti diversi da quelli previsti dalla legge; ii) in

---

[228] Sui limiti nell'utilizzo dei dati contenuti in banche di dati v. supra par. 1 del presente capitolo.

[229] Secondo un orientamento dottrinale largamente condiviso occorre distinguere tra il richiamo alla liceità effettuato dall'art. 5 co.1 lett. a) GDPR e l'art. 6 GDPR rubricato "Liceità del trattamento". Secondo tale dottrina, mentre il richiamo all'art. 6 è volto ad accertare e assicurare la liceità a monte, ossia nel momento iniziale. L'art. 5 co.1 lett. a) intende la liceità quale conformità in concreto del trattamento a tutte le norme dell'ordinamento giuridico di riferimento, a prescindere dalla base giuridica adottata. In altri termini il richiamo all'art. 5 consisterebbe in un richiamo generale alla non antigiuridicità del trattamento tout court a prescindere dall'adozione di una corretta base giuridica. Alla luce di queste considerazioni quindi vi è un processo di valutazione di tale requisito su due livelli: l'art. 6 funge da filtro di selezione predeterminando in anticipo quando un trattamento è lecito, guardando esclusivamente alla base giuridica adottata. Mentre l'art. 5 impone un costante e concreto rispetto della liceità mentre il trattamento è posto in essere.
(In tal senso v. PIRAINO, *La liceità e la correttezza*, in *La Libera circolazione e la protezione dei dati personali*, (a cura di) PANETTA I, vol. I, Giuffrè, Milano, 2006, 750 ss.; IAMICELI, *Liceità, correttezza, finalità del trattamento dei dati personali*, in *Diritto alla riservatezza e circolazione dei dati personali*, (a cura di) PARDOLESI, I, Giuffrè, Milano, 2003. 411 ss.; Bravo, *Il consenso e le altre condizioni di liceità del trattamento*, in *Il nuovo Regolamento europeo sulla privacy e la protezione dei dati personali*, (a cura di) G. FINOCCHIARO, Zanichelli, Bologna, 2017, 111 ss.).

secondo luogo, è sempre necessario che il trattamento persegua uno scopo legittimo[230]. L'art. 6 del nuovo regolamento rubricato «Liceità del trattamento» disciplina 6 fondamenti legittimi alternativi sulla base dei quali il trattamento dei dati personali può avvenire, tale articolo assolve ad una funzione selettiva dei trattamenti ammessi dall'ordinamento individuando i presupposti di legittimazione al trattamento[231]. Nel caso di studio che qui interessa, ossia l'ipotesi di trattamento di dati personali all'interno di un database con finalità di profilazione commerciale, la base giuridica maggiormente utilizzata e utilizzabile è, come chiarito nel precedente capitolo, il consenso dell'interessato al trattamento dei propri dati personali per finalità specifiche.

È chiaro che così facendo il costitutore di banche di dati sulla base dell'informativa fornita all'interessato e sulla base della relativa richiesta di consenso potrà già decidere le strategie di utilizzo dei dati personali così ottenuti, consentendo o impedendo a monte il futuro utilizzo di quelle informazioni ad altri soggetti. Infatti, quando l'impresa fornisce l'informativa e richiede il consenso opta già per una determinata politica di utilizzo di quei dati. In questo modo se il costitutore ha deciso di raccogliere i dati per utilizzarli lui stesso per finalità di profilazione non potrà in alcun modo cedere gli stessi ad altri soggetti, terzi rispetto all'interessato, né questi potranno avvalersi della sua banca dati senza commettere un illecito. Viceversa, se l'impresa ha informato l'interessato e ha ottenuto il consenso per un utilizzo più ampio che comprende anche la possibilità di comunicare gli stessi a terzi affinché anche questi possano effettuare attività di profilazione, lo scenario cambia e il costitutore potrà concedere in licenza l'utilizzo delle informazioni così raccolte[232]. Risulta così fondamentale progettare a monte il trattamento che si vuole realizzare per poter stabilire il regime a cui sottoporre i dati personali raccolti. In questo modo, diversamente dalle ipotesi viste nel precedente paragrafo, il costitutore ha una piena padronanza sulla circolazione dei dati contenuti

---

[230] Cfr. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali, dalla direttiva 95/46 al nuovo regolamento europeo*, cit., 241 e 242.

[231] BRAVO, op. cit., 121 ss..

[232] Un esempio che permette di comprendere il modo di operare del principio di liceità relativo alla disciplina della protezione dei dati personali nei confronti della disciplina autorale delle banche dati è costituito dalla disciplina transitoria introdotta dal decreto Milleproroghe del 2009. Tramite tale decreto il legislatore ha permesso, fino al 31 dicembre 2009, alle società di trattare dati personali raccolti prima del 1 agosto 2005 senza il consenso informato dell'interessato. Il garante, successivamente con un apposito provvedimento ha dettagliato l'utilizzo dei dati personali contenuti nelle banche di dati costituite prima del 1 agosto 2005 dalle società di telemarketing, precisando che in alcun modo altre società possono utilizzare i dati ivi contenuti e che lo stesso titolare non può utilizzarli per scopi diversi dal telemarketing (sul punto v. CALABRÒ, *Diritto delle comunicazioni elettroniche*, Giuffrè, Milano, 2010, 260 ss..; Garante per la protezione dei dati personali, Provv. del 12 marzo 2009).

nella sua banca di dati. Se quindi il costitutore da una parte è avvantaggiato nei confronti della concorrenza, dall'altra parte deve sottostare ad una serie di limiti nell'utilizzo dei dati personali raccolti dettati dai principi che governano la normativa relativa alla protezione dei dati personali[233] e dai diritti dell'interessato di cui agli artt. 15 ss. del regolamento. Nell'ipotesi esaminata i principali limiti, ulteriori rispetto a quelli relativi alla liceità, che incidono sul controllo dell'utilizzo dei dati personali inseriti nella banca di dati da parte del costitutore della stessa riguardano il rispetto del principio di limitazione delle finalità, di conservazione, il diritto alla portabilità dei dati e il diritto di ritirare il consenso al trattamento dei dati personali.

Per quanto riguarda il principio di limitazione delle finalità si rimanda a quanto già riportato nel primo capitolo, per cui i dati personali contenuti nella banca dati potranno essere utilizzati solo per il fine di profilazione commerciale e non per altri fini, salvo un eventuale utilizzo ulteriore e compatibile degli stessi effettuato alla luce delle condizioni evidenziate nel capitolo precedente. Rispetto alla disciplina ordinaria applicabile alle banche di dati il titolare paga a caro prezzo la possibilità di controllare l'utilizzo e la circolazione dei dati personali che ha raccolto. Difatti nell'ipotesi in cui il database contenga elementi non qualificabili come dati personali vi è una maggior libertà sull'impiego degli stessi e non vi è alcun vincolo di destinazione.

Per quanto riguarda il principio di conservazione la legge, sia il codice privacy che il nuovo regolamento, non predetermina un periodo di conservazione dei dati personali applicabile a qualsiasi tipologia di trattamento ma piuttosto con disposizioni di carattere aperto impone di effettuare un bilanciamento tra i contrapposti interessi in gioco. In

[233] Art. 5 GDPR: «1.I dati personali sono: a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»); b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»); c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»); d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»); f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»). 2.Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).»

Italia in molti casi è stato lo stesso Garante ad effettuare tale contemperamento[234]. Per quanto riguarda la profilazione commerciale infatti, con il provvedimento del 24 febbraio 2005, il Garante, dopo aver richiamato il principio di cui all'art. 11 co. 1 lett. e) del Codice Privacy che impone la conservazione per un tempo non superiore agli scopi per i quali i dati sono trattati, statuisce che i dati personali conservati per finalità di profilazione non possono essere conservati per un termine superiore ai dodici mesi. Tuttavia, il Garante lascia uno spiraglio acconsentendo l'eventualità che si possa fare profilazione per un termine ulteriore, purché prima, in ossequio all'art. 17 del Codice Privacy, si sottoponga tale intenzione ad una previa valutazione dello stesso Garante[235]. A tal proposito diverse società hanno tentato questa strada, e il Garante in diversi casi ha concesso la possibilità di conservare i dati personali dei clienti per un periodo molto più lungo arrivando a concedere periodi notevoli fino a 15 anni nel provvedimento del 30 giugno 2016. L'allungamento del periodo di conservazione è stato concesso alla luce della finalità perseguita, la profilazione, rapportata al tipo di beni o servizi per i quali essa veniva fatta. Cosi ad esempio nel caso di Tecnocasa si è ritenuto non utile il rispetto del periodo di un anno perché i beni o servizi offerti dalla suddetta società non potevano in alcun modo interessare i clienti che avevano già effettuato un acquisto l'anno precedente[236]. La stessa valutazione era stata fatta in precedenza per quelle società che operano nel settore dei beni di lusso[237]. Il Garante per la protezione dei dati personali in ciascuno di questi casi ha concesso l'allungamento del periodo di conservazione perché ha ritenuto sussistente una ragione oggettiva sottesa a tale conservazione. Il Garante privacy ha effettuato un contemperamento tra gli interessi del titolare e dell'interessato e di conseguenza ha determinato il periodo di conservazione.

Il quarto limite, di recente introduzione, che incide in modo decisivo sul diritto del costitutore della banca di dati è il diritto dell'interessato alla portabilità disciplinato all'art. 20 del GDPR. Tale diritto incide non tanto sulla fruibilità dei dati personali da

---

[234] I limiti di conservazione stabiliti in base ai provvedimenti del Garante risulterebbero ancora applicabili alla luce del considerando 171 che fa salvi i provvedimenti dell'autorità di controllo adottati sulla base della direttiva 95/46/CE purché, ovviamente, tali provvedimenti non si pongano in contrasto con il nuovo Regolamento e non siano modificati o sostituiti.

[235] Garante per la protezione dei dati personali, Provvedimento 24 febbraio 2005, **"***Fidelity card' e garanzie per i consumatori. Le regole del Garante per i programmi di fidelizzazione"*, 5.

[236] V. Garante per la protezione dei dati personali, Provvedimento 30 giugno 2016, *"Conservazione dei dati personali riguardanti la clientela per attività di profilazione e di marketing"*.

[237] Cfr. nel settore dei beni di lusso, Garante per la protezione dei dati personali, Provvedimento 24 aprile 2013, n. 219; Id., Provvedimento 30 maggio 2013, n. 263; Id, Provvedimento 7 novembre 2013, n. 500; Id., Provvedimento 2 dicembre 2015, n. 632.

parte del titolare del trattamento ma più che altro sulla possibilità da parte dello stesso di controllarne la circolazione. È un diritto con una duplice valenza: da una parte permette all'interessato un maggior potere di controllo sui propri dati personali e sulla loro circolazione, con l'intento di svincolare l'interessato dalla posizione di dipendenza che lo tiene legato al fornitore del servizio a cui ha fornito i suoi dati; dall'altra è stato concepito come uno strumento antimonopolistico volto ad agevolare un mercato concorrenziale dei servizi della società dell'informazione permettendo anche ai nuovi operatori di acquisire rapidamente il patrimonio operativo di cui dispongono coloro che operano già da tanto tempo in un determinato settore, con l'intento di eliminare un importante ostacolo all'ingresso sul mercato[238].

Il diritto alla portabilità dei dati personali consta di due facoltà: diritto dell'interessato di ricevere i dati personali forniti al titolare e diritto di trasmettere tali dati ad un diverso titolare. La comunicazione dei dati personali dovrà avvenire utilizzando un formato strutturato di uso comune e leggibile meccanicamente. Oggetto della comunicazione possono essere solamente quei dati che vengono trattati con sistemi automatizzati sulla base del consenso o di un contratto con l'interessato e che vengono forniti dallo stesso in modo consapevole e attivo. Il titolare originario potrà continuare ad utilizzare i dati oggetto della comunicazione, salvo un eventuale richiesta di cancellazione ex. art. 17 GDPR, e inoltre, non è tenuto a comunicare tutti quei dati personali che sono stati generati utilizzando come input i dati osservati o forniti direttamente dall'interessato, ossia i dati inferenziali e derivati ricavati applicando un algoritmo ai dati personali forniti in modo attivo dall'interessato[239]. L'esercizio del diritto alla portabilità dei dati non incide in alcun modo sul potere di utilizzo dei dati da parte del titolare.

Alla luce dell'art. 20 del GDPR il titolare di una banca dati che tratta informazioni personali dovrà innanzitutto adottare procedure e sistemi che gli permettano di rispondere alle eventuali richieste degli interessati e non potrà in alcun modo impedire ad un altro concorrente la possibilità di fruire di quei dati personali se vi è una domanda in tale senso da parte dell'interessato. Tuttavia, restano salvi i risultati ottenuti tramite l'analisi big data, dato che, come appena evidenziato, i dati ricavati dall'applicazione di

---

[238] Cfr. RICCI, *I diritti dell'interessato*, in *Il nuovo Regolamento europeo sulla privacy e la protezione dei dati personali*, (a cura di) G. FINOCCHIARO, Zanichelli, Bologna, 2017, 219 e 220; PELINO, *I diritti dell'interessato*, in *Il Regolamento privacy europeo*, (a cura di) BOLOGNINI, PELINO e BISTOLFI, Giuffrè, Milano, 2016, 249.

[239] V. WP29, "*Linee guida sul diritto alla portabilità dei dati*", 3 e 5 e 7 – 11.

un algoritmo non devono essere ceduti. Secondo un autore in questo caso resta salva la possibilità dell'interessato di accedere ex. art. 15 GDPR a tali dati[240], mentre non è possibile richiedere il trasferimento degli stessi ad un diverso titolare[241]. Questa affermazione è conseguenza della qualificazione del diritto alla portabilità dei dati quale sviluppo del diritto di accesso previsto già dalla direttiva 95/46/CE[242]. Le stesse considerazioni fatte per il diritto alla portabilità dei dati possono essere fatte nell'ipotesi in cui l'interessato eserciti il suo diritto di revoca del consenso al trattamento dei suoi dati personali. Resta sempre salva la liceità del trattamento effettuato prima che l'interessato esercitasse i suoi diritti.

Vi sono anche degli ulteriori limiti, che vengono in gioco in situazioni patologiche del trattamento, nei casi in cui vi sia stata una violazione della normativa privacy e i dati personali sono stati trattati in modo non lecito, l'interessato ha diritto d'opporsi al trattamento, di chiedere una limitazione dello stesso oppure di chiedere la cancellazione dei propri dati personali.

Nonostante la maggior possibilità di controllo e di esclusività nell'utilizzo dei dati contenuti nella banca dati, qualora questi siano personali l'imprenditore dovrà sopportare costi notevoli e rischi notevoli. Infatti, prendendo in considerazione l'esempio posto inizialmente, la profilazione per promozioni commerciali avvalendosi di tecnologie che implementano soluzioni di analisi big data, può comportare il rispetto di determinati adempimenti particolarmente onerosi in termini di compliance, quali ad esempio: la valutazione di impatto[243] e la nomina di un responsabile per la protezione dei dati[244], nonché l'adozione di adeguati meccanismi che assicurino il rispetto dei

---

[240] RICCI, op. cit., 223.

[241] WP29, "*Linee guida sul diritto alla portabilità dei dati*", 3 ss..

[242] Cfr. WP29, ibidem; Pelino, op. cit., 249; Ricci, op. cit.,219;

[243] V. art. 35 GDPR: Quando un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche il regolamento impone di procedere ad una valutazione di impatto. Tale adempimento consiste nel realizzare un documento in cui si descrive il trattamento, valutando le necessità e il rispetto dei principi che governano la materia, indicando le soluzioni che si intendono adottare per far fronte ai rischi del trattamento a cui potrebbero essere esposti gli interessati (per un approfondimento v. WP29, *Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679*, 3 ss.).

[244] V. art. 37 GDPR: Nei casi in cui il trattamento sia posto in essere da un'autorità pubblica, o comporti un regolare e sistematico controllo su larga scala degli interessati, oppure implichi il trattamento di categorie particolari di dati o dati giudiziari il GDPR impone l'obbligo di nominare un Responsabile della protezione dei dati. Tale soggetto ha il compito di controllare che tutti i trattamenti posti in essere dalla società in cui è stato nominato siano conformi al regolamento e ogni operazione che ha un qualche impatto privacy dovrà ricevere la sua approvazione. Inoltre esso funge da strumento di raccordo tra la società e il garante, costituendo una sorta di garante interno (per un approfondimento v. WP29, *Guidelines on Data Protection Officers ('DPOs')*).

principi sanciti dall'art. 5 del regolamento. Il mancato corretto adempimento di tali obblighi espone il titolare a sanzioni, che alla luce del GDPR, sono estremamente elevate[245]. Infine, come emerge chiaramente dal considerando 70 del GDPR e come già anticipato, in caso di profilazione commerciali l'interessato in qualsiasi momento può ritirare il proprio consenso e impedire così al titolare il trattamento dei suoi dati personali[246].

Quindi a fronte dei vantaggi vi potrebbero essere costi notevoli che tuttavia ritengo non incidano in modo eccessivo sull'investimento realizzato. Tali costi non vi sarebbero qualora si procedesse ad utilizzare dati anonimi. Per ridurre o evitare tali costi è pur sempre possibile, seguendo il percorso indicato dal Garante Privacy, raccogliere i dati personali e trattarli per finalità di profilazione nel termine di un anno o in quello ulteriore, ottenuto a seguito di previa valutazione interna tenendo in considerazione gli orientamenti seguiti dall'Autorità di controllo, per poi procedere ad anonimizzarli e continuare a beneficiare, seppur in modo limitato, dei vantaggi derivanti dal patrimonio informativo acquisito[247]. In tale ipotesi, in un primo momento si applicherà la disciplina prevista dalla legge 633 del 1941 con i correttivi appena visti imposti dalla normativa sulla protezione dei dati personali, per poi applicarsi unicamente la disciplina prevista dalla legge sul diritto d'autore.

3. Rispetto alla protezione stabilita per le banche dati quella per il segreto industriale ha il vantaggio che può riguardare direttamente una specifica informazione o uno specifico dato. Non rileva infatti, come nelle banche di dati, la distinzione tra investimento rilevante ai fini dell'organizzazione e quello realizzato ai fini della

---

[245] Negli articoli 83 e 84 del GDPR il legislatore comunitario si limita a prevedere i criteri in base ai quali l'ammontare delle sanzioni deve essere determinato. Rispetto al passato il legislatore ha deciso, per alcune violazioni, di fare riferimento ad un tetto massimo della sanzione individuato non in termini assoluti ma tramite una percentuale del fatturato mondiale del soggetto che ha effettuato la violazione. In concreto, quindi la violazione di queste norme può avere delle conseguenze molto gravi nei confronti della singola impresa (v. RATTI, *Il regime sanzionatorio previsto dal regolamento per l'illecito trattamento dei dati personali*, in FINOCCHIARO(a cura di), cit. 595 ss.; PELINO, *Le tutele e il danno risarcibile*, in BOLOGNI, PELINO e BISTOLFI (a cura di), cit., 573 ss.).

[246] Un ulteriore costo da tenere in considerazione, specie data la maggior sensibilità sul tema della protezione dati personali, è la strategia di marketing per presentare agli interessati il trattamento a cui li si vuole sottoporre.

[247] V. Garante per la protezione dei dati personali, Provv. del 24 febbraio 2005, cit., 5. La notevole difficoltà nel seguire gli orientamenti dell'Autorità di controllo è dettata dal fatto che, soprattutto nel contesto online, i trattamenti avvengono nei confronti di interessati appartenenti a diversi stati. Per questo motivo occorre tenere in considerazione gli orientamenti delle diverse autorità di controllo e muoversi di conseguenza, magari differenziando stato per stato il periodo di conservazione dei dati.

creazione dell'informazione[248]. Nell'ordinamento italiano le informazioni segrete ricevono tutela in diversi ambiti, compreso il diritto industriale e della concorrenza. Nel diritto industriale le norme di riferimento sono costituite dagli articoli 98 e 99 del c.p.i., mentre nel diritto della concorrenza l'appropriazione di informazioni segrete rientra in quelle condotte contrarie ai principi di correttezza e lealtà a cui devono attenersi le imprese e che sono richiamati dalla clausola generale contenuta nel terzo comma dell'articolo 2598 cod. civ.. Fino al d.lgs. n. 131 del 2010 l'opinione dottrinale e giurisprudenziale più diffusa riteneva che l'articolo 99 c.p.i. configurasse un diritto esclusivo esercitabile erga omnes in capo al detentore legittimo delle informazioni segrete. Cosicché tale diritto poteva essere fatto valere nei confronti di chiunque a prescindere dal fatto che vi fosse un rapporto di concorrenza o a prescindere dalle concrete modalità mediante le quali si erano ottenute tali informazioni[249]. Per tale orientamento non rilevava in alcun modo quanto stabilito dall'articolo 39 TRIPS che subordina la sussistenza dell'illecito alla violazione dei principi di onesta che governano le pratiche commerciali. Dopo la modifica apportata dal d.lgs. del 2010 è esclusa espressamente dal testo dell'articolo la possibilità di impedire al terzo l'utilizzo di tutte le informazioni che abbia conseguito in modo indipendente[250]. Così è opinione largamente diffusa che a seguito di questa modifica non vi sarebbe più una tutela assoluta esercitabile erga omnes, ma una tutela relativa, ravvisando nella modifica introdotta nel 2010 l'intenzione del legislatore di riconciliarsi con quanto stabilito dall'articolo 39 TRIPS[251]. Ciò comporta diverse conseguenze, la principale e più importante per le caratteristiche del mondo big data è la seguente: se la fonte da cui sono ricavate le informazioni, come spesso avviene nel mondo dell'Internet of things e del digitale in genere, è «pubblica[252]» nel senso che chiunque potenzialmente può

---

[248] V. OTTOLIA, *Big data e innovazione computazionale*, cit., 58.

[249] In tal senso v. BERTANI, *Proprietà intellettuale e nuove tecniche di protezione delle informazioni*, cit., 14; FLORIDIA, *Il riassetto della proprietà industriale*, Giappichelli, Torino, 2006, 608; DE ANGELIS, *Informazioni segrete e diritti di proprietà industriale non titolati*, in SCUFFI e FRANZOSI (a cura di), *Diritto industriale italiano*, vol. I, CEDAM, 2014, Padova, 895; Trib. Bologna, 4 luglio 2008, in *GADI* 2008, 5298, 977.

[250] V. DE ANGELIS, op. cit., 896.

[251] Cfr. C. GALLI, *La riforma del codice della proprietà industriale*, in www.filodiritto.com, 2010, 4; DE ANGELIS, ibidem.

[252] Con il termine pubblica si vuole intendere una fonte a cui potenzialmente qualsiasi fornitore di IoT o qualsiasi impresa che sfrutta e analizza i dati condivisi online può accedere con facilità. Si veda l'esempio fatto nel paragrafo 1 del primo capitolo dei dati sul traffico, oppure si consideri l'esempio del social listening ecc… In tutti questi casi, chiunque tramite le opportune autorizzazioni, licenze, e risorse può accedere e ottenere i dati ricavati in tali contesti.

accedere a tale fonte, di fatto una tutela relativa troverebbe pochissimo spazio in tale ambito[253]. Non conterebbe più come in passato l'anteriorità del risultato o della scoperta.

Questa difficoltà non potrebbe essere superata nemmeno se si accogliesse il meno diffuso e contrapposto orientamento che considera ancora presente la tutela reale e vede nella modifica del 2010 l'introduzione di un'esplicita misura di salvaguardia della buona fede del terzo che ha ottenuto indipendentemente quei dati senza immaginare che altri potessero aver già avuto un qualche accesso[254]. La situazione non pare essere destinata a cambiare con la direttiva sui segreti commerciali (dir. UE n. 943/2016). Tale direttiva all'articolo 3 comma 1 lett. a) espressamente ribadisce che l'acquisizione di un segreto commerciale è considerata lecita quando è frutto di una scoperta o di una creazione indipendente. Alla lettera b) del medesimo articolo sembra che il legislatore europeo abbia proprio considerato l'ipotesi anzi dette del digitale e dell'IoT affermando che l'acquisizione è altresì considerata lecita quando è frutto di «osservazione, studio, smontaggio o prova di un prodotto o di un oggetto messo a disposizione del pubblico o lecitamente in possesso del soggetto che acquisisce le informazioni, il quale è libero da qualsiasi obbligo giuridicamente valido di imporre restrizioni all'acquisizione del segreto commerciale».

Per quanto concerne l'oggetto della tutela non paiono esservi particolari difficoltà a farvi rientrare qualsiasi tipo di informazione ivi compresi anche i dati purché siano rispettati i requisiti di tutela stabiliti nell'articolo 98 c.p.i.: segretezza, valore economico come conseguenza della segretezza e misure di sicurezza volte a mantenere la segretazione[255]. Tale orientamento trova una evidente conferma anche per il futuro

---

[253] Quest'orientamento è ulteriormente motivato alla luce della nozione di detentore del segreto accolta nell'art. 2 num. 2) della dir. UE 943 del 2016, in questa disposizione è definito detentore colui che ha un potere di controllo legittimo sull'informazione, ossia chiunque sia legittimato (in virtù di un contratto, di un'autorizzazione dell'interessato nel caso in cui si tratti di dati personali, o altro titolo previsto dalla legge) ad accedere alla fonte «pubblica» (per come intendere l'accezione di fonte «pubblica» v. la nota precedente).

[254] V. CAMUSSO, *Le informazioni segrete*, in BOTTERO, *La riforma del codice della proprietà industriale*, Giuffrè, Milano, 2011, 288.

[255] In questo senso v. DE ANGELIS, op. cit., 904 e 905; e per la giurisprudenza v. Cass., 27 febbraio 1985, n. 1699, in *Giur. Comm.* 1986, II, 821; App. Bologna, 19 giugno 1995, in *GADI* 1996, 3426, 355; App. Milano, 10 novembre 1992, in *GADI* 1992, 2859, 862; App. Milano, 22 settembre 1992, in *GADI* 1993, 2910, 201. Contra ma per ragioni ormai superate alla luce della modifica del 2010: BERTANI, *Proprietà intellettuale e nuove tecniche di protezione delle informazioni*, cit.,14 ; FALCE, *Profili pro- concorrenziali dell'istituo brevettuale*, Giuffrè, Milano, 2008, 171. Questi autori ritenevano che una tutela assoluta così ampia avrebbe creato un effetto monopolistico eccessivo, dopo la modifica del 2010, salvo opinioni di

nell'articolo 2 della direttiva sui segreti commerciali che definisce l'informazione commerciale come quell'informazione che sia corredata dai tre requisiti sopra menzionati[256]. Risulta quindi ormai superato l'orientamento seguito da parte della dottrina che faceva rientrare nella protezione del segreto industriale come disciplinato dall'art. 98 c.p.i. solamente quelle informazioni inerenti l'area del brevettabile[257].

Come anzi detto, la normativa del segreto industriale per poter essere applicata necessità, come si ricava, dall'art. 98 comma 1 c.p.i. e anche dalla direttiva approvata nel 2016, il rispetto di tre requisiti: a) il primo è che le informazioni siano segrete, nel senso che non siano nel loro insieme o nella precisa configurazione e combinazione dei loro elementi generalmente note o facilmente accessibili agli esperti ed agli operatori del settore; b) abbiano valore economico in quanto segrete; c) siano sottoposte, da parte delle persone al cui legittimo controllo sono soggette, a misure da ritenersi ragionevolmente adeguate a mantenerle segrete.

I tre requisiti appena menzionati alla luce delle modifiche introdotte dal legislatore nel 2010 che hanno determinato un passaggio da una tutela assoluta ad una tutela relativa vanno di conseguenza intesi in senso relativo e non assoluto[258]. Così la segretezza non implica necessariamente una non conoscenza specifica da parte di alcuni soggetti dell'informazione. È importante che vi sia un'accessibilità almeno incompleta ed una possibilità di acquisizione dell'informazione non agevole, che non vi sia stato alcun atto di divulgazione e che l'informazione non sia già di pubblico dominio[259]. Il secondo requisito richiede un riscontro oggettivo: l'informazione permette di acquisire una quota di mercato e di essere in una posizione di vantaggio rispetto ai concorrenti che ne sono

---

minoranza, è pacifico poter affermare che la tutela sia relativa e quindi tale preoccupazione non abbia più motivo d'essere.

[256] Art. 2 n. 1) dir. UE n. 943/2016: «1) «segreto commerciale», informazioni che soddisfano tutti i seguenti requisiti: a) sono segrete nel senso che non sono, nel loro insieme o nella precisa configurazione e combinazione dei loro elementi, generalmente note o facilmente accessibili a persone che normalmente si occupano del tipo di informazioni in questione; b) hanno valore commerciale in quanto segrete; c) sono state sottoposte a misure ragionevoli, secondo le circostanze, da parte della persona al cui legittimo controllo sono soggette, a mantenerle segrete; »

[257] Cfr. BERTANI, *Proprietà intellettuale e nuove tecniche di appropriazione delle informazioni*, cit., 34 ss.; contra OTTOLIA, *Big data e innovazione computazionale*, cit., 43 ss..

[258] In questo senso v. GIOV. GUGLIELMETTI, *La tutela del segreto*, in *Le nuove frontiere del diritto dei brevetti*, Torino, 2003, 127 ss.; BERTANI, *Proprietà intellettuale e nuove tecniche di protezione delle informazioni*, cit., 36; DE ANGELIS, op. cit., 906.

[259] In questo senso v. GIOV. GUGLIELMETTI, *La tutela del segreto*, in Le nuove frontiere del diritto dei brevetti, cit., 127 ss.; BERTANI, *Proprietà intellettuale e nuove tecniche di protezione delle informazioni*, cit., 36; DE ANGELIS, op. cit., 906; per la giurisprudenza v. Trib. Roma, ord. 10 febbraio 2005, *SPI* 2005, I, 291; Trib. Milano, 31 marzo 2004, *GADI* 2004, 4734,979.

sprovvisti[260]. Infine, il terzo requisito è valutabile da un punto di vista fattuale: è necessaria l'adozione di una serie di misure tecnologiche, negoziali e precauzionali. Cosi ad esempio il terzo o il dipendente che viene a contatto con l'informazione deve essere sempre informato della segretezza dell'informazione. Si fa riferimento quindi, ad una serie di cautele, che è necessario prendere non solo a livello fisico (i.e. tecnologico-informatico), ma anche a livello di organizzazione aziendale[261].

I tre requisiti previsti dall'art. 98 co. 1 c.p.i. non possono essere rispettati con facilità nel contesto dell'internet of things, ossia più specificatamente, nel caso di dati prodotti da sensori annessi ai cd. prodotti smart. In primo luogo, è evidente che vi è un problema di segretezza; infatti finché il sensore che raccoglie dati è annesso ad una macchina che opera in una fabbrica o industria non vi è difficolta a mantenere segreti i dati raccolti, ma laddove i dati siano raccolti da sensori su auto che circolano su strade pubbliche è evidente che tali informazioni possano essere raccolti e utilizzati anche da altre imprese che si avvalgono di strumenti di raccolta analoghi[262]. Questo problema potrebbe essere superato con il dato normativo sia l'art. 98 c.p.i che l'art. 2 n. 1 lett. a) della direttiva 2016/943 fanno riferimento ad informazioni che non siano generalmente note o facilmente accessibili da parte degli esperti e degli operatori del settore a cui si riferiscono[263]. Laddove si ritenesse superabile la difficoltà relativa al requisito della segretezza, vi sarebbe comunque un notevole ostacolo a rispettare il secondo requisito quello relativo al valore economico dell'informazioni in quanto segrete. Infatti, pur essendo evidente al giorno d'oggi il valore economico dei dati non è provato il legame tra questo valore e la loro segretezza. Inoltre, nel contesto dell'analisi big data un singolo dato può non avere valore se non considerato unitamente ad altri dati. Infine, non è chiaro quali misure debbano prendere i titolari del segreto per mantenere tali dati riservati, e in un contesto di rete dinamica in cui continuano a passare flussi di dati è molto difficile mantenere segreti questo tipo di informazioni e non è immediato comprendere in che fase vada ad instaurarsi la protezione. Inoltre, a conferma di una difficile applicazione della tutela del segreto industriale, si consideri che le informazioni segrete per loro natura hanno una limitata e difficile circolazione negoziale: fin quando

[260] DE ANGELIS, op. cit., 908.
[261] Per un approfondimento v. DE ANGELIS, op. cit., 908 ss..
[262] In questo senso v. DREXL, op. cit., 20 ss.; Commissione Europea, Comunicazione: Costruire un'economia dei dati in Europa, COM (2017)9.
[263] Cfr. OTTOLIA, *Big data e innovazione computazionale*, cit., 52 e 53.

chi voglia acquistarle non né è messo a conoscenza non può stimarne a pieno il valore; dopo esserne venuto a conoscenza non ha più interesse a pagare per farsele rivelare ed inoltre nel determinare il compenso per la rivelazione deve scontare la diminuzione di valore che dipende dalla loro condivisione con il detentore originario (ed i suoi altri eventuali aventi causa)[264].

La nuova direttiva adottata dal legislatore europeo, invece di riconoscere un controllo esclusivo su qualsiasi uso delle informazioni protette, come sarebbe tipico per i regimi di proprietà intellettuale, implementa un approccio tipico della responsabilità civile che vieta un comportamento specifico relativo all'acquisizione, la diffusione, e l'utilizzo di segreti industriale che possa essere considerato come sleale. Il segreto industriale per come disciplinato sembra quindi più adatto a trovare un equilibrio tra il libero accesso e l'interesse alla tutela rispetto a riconoscere un diritto di proprietà in capo al detentore dei dati[265].

Nella prassi poi può essere particolarmente difficoltoso cedere o concedere in licenza i dati personali raccolti dal cedente(licenziante) perché chi ha interesse ad acquistarli o ad utilizzarli per evitare di incorrere in sanzioni per violazione della normativa sulla protezione dei dati personali ha interesse a leggere i testi delle informative fornite agli interessati per verificare se tale cessione o concessione è possibile. Inoltre, l'acquirente vorrà verificare almeno a campione il consenso specifico dato dagli interessati per la comunicazione dei loro dati. Infine, l'acquirente avrà interesse a farsi garantire per iscritto che il trattamento dei dati personali sia avvenuto nel rispetto della legge[266].

Tutto ciò crea notevoli difficoltà è ben più facile che sia direttamente il titolare originario dei dati personali che procederà al trattamento per conto dell'impresa interessata offrendo eventualmente un servizio in abbinato[267].

---

[264] In questo senso v. BERTANI, *Proprietà intellettuale e nuove tecniche di appropriazione delle informazioni*, cit., 32 ss.. L'obiezione dell'autore è superabile almeno in parte con l'adozione di apposite misure pre-contrattuali.

[265] WIEBE, *Protection of industrial data- a new property right for the digital economy, Journal of Intellectual Property Law & Practice*, Volume 12, 2017, 880.

[266] Resta da precisare che anche nell'ipotesi di una dichiarazione scritta del concedente, il concessionario non è esente da responsabilità amministrativa nel caso in cui si rilevi che il trattamento posto in essere è illecito.

[267] Questo è il caso ad esempio di Facebook che offre strumenti per la sentiment analisys effettuata sui dati personali condivisi dagli utenti sul social e quindi trattati dallo stesso. In questo modo l'impresa che compra questo servizio è interessata unicamente al risultato e non ha alcun interesse nel trattare direttamente i dati personali degli utenti e porre in essere tutti i necessari adempimenti privacy, preferendo avere un risultato in forma aggregata e anonima da utilizzare per le sue strategie di mercato.

Alla luce di tutte le difficoltà sopra evidenziate pare evidente che la tutela del segreto industriale non è lo strumento decisivo per regolare l'appartenenza e la circolazione dei dati, anche se rispetto alla tutela giuridica prevista a favore delle banche dati il segreto industriale può sorgere anche in una fase precedente, ossia quella relativa alla produzione dei dati[268]. Motivo per cui la tutela giuridica ottimale[269], probabilmente, non è costituita da uno solo degli strumenti di tutela applicabili, ma da una loro combinazione per fasi.

Occorre interrogarsi sulla possibilità di ricorrere allo strumento brevettuale per regolare la circolazione dei dati siano essi personali o non. In via generale occorre premettere che il ricorso alla tutela brevettuale per i dati è da escludere in base all'art. 45 co 2 lett. c) c.p.i.. Infatti tale norma non consente di considerare come invenzioni la presentazione di informazioni e le scoperte[270]. Tale disposizione riflette un principio pacifico nel nostro ordinamento che non riconosce alcuna tutela alle informazioni in sé e per sé. Resta da chiedersi se possano ricevere tutela brevettuale le informazioni che siano prodotti di invenzioni di procedimento, per cui potrebbe ottenere tutela il metodo di produzione e ottenimento e indirettamente i dati. Infatti il brevetto di procedimento potrebbe offrire una tutela indiretta anche al prodotto ottenuto tramite tale procedimento, infatti come si ricava anche dall'art. 25 degli Agreement on the Unifiedpatent Court: il diritto di procedimento contiene anche il diritto di prevenire che terzi possano offrire sul mercato un prodotto ottenuto direttamente tramite il processo oggetto di brevetto[271]. Per esempio, si consideri il caso in cui i dati sono prodotti da un'impresa applicando il metodo di produzione brevettato. In questo caso se il procedimento ed il relativo prodotto sono utilizzati senza il consenso del titolare del brevetto si avrebbe una violazione. Il motivo per cui la legislatura estende la protezione del brevetto di procedimento alla commercializzazione dei prodotti è che la tutela brevettuale del procedimento è molto più debole di quella prevista per i prodotti. Infatti, il prodotto brevettato è tutelato contro qualsiasi imitazione mentre il prodotto ottenuto tramite il procedimento non ottiene tutela se si riesce ad avere lo stesso risultato con un

---

[268] OTTOLIA, *Big data e innovazione computazionale*, 81 ss.

[269] Ottimale nel senso che deve tutelare non solo il detentore del dato ma deve trovare un equilibrio tra le libere utilizzazioni, la diffusione e condivisione dei dati e l'esclusività del relativo sfruttamento economico.

[270] Per un approfondimento v. FRANZOSI, *L'oggetto del brevetto*, in SCUFFI e FRANZOSI (a cura di), *Diritto industriale italiano*, vol. I, CEDAM, Padova, 2014, 533 ss..

[271] Contra OTTOLIA, *Big data e innovazione computazionale*, cit., 145 ss..

processo alternativo[272]. E così si risolve anche il problema relativo alla realizzazione del procedimento per l'ottenimento del prodotto all'estero in un paese in cui il brevetto non è registrato, per poi importare il prodotto nel paese in cui il brevetto di procedimento è tutelato. Resta il problema che questa è una tutela indiretta e di difficile applicazione e quindi non rappresenta una soluzione ottimale per colmare la lacuna della mancanza di una tutela specifica per i dati.

4. Non esistono dunque, allo stato attuale, strumenti giuridici appositi previsti dall'ordinamento interno o da quello europeo per lo sfruttamento economico dei dati, siano essi personali o prodotti da delle macchine. Anche qualora vi siano degli strumenti giuridici adatti la tutela offerta è incompleta, perché essi non sono stati ideati per far fronte a tale evenienza. Occorre esaminare ancora quali soluzioni possa offrire il diritto contrattuale. Infatti, nonostante allo stadio normativo attuale, come si vedrà meglio nel successivo capitolo, non sia possibile ricavare l'esistenza di un diritto di proprietà sui dati, secondo alcuni autori l'economia dei dati non soffre di questa mancanza, perché vengono introdotte delle esclusività in via contrattuale e inoltre i detentori dei dati sono in grado attraverso misure tecnologiche di protezione di assicurare un'adeguata tutela al dato[273].

I dati possono essere trasferiti in diversi modi, i due principali sono: i) la cessione del bene immateriale che li contiene (es. una banca dati); ii) il contratto di somministrazione[274]. Come si vedrà meglio nel prosieguo del testo tali modalità possono essere utilizzate, anche se con opportuni aggiustamenti, per il trasferimento di dati personali[275].

Nella prima ipotesi la cessione può riguardare tutte le facoltà di utilizzazione economica dell'opera oppure essere parziale e riguardare solo alcuni diritti di utilizzazione economica, in tal caso, secondo una recente dottrina, tra queste possibilità di utilizzo deve essere ricompresa la facoltà di utilizzazione computazionale[276], in quanto rientra in una facoltà di utilizzazione economica del bene cedibile ex art. 19 l. 633/1941

[272] In questo senso v. VANZETTI e DI CATALDO, op.cit., 403 ss..
[273] Cfr. ZECH, op. cit., 60 ss..; DREXL, op. cit., 29 ss.; OTTOLIA, *Big data e innovazione computazionale*, cit. 221 ss..
[274] Per un approfondimento su queste soluzioni negoziali e su altre soluzioni percorribili per il trasferimento, la condivisione e l'elaborazione di dati si v. OTTOLIA, *Big data e innovazione computazionale*, cit., 221 ss..
[275] V. OTTOLIA, *Big data e innovazione computazionale*, cit., 221 ss..
[276] Cfr. OTTOLIA, *Big data e innovazione computazionale*, cit., 222 e 223.

separatamente[277]. Secondo un autore tale soluzione negoziale non è percorribile per i dati personali, perché non sarebbe possibile immettere l'acquirente nella stessa posizione del dante causa[278]. Pur essendo condivisibile quest'orientamento, a parere di chi scrive, una banca dati contenente dati personali può senz'altro essere trasferita ad altri, anche se il dante causa non sarà nella stessa esatta posizione dell'avente causa, acquistando i dati personali in qualità di autonomo titolare, ed essendo immesso in tale posizione dal cedente o sia da quest'ultimo che direttamente dall'interessato che ha acconsentito a tale comunicazione di dati personali. Infatti, come già visto nel secondo paragrafo del presente capitolo, il codice privacy e anche il GDPR permettono la comunicazione di dati personali, purché questa avvenga nel rispetto di determinate condizioni[279]. Per poter trasferire una banca dati contenente dati personali a terzi che vogliono utilizzarla con finalità commerciali, è necessario informare gli interessati e chiedere loro il consenso[280]. Così potranno essere trasferiti solamente i dati personali di quegli interessati che hanno acconsentito a tale evenienza. Resta fermo che non si trasferisce un diritto stabile sui dati personali e che l'utilizzo dei dati personali da parte del nuovo acquirente deve avvenire nel rispetto del principio di conservazione, per cui sarà possibile utilizzare i dati personali solo per un periodo limitato, e resta ferma la possibilità per ogni interessato di ritirare il proprio consenso a tale trattamento. È possibile trasferire un diritto più stabile sui dati personali tramite la cessione del bene immateriale, se il nuovo acquirente tratta i dati personali acquisiti solo per fini statistici e nel rispetto delle condizioni previste dalla normativa per porre in essere un trattamento ulteriore e compatibile[281]. Resta ferma comunque la necessità che gli interessati al momento in cui forniscono i loro dati personali siano avvertiti nell'informativa privacy

---

[277] Nel sistema statunitense grazie all'istituto del fair use è possibile effettuare un utilizzo computazionale del bene senza necessità di chiedere il consenso al titolare dello stesso, purché l'uso sia trasformativo (sul punto cfr. OTTOLIA, *L'utilizzo computazionale dell'opera dell'ingegno*, in *AIDA* 2014, 388 ss.). Nell'ordinamento europeo un ruolo analogo potrebbe essere svolto dall'art. 10 della CEDU (v. HUGHENHOLTZ, *Copyright and freedom of expression in Europe*, in DREYFUSS - FIRST – ZIMMERMAN (a cura di), *Innovation Policy in an Information age*, Oxford, 2000, passim; contra OTTOLIA, *L'utilizzo computazionale dell'opera dell'ingegno*, cit., 401 ss.). Sull'interpretazione giurisprudenziale dell'art. 10 della CEDU v. CEDU, 24 febbraio 1994, Casado Coca c. Spagna; CEDU, 10 gennaio 2013, Donald et autres c. France.

[278] V. OTTOLIA, *Big data e innovazione computazionale*, cit. 223.

[279] V. supra par. 2.

[280] Il riferimento al consenso è esemplificativo, in alcuni casi non si esclude la possibilità nel rispetto di quanto precisato nel cap. 1 par. 2, di ricorrere al legittimo interesse del Titolare. Resta fermo che vi saranno notevoli complicazioni dettate dall'esercizio dei diritti degli interessati e occorre prevedere uno sfruttamento dei dati che permetta agli interessati in qualsiasi momento di esercitare i loro diritti.

[281] V. supra cap. 1.

di quest'evenienza. In quest'ultimo caso i dati personali acquisiti potranno essere utilizzati senza consenso dell'interessato, se trattati nel rispetto delle condizioni evidenziate nel primo capitolo ed essendo ravvisabile un interesse legittimo, gli interessati non potranno nemmeno esercitare il diritto alla portabilità dei dati[282]. Quanto qui riportato è valido e resta fermo nel caso in cui il trasferimento avvenga tra titolari del trattamento che operano all'interno dell'Unione Europea e i dati personali così trasferiti non transitino in paesi terzi. Nell'ipotesi di trasferimento extra Ue dei dati personali occorre porre attenzione ad adempimenti ulteriori posti dalla normativa che sono volti a proteggere l'interessato[283].

Uno dei principali difetti del primo metodo in analisi per la cessione di dati è costituito dagli elevati costi di transazione che derivano principalmente da due circostanze. Le

---

[282] Cfr. RICCI, op. cit, 219 ss.. V. supra cap. 1 par. 2

[283] Sul punto v. MENEGHETTI, op. cit., 423 ss.. I due principi alla base della circolazione dei dati personali sono: libera circolazione e circolazione controllata. Il primo opera all'interno ed è volto a consentire la libera circolazione dei dati personali, il secondo principio invece opera sui flussi di dati personali in uscita dall'Unione Europea (MENEGHETTI, op. cit., 432 ss..). In base a questo principio il Regolamento individua gli strumenti giuridici che possono permettere questo il trasferimento dei dati. Innanzitutto vi è la decisione di adeguatezza, in forza della quale la Commissione Europea, ai sensi dell'art. 45 del Regolamento europeo sulla protezione dei dati personali, autorizza il trasferimento extra UE verso un Paese terzo o una zona di tale paese o un organizzazione internazionale se ritiene che in tale luogo ci sia un livello di protezione adeguato. La valutazione della Commissione è condotta tenendo conto di diversi parametri elencati all'art. 45: i) il rispetto dei diritti e delle libertà fondamentali; ii) l'esistenza di autorità di controllo indipendenti preposte alla vigilanza sul rispetto della normativa posta a protezione dei dati personali; iii) gli impegni internazionali assunti dal Paese terzo o dall'organizzazione. La valutazione della Commissione, soprattutto per quanto riguarda il primo parametro sopra riportato, non si attesta ad un livello formale ma è sostanziale: si verifica se le tutele dei diritti e libertà fondamentali siano effettive ed azionabili dagli interessati specie per quanto riguarda la protezione dei dati personali. Qualora non fosse possibile seguire questa soluzione vi sono altre strade percorribili: i trasferimenti soggetti a garanzie adeguate(per un approfondimento MENEGHETTI, op. cit.,442 ss.). Per quanto riguarda il trasferimento soggetto a garanzie adeguate l'art. 46 del regolamento individua diversi criteri che se implementati possono sopperire alla mancanza di una decisione di adeguatezza. Così ad esempio le norme vincolanti d'impresa, l'utilizzo delle clausole standard adottate dalla Commissione, i meccanismi di certificazione, l'adesione ad un codice di condotta. Allo stato attuale sono maggiormente utilizzate le clausole standard e per i trasferimenti infra gruppo le norme vincolanti di impresa. Le prime sono dei veri e propri testi contrattuali adottate dalla Commissione Europea direttamente oppure adottate da un Autorità di controllo di uno dei Paesi membri e in seguito approvate dalla Commissione. Tali clausole impongono in capo all'esportatore e all'importatore una serie di obblighi inerenti principalmente l'adozione di misure di sicurezza idonee e il rispetto dei principi posti a protezione dei dati personali previsti dalla normativa europea. Le norme vincolanti di impresa che rappresentano una novità introdotta nel regolamento, sono norme che autodisciplinano il trasferimento dei dati personali tra imprese appartenenti allo stesso gruppo (per un approfondimento sulle norme vincolanti di imprese v. WP29, 19 aprile 2013, *Documento esplicativo sulle norme vincolanti d'impresa per gli incaricati del trattamento* e l'art. 47 del GDPR). L'art. 48 del GDPR permette poi il trasferimento che si basi su una decisione, giudiziaria o di un'autorità di controllo non appartenente all'UE, i cui effetti sono riconosciuti tramite apposite convenzioni all'interno dell'Unione Europea. Al di fuori di tutte queste ipotesi in via residuale l'art. 49 del regolamento europeo individua delle deroghe specifiche che permettono di procedere al trasferimento dei dati: consenso a seguito di un'informativa che illustri i rischi di tale trasferimento; esecuzione di un contratto o di misure precontrattuali; importanti motivi di interesse pubblico; esercizio di un diritto in sede giudiziaria; tutela interessi vitali interessato o di altre persone; trasferimento effettuato sulla base di un registro in conformità all'ordinamento europeo(per un approfondimento MENEGHETTI, op. cit., 478).

imprese che compiono studi e analisi sui dati hanno bisogno di accedere ad enormi quantità di dati provenienti da fonti eterogenee. Inoltre tali imprese per accedere a tali dati devono acquistare gli appositi diritti e molto spesso all'interno dei loro giacimenti vi sono diversi diritti sui singoli set di dati e ciò comporta inevitabilmente anche dei costi di gestione[284]. Per risolvere questo problema un autore ritiene che sia possibile ricorrere a strutture negoziali ad hoc: i data pool, che potranno essere configurati secondo le esigenze delle parti[285].

Il secondo modo più diffuso e più adeguato alla cessione dei dati è il contratto di somministrazione[286]. Ai sensi dell'articolo 1559 del codice civile il contratto di somministrazione è un contratto di durata che vincola una parte, in cambio di un corrispettivo, ad erogare un bene in modo continuativo o periodico ad un'altra parte per soddisfare il bisogno di quest'ultima. Tale contratto può essere utilizzato anche per quanto riguarda i dati personali, ferme le peculiarità e i limiti analizzati per la prima ipotesi di cessione, consistente nel trasferimento di un bene contenente dati personali.

Il contratto di somministrazione permette di far fronte al bisogno duraturo di dati di cui spesso necessitano diverse imprese per lo svolgimento della loro attività economica[287]. Inoltre, per certi aspetti meglio si ritaglia alla realtà dinamica dei dati, permettendo all'avente causa di ricevere elementi aggiornati non appena questi vengano ricavati da un determinato fenomeno[288]. Uno dei principali limiti derivanti dall'utilizzo del contratto di somministrazione è dettato dall'art. 1569 del codice civile, essendo un contratto di durata è possibile non stabilire un termine. Cosicché ciascuna delle parti può recedere dal contratto dando un congruo preavviso (stabilito nel contratto, imposto dagli usi, o che tenga conto della natura della somministrazione). Come si vedrà meglio nel prossimo capitolo, ciò aumenta notevolmente il potere economico delle grandi imprese che detengono i maggiori set di dati (si pensi ad es. a Google o a Facebook). Se tali imprese decidessero di "chiudere" nei confronti di alcune imprese il flusso di dati,

---

[284] V. OTTOLIA, *L'utilizzo computazionale dell'opera dell'ingegno in internet*, cit., 397 ss.; OTTOLIA, *Big data e innovazione computazionale*, cit., 269 e 270;

[285] In questo senso e sul punto v. OTTOLIA, *Big data e innovazione computazionale*, cit., 272 ss..

[286] Sul punto v. OTTOLIA, *Big data e innovazione computazionale*, cit., 237 ss.. L'autore distingue tra somministrazione di consumo e somministrazione d'uso. La prima determina atti traslativi, la seconda solo l'utilizzo degli stessi per determinati fini, quali studio e uso computazionale. Per la prima ipotesi di somministrazione l'integrazione della disciplina è offerta dalle norme codicistiche sulla compravendita, per la seconda ipotesi invece occorre fare riferimento alle norme sulla locazione.

[287] Per un approfondimento sul contratto di somministrazione v. CAGNASSO, *v. Somministrazione*, in *Digesto disc. priv.*, XIV, Torino, 1997, 467 ss..

[288] Sull'utilità dei rapporti di durata nell'economia di scambio dei dati v. OTTOLIA, *Big data e innovazione computazionale*, cit., 236 ss..

queste trovandosi in una situazione di dipendenza economica potrebbero subire un notevole danno. Per questo motivo la disciplina della somministrazione, in alcuni casi, dovrà essere integrata con i correttivi posti dalla disciplina antitrust in materia di abuso di posizione dominante ed essential facility[289].

Resta da precisare che, sia si tratti di cessione di bene immateriale tutelato dalla legge 633 del 1941, sia che si tratti di somministrazione di dati avvalendosi come supporto di un bene immateriale sempre protetto dalla medesima legge, entra in gioco la teoria dello scopo, immanente al campo dei diritti d'autore e connessi[290]. Alla luce di tale principio l'utilizzo computazionale dell'opera deve essere espressamente attribuito dal dante causa all'avente causa, altrimenti l'acquirente commette un'utilizzazione illecita[291]. Per questi motivi il trasferimento del bene deve avere ad oggetto espressamente tale diritto e per concedere tale diritto e questo inevitabilmente costituisce un freno alla circolazione dei dati. Tuttavia occorre precisare che illiceità dell'utilizzo del bene non determina l'inutilizzabilità dei risultati conseguiti, a meno che gli stessi non contengano elementi tutelati dell'opera originaria, ipotesi rara poiché il risultato conseguito dall'analisi dei dati è costituito da correlazioni o inferenze statistiche[292].

In aggiunta alle misure negoziali a disposizione delle imprese si consideri che un ulteriore protezione sui dati è costituita dalle norme del diritto penale che puniscono l'accesso non autorizzato a dati o computer per motivi di spionaggio, cosicché vi può di fatto essere una tutela del dato adeguata anche in assenza dell'introduzione di un diritto di proprietà.

Alla luce di questa breve analisi sembrerebbe che i titolari dei dati siano già in grado, pur con ancora alcuni limiti, tramite un controllo fattuale di regolare parzialmente la circolazione dei dati all'interno del mercato. Tuttavia in molti casi vi sono ancora pochi

---

[289] Sul punto v. infra capitolo 3.

[290] Per un approfondimento sulla teoria dello scopo (c.d. *Zweckubertragungslehre)* cfr. AUTERI, *Contratti traslativi del diritto di autore e principio di indipendenza delle facoltà di utilizzazione*, in *Riv. dir. ind.* 1963, II, 105 ss.; RICOLFI, *Il diritto d'autore*, in Trattato Cottino, vol. II, *Diritto industriale*, CEDAM, Padova, 2001, 394; COGO, *I contratti di diritto d'autore nell'era digitale*, Giappichelli, Torino, 2010, 184 ss..

[291] Sul punto cfr. anche OTTOLIA, *Big data e innovazione computazionale*, cit., 239.

[292] In questo senso v. OTTOLIA, *Big data e innovazione computazionale*, cit., 255 ss.. L'autore ritiene immanente all'ordinamento il principio per cui i risultati innovativi ottenuti dall'utilizzo di un bene immateriale preesistente, non determinano alcun veto sullo sfruttamento economico di tali risultati. Una chiara dimostrazione di questo principio è costituita dallo statuto dell'elaborazioni creative, laddove l'illiceità di utilizzo dell'opera derivata realizzata senza il consenso del titolare dei diritti sull'originale vi è in quanto lo sfruttamento economico della prima comporta l'uso di parti della seconda (sul punto cfr. BERTANI, *Diritto d'autore e connessi*, cit., 295).

incentivi a far circolare gli stessi all'interno del mercato. Come evidenziato dalla Commissione nella comunicazione del 10 gennaio 2017 vi è la tendenza, da parte delle società che detengono il controllo di enormi quantità di dati, di studiare e analizzare al proprio interno tali set di dati. Inoltre molto spesso le imprese che in virtù della loro attività, producono dati mediante la realizzazione di prodotti o l'effettuazione di servizi hanno la tendenza a non condividerli, limitando inevitabilmente un possibile utilizzo degli stessi in altri settori a valle. Infine, la Commissione Europea rileva che vi è anche un forte problema di condivisione dei dati determinato da barriere tecnologiche non ancora superate da tutte le imprese: «…Molte imprese non dispongono di interfacce di programmazione delle applicazioni (API) facili da usare o non le annoverano fra le opzioni possibili (sono interfacce che specificano come le diverse applicazioni debbano interagire le une con le altre), nonostante possano servire da punti di accesso sicuro per usi nuovi e innovativi dei dati detenuti dalle imprese.» [293] A parere della Commissione tutto questo insieme di fattori fa si che la circolazione dei dati risulti essere fortemente limitata.

Secondo la Commissione il ricorso al diritto contrattuale vigente e agli strumenti del diritto della concorrenza messi a disposizione dall'ordinamento europeo potrebbe essere una risposta adeguata per far fronte anche a quelle situazioni di diseguaglianza presenti nel mercato dei dati. Per questo motivo nel prossimo capitolo si esaminerà quali soluzioni vi possono essere per superare queste disparità tra imprese, guardando ai profili della concorrenza per poter comprendere a pieno se sia configurabile o auspicabile un diritto di proprietà sui dati; oppure se sia preferibile un diritto d'accesso e quali correttivi possono essere adottati per evitare abusi da parte di quelle imprese che ricoprono sul mercato una posizione dominante.

[293] Commissione Europea, Comunicazione del 10 gennaio 2017, cit.,10.

CAPITOLO TERZO

Diritto di proprietà o diritto d'accesso ai dati

Sommario 1. La configurabilità di un diritto di proprietà sui dati – 2. Abuso di posizione dominante – 3. (segue) Alcuni esempi di abuso di posizione dominante nell'utilizzo dei dati e correttivi per migliorare l'attuale assetto concorrenziale

1. Alla luce del fatto che l'economia dei dati si caratterizza per l'inevitabile necessità di comunicazione e interscambio di dati tra imprese. L'introduzione di un nuovo diritto di proprietà non è ben accetto dal mondo delle imprese[294]. L'avversità delle imprese verso questa introduzione è determinata principalmente da due ragioni. In primo luogo molte aziende producono dati e allo stesso tempo hanno accesso ai dati di altre imprese, non è chiaro se l'introduzione di un nuovo diritto possa portare maggiori benefici rispetto agli svantaggi. In secondo luogo non è chiaro il criterio in base al quale individuare chi possa essere qualificato il titolare del nuovo diritto di proprietà. Infatti ad uno stesso set di dati frequentemente contribuiscono diverse imprese che possono avere interessi distanti su quei dati. Per questo l'allocazione dei dati in una logica proprietaria è una questione molto importante. Se ciascuno dei soggetti che utilizza un determinato set è considerato proprietario si viene a creare una co-titolarità sugli stessi dati che comporterebbe notevoli effetti negativi sull'accesso agli stessi e sulla loro circolazione[295]. Inoltre si consideri che l'analisi big data consiste nella lettura di grandi set di dati per scoprire un nuovo significato, nel senso dell'informazione semantica. L'informazione è ricavata ponendo in rapporto tra di loro i diversi tipi di dati, il risultato di tale tipo di analisi quindi è nascosto all'interno del data set e viene alla luce tramite le diverse correlazioni possibili che non sono predeterminabili ex ante. Quindi diventa problematico riconoscere un diritto in capo a chi controlla l'accesso al data set su tutte le informazioni semantiche ricavabili da esso. È il contributo dell'analista dei dati che porta alla scoperta di tali informazioni e, di conseguenza, l'eventuale diritto su questa informazione semantica dovrebbe essere affidato all'analista dei dati, e non al titolare di

[294] Cfr. DREXL, op. cit, passim. L'autore riporta un sentimento diffuso in Germania che, a parere di chi scrive, è da ritenere condiviso all'interno di tutta l'Unione Europea.
[295] Cfr. MORO VISCONTI, *Internet delle cose, Networks e plus valore della connettività*, cit., 536 ss..; Drexl, ibidem.

set di dati che vengono analizzati[296]. Occorre chiedersi se vi è la possibilità di rifarsi alla normativa della proprietà intellettuale in materia di appartenenza dei risultati creativi dei dipendenti. Infatti qualora l'analista lavori su un set di dati in qualità di dipendente del titolare del diritto sui dati, questo problema non si porrebbe. In altri termini se si configurasse il diritto non come un diritto di proprietà nel senso civilistico del termine, ma come un diritto di proprietà intellettuale quest'ultimo aspetto problematico potrebbe essere risolto applicando il principio immanente al sistema della proprietà intellettuale che riconosce in capo al datore di lavoro, ovvero colui che dispone l'investimento e che mette a disposizione le proprie risorse economiche, la titolarità dei diritti del risultato del dipendente[297].

Poste queste premesse che evidenziano una difficoltà di individuazione dei profili soggettivi di un eventuale diritto di proprietà sui dati, occorre interrogarsi sui profili oggettivi, partendo dalla ricostruzione della nozione civilistica di proprietà. La nozione civilistica di proprietà si caratterizza per due componenti fondamentali: il potere di godimento sul bene e il diritto di disporre tale bene[298]. Tali elementi si declinano a loro volta in diverse caratteristiche: l'autonomia; l'assorbimento automatico degli effetti esterni; l'immunità e la responsabilità; la perpetuità; l'elasticità, il diritto al possesso ecc[299]… Di seguito si analizzeranno alcuni di questi caratteri per dimostrare come tali caratteristiche non possano ravvisarsi quando il potere di godimento e il diritto di disporre è esercitato su un dato o su un set di dati. Per quanto concerne l'autonomia, intesa come il potere di controllo sull'accesso al bene oggetto del diritto di proprietà[300], risulta difficile riscontrarla in alcune ipotesi riguardanti i dati. Così qualora si tratti di dati personali l'autonomia è fortemente limitata dal fatto che l'interessato in alcuni casi può opporsi al trattamento, revocare l'eventuale consenso, impedire che questi dati

---

[296] Cfr. MORO VISCONTI, ibidem*;* Drexl, ibidem.

[297] Per un approfondimento sul punto cfr. OPPO, *Creazione intellettuale, creazione industriale e diritti di utilizzazione economica*, in *Riv. dir. civ.*, 1969, 1 ss.; L.C. UBERTAZZI, *Profili soggettivi del brevetto*, Giuffrè, Milano, 1985, passim; BETTINI, *L'attività inventiva nel rapporto di lavoro*, Giuffrè, Roma, 1993, passim; CAROSONE, *L'opera dell'ingegno creata nel rapporto di lavoro autonomo e subordinato*, 2 ed., Giuffrè, Milano, 1999, passim; L.C. UBERTAZZI, *L'appartenenza dei risultati creativi dei dipendenti*, in *AIDA* 2010, 516 ss.. Per la giurisprudenza ex multis: Cass., 1 luglio 2004 n. 12089, in *AIDA* 2005, *1019*; Trib. Firenze, 18 settembre 2006, in *AIDA* 2008, *1210*.

[298] GAMBARO, *La proprietà, Beni, proprietà e possesso*, in *Trattato di diritto Privato*, IUDICA e ZATTI (a cura di), Giuffrè, Milano, 2017, 218. Si veda anche MATTEI, *I diritti reali*, 2, *La proprietà*, in *Trattato di diritto civile*, SACCO (a cura di), 2 ed., Utet, Torino, 2015, passim.

[299] Per un approfondimento sul punto cfr. GAMBARO, op. cit. 218 ss..

[300] Sul punto sempre GAMBARO, op. cit., 219 ss..

vengano trasferiti, e limitare in modo notevole l'autonomia del titolare[301]. Non solo l'autonomia non è riscontrabile in quest'ipotesi ma alla luce del principio di conservazione sancito dall'art. 5 lett. e) del regolamento europeo in materia di protezione di dati personali non è ravvisabile neanche il requisito della perpetuità. I dati personali possono essere conservati solo per un tempo limitato. Inoltre si consideri che un diritto di proprietà non è configurabile neppure in capo all'interessato che in diverse circostanze non ha un controllo pieno dei suoi dati personali.

Alla luce di queste prime considerazioni è sicuramente esclusa la possibilità di configurare un diritto di proprietà sui dati personali. In altri casi quando l'accesso ai dati non personali è pubblico, nel senso che chiunque può ricavare quei dati o quel determinato set di dati diventa evidente che risulti priva di effettività, la pretesa del titolare di esercitare la propria autonomia su quelle informazioni. In molti casi il titolare non è nella posizione di respingere tutte le ingerenze indesiderate da parte di terzi. Solo da questo primo argomento risulterebbe compromessa la possibilità di riconoscere in via generale un diritto di proprietà sul dato o su set di dati, potendosi eventualmente riconoscere solo in alcune ipotesi specifiche. Resta quindi da verificare se in alcuni casi dati privi di elementi di identificazione possono essere oggetto di un diritto di proprietà nel senso civilistico del termine.

Un ulteriore elemento che normalmente caratterizza il diritto di proprietà su un bene tangibile è il possesso[302]. La nozione civilista di possesso contenuta nell'art. 1140 del codice civile presuppone l'esercizio di un potere sul bene che può tradursi nel suo utilizzo come nella sua distruzione. Nel mondo dei dati questo elemento può essere tradotto come accesso al dato, ossia come possibilità per il titolare di accedere in qualsiasi momento al dato[303]. Tuttavia, rispetto ai beni tangibili c'è la differenza dovuta al fatto che il possesso nella configurazione civilistica implica una piena situazione di controllo, ciò non sempre può avvenire nei confronti dei dati, perché l'accesso ad un'informazione non sempre è esclusivo[304]. Questa constatazione inevitabilmente si riflette negativamente sulla possibilità di configurare il diritto di proprietà sui dati.

---

[301] V. supra cap. 1 e 2

[302] Cfr. GALGANO, *v. Possesso*, *Diritto civile*, in *Enc. Giur. Trecc.*, Roma, 1990, XXIV, passim; SACCO e CATERINA, *Il possesso*, in *Trattato Cicu-Messineo*, Milano, III ed., 2014, ZACH, op. cit., 56; GAMBARO, op. cit., 238 ss..

[303] Cfr. ZACH, op. cit., 56.

[304] Cfr. ZACH, ibidem. E per questo modo di interpretare la nozione di possesso cfr. anche ASCARELLI, *Teorie della concorrenza e dei beni immateriali*, Giuffrè, Milano, 1960, 264.

Posto che non è configurabile un diritto di proprietà nel senso civilistico del termine sui dati, è doveroso interrogarsi sulla possibilità di introdurre un diritto di proprietà intellettuale sui dati[305].

In una prospettiva de iure condendo la possibilità di introduzione di un diritto di proprietà intellettuale deve essere vagliata partendo dalla constatazione che un nuovo diritto immette nel sistema una nuova forma di regolazione del mercato e questa vi può essere solo se sorretta da una giustificazione economica[306]. Per poter comprendere l'eventuale giustificazione economica alla base dell'introduzione di questo nuovo diritto è necessario analizzare e comprendere le peculiarità dell'economia dei dati. L'obiettivo di una regolazione, che garantisca il diritto di proprietà e la concorrenza, dovrebbe essere, come in altri campi della proprietà intellettuale, quello di incentivare l'innovazione. Dovrà tenersi in considerazione la dimensione concorrenziale nel disegnare le regole del nuovo diritto di proprietà, così d'evitare di ricorrere al regime concorrenziale per compensare la mancanza di incentivi. Quindi le future legislazioni che si occuperanno di regolare il regime della proprietà sui dati dovranno tenere inevitabilmente in considerazione anche il mantenimento dell'accesso ai dati nell'interesse della società[307]. Per poter capire se l'introduzione di un diritto di proprietà sui dati sia funzionale da un punto di vista concorrenziale occorre capire il valore economico dei dati, tenendo presente che tale valore è generato diversamente rispetto all'economia tradizionale. Nell'economia tradizionale, il paradigma ancora dominante si riferisce a catene del valore verticali. Vi sono i cd. Fabbricanti di input per la produzione di beni nei mercati a monte che poi li vendono attraverso le catene di distribuzione, spesso anche grossisti e distributori, al consumatore. Ad ogni livello della catena di produzione e di distribuzione, viene aggiunto un valore economico. Mentre nel caso dell'economia dei dati non vi è nessuna catena tutto avviene nel contesto dinamico della rete. Per cui i dati vengono utilizzati dalle imprese per ottimizzare le loro decisioni. Inoltre l'automazione totale, oltre a cambiare l'uso del prodotto, velocizza la

---

[305] Inevitabilmente alla luce delle considerazioni svolte in precedenza, qui cambia la prospettiva dell'analisi da de iure condito a de iure condendo. A parere di chi scrive è preferibile l'orientamento che sposa la tesi del numerus clausus dei diritti esclusivi. In questo senso v. GHIDINI, *Profili evolutivi del diritto industriale*, Milano, 2008, passim; contra L.C. UBERTAZZI, *Numerus clausus dei diritti esclusivi di proprietà intellettuale?*, in *JURISMAT*, Portimào, n. 4, 2014, 187 ss.. Per un approfondimento sul punto v. L.C. UBERTAZZI, *Introduzione*, in *La proprietà intellettuale*, (a cura di) L. C. UBERTAZZI, Giappichelli, Torino, 2011, 13 ss..

[306] Cfr. ASCARELLI, op. cit., passim; DREXL, op. cit., 15 ss.. Sul rapporto tra proprietà intellettuale e concorrenza v. anche GHIDINI, op. cit., 13 ss..

[307] In questo senso v. DREXL, op. cit., 17 ss..

produzione e diminuisce significativamente il rischio di difetti di fabbricazione. La connettività permette di regolare la produzione in base ai bisogni dei clienti. Questo insieme di fattori aumenta in maniera esponenziale l'importanza degli intermediari che acquisiscono un vantaggio notevole nei differenti mercati e settori in cui i prodotti smart vengono realizzati. Per questo i colossi del web come Google puntano ad espandersi continuamente anche nei diversi settori industriali, acquisendo così un elevato potere di mercato[308]. Quindi riconoscere un diritto di proprietà su questi dati può determinare l'effetto indesiderato di rafforzare il potere di mercato di queste imprese, mentre dal punto di vista della concorrenza sarebbe più saggio incentivare l'accesso ai dati così da permettere anche ad altri operatori del mercato di entrare ed operare in tali settori[309]. L'attribuzione di un diritto di proprietà ad un solo soggetto bloccherebbe le condivisioni interrompendo la rete di valore che fino a questo momento ha caratterizzato i big data. Si consideri infatti, che grandi quantità di dati sono a disposizione di un numero limitato di soggetti che controllano i relativi flussi informativi, (es. la Pubblica Amministrazione, gli intermediari dei servizi di informazione, le società che offrono servizi di consulenza in ambito creditizio ecc..) riconoscere a questi enti una posizione giuridica assoluta rafforzerebbe eccessivamente la loro posizione precludendo ai soggetti più deboli presenti sul mercato la possibilità di accedere[310].

Alla luce di queste premesse sembrerebbe anticoncorrenziale l'introduzione di un diritto di proprietà intellettuale a ciò si aggiunga un ulteriore complessità da un punto di vista giuridico: per introdurre nel sistema un nuovo diritto di proprietà intellettuale occorre individuare e tenere in considerazione una serie di elementi caratterizzanti il mondo dell'intellectual property. Occorrerebbe porre attenzione e definire tutti gli elementi caratterizzanti un diritto esclusivo di proprietà intellettuale, tra cui: i) l'oggetto della protezione; ii) la fattispecie costitutiva; iii) il titolare del diritto; iv) lo scopo della protezione; v) le eccezioni e limitazioni; vi) le sanzioni derivanti dalla violazione del

---

[308] Per un approfondimento in tal senso v. Commissione UE, Comunicazione del 27 giugno 2017. Con tale provvedimento, come si vedrà meglio infra, la Commissione Europea condanna Google al pagamento di una pesante sanzione di 2,42 miliardi di euro, per l'abuso di posizione dominante perpetrato nel fornire il servizio di motore di ricerca abbinato a quello di piattaforma online per lo shopping. Questo caso è esemplificativo dell'enorme potere assunto dagli intermediari che operano su internet.

[309] V. DREXL, op. cit., 17 ss..

[310] Cfr. MANTELERO, *Big Data: I rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, cit., 135 e 136; MAGGIOLINO, op. cit., 174.

diritto; vii) la durata della tutela e la fattispecie estintiva[311]. Per quanto concerne il primo punto, ossia l'oggetto della protezione, è necessario effettuare due decisioni. La prima riguarda il livello qualitativo dell'oggetto della protezione, in altri termini si vuole tutelare il dato al suo livello sintattico o al suo livello semantico[312]. La tutela del dato al suo livello semantico pur essendo quella più utile potrebbe creare conflitti con la libera circolazione delle informazioni e vi sarebbero delle difficoltà notevoli a comprendere quando un'informazione possa dirsi nuova. E invece la tutela del dato a livello sintattico rischia di essere priva di specificità alcuna, perché mancherebbero elementi chiari per identificare e distinguere due dati diversi tra loro. In altri termini sarebbe opportuno andare oltre la specifica di bit o bites[313]. Se si riuscisse ad effettuare una scelta opportuna su questi problemi resterebbe da risolvere il secondo aspetto rilevante in tema di oggetto di protezione: si intende tutelare il singolo dato oppure un set di dati. Se ogni singolo dato fosse protetto vi sarebbe un problema di effettività e di enforcement per garantire la tutela, per non parlare del problema relativo alla gestione dei diritti. Da sole queste prime riflessioni indurrebbero a ritenere impossibile l'introduzione di un nuovo diritto di proprietà intellettuale. Inoltre si consideri che il dato non cessa di aver valore al suo riutilizzo ma mantiene inalterato tutto il suo potenziale, potendosi definire un bene a consumo non competitivo e non esclusivo, acquisendo maggior valore se tenuto insieme ad altri dati e se riutilizzato molto spesso si arricchisce di ulteriori elementi crescendo di valore[314]. Occorre quindi individuare un'altra valida alternativa che potrebbe essere costituita dall'individuazione di un regime d'accesso e la proposizione, in una prospettiva de iure condendo, di eventuali migliorie che tengano conto della catena di valore dei dati. Per poter individuare l'esistenza di un regime d'accesso è opportuno partire dall'analisi della normativa antitrust, per comprendere a che limiti è sottoposto un controllo fattuale o giuridico delle informazioni e se all'attuale stato delle cose è già individuabile una qualche forma di accesso riconosciuta e tutelata dall'ordinamento.

---

[311] V. ZECH, op. cit., 51 ss.; L.C. UBERTAZZI, *Numerus clausus dei diritti esclusivi di proprietà intellettuale?*, cit., 187 ss.; L.C. UBERTAZZI, *Introduzione*, cit., 13 ss..
[312] Sul punto si rimanda supra al par. 1 del cap. 1.
[313] V. Zech, op. cit., 51 ss..
[314] In questo senso cfr. GRAZZINI, *L'economia della conoscenza oltre il capitalismo. Crisi dei ceti medi e rivoluzione lunga*, Torino, Codice, 2008; OREFICE, *I big data, Regole e Concorrenza*, in *Politica del diritto* 2016, fasc. 4, 703 e 704.

2. Come si cercherà di dimostrare in questo e nei prossimi paragrafi l'introduzione o la verifica sulla sussistenza di un regime d'accesso può essere giustificata dalla constatazione dell'esistenza di una posizione dominante e dall'evidenza che l'assenza di un tale regime potrebbe comportare abusi da parte dei detentori di tale quota di mercato. Occorre quindi approfondire la nozione di posizione dominante e la nozione di abuso di posizione dominante. In via estremamente sintetica l'abuso può avvenire in presenza di due condizioni cumulative: innanzitutto l'autore deve essere in una posizione dominante nel mercato della propria opera o in quelli derivati che riguardano le elaborazioni; in secondo luogo il soggetto deve abusare di questa sua posizione.

La nozione di posizione dominante non è definita né dal legislatore comunitario né da quello italiano. La Corte di giustizia della CE in una nota sentenza la definisce come «una situazione di potenza economica» attraverso la quale l'impresa che ne è titolare può ostacolare la concorrenza e può agire in maniera indipendente nei confronti dei suoi concorrenti e dei consumatori[315]. In concreto la posizione di dominanza è svelata da una serie di indizi rilevatori, elaborati dalla prassi e dalla giurisprudenza comunitaria[316]. Il principale fattore valutato per verificare la sussistenza di questa situazione è la quota di mercato detenuta dall'impresa che è calcolata tenendo conto di diversi elementi quali: i fatturati, le quantità vendute oppure la capacità di offerta. In generale in presenza di una quota di mercato superiore al 70 % si ritiene sempre esistente una posizione dominante, mentre se la quota è compresa tra il 50% ed il 70% si presume, salva prova contraria, la sussistenza di tale situazione. Una quota compresa tra il 30% ed il 50% costituisce un forte indizio di posizione dominante ed infine una fetta di mercato inferiore al 30% crea la presunzione dell'inesistenza di tale situazione. Quindi, salvo che la quota superi il 70 %, il possesso di un'elevata parte di mercato spesso non è sufficiente al fine di affermare la sussistenza della posizione dominante, devono essere valutati anche un'altra serie di fattori, come ad esempio: la distanza rispetto al titolare della seconda quota di mercato, il livello di polverizzazione delle altre quote che per essere un utile indizio deve raggiungere un grado elevato[317]. Inoltre è necessario che il possesso della

[315] V. CGCE 14 febbraio 1978, C-27/76, United Brands, in *www.curia.eu*.
[316] V. CGCE 13 febbraio 1979, C-85/76, Hoffmann-La Roche, in *www.curia.eu.*
[317] V. CGCE 14 febbraio 1978, C-27/76, United Brands, cit.: in questa sentenza la Corte, al fine di verificare la sussistenza di una posizione dominante, dichiara la necessità di valutare la quota di mercato posseduta dall'United Brands Company in rapporto alla forza ed al numero delle altre imprese concorrenti sul mercato.

quota di mercato sia stabile nel tempo, normalmente la stabilità si valuta in un arco temporale di cinque anni, nel caso in cui la quota di mercato posseduta dall'impresa superi il 50% è sufficiente per ritenere sussistente la posizione di dominanza il possesso duraturo di tale parte di mercato per almeno tre anni[318].

La Corte di Giustizia dell'Unione Europea ha evidenziato che la posizione di dominanza permette di ostacolare la concorrenza delle altre imprese presenti sul mercato, quindi per valutare la sussistenza di tale situazione di potenza economica devono essere presi in considerazione anche tutti quei fattori che offrono all'impresa notevoli vantaggi concorrenziali, come ad esempio: la titolarità di diritti di proprietà intellettuale che le permettono un significativo vantaggio sul piano tecnologico; oppure la reputazione derivante dalla notorietà del marchio presso i consumatori; oppure elevata capacità finanziaria e commerciale dell'impresa ecc....

La posizione dominante può far capo collettivamente a diverse imprese indipendenti che, in ragione di vincoli particolarmente stringenti[319], si presentano su un mercato specifico come un'entità collettiva con una linea d'azione comune che le rende in grado di agire autonomamente rispetto ai comportamenti tenuti dai concorrenti, dai clienti e dai consumatori. La presenza di una posizione dominante collettiva all'interno di un mercato è dimostrata dalla presenza di tre condizioni[320]: l'esistenza di un mercato trasparente che permetta alle diverse imprese di verificare il rispetto della linea d'azione comune[321]; l'esistenza di meccanismi tempestivi di rappresaglia finalizzati ad opporsi all'impresa che si allontana dalla linea d'azione comune provocandogli un pregiudizio economico maggiore rispetto ai benefici derivanti dal comportamento contrario al piano comune[322]; infine è richiesta l'incapacità degli attori esterni all'oligopolio di opporsi all'equilibrio raggiunto dalle imprese interne ad esso.

---

[318] CGCE 14 febbraio 1978, C-27/76, United Brands, cit.; CGCE, 13 febbraio 1979, C-85/76, Hoffmann-La Roche, cit..

[319] V. TODINO, *sub. art. 102 TFUE*, in L.C. UBERTAZZI, *Commentario breve alle leggi sulla proprietà intellettuale e concorrenza*, 5 ed., CEDAM, Padova, 2012: «I vincoli possono derivare da legami contrattuali e/o strutturali che pongono le imprese coinvolte nelle condizioni di comportarsi, commercialmente, come un entità coesa capace di attuare i medesimi comportamenti…».

[320] Queste tre condizioni sono state elaborate dal Trib. di primo grado CE 6 giugno 2002, T-342/99, Airtours, in *www.curia.ue*.

[321] Il Tribunale, nel porre la prima condizione, afferma la necessità di una trasparenza di mercato tale da consentire a ciascun membro dell'oligopolio dominante di conoscere in modo preciso ed immediato il cambiamento del comportamento sul mercato di ciascuno degli altri membri.

[322] Il Tribunale ritiene necessario «che ciascun membro dell'oligopolio dominante sappia che un'azione fortemente concorrenziale da parte sua diretta ad accrescere la sua quota di mercato provocherebbe un'azione identica da parte degli altri, di modo che egli non trarrebbe alcun vantaggio dalla sua iniziativa.»

Il legislatore comunitario, come quello nazionale, non mira a reprimere posizioni monopolistiche od oligopolistiche presenti sul mercato, si preoccupa soltanto di evitare che le imprese in posizione dominante pongano in essere comportamenti che siano pericolosi per i concorrenti e per i consumatori. La norma di riferimento in ambito comunitario è l'art. 102 TFUE, mentre nell'ordinamento interno si applica in via residuale una disposizione sostanzialmente identica: l'art. 3 della L 287/1990. Entrambe le norme presentano una clausola generale accompagnata da quattro ipotesi tipiche di condotta. La clausola generale vieta a tutte le imprese in posizione dominante di abusare di questa loro situazione di vantaggio. Detta clausola spesso è stata utilizzata dalla giurisprudenza comunitaria per reprimere comportamenti abusivi atipici. La prima condotta presa in considerazione dalle norme vieta l'imposizione di prezzi o di altre condizioni contrattuali non eque[323] o ingiustificatamente gravose[324]. Quindi sono vietati sia i prezzi troppo elevati che i prezzi troppo bassi. I prezzi troppo elevati possono essere finalizzati ad approfittare di una situazione di monopolio sul mercato; oppure sono volti a trasferire la posizione di dominanza di un'impresa anche in mercati a valle rispetto a quello in cui essa opera. I prezzi eccessivamente ribassati hanno il principale scopo di eliminare la concorrenza dal mercato. In questo caso l'impresa in posizione dominante tiene prezzi non remunerativi in modo da indurre gli altri concorrenti presenti sul mercato ad abbandonarlo. Una volta acquisito il monopolio l'impresa potrà alzare i prezzi provocando così un danno non solo ai concorrenti ma anche ai consumatori. La seconda condotta vietata riguarda la creazione di barriere all'ingresso di un determinato mercato in modo da ostacolare la concorrenza. In quest'ipotesi rientra il rifiuto assoluto di contrattare con le altre imprese concorrenti in modo da impedire loro la possibilità di usufruire ad esempio di una determinata materia prima o di un determinato prodotto funzionale ad attività economiche su mercati secondari. Il rifiuto è illecito solo se non è sorretto da una causa di giustificazione oggettiva. Alla lettera c) di entrambe le norme sono vietati i comportamenti discriminatori che determinino svantaggi nella concorrenza, le disposizioni vietano l'applicazione, ai contraenti in posizione concorrenziale rispetto all'impresa dominante, di condizioni oggettivamente più gravose rispetto a quelle applicate agli operatori ritenuti non concorrenti. La quarta fattispecie tipica riguarda l'ipotesi in cui l'impresa in posizione dominante subordina la

[323] V. art. 102 TFUE.
[324] V. art. 3 l. 287/1990.

conclusione del contratto principale all'accettazione da parte degli altri contraenti di prestazioni supplementari non connesse con l'oggetto del contratto principale. In questo modo l'impresa mira ad ottenere una posizione dominante anche sui mercati dei prodotti contenuti nelle prestazioni supplementari. L'acquirente non potendo trovare altrove il prodotto principale sarà indotto ad accettare anche le prestazioni supplementari[325]. Qui di seguito si propone un'analisi delle controversie più significative che hanno riguardato l'interpretazione della nozione di abuso di posizione dominante.

La Commissione europea aveva contestato l'abuso di posizione dominante a dell'emittenti televisive: l'ITP, RTE e la BBC. Esse detenevano un monopolio di fatto sulle informazioni dei palinsesti televisivi e rifiutavano di fornire tali informazioni grezze all'impresa Magil ed a qualsiasi altro operatore impedendo loro di realizzare una rivista settimanale che contenesse tali informazioni accompagnate da commenti ed immagini. In questo modo il telespettatore che volesse informarsi sulla programmazione televisiva della settimana seguente era obbligato ad acquistare la guida settimanale di ogni emittente. La Corte di giustizia nel risolvere la controversia aveva individuato tre condizioni in presenza delle quali si poteva ritenere sussistente la condotta di abuso di posizione dominante. In primo luogo il rifiuto di contrattare deve impedire l'emergere di un prodotto nuovo che incontra l'interesse potenziale dei consumatori e che può essere realizzato solo con la materia prima detenuta dall'impresa in posizione dominante. Nel caso Magil il prodotto nuovo era costituito dalla guida televisiva settimanale che non era offerta dalle due ricorrenti e la materia prima erano le informazioni grezze sulla programmazione televisiva. La seconda condizione riguarda il rifiuto di contrattare che non deve essere sorretto da una giustificazione oggettiva. La Corte di giustizia in questa sentenza non aveva ravvisato alcuna giustificazione né dall'attività di diffusione radiotelevisiva né da quella di pubblicazione di guide televisive. Infine il rifiuto deve comportare il sorgere di una posizione dominante su un mercato derivato. Secondo la Corte ciò è avvenuto nel caso Magil poiché le ricorrenti, non cedendo la materia prima costituita dall'informazione grezza sui palinsesti televisivi, impedivano ad altre imprese di elaborare guide televisive. In questo modo non poteva nascere la concorrenza sul mercato derivato[326]. Questa pronuncia è molto

[325] V. VANZETTI e DI CATALDO, op. cit., 625 ss..

[326] Per un'altra decisione che ha fatto applicazione di queste condizioni elaborate dalla corte v. Trib. di primo grado CE, 12 giugno 1997, T-504/93, in *AIDA* 1998, *503*.

importante perché evidenzia la possibilità di licenze obbligatorie nel diritto d'autore quando il rifiuto di concederle costituisca abuso di posizione dominante.

Per accertare l'esistenza di una posizione dominante occorre effettuare un duplice passaggio: in primo luogo è necessario individuare il mercato geografico e merceologico di riferimento; successivamente bisogna verificare se l'impresa in esame abbia una posizione dominante su tale mercato. In base a questo metodo di accertamento parte della dottrina esclude l'esistenza di posizione dominanti nel caso delle opere dell'ingegno classiche, mentre in presenza di alcune condizioni la ritiene ravvisabile nel campo delle creazioni utili[327]. Per la prima tipologia di opere il mercato di riferimento è assai ampio e vasto: la creazione di un prodotto dell'ingegno crea un monopolio concernente solo quel determinato bene ma non incide sulla realizzazione di altre opere presenti su quel determinato mercato. La concorrenza fra opere dell'ingegno è sempre garantita e ciò è dimostrato anche dai fatti: il successo di un romanzo non ostacola in alcun modo la possibilità di successo di un'altra opera letteraria. Non vi è alcun potere di mercato fondamentalmente per due circostanze: in primo luogo il prestigio di una creazione non incide sul suo prezzo e su quello di altre opere; inoltre il diritto d'autore tutela soltanto la forma espressiva e non il contenuto quindi non si crea alcuna preclusione decisiva per la realizzazione di opere successive.

Diversamente dalle opere dell'ingegno classiche le creazioni utili hanno un mercato molto ristretto se infatti: «un libro concorre con un libro, un film con un altro film»[328] e cosi via, le opere con una funzione utilitaria invece concorrono soltanto con le altre creazioni che si pongono al servizio dello stesso bene principale. Così per fare un esempio: un software di analisi diagnostica creato per effettuare diagnosi e assistenza solo su determinati elaboratori non si pone in concorrenza con altri analoghi strumentali allo stesso tipo di interventi per altre marche di computers[329]. Quest'orientamento, una volta individuato il mercato di riferimento delle creazioni utili, ritiene sussistente la posizione di dominanza in tutti quei casi in cui si è soliti parlare di essential facilities[330], come ad esempio nel caso Magil. Quindi l'abuso è presente qualora si verifichino le tre

[327]RICOLFI, *Diritto di autore ed abuso di posizione dominante*, in *Riv. dir. ind.* 2001, I, 149 ss..
[328]RICOLFI, *Diritto di autore ed abuso di posizione dominante*, cit., 162.
[329]RICOLFI, *Diritto di autore ed abuso di posizione dominante*, cit., 163.
[330] L'essential facility ricorre quando un'impresa detiene il controllo di una risorsa funzionale allo svolgimento di talune attività economiche svolte da altre imprese in settori diversi rispetto a quello in cui opera la prima impresa. Per un approfondimento v. VANZETTI e DI CATALDO, op. cit., 635 ss..

condizioni individuate dalla Corte di giustizia nel predetto caso[331]. Per tale dottrina queste condizioni possono verificarsi solamente quando il diritto d'autore offre una tutela eccessivamente ampia che non si limiti alla forma espressiva ma acceda anche al contenuto ed all'idee, come nel caso Magil per la protezione offerta dal diritto d'autore irlandese. Le conseguenze di questa tesi comporterebbero l'impossibilità di configurare l'abuso di posizione dominante nell'ipotesi di un eventuale rifiuto di concedere la licenza di elaborazione, poiché l'opera derivata comporta soltanto una modifica della forma interna e/o della forma esterna.

Altra parte della dottrina individua due finalità fondamentali nella disciplina delle privative: la prima riguarda la realizzazione di economie di scala per sfruttare al meglio gli investimenti impiegati per l'immissione dell'opera sul mercato; la seconda finalità risponde all'interesse della collettività ad intensificare la diversificazione di opere presenti sul mercato[332]. Questi due scopi possono essere perseguiti solo attraverso l'utilizzo di licenze esclusive. Infatti l'economia di scala può essere realizzata solo quando si ottiene un livello elevato di specializzazione nella produzione di quel determinato bene e ciò sarà conveniente solo nel caso in cui si abbia un'esclusiva su quel bene. La seconda finalità può essere raggiunta solamente quando ai potenziali concorrenti viene impedito lo sfruttamento di una risorsa, cosicché essi siano incentivati alla realizzazione di un'opera concorrente a quella già immessa sul mercato. Per tale indirizzo dottrinale il rifiuto di concedere licenze sarà lecito fin tanto che sia orientato verso la realizzazione di tali obiettivi. Così ad esempio nel caso Magil il diniego della licenza precludeva l'offerta sul mercato derivato di guide televisive, che per loro natura non sono un prodotto standardizzato. Mentre il rifiuto di concedere licenze per la pubblicazione di raccolte di figurine contenente immagini degli atleti non dovrebbe essere considerato illecito poiché la collezione di figurine è un prodotto standardizzato[333].

---

[331] Le tre condizioni elaborate nel caso Magil possono essere così sintetizzate:

- possesso di una risorsa essenziale per la creazione di un nuovo prodotto che incontra l'interesse degli acquirenti;
- rifiuto ingiustificato di cedere tale risorsa;
- acquisizione di una posizione di dominanza sul mercato derivato da parte dell'impresa che controlla la prima risorsa;

In alcune ipotesi, come spiegato meglio più avanti, dottrina e giurisprudenza individuano quattro condizioni ma questo non ha alcuna conseguenza da un punto di vista sostanziale.

[332] SARTI, *Proprietà intellettuale, interessi protetti e diritto antitrust*, in *Riv. dir. ind*. 2002, I, 564 ss..

[333] In senso contrario v. AGCM, Parere 31 ottobre 1996 n. 4381.

Un'ultima posizione dottrinale pone l'accento su una finalità comune al diritto antitrust ed al sistema delle privative: l'incentivo all'innovazione. Secondo tale orientamento il diritto antitrust dovrebbe intervenire ogni volta che il rifiuto di concedere delle licenze ostacoli l'innovazione, ossia la nascita e la diffusione di un'opera capace di portare ad un progresso nel campo culturale[334].

Nel caso Magil l'oggetto della decisione sembrerebbe essere la privativa sul diritto d'autore, ma in realtà, come in altri casi, ad esempio il caso IMS Health, la decisione ha evidenti effetti sulla circolazione delle informazioni. Nel caso IMS Health[335] ciò è maggiormente evidente poiché si tratta della possibilità di avere accesso e poter utilizzare una banca dati contenente informazioni riguardanti le vendite di prodotti farmaceutici, per conto dei grossisti, alle farmacie. Per dirimere la controversia la Corte di Giustizia ha fatto ricorso alla dottrina dell'essential facility, andando a verificare la presenza delle tre condizioni cardine per poter applicare la suddetta disciplina: i) possesso di una risorsa essenziale per la creazione di un nuovo prodotto che incontra l'interesse degli acquirenti; ii) rifiuto ingiustificato del titolare di cedere tale risorsa; iii) il rifiuto deve determinare l'acquisizione di una posizione di dominanza sul mercato derivato da parte dell'impresa che controlla la prima risorsa. In altri termini la Corte di giustizia ha verificato se l'esercizio del diritto esclusivo sulla banca dati persegua uno scopo contrario alla normativa antitrust, ossia se risulti evidente l'ostacolo insormontabile all'innovazione posto dall'esercizio di quel determinato diritto[336]. In altri termini l'abuso è dimostrato quando l'oggetto del diritto è un'infrastruttura essenziale per lo sviluppo di un mercato derivato. In questo caso secondo rilevante dottrina la Corte di Giustizia compie una forzatura interpretativa ritenendo applicabile l'essential facility doctrine anche se è difficile riscontrare un mercato derivato[337]. L'atteggiamento qui palesato dalla Corte di giustizia è di evidente favore nei confronti della circolazione delle informazioni e contro la possibilità di avere un diritto di proprietà intellettuale che impedisca l'accesso a patrimoni informativi. A favore di un regime di accesso si espressa anche la Commissione europea nella comunicazione del 10 gennaio 2017 laddove ha auspicato l'introduzione di un regime generale di accesso

---

[334] V. MELI, *Rifiuto di contrattare e tutela della concorrenza nel diritto antitrust comunitario*, Giappichelli, Torino, 2003, 233 ss.. Cfr. anche Ghidini, op. cit., 15 ss..

[335] V. CGCE, 29 aprile 2004, C- 418/01, in *Riv. dir. ind.* 2004, 314 ss..

[336] V. PARDOLESI e GRANIERI, *Licenza obbligatoria ed essential facilities nell'antitrust comunitario*, in *Riv. dir. ind*. 2004,327.

[337] In questo senso v. PARDOLESI e GRANIERI, op. cit., 328 ss..

dietro compenso rifacendosi alle condizioni FRAND[338]. Occorre quindi interrogarsi sulla possibilità di applicare il test elaborato dalla giurisprudenza comunitaria in passato nei casi: Magil, Microsoft, Ims Health nel campo dei dati. L'applicazione di tale test serve per verificare se il ricorso all'art. 102 TFUE possa garantire l'accesso ai dati. Come già detto, occorre quindi verificare la sussistenza delle quattro condizioni in presenza delle quali si può ritenere sussistente la condotta di abuso di posizione dominante: i) il rifiuto di cedere un determinato prodotto o un determinato servizio deve impedire l'emergere di un prodotto in un mercato a valle (dati pubblici o privati); ii) il rifiuto deve comportare il sorgere di una posizione dominante sul mercato a valle; iii) il prodotto nuovo incontra l'interesse potenziale degli acquirenti; iv) il rifiuto di contrattare che non deve essere sorretto da una giustificazione oggettiva[339].

Innanzitutto, occorre ricordare che le informazioni e i dati considerati al loro livello semantico possono, tramite inferenze statistiche, essere utili per ricavare nuove conoscenze da utilizzare poi successivamente come strategia di mercato. Per soddisfare la prima condizione del test sopra menzionato i dati non devono in alcun modo essere accessibili e per ciò l'accesso ai dati deve essere indispensabile per l'emersione del prodotto nel mercato a valle. Qui si pone una prima distinzione tra dati privati e dati pubblici. Per i secondi intendendo tutti quei dati raccoglibili in spazi pubblici e non all'interno della catena di produzione di una determinata azienda, per esempio i dati sul traffico raccolti tramite dispositivi su automobile. È evidente che in questo caso il set di dati così formatosi è ottenibile da diversi soggetti e viene meno il carattere dell'indispensabilità. Per quanto riguarda invece i dati privati occorre chiedersi se sia applicabile la nozione di indispensabilità fatta propria dalla Corte di giustizia nel caso

[338] Commissione Europea, Com. 10 gennaio 2017: «**Accesso dietro compenso**: si potrebbe elaborare un quadro, potenzialmente basato su determinati principi fondamentali quali le condizioni eque, ragionevoli e non discriminatorie (condizioni FRAND), per consentire ai titolari dei dati, quali fabbricanti, prestatori di servizi o di altri soggetti, di fornire accesso ai dati in loro possesso in cambio di remunerazione, previa anonimizzazione dei dati stessi. Occorrerebbe prendere in considerazione i pertinenti legittimi interessi e la necessità di tutelare il segreto commerciale. Si potrebbe anche considerare il ricorso a diversi regimi di accesso per settori e/o modelli commerciali diversi, per tener conto delle peculiarità di ciascun settore. Per esempio, in alcuni casi il libero accesso ai dati (totale o parziale) potrebbe essere la migliore scelta sia per le imprese sia per la società.» In questo senso v. anche DREXL, op. cit., 44 ss..

[339] Come riportato supra, in alcuni casi le condizioni alla base dell'essential facility doctrine individuate dalla dottrina e dalla giurisprudenza sono 4 e in altri casi sono 3. Si tratta pur sempre delle stesse condizioni, con l'unica differenza che nell'ipotesi in cui ne vengono individuate tre: la condizione i) *il rifiuto deve comportare il sorgere di una posizione dominante sul mercato a valle* è unita al numero iii) *il prodotto nuovo incontra l'interesse potenziale degli acquirenti*. Questa diversa ripartizione è puramente stilistica e non ha alcuna valenza da un punto di vista sostanziale.

Bronner[340], unicità della struttura in questo caso del set di dati e non sostituibilità della risorsa che non sia dovuta ad una semplice sconvenienza economica da parte del richiedente.

Secondo autorevole dottrina vi è una difficoltà concreta a comprendere se i dati siano sostituibili oppure no, perché molto spesso di fronte a set così ampi anche i migliori analisti possono avere delle difficoltà a comprendere il valore semantico di questi dati e le informazioni che possono essere ricavati dall'osservazioni delle loro correlazioni[341]. Quest'argomento è opinabile se si fa riferimento al procedimento con cui sono stati ottenuti i dati. Per verificare la sussistenza del primo requisito occorre indagare il concetto di indispensabilità fatto proprio dalla giurisprudenza comunitaria. A tal fine può essere utile riferirsi al caso Bronner laddove la Corte di giustizia afferma che l'indispensabilità è dimostrata solo se non è possibile conseguire in alcun modo quel determinato risultato senza ricorrere al prodotto o servizio detenuto dall'impresa in posizione dominante, non importando la maggior convenienza derivante dall'utilizzo del prodotto o servizio del concorrente[342]. L'indispensabilità forse potrebbe essere ravvisabile nei dati raccolti dai colossi del web che sono prodotti da coloro che usufruiscono dei loro servizi[343].

Per quanto concerne il secondo requisito il rifiuto di concedere l'accesso ai dati deve impedire nel mercato a valle la creazione di una situazione concorrenziale. Ciò nel caso dei dati avviene quando i dati sono raccolti e utilizzati per uno scopo ma poi vengono riutilizzati in altri settori completamente diversi per differenti scopi. Per cui il soggetto detentore dei dati potrebbe operare in un settore completamente diverso rispetto a quello in cui opera l'impresa che avanza la richiesta di accedere a tali dati[344]. Questo spesso è ravvisabile nelle condotte tenute dai colossi del web che operano sulle piattaforme digitali. Tali soggetti cercano di entrare in nuovi mercati secondari con i propri servizi in modo da: ampliare i loro set di dati; aumentare la soddisfazione dei propri utenti

---

[340] CGCE, 26 novembre 1998, C-7/97, in www.curia.europa.eu.

[341] In questo senso v. Drexl, op. cit., 44 ss..

[342] V. CGCE, 26 novembre 1998, C-7/97, in www.curia.europa.eu, cons. 41 e seguenti: «41…occorrerebbe … non solo che il diniego del servizio costituito dal recapito a domicilio possa eliminare del tutto la concorrenza sul mercato dei quotidiani da parte della persona che richiede il servizio e non sia obiettivamente giustificabile, ma anche che detto servizio sia, di per sé, indispensabile per l'esercizio dell'attività di tale persona, nel senso che non esiste alcun modo di distribuzione che possa realmente o potenzialmente sostituirsi al predetto sistema di recapito a domicilio».

[343] In questo senso vedi MAGGIOLINO, op.cit., 327.

[344] Come nel caso di Google o di Auditel, o più in generale delle piattaforme digitali (v. in tal senso MAGGIOLINO, op. cit., 64).

incrementando la qualità della loro esperienza con servizi ulteriori, impedire l'utilizzo del nuovo mercato ad altri concorrenti[345].

Per quanto riguarda il terzo requisito innanzitutto occorre precisare che risultato dell'analisi big data sono innanzitutto informazioni o conoscenze e non nuovi prodotti come precisa la Corte di Giustizia nei casi sopra elencati. In secondo luogo è veramente difficile comprendere quando queste informazioni siano nuove[346]. Infine, per quanto concerne le giustificazioni oggettive resta da precisare che non è ancora chiaro che conseguenze economiche comporti il rifiuto dell'accesso ai dati. Sul tema vi sono due decisioni significative dell'AGCM che contengono degli esempi importanti su quando e quanto il controllo dei dati possa ostacolare la libera concorrenza e debba essere rimosso e sul tipo di nocumento possa causare la mancata condivisione di informazioni[347]. Vi sono situazioni in cui un'impresa interrompendo il flusso di condivisione di dati potrebbe causare un importante danno agli operatori economici di un determinato settore. Ciò può accadere in diversi ambiti, come si vedrà nel paragrafo successivo, per il settore dell'IOT[348] e nel mondo finanziario[349].

3. L'internet delle cose è un termine che viene comunemente utilizzato per indicare tutti quei dispositivi che registrano e raccolgono dati e li elaborano solitamente per automigliorarsi o per meglio calibrare il servizio fornito sulla richiesta dell'utente[350].

---

[345] MAGGIOLINO, op. cit., 64, 264 ss..

[346] MAGGIOLINO, op. cit., 327 e 328.

[347] AGCM, A422 – Sky Italia/Auditel, dec. n. 23112, del 14 dicembre 2011, in Boll. n. 50, 2011; AGCM, A424 – Epolis/ Audipress, dec. n. 22320, del 20 aprile 2011, in Boll. n. 16, 2011.
Nella decisione del 20 aprile 2011, che vede contrapposte nel procedimento Audipress S.r.l. e E.Polis S.p.a., AGCM non commina una sanzione nei confronti di Audipress perché ha posto rimedio alla sua condotta abusiva riprendendo la sua attività. Audipress è una società che realizza indagini statistiche sulla lettura delle riviste (giornali, quotidiani, periodici). Lo scopo delle sue indagini è quello di descrivere i lettori delle riviste sulla base delle loro caratteristiche socio-demografiche, così da facilitare la comprensione dell'attitudine a diventare destinatari utili della comunicazione veicolata attraverso le diverse testate. Il mancato svolgimento di quest'attività determina un nocumento notevole alle testate e per questo motivo la mancata erogazione di tale servizio senza un giustificato motivo può costituire abuso di posizione dominante.

[348] Cfr. sul punto RICOLFI, *Iot and the ages of antitrust*, in *Concorrenza e mercato* 2017, 221 ss..

[349] Cfr. sul punto DI PORTO, *Scambi di informazione e abusi di posizione dominante: una rilettura degli "Abusi Informativi" e dei relativi rimedi*, in *Concorrenza e Mercato* 2014, 35 ss.; BERTANI, *Big data, Proprietà intellettuale e mercati finanziari*, cit., passim. Pur se chi scrive non ha alcuna competenza sul tema dei mercati finanziari e sul loro funzionamento, l'inserimento di tale argomento all'interno della trattazione segue l'intento di mostrare come vi siano sia settori non regolati che settori regolati in cui si possa verificare un abuso di posizione dominante.

[350] V. MORO VISCONTI, *Internet delle cose networks e plus valore di connettività*, cit., 536 ss; GERMANI e FEROLA, *Il wearable computing e gli orizzonti futuri della privacy*, in *Dir. inf.* 2014, 75 ss.. V. anche supra cap. 1 par. 1 GAETA, *La protezione dei dati personali nell'Internet of Things: l'esempio dei veicoli autonomi*, in *Dir. inf.* 2018, 148; MAGGIOLINO, op. cit., 194.

Gran parte dei dati che vengono raccolti in questo modo sono poi oggetto di studio e rielaborazione e permettono il raggiungimento di notevoli livelli di conoscenza. Per questo motivo i set di dati raccolti da questi dispositivi hanno un enorme valore sul mercato. È necessario interrogarsi se ed in presenza di quali condizioni il controllo di questi set di dati possa costituire un'essential facility. Nell'ipotesi dell'Internet delle cose i dati raccolti sono informazioni inerenti all'utilizzo del prodotto a cui il sensore è annesso. Tali dati possono essere trattati per una duplice finalità migliorare il servizio rivolto all'utente finale, cui i dati si riferiscono (i.e. nel senso di personalizzare il servizio), oppure anonimizzare e studiare in ottica di analisi big data i dati in modo da estrapolare informazioni generali utili sia per migliorare il prodotto o servizio reso e renderlo sempre più competitivo sul mercato, sia per creare o migliorare un prodotto o servizio destinato ad un diverso settore. È evidente che in tale ultima ipotesi l'impossibilità per i concorrenti di accedere al set di dati raccolti dal «proprietario del prodotto Iot»[351] può essere gravemente pregiudizievole e potrebbe, al ricorrere dei requisiti menzionati nel precedente paragrafo, determinare un abuso di posizione dominante. Infatti nell'Internet of things tipicamente il fornitore del bene impone contrattualmente all'utente finale sia l'invio dei dati raccolti tramite gli oggetti smart messi a disposizione, sia l'incomunicabilità dei dati raccolti a terzi. Inoltre si consideri che, come anticipato, normalmente per garantirsi che questo avvenga il fornitore da una parte mette a disposizione un infrastruttura tecnologica che si interfacci con il dispositivo; dall'altra parte tramite i dati raccolti offre allo stesso utente finale un servizio migliorato (i.e. personalizzato) sulla base dei dati raccolti durante l'utilizzo dello stesso dispositivo, così da fidelizzare il cliente[352]. Tramite questi vincoli contrattuali e tecnologici il fornitore consolida direttamente la sua posizione con gli utenti finali e indirettamente quella sul mercato impedendo alle imprese concorrenti di sviluppare anche nei mercati a valle servizi che si basino sull'utilizzo in ottica di analisi big data di quei dati.

L'analisi big data riveste un ruolo importantissimo nel mercato finanziario, dove lo studio e l'analisi dell'incontro tra domanda e offerta avvenuto nel passato permette di predire con notevole precisione il futuro[353]. A differenza dell'Internet of things il

[351] Per «proprietario del prodotto Iot» si vuole far riferimento al colui che sfrutta i dati raccolti dal sensore. In altri termini colui che ha la disponibilità materiale dei dati raccolti tramite i sensori.
[352] In questo senso v. OTTOLIA, *Big data e innovazione computazionale*, 318 ss..
[353] BERTANI, *Big data, proprietà intellettuale e mercati finanziari*, cit., 538.

mercato finanziario è regolato e vi sono una serie di obblighi informativi in capo ai gestori dei trading venues[354]. Infatti, si consideri che per le informazioni borsistiche il legislatore europeo e quello interno hanno dettato negli anni un corpo normativo consistente che prevede un regime all'insegna della trasparenza[355]. I titolari di queste informazioni molto spesso pongono in essere comportamenti abusivi fornendo in modo asimmetrico le informazioni agli operatori, pur sempre nel rispetto degli obblighi di disclosure previsti dalla normativa. In alcuni casi il rifiuto di fornire informazione anche se lecito e ammesso dalla normativa settoriale vigente, pone gli operatori nell'impossibilità di operare. Come è avvenuto nel caso Standard & Poor's, in cui tale società avendo il controllo dei codici identificativi ISIN (codici identificativi dei prodotti finanziari) impediva l'accesso a tali codici se coloro che volevano accedere a tali informazioni non erano disposti a pagare una licenza particolarmente alta. Inoltre veniva impedita la portabilità delle informazioni, così che non ci si potesse rivolgere ad altra società in un momento successivo[356].

Le due decisioni dell'AGCM citate nel precedente paragrafo, come le altre decisioni della Corte di Giustizia riportate in questi paragrafi, mostrano un'attenzione particolare dell'ordinamento europeo e di quello interno alle situazioni di controllo delle informazioni, ponendosi in alcuni casi a favore della condivisione di dati e al riconoscimento di un regime di accesso ai concorrenti. Il fulcro del problema consiste nell'individuazione di un giusto equilibrio tra l'incentivo economico alla creazione dei set di dati e di patrimoni informativi e il loro accesso. In altri termini, si deve riconoscere una qualche forma di esclusiva a chi raccoglie e produce dati e una possibilità di accesso all'eventuali imprese concorrenti così da evitare situazioni di abuso da chi detiene patrimoni informativi consistenti. Occorre individuare un equilibrio tra il diritto alla remunerazione del proprio investimento da parte dell'impresa che ha realizzato o contribuito a realizzare i set di dati, il diritto alla libera iniziativa economica dei terzi che desiderano avere accesso a tali dati e il diritto della collettività a poter acquisire quel patrimonio informativo per innovarsi.

---

[354] Per un approfondimento sugli obblighi informativi v. BERTANI, *Big data, proprietà intellettuale e mercati finanziari*, cit., 563 e 564.

[355] BERTANI, *Big data, proprietà intellettuale e mercati finanziari*, cit., 540 e 541; dir. CE 39/2004, Reg di attuazione 1287/2006; dir. UE 65/2014, Reg. UE 600/2014, D. lgs. N. 58/1998, Reg. Consob n. 16191 del 29 ottobre 2007.

[356] Cfr. Commissione Europea, Decisione del 15 novembre 2011, relativa a un procedimento a norma dell'art. 102 TFUE e 54 dell'Accordo SEE, Caso COMP/39.592 – Standard & Poor's; DI PORTO, op. cit., 36 ss..

A tal proposito secondo un recente orientamento dottrinale la migliore soluzione sarebbe rifarsi alle condizioni FRAND[357], la Corte di giustizia nel caso Huawei deciso il 16 gennaio 2015 ha evidenziato come vi possono essere anche delle ipotesi ulteriori in cui il rifiuto di concedere licenza possa costituire un abuso di posizione dominante, come nel caso in cui non vengano rispettate le condizioni FRAND (fair-reasonable and non-discriminatory) in ipotesi di un SEP[358]. In estrema sintesi nel caso Huawei la Corte di giustizia arriva ad affermare la necessità che il titolare di un SEP possa agire per contraffazione se prima di promuovere l'azione abbia sottoposto al presunto contraffattore una proposta di licenza contenente le condizioni FRAND[359]. Secondo l'impostazione dell'orientamento dottrinale qui proposto ogni patrimonio informativo dovrebbe essere accessibile a condizioni FRAND. Ovviamente l'obbligo d'accesso dovrebbe riguardare esclusivamente quelle informazioni da considerarsi rilevanti per i concorrenti. La rilevanza deve essere intesa nel senso che i dati devono essere necessari per la creazione di un nuovo prodotto o servizio, o per competere nei mercati a valle[360]. La stessa Commissione europea nella comunicazione del 10 gennaio 2017 si è schierata a favore di una libera circolazione dei dati[361] e ha ribadito questa posizione anche nella proposta di regolamento europeo relativo ad un quadro applicabile alla libera circolazione dei dati non personali nell'UE, adottato il 13 settembre 2017. Quanto qui sostenuto sembra valere esclusivamente per i dati che non siano personali, laddove vi sono dati personali tali condizioni non potrebbero essere applicate senza entrare in contrasto con i limiti posti dalla disciplina a protezione dei dati personali[362]. Il Titolare del trattamento non potrebbe condividere set di dati senza un passaggio obbligatorio dall'interessato sia in termini di informativa che probabilmente di consenso. Per questo motivo è espressamente previsto nel GDPR un rimedio all'art. 20 del Regolamento

---

[357] V. DREXL, op. cit., 44 ss.; RICOLFI, *Iot and the ages of antitrust*,cit., passim.
[358] CGUE, 16 luglio 2015, C-170/2013, in www.curia.europa.eu.
[359] CGUE, 16 luglio 2015, C-170/2013, in www.curia.europa.eu.
[360] Per questa ricostruzione del concetto di rilevanza confronta DI PORTO, op. cit., 36. Nell'ipotesi presa qui in considerazione le licenze FRAND sarebbero concesse dal titolare non perché questi ha un diritto esclusivo sui dati (v. supra par. 1 del presente capitolo), ma semplicemente perché è nella posizione fattuale di controllo sul set di dati oggetto della licenza. Contra la possibilità di ricorrere al sistema delle licenze obbligatorie nel contesto big data v. MAGGIOLINO, op. cit., 329 ss.. L'autrice ravvisa diverse difficoltà: i)individuazione dei set di dati rilevanti ai fini della licenza; ii) rapida obsolescenza dei dati; iii) problemi legati alla privacy per le piattaforme digitali non potrebbe esserci condivisione dei dati personali senza entrare in contrasto con la normativa posta a protezione dei dati personali; iv) la determinazione del prezzo della licenza.
[361] Commissione Europea, COM 10 gennaio 2017, *Costruire una economia dei dati europea*, passim.
[362] MAGGIOLINO, op. cit., 331.

europeo che sancisce il diritto alla portabilità dei dati[363]. Tale diritto, anche se tutela direttamente gli utenti finali, indirettamente incide sulla circolazione delle informazioni, permettendo una corretta situazione concorrenziale, dettata sia dal fatto che maggiore è l'appetibilità del prodotto o servizio offerto e maggiore sarà il set di dati che l'impresa potrà riuscire a crearsi[364], sia che inevitabilmente si viene a creare una situazione più fluida dove è più facile che vi sia il passaggio dei dati personali tra imprese concorrenti[365]. Infatti, Il diritto alla portabilità, come già in parte analizzato nel secondo paragrafo del precedente capitolo, permette agli interessati di ricevere in un formato facilmente consultabile e leggibile i loro dati personali oggetto di un determinato trattamento. L'intento del legislatore europeo è quello di aumentare il potere di controllo sulla circolazione e sull'utilizzo dei propri dati personali da parte degli interessati. Allo stesso tempo l'aumento del potere di controllo in capo agli interessati tramite l'introduzione del diritto alla portabilità vuole incentivare la concorrenza nei servizi dell'informazione, facilitando la transizione da un titolare ad un altro titolare che fornisce lo stesso servizio o uno simile [366]. L'aspetto originale dell'introduzione del diritto alla portabilità consiste nell'immettere nel mercato uno strumento regolatore dall'interno e non calato dall'alto da un'autorità indipendente. In altri termini si vuole che siano coloro che usufruiscono del servizio a permettere la regolazione del mercato evitando un intervento ex post dell'autorità antitrust[367]. Il limite principale del diritto alla portabilità così come è strutturato all'art. 20 del Regolamento europeo sulla protezione dei dati personali, riguarda il fatto che non rientrano in tale diritto i dati di seconda generazione (dati inferenziali o derivati), per tali intendendo i dati prodotti dal titolare studiando i dati personali dell'interessato, anche se quei dati vengono poi utilizzati per costruire profili utenti. Questo limite permette alle imprese di salvaguardare le informazioni derivanti dalle analisi big data[368] .

A parere di chi scrive, allo stato attuale, vi sono dei dubbi sulla concreta operatività e affidabilità dell'istituto della portabilità. È forse troppo presto, in considerazione della

---

[363] Cfr. RICCI, op. cit., 223 ss..

[364] In questo senso v. RICOLFI, *Iot and the ages of antitrust*,cit., 224. Se le imprese devono misurarsi con altre imprese concorrenti punteranno ad avere un prodotto migliore che soddisfi le esigenze dei consumatori in modo da evitare che questi esercitino il loro diritto alla portabilità.

[365] V. DE BIASE, *Il mercato dei dati personali tra portabilità e concorrenza*, in *Il Sole 24 ore online* 2018; DI PORTO, op. cit., 30.

[366] WP29, Estratto linee guida sul diritto alla portabilità, 1 ss..

[367] Sul ruolo del diritto alla portabilità nella concorrenza v. MAGGIOLINO, op. cit., 346 ss..

[368] WP29, Estratto linee guida sul diritto alla portabilità, 10 ss..

sua così recente introduzione, per poter comprendere a pieno l'effettiva portata di tale diritto nel mondo della concorrenza. Resta da precisare che la Commissione europea è convinta del funzionamento di tale istituto, dato che ha previsto l'introduzione di un diritto analogo nella proposta di regolamento europeo sulla circolazione dei dati non personali del 13 settembre 2017[369].

Oltre a questo primo aspetto relativo alla possibilità di acconsentire a chiunque possa esser danneggiato dal mancato accesso ad un determinato set di dati, di accedere a tali informazioni. Vi è un aspetto ulteriore che sta prendendo forma ed emergendo con chiarezza. Tale aspetto è relativo alle modalità di accesso e fornitura delle informazioni controllate dall'impresa che si trova in posizione dominante. Ne è un chiaro esempio il caso sopracitato deciso da AGCM.

L'AGCM nel 2011 ha condannato Auditel al pagamento di una sanzione perché ha ritenuto tale società colpevole di abuso di posizione dominante in considerazione del suo comportamento relazionato con l'effettiva situazione di controllo di informazioni fondamentali per l'attività economica dell'emittenti televisive. Auditel è una società che si occupa di elaborare i sondaggi sugli ascolti televisivi ed ha il monopolio in questo settore, che è fondamentale per le emittenti televisive. I sondaggi costituiscono la base della concorrenza tra emittenti. Secondo l'AGCM Auditel, dato che ha il monopolio sulla rilevazione dei sondaggi è tenuta a svolgere la sua attività in modo da evitare qualsiasi imprecisione o errore e cercando di acconsentire alle richieste di rimozione di eventuali ostacoli, avanzate dalle singole emittenti televisive. In particolare l'Autorità Garante per la concorrenza e il mercato rimprovera ad Auditel di aver rilevato l'indice di ascolto di ciascun singolo canale senza precisazione alcuna sulla fonte d'origine dei dati, in altri termini viene presentata in forma aggregata la percentuale di ascolti di quel canale senza distinzione alcuna sulla piattaforma di provenienza degli ascolti. Per le emittenti televisive, tra cui Sky (la prima società a lamentarsi del comportamento abusivo di Auditel) è estremamente utile conoscere le fonti d'origine dei dati. Inoltre, viene rimproverato ad Auditel il fatto che i dati di ascolto sono espansi per la totalità dei

[369] Nell'art. 6 della proposta la Commissione incoraggia le imprese all'elaborazione di codici di condotta che prevedano il diritto alla portabilità dei dati non personali. La Commissione Europea inizialmente aveva optato per una soluzione più simile a quella implementata nel GDPR, tuttavia a seguito del parere negativo del Comitato per il controllo normativo ha optato per la strada dell'autoregolamentazione prevedendo misure che incoraggino l'elaborazione di codici di condotta che disciplinino tale aspetto (v. Commissione Europea, "Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione Europea", 13 settembre 2017,8).

residenti in Italia, compresi coloro che non hanno un apparecchio televisivo, senza la previsione di alcun elemento di correzione che tenga conto di questo fattore. Nella procedura di espansione non si utilizza alcun fattore di ponderazione per considerare tale dato, per questo motivo i risultati sono leggermente falsati[370].

Al ricorrere delle condizioni richiamate nei paragrafi precedenti che configurano un abuso di posizione dominante, a carico dell'impresa non vi sarebbe solo l'onere di acconsentire l'accesso alle informazioni, ma anche di fornire i dati in modo tale da permettere un effettivo esercizio dell'attività economica alle imprese concorrenti[371]. L'impresa che ricopre una posizione dominante ha una speciale responsabilità che prescinde dall'accertamento della mala fede, ossia di un intento anticompetitivo[372]. Per questo motivo l'onere a carico di tale impresa può essere particolarmente pregnante e non limitarsi ad acconsentire l'accesso alle imprese concorrenti. In altri termini, si riconosce in capo all'impresa dominante un vero e proprio dovere di rendere effettivo l'accesso da parte delle altre imprese interessate[373].

Infine si segnala, come in parte già anticipato, che per ridurre la dipendenza da parte delle imprese da determinati fornitori, in particolare da coloro che forniscono servizi cloud, è stata elaborata una proposta di regolamento sul libero flusso dei dati non personali. La proposta di regolamento elaborata dalla Commissione Europea, nell'ambito della strategia per il mercato unico digitale, è volta a rimuovere i principali

---

[370] AGCM, A422 – Sky Italia/Auditel, dec. n. 23112, del 14 dicembre 2011, in Boll. n. 50, 2011.

[371] Con tale accezione intendendo le imprese che operano nel mercato a valle del mercato in cui opera l'impresa in posizione dominante e che beneficiano dell'attività di quest'ultima per lo svolgimento della loro attività economica. Così in parte anche OREFICE, op. cit., 714, che ritiene come immediata conseguenza del non riconoscere un diritto di accesso a set di dati strutturati in un formato pienamente fruibile un contrasto con l'art. 41 della Costituzione limitando fortemente la libera iniziativa economica del singolo.

[372] Per un approfondimento su tale concetto v. CGCE, AKZO Chemie BV v. Commissione Europea, C-62/86, 3 luglio 1991, www.curia.europa.eu; CGCE, NV Nederlandsche Banden Industrie Michelin v. Commissione Europea, C- 322/81, 9 novembre 1983, www.curia.europa.eu; Trib. UE, T-321/05, 1 luglio 2010, www.curia.europa.eu; Trib. CE, Irish sugar plc v. Commissione Europea, T-228/97, 7 ottobre 1999, www.curia.europa.eu; BUTTARELLI, *Antitrust, Privacy and Big Data*, Bruxelles 3 Febbraio 2015. Anche la Commissione Europea di recente ha dato un'evidente prova di sostenere questa tesi condannando Google ad una sanzione di 2,42 miliardi di euro, poiché Google, a detta della Commissione, abusando della sua posizione dominante ha gestito in modo inadeguato l'accesso alle informazioni raccolte dal suo motore di ricerca (per un approfondimento v. Commissione Europea, Comunicazione del 27 giugno 2017).

[373] Tale aspetto è particolarmente evidente nel settore delle telecomunicazioni e nel settore energetico (cfr. DI PORTO, op. cit., 38 ss.; Commissione Europea, decisione del 22 giugno 2011, Telekomunikacja Plska, C(2011) 4378; AGCM, A426 – Telecom Italia – Gare affidamento servizi telefonia fissa e connettività IP, dec. n. 23677, 19 giugno 2012, in Boll. n. 25/2012; AGCM, A410 – Exergia/Enel – Servizio di salvaguardia, dec. n. 20549, 10 dicembre 2009, in Boll. n. 49/2009). In tutti i casi appena citati un'impresa in posizione dominante forniva in modo non appropriato le informazioni commettendo a detta dell'autorità competente abuso di posizione dominante.

ostacoli alla libera circolazione dei dati non personali per permettere la creazione di un mercato comune europeo dei dati. Nelle consultazioni con i portatori di interessi del 2015 la Commissione ha rilevato che gran parte delle imprese, PMI incluse, è stata influenzata nell'elaborazione della propria strategia aziendale dalle norme e dalle limitazioni in materia di localizzazione dei dati. Tale rilevazione è stata poi confermata da una seconda consultazione del 2017[374].

Gli elementi fondanti della proposta sono quattro: i) eliminare le norme nazionali che limitano la possibilità di scegliere il luogo di archiviazione o elaborazione dei dati; ii) garantire alle autorità competenti, tramite anche l'introduzione di meccanismi di cooperazione, la possibilità di accedere ai dati archiviati od elaborati in un altro stato membro con gli stessi poteri che avrebbero quando i dati sono archiviati o elaborati nel paese di loro competenza; iii) incoraggiare l'elaborazione di codici di condotta che facilitino la portabilità, ossia la possibilità di cambiare fornitore dei servizi cloud e che disciplinino la trasparenza (i.e. l'onere informativo a capo del fornitore prima della conclusione del contratto); iv) creare un unico punto di contatto all'interno di ciascuno stato membro che collabori con la Commissione e con le altre autorità degli stati membri, con l'intento di garantire il rispetto delle nuove disposizione sulla libera circolazione dei dati non personali. A parere della Commissione l'eliminazione di restrizione sulla localizzazione dei dati garantirebbe alle imprese una maggiore flessibilità nella gestione e analisi dei dati, ridurrebbe i costi dei servizi, amplierebbe la possibilità di scelta dei fornitori. Le principali restrizioni alla localizzazione attualmente in essere interessano diversi settori compreso quello pubblico, nella comunicazione della Commissione Europea titolata "Un quadro per il libero flusso dei dati non personali in Europa" del 19 settembre 2017 ne vengono individuati tre a titolo esemplificativo: i) le raccomandazioni delle autorità di vigilanza ai fornitori dei servizi finanziari; ii) le restrizioni normative in materia di segreto professionale; iii) le norme nazionali sull'archiviazione locale delle informazioni provenienti dal settore pubblico[375]. L'unico limite che viene mantenuto fermo dalla proposta è quello derivante da motivi di sicurezza pubblica. È previsto all'art. 4, per rendere effettiva la libera

[374] Commissione Europea, "Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione Europea", 13 settembre 2017.

[375] Commissione Europea, Comunicazione del 19 settembre 2017, "Un quadro per il libero flusso dei dati non personali in Europa", 1 ss..

circolazione, un onere di collaborazione in capo agli Stati membri che devono: i) notificare qualsiasi progetto di atto che introduca o modifichi limitazioni sulla localizzazione dei dati; ii) eliminare entro 12 mesi dall'entrata in vigore del Regolamento, qualsiasi restrizione alla localizzazione che non sia dettata da necessità di sicurezza pubblica, giustificando alla Commissione gli obblighi che intendono mantenere per tale ragione; iii) rendere pubbliche attraverso un apposito portale gli obblighi di localizzazione vigenti nel proprio territorio; iv) comunicare alla Commissione l'indirizzo web del portale.

La proposta della Commissione Europea, sebbene abbia il merito di semplificare la gestione dei dati non personali e ridurre i costi relativi alla localizzazione, non è risolutiva nel contesto dell'analisi big data, infatti non prende in considerazione l'aspetto maggiormente problematico relativo all'esercizio di un potere di controllo sulla circolazione dei dati e sulle possibilità di accesso ai dati da parte delle imprese concorrenti a quella che detiene il controllo del patrimonio informativo. A parere di chi scrive tale gap normativo può essere in parte colmato rifacendosi alla soluzione sopra riportata che fa perno sull'essential facility doctrine e sul ricorso alle condizioni FRAND.

Bibliografia

Dottrina

- ARE, *L'oggetto del diritto d'autore*, Giuffrè, Milano, 1963
- ASCARELLI, *Teorie della concorrenza e dei beni immateriali*, Giuffrè, Milano, 1960;
- AUTERI, *Contratti traslativi del diritto di autore e principio di indipendenza delle facoltà di utilizzazione*, in *Riv. dir. ind.* 1963, II
- BANTERLE, *Brevi cenni sulla titolarità dei dati comportamentali nei big data tra privacy e proprietà intellettuale*, in *AIDA* 2016, 579.
- BELVEDERE, *Aspetti ideologici delle definizioni nel linguaggio del legislatore e dei giuristi*, in *Definizioni giuridiche e ideologiche*, (a cura di) BELVEDERE, JORI e LANTELLA, Giuffrè, Milano, 1979, 349 ss..
- BERTANI, *nota a Trib. Torino 17 luglio 1997*, in *AIDA* 1998
- BERTANI, *Impresa culturale e diritti esclusivi*, Giuffrè, Milano, 2000, 342
- BERTANI, *Proprietà intellettuale e nuove tecniche di appropriazione delle informazioni*, in *Studi in onore di Gerhard Schricker*, Giuffrè, Milano, 2005
- BERTANI, *Diritto d'autore e connessi*, in *La proprietà intellettuale*, (a cura di) L. C. UBERTAZZI, Giappichelli, Torino, 2011
- BERTANI, *Big data, Proprietà intellettuale e mercati finanziari*, in *AIDA* 2017
- BETTINI, *L'attività inventiva nel rapporto di lavoro*, Giuffrè, Roma, 1993
- BOCCHI, *Privacy: sotto natale siamo tutti più buoni…o contatti no?*, in www.lcalex.it, 2017.
- BOLLIER, *The promise and peril of big data*, in https://www.emc.com/collateral/analyst-reports/10334-ar-promise-peril-of-big-data.pdf, 2010
- BRAVO, *Il consenso e le altre condizioni di liceità del trattamento*, in *Il nuovo Regolamento europeo sulla privacy e la protezione dei dati personali*, (a cura di) G. FINOCCHIARO, Zanichelli, Bologna, 2017
- BUTTARELLI, *Antitrust, Privacy and Big Data*, Bruxelles 3 Febbraio 2015
- C. GALLI, *La riforma del codice della proprietà industriale*, in www.filodiritto.com, 2010

- CAGNASSO, *v. Somministrazione*, in *Digesto disc. priv.*, XIV, Torino, 1997
- CALABRÒ, *Diritto delle comunicazioni elettroniche*, Giuffrè, Milano, 2010
- CAMUSSO, *Le informazioni segrete*, in BOTTERO, *La riforma del codice della proprietà industriale*, Giuffrè, Milano, 2011
- CARDARELLI, *Le banche dati pubbliche: una definizione*, in *Dir. inf.* 2002
- CAROSONE, *L'opera dell'ingegno creata nel rapporto di lavoro autonomo e subordinato*, 2 ed., Giuffrè, Milano, 1999
- CATE and MAYER SCHONBERGER, *Tomorrow 's privacy notice and consent in a world of big data*, in *international data privacy law review*, 2013,
- CAVOUKIAN and ELEMAM, *Dispelling the myths surrounding de-identification: Anonymization remains a strong tool for protecting privacy*, IPC, June 2011
- CHIAROLLA, *Diritto d'autore: La prima volta delle banche dati in Italia*, in *Foro it*. 1990, I
- CODIGLIONE, *I dati personali come corrispettivo della fruizione di un servizio di comunicazione elettronica e la "consumerizzazione" della privacy*, in *Dir. Inf.* 2017, n. 2, 418 ss..
- COGO, nota a CGCE, 9 novembre 2004, in *AIDA* 2005
- COGO, *I contratti di diritto d'autore nell'era digitale*, Giappichelli, Torino, 2010
- CONFORTI, *Diritto internazionale*, VIII ed., ES, Napoli, 2010
- D'ACQUISTO e NALDI, *Big Data e Privacy By Design, Anonimizzazione Pseudonimizzazione Sicurezza*, Giappichelli, Torino, 2017
- DAVISON, *The legal protection of Databases*, Cambridge University Press, Londra, 2003
- DE ANGELIS, *Informazioni segrete e diritti di proprietà industriale non titolati*, in SCUFFI e FRANZOSI (a cura di), *Diritto industriale italiano*, vol. I, CEDAM, 2014, Padova
- DE BIASE, *Il mercato dei dati personali tra portabilità e concorrenza*, in *Il Sole 24 ore online* 2018
- DE MEO, *Autodeterminazione e consenso nella profilazione dei dati personali*, in *Dir. Inf.* 2013, n. 3, 587 ss..
- VAL DE SANCTIS, *Il contratto di edizione*, Giuffrè, Milano, 1984

- V.M. DE SANCTIS, *Il carattere creativo delle opere dell'ingegno*, Giuffrè, Milano, 1971
- V.M. DE SANCTIS, *Il diritto d'autore*, Giuffrè, Milano, 2012
- DI CATALDO, *Banche dati e diritto sui generis: la fattispecie costitutiva*, in *AIDA* 1997, 21
- DI PORTO, *Scambi di informazione e abusi di posizione dominante: una rilettura degli "Abusi Informativi" e dei relativi rimedi*, in *Concorrenza e Mercato* 2014
- DREXL, *Designing competitive markets. For industrial data, between propertisation and access,*in *Max Planck Institute for innovation and competition research paper*, 2016
- FALCE, *Profili pro- concorrenziali dell'istituo brevettuale*, Giuffrè, Milano, 2008
- FINOCCHIARO, *Il contratto nell'era dell'intelligenza artificiale*, in *Riv. trim. dir e proc. civ*. 2018
- FINOCCHIARO, *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, in FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017
- FINOCCHIARO, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*, in RESTA e ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali, dai "Safe Harbour principles" al "Privacy Shields"*, RomaTrE Press, Roma, 2017
- FINOCCHIARO, *Privacy e protezione dei dati personali, Disciplina e strumenti operativi*, Zanichelli, Bologna, 2012, 1 ss..
- FLORIDIA, *Il riassetto della proprietà industriale*, Giappichelli, Torino, 2006
- FRA, CED e COE, *Manuale sul diritto europeo in materia di protezione dei dati*, Belgio, 2014.
- FRANZOSI, *L'oggetto del brevetto*, in SCUFFI e FRANZOSI (a cura di), *Diritto industriale italiano*, vol. I, CEDAM, Padova, 2014
- FRASSI, *Creazioni utili e diritto d'autore*, Giuffrè, Milano, 1997
- GAETA, *La protezione dei dati personali nell'Internet of Things: l'esempio dei veicoli autonomi*, in *Dir. inf.* 2018 GERMANI e FEROLA, *Il wearable computing e gli orizzonti futuri della privacy*, in *Dir. inf.* 2014
- GALGANO, *v. Possesso*, *Diritto civile*, in *Enc. Giur. Trecc.*, Roma, 1990, XXIV

- GAMBARO, *La proprietà, Beni, proprietà e possesso*, in *Trattato di diritto Privato*, IUDICA e ZATTI (a cura di), Giuffrè, Milano, 2017
- GHIDINI, *Profili evolutivi del diritto industriale*, Giuffrè, Milano, 2008
- GRAZZINI, *L'economia della conoscenza oltre il capitalismo. Crisi dei ceti medi e rivoluzione lunga*, Torino, Codice, 2008;
- GRECO e VERCELLONE, *I diritti sulle opere dell'ingegno*, UTET, Torino, 1974
- GIOV. GUGLIELMETTI, *La tutela delle banche dati con diritto sui generis nella direttiva 96/9/CE*, in *Contratto e impresa Europa* 1997
- GIOV. GUGLIELMETTI, *Commento all'art. 5, in Aa.Vv., Attuazione della direttiva 96/9/CE relativa alla tutela giuridica delle banche dati*, a cura di AUTERI, in *NLCC* 2003
- GIOV. GUGLIELMETTI, *La tutela del segreto*, in *Le nuove frontiere del diritto dei brevetti*, Torino, 2003
- HILDEBRANDT and GUTWIRTH, *Profiling the European Citizen, Cross-Disciplinary Perspectives*, Springer, 2008.
- HUBMANN, *Urheber-und Verlagsrecht: ein studienbuch*, Munchen Juristische Kurz-Lehrbücher, 1959
- HUGHENHOLTZ, *Copyright and freedom of expression in Europe*, in DREYFUSS - FIRST – ZIMMERMAN (a cura di), *Innovation Policy in an Information age*, Oxford, 2000
- IAMICELI, *Liceità, correttezza, finalità del trattamento dei dati personali*, in *Diritto alla riservatezza e circolazione dei dati personali*, (a cura di) PARDOLESI, I, Giuffrè, Milano, 2003
- INTROVIGNE, *Computer data bases e proprietà intellettuale in diritto comparato*, in ALPA, *La tutela giuridica del software*, Giuffrè, Milano, 1984
- LEISTNER, *The legal protection of telephone directories relating to the new database maker's right*, in *IIC* 2000
- MAGGIOLINO e MONTAGNANI, *Marketing e diritto*, Egea, Milano, 2009
- MAGGIOLINO, *I big data e il diritto antitrust*, Egea, Milano, 2018
- MAGLIO, *Il valore economico dei dati personali: spunti per un'analisi economica della data protection*, in MAGLIO POLLINI e TIGLI (a cura di),

Manuale di diritto alla protezione dei dati personali, La privacy dopo il Regolamento UE 2016/679, Maggioli Editore, Milano, 2017

- MANCINI, *La protezione dei dati personali*, in MEGALE, *ICT e diritto nella società dell'informazione*, Giappichelli, Torino, 2017
- MANTELERO e VACIAGO, *The "Dark side" of Big Data, Private and Public Interaction in Social Surveillance*, in *Cri 6/2013*
- MANTELERO, *Big data: I rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Dir. inf.* 2012
- MANTELERO, *Personal data for decisional purposes in the age of analytics: from an individual to a collective dimension of data protection*, in *Computer law and security review*, 2016
- MANTELERO, *Rilevanza e tutela della dimensione collettiva della protezione dei dati personali*, in *Contratto e impresa/Europa*, 2015
- MATTEI, *I diritti reali*, 2, *La proprietà*, in *Trattato di diritto civile*, SACCO (a cura di), 2 ed., Utet, Torino, 2015
- MATTIOLI, *Disclosing Big Data*, Maurer Faculty Paper 2014 disponibile al seguente indirizzo: www.repositorylaw.indiana.edu/facpub/1480
- MAYER SCHOENBERGER and PADOVA, *Regime change? Enabling big data through europe's new data protection regulation*, in *17 Colum. Sci&Tech. L. Rev. 41(2016)*,http://www.stlr.org/cite.cgi?volume=17&article=SchonbergerPadova**,**
- MELI, *Le utilizzazioni libere nella direttiva 96/9/CEE sulla protezione giuridica delle banche dati*, in *AIDA* 1997
- MELI, *Rifiuto di contrattare e tutela della concorrenza nel diritto antitrust comunitario*, Giappichelli, Torino, 2003
- MENEGHETTI, *Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali*, in FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e la protezione dei dati personali*, Zanichelli, Bologna, 2017
- MORELATO, *Anonimato e protezione dei dati personali*, in *Diritto all'anonimato*, (a cura di) FINOCCHIARO, CEDAM, Padova, 2008
- MORO VISCONTI, *Internet delle cose networks e plus valore di connettività*, in *IDI* 2016

- MORO VISCONTI, *Valutazione dei big data e impatto su innovazione e digital branding*, in *IDI* 2016
- NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, CEDAM, Padova, 2006
- OHM, *Broken promises of privacy: responding to the surprising failure of anonymization*, *Ucla Law Review*, 2010
- OPPO, *Creazione intellettuale, creazione industriale e diritti di utilizzazione economica*, in *Riv. dir. civ.*, 1969
- OREFICE, *I big data, Regole e Concorrenza*, in *Politica del diritto* 2016, fasc. 4
- OTTOLIA, *Big data e innovazione computazionale*, Giappichelli, Torino, 2018
- OTTOLIA, *L'utilizzo computazionale dell'opera dell'ingegno*, in *AIDA* 2014
- OTTOLIA, *Proprietà intellettuale e trattamento dei dati personali: riflessioni su privacy " per il sistema" e "nel sistema"*, in *AIDA* 2010
- PAGALLO, *La tutela della privacy negli Stati Uniti d'America e in Europa*, Giuffrè, Milano, 2008
- PAGALLO and BASSI, *Open data protection: Challenges, perspectives, and tools, in Digital enlightenment year book 2013: the value of personal data*, a cura di HILDEBRANDT, O'HARA, WAIDNER, IOS press, Amsterdam, 2013
- PAGALLO, *Il diritto nell'età dell'informazione: il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti*, Giappichelli, Torino, 2014
- PARDOLESI. *Banche dati al guado*, in *Foro it.* 1987, IV
- PARDOLESI, *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, in PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Giuffrè, Milano, 2003
- PARDOLESI e GRANIERI, *Licenza obbligatoria ed essential facilities nell'antitrust comunitario*, in *Riv. dir. ind*. 2004
- PELINO, *I diritti dell'interessato*, in *Il Regolamento privacy europeo*, (a cura di) BOLOGNINI, PELINO e BISTOLFI, Giuffrè, Milano, 2016
- PELINO, *Le tutele e il danno risarcibile*, in *Il Regolamento privacy europeo*, (a cura di) BOLOGNINI, PELINO e BISTOLFI, Giuffrè, Milano, 2016

- PINO, *L'identità personale degli enti collettivi*, in *Libera circolazione e protezione dei dati personali*, (a cura di) PANETTA, vol. I, Giuffrè, Milano, 2006
- PIRAINO, *La liceità e la correttezza*, in *La Libera circolazione e la protezione dei dati personali*, (a cura di) PANETTA I, vol. I, Giuffrè, Milano, 2006
- PIZZETTI, *Lezione al Politecnico di Torino del 24 novembre 2017*
- PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali, dalla direttiva 95/46 al nuovo regolamento europeo*, Giappichelli, Torino, 2016
- POLONETSKY, TENE, KELSEY, *Shades of Gray: Seeing the full spectrum of pratical data deidentification*, in *Santa Clara law review* 2016
- RATTI, *Il regime sanzionatorio previsto dal regolamento per l'illecito trattamento dei dati personali*, in FINOCCHIARO (a cura di), cit. 595 ss.
- RESTA, *La tutela dei dati personali dopo il "decreto sviluppo"*, in GAROFOLI e TREU, *Il libro dell'anno del diritto 2012*, Enciclopedia Treccani, Roma, 2012
- RICCI, *I diritti dell'interessato*, in *Il nuovo Regolamento europeo sulla privacy e la protezione dei dati personali*, (a cura di) G. FINOCCHIARO, Zanichelli, Bologna, 2017
- RICOLFI, *Diritto di autore ed abuso di posizione dominante*, in *Riv. dir. ind.* 2001, I
- RICOLFI, *Il diritto d'autore*, in Trattato Cottino, vol. II, *Diritto industriale*, CEDAM, Padova, 2001
- RICOLFI, *Iot and the ages of antitrust*, in *Concorrenza e mercato* 2017
- RODOTÀ, *La "privacy" tra individuo e collettività*, in *Politica del diritto* 1974
- RUSSO, *L'interpretazione dei testi normativi comunitari*, Giuffrè, Milano, 2008, 235
- SACCO e CATERINA, *Il possesso*, in *Trattato Cicu-Messineo*, Milano, III ed., 2014;
- SAPPA, *nota a Trib. Roma, ord. 5 giugno 2008*, in *AIDA* 2010, 692
- SARTI, *Proprietà intellettuale, interessi protetti e diritto antitrust*, in *Riv. dir. ind*. 2002, I
- SCHWARTZ, *Data protection Law and the ethical use of analytics*, CIPL, in http://www.huntonfiles.com/files/webupload/cipl_ethical_undperinnings_of_analytics_paper.pdf, 2010

- SENOR, *La reticenza italiana sul legittimo interesse del titolare quale base giuridica del trattamento di dati personali*, in www.filodiritto.com, 2018
- SPEDICATO, *Gradiente creativo dell'opera dell'ingegno e proporzionalità della tutela*, in *IDA* 2012
- SPOLIDORO, *Il contenuto del diritto connesso sulle banche di dati*, in *AIDA* 1997, 45 ss.
- STIX HACKL, Concl. Avv. Gen. CGCE, 8 giugno 2004, C-444/02, , in www.curia.eu
- STOLFI, *Il diritto d'autore,* vol. I, SEL, Milano, 1932
- TENE&POLONETSKY, *Big Data for All: Privacy and User Control in the Age of Analytics*, in *Northwestern Journal of Technology and Intellectual Property*, 2013
- TODINO, *sub. art. 102 TFUE*, in L.C. UBERTAZZI, *Commentario breve alle leggi sulla proprietà intellettuale e concorrenza*, 5 ed., CEDAM, Padova, 2012
- L. C. UBERTAZZI, *Raccolte elettroniche di dati e diritto d'autore: prime riflessioni*, in *Foro it.* 1984, V
- L.C. UBERTAZZI, *Profili soggettivi del brevetto*, Giuffrè, Milano, 1985
- L.C. UBERTAZZI, *L'appartenenza dei risultati creativi dei dipendenti*, in *AIDA* 2010
- L.C. UBERTAZZI, *Introduzione*, in *La proprietà intellettuale*, (a cura di) L. C. UBERTAZZI, Giappichelli, Torino, 2011
- L.C. UBERTAZZI, *Numerus clausus dei diritti esclusivi di proprietà intellettuale?*, in *JURISMAT*, Portimào, n. 4, 2014
- L.C. UBERTAZZI, *Proprietà intellettuale e privacy*, in *AIDA* 2014
- T.M. UBERTAZZI, *Il diritto alla privacy, natura e funzione giuridiche*, CEDAM, Padova, 2004
- VANZETTI e DI CATALDO, Manuale di diritto industriale, VII ed., Giuffrè, Milano, 2012
- Vice Commissario REDING, "P*ersonal data is the currency of today's digital market*", in *The EU Data Protection Reform* 2012: *Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age* – Innovation Conference Digital, Life, Design, Monaco, 22 gennaio 2012

- W.R. CORNISH e D. LLEWELYN, *Intellectual property*, 6 ed., Sweet & Maxwell, Londra, 2007
- WARREN and BRANDEIS, *The right of privacy*, in *Harv. L. rev.*, 1890
- WIEBE, *Protection of industrial data- a new property right for the digital economy*, *Journal of Intellectual Property Law & Practice*, Volume 12, 2017
- WILLICOX, *Definitions of statitics*, in *Review of the international statistical institute*, vol. 3, no. 4 (1936)
- ZECH, *Data as tradeable commodity*, in *European contract law and the digital single market*, DE FRANCESCHI (a cura di), Intersentia, 2016
- ZOPPINI, *I diritti della personalità delle persone giuridiche (e dei gruppi organizzati)*, in *Riv. dir. civ.*, I, 2002

Giurisprudenza

- CEDU, 10 gennaio 2013, Donald et autres c. France
- CEDU, 16 febbraio 2000, causa Amann/Switzerland
- CEDU, 24 febbraio 1994, Casado Coca c. Spagna

- CGUE, 6 ottobre 2015, C-362/14, Schrems contro Data Protection Commissioner, in www.curia.europa.eu
- CGUE, 16 luglio 2015, C-170/2013, in www.curia.europa.eu
- CGUE, C-131/12, Google v. AgenciaEspanola de Protecciòn de Datos ECLI, in curia.europa.eu
- CGUE, 13 maggio 2014, C-131/12
- CGUE, 19 dicembre 2012, C- 202/12, in *Diritto comunitario online* 2014
- CGUE, 1 marzo 2012, C-604/10, in www.curia.europa.eu
- CGUE, 24 novembre 2011, C-70/10, in *AIDA* 2012, *1461*
- CGUE, 5 maggio 2011, Deutsche Telekom AG c. Germania, C-543/09, in curia.europa.eu.
- CGUE, 16 luglio 2009, C-5/2008, in *AIDA* 2009, *1261*
- CGUE, 5 marzo 2009, C-545/07, in *www.curia.eu*
- CGCE, 9 ottobre 2008, C- 304/07, in *www.curia.eu*
- CGCE, 29 gennaio 2008, C-275/06, in *AIDA* 2008, *1190*

- CGCE, 9 novembre 2004, C-203/02, in www.curia.europa.eu
- CGCE, 9 novembre 2004, C-444/02, in *AIDA* 2005, *1016*
- CGCE, 29 aprile 2004, C- 418/01, in *Riv. dir. ind.* 2004, 314 ss..
- CGCE, 8 giugno 2004, C- 444/02, in www.curia.europa.eu
- CGCE, Fixture Marketing, 9 novembre 2004, C-444/02, in www.curia.europa.eu.
- CGCE, 6 novembre 2003, C- 101/2001, Lindqvist
- CGCE, 26 novembre 1998, C-7/97, in www.curia.europa.eu.
- CGCE, C-200/96, MetronomeMusik v. Music point Hokamp
- CGCE, AKZO Chemie BV v. Commissione Europea, C- 62/86, 3 luglio 1991, www.curia.europa.eu
- CGCE, 12 dicembre 1985, Krohn c. Balm, C-165/84, in www.curia.eu.
- CGCE, NV Nederlandsche Banden Industrie Michelin v. Commissione Europea, C- 322/81, 9 novembre 1983, www.curia.europa.eu
- CGCE 13 febbraio 1979, C-85/76, Hoffmann-La Roche, in *www.curia.eu.*
- CGCE 14 febbraio 1978, C-27/76, United Brands, in *www.curia.eu*.

- Trib. UE, T-321/05, 1 luglio 2010, www.curia.europa.eu
- Trib. di primo grado CE 6 giugno 2002, T-342/99, Airtours, in www.curia.ue.
- Trib. CE, Irish sugar plc v. Commissione Europea, T-228/97, 7 ottobre 1999, www.curia.europa.eu
- Trib. di primo grado CE, 12 giugno 1997, T-504/93, in *AIDA* 1998, 503.

- Cass., 1 luglio 2004 n. 12089, in *AIDA* 2005, *1019*;
- Cass., 13 dicembre 1999, in *AIDA* 2000, *659*
- Cass. 2 dicembre 1993, n. 11953, in *Riv. dir. ind.* 1994, II, 157 ss.
- Cass., 19 luglio 1990, n. 7397, in *Giur. it. Mass.* 1990, 867
- Cass., 27 febbraio 1985, n. 1699, in *Giur. Comm.* 1986, II, 821
- Cass., 27 maggio 1975, n. 2129, in *Mass. Giur. It.*, 1975,594
- Cass., 14 dicembre 1959, n. 3544, in *Foro it.* 1960, I, 54

- Trib. Milano, 8 settembre 2014, in *AIDA* 2015, *1691*
- Trib. Milano, 16 febbraio 2012, in *AIDA* 2013, Rep. I. 13bis.
- Trib. Bologna, 4 luglio 2008, in *GADI* 2008, 5298, 977
- Trib. Venezia, 19 ottobre 2007, in *AIDA* 2009, *1270*
- Trib. Firenze, 18 settembre 2006, in *AIDA* 2008, *1210*.
- Trib. Bologna ord. 17 gennaio 2006, in *AIDA* 2008, *1205*
- Trib. Roma, ord. 10 febbraio 2005, *SPI* 2005, I, 291
- Trib. Catania, 24 novembre 2004, in *AIDA* 2006, *1077*
- Trib. Milano, 31 marzo 2004, *GADI* 2004, 4734,979.
- Trib. Catania, 27 agosto 2001, in *IDI* 2002, 97 ss.
- Trib. Monza ord. 15 maggio 2000, in *AIDA* 2001, *765*
- Trib. Torino, ord. 16 dicembre 1997, in *AIDA* 1998, 550
- Trib. Pavia, ord. 22 marzo 1997, in *AIDA* 1998, 526
- Trib. Milano, 29 gennaio 1997, in AIDA 1997, *489*
- App. Bologna, 19 giugno 1995, in GADI 1996, 3426, 355
- Trib. Firenze, 16 febbraio 1994, in *AIDA* 1995, *318*
- Trib. Milano, 28 giugno 1993, in *Foro it. online*.
- App. Milano, 10 novembre 1992, in GADI 1992, 2859, 862
- App. Milano, 22 settembre 1992, in GADI 1993, 2910, 201
- Pret. Monza, 4 dicembre 1991, in AIDA 1992, *77*
- Pret. Roma, 14 dicembre 1989, in *Dir. inf.* 1990, 219
- Trib. Bari, 17 giugno 1974, in *IDA* 1975, 93;
- Pret. Roma, 22 febbraio 1952, in *Rep. Foro it*. 1952, v. *Diritto d'autore*, n. 94.
- App. Torino, 16 maggio 1944, in Giur. tor. 1944, 171.
- App. Venezia, 24 febbraio 1933, in IDA 1933, 339 ss.

Altre fonti

- Commissione Europea, Comunicazione del 19 settembre 2017, "Un quadro per il libero flusso dei dati non personali in Europa"

- Commissione Europea, “Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a un quadro applicabile alla libera circolazione dei dati non personali nell’Unione Europea”, 13 settembre 2017
- Commissione Europea, Comunicazione del 27 giugno 2017.
- Commissione Europea, 10 gennaio 2017, *Comunicazione: costruire un’economia dei dati europea*, 9;
- Commissione Europea, Evaluation of the implementation of the data protection directive, 2012
- Commissione Europea, Decisione del 15 novembre 2011, relativa a un procedimento a norma dell’art. 102 TFUE e 54 dell’Accordo SEE, Caso COMP/39.592 – Standard & Poor’s
- Commissione Europea, decisione del 22 giugno 2011, Telekomunikacja Plska, C(2011) 4378

- EDPS, Opinion 7/2015, Meeting the challenges of big data
- ENISA(European union agency for network and information security)G. D’ACQUISTO, DOMINGO FERRER, PANAYIOTIS KIKIRAS, VINCENCTORRA, YVES ALEXANDRE DE MONTOJOYE, ATHENA BOURKA, *Privacy by design in big data , an overview of privacy enhancing technologies in the era of big data analytics*, December 2015, in www.enisa.europa.eu
- *European Data Market Study*, *Second Interim Report*, Giugno 2016, in *www.datalandscape.eu/study-reports*

- Comitato dei ministri, 23 novembre 2010, Raccomandazione sulla protezione delle persone fisiche con riguardo al trattamento automatizzato di dati personali nel contesto dell’attività di profilazione CM/Rec(2010)13

- WP29, *Position Paper on the derogations from the obligation to maintain record of processing activities pursuant to Article 30 GDPR* , aprile 2018

- WP29, *Guidelines on personal data breach notification under Regulation 2016/679*, 6 febbraio 2018

- WP29, Guidelines on consent, 28 novembre 2017
- WP29, *Guidelines on Data Protection Officers ('DPOs')*).
- WP29, *Linee guida in materia di valutazione di impatto sulla protezione dei dati e determinazione della possibilità che il trattamento possa presentare un rischio elevato ai fini del regolamento* (UE) 2016/679, 4 ottobre 2017.
- WP29, *Guidelines on Automated individual decision – making and Profiling for the purposes of Regulation 2016/679*, 3 ottobre 2017
- WP29, 5 aprile 2017, "*Linee guida sul diritto alla portabilità dei dati*"
- WP29, *Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU*, 16 settembre 2014, 1 ss..
- WP29, Opinion 8/2014 on the Recent Developments on the Internet of Things
- WP29 n. 6/2014, Opinion on legitimate interest
- WP29 parere n. 5 del 2014 sull'anonimizzazione
- WP29, 19 aprile 2013, *Documento esplicativo sulle norme vincolanti d'impresa per gli incaricati del trattamento*
- WP29, Opinion 02/2013, on apps on smart devices
- WP29, Opinion 03/2013 *on purpose limitation*
- WP29, parere n. 15/2011, sulla definizione di consenso
- WP29, parere n. 3 del 2010, sul principio di responsabilità
- WP29, parere 4/2007 sul concetto di dato personale

- Garante per la protezione dei dati personali, *Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali*, in www.garanteprivacy.it/regolamentoue/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali.
- Garante per la protezione dei dati personali, Provvedimento 30 giugno 2016, *"Conservazione dei dati personali riguardanti la clientela per attività di profilazione e di marketing".*
- Garante per la protezione dei dati personali, Provvedimento 2 dicembre 2015, n. 632

- Garante per la protezione dei dati personali, Linee guida in materia di trattamento di dati personali per profilazione on line, 19 marzo 2015, doc. web n. 3881513
- Garante per la protezione dei dati personali, *Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie*, 8 maggio 2014, doc. web. n. 3118884.
- Garante per la protezione dei dati personali, Provvedimento 7 novembre 2013, n. 500
- Garante per la protezione dei dati personali, Provvedimento 30 maggio 2013, n. 263
- Garante per la protezione dei dati personali, Provvedimento 24 aprile 2013, n. 219
- Garante per la protezione dei dati personali, Provv. 20 settembre 2012, n. 262 [doc. web n. 2094932].
- Garante per la protezione dei dati personali, Provv. 15 luglio 2010, Raccolta di dati via internet per finalità promozionali, doc. web 1741998
- Garante per la protezione dei dati personali, Provv. del 12 marzo 2009
- Garante per la protezione dei dati personali, parere n. 1/2008, 9 ss.
- Garante per la protezione dei dati personali, Provv. 15 novembre 2007, Trattamento dei dati personali e fidelizzazione della clientela, doc. web n. 1466898
- Garante per la protezione dei dati personali, Provv. 24 febbraio 2005, Fidelity card e garanzie per i consumatori, doc. web n. 1103045
- Garante per la protezione dei dati personali, Provv. 3 febbraio 2005, Tv interattiva, doc. web n. 1109503

- ICO, *"Gdpr guidance legitimate interests sample lia template*".
- ICO, *Big data and data protection*, 2014
- ICO, *Legitimate interests guidance*, in https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

- AGCM, A426 – Telecom Italia – Gare affidamento servizi telefonia fissa e connettività IP, dec. n. 23677, 19 giugno 2012, in Boll. n. 25/2012
- AGCM, A422 – Sky Italia/Auditel, dec. n. 23112, del 14 dicembre 2011, in Boll. n. 50, 2011
- AGCM, A424 – Epolis/ Audipress, dec. n. 22320, del 20 aprile 2011, in Boll. n. 16, 2011.
- AGCM, A410 – Exergia/Enel – Servizio di salvaguardia, dec. n. 20549, 10 dicembre 2009, in Boll. n. 49/2009
- AGCM, Parere 31 ottobre 1996 n. 4381

- (voce) Statistica, in Vocabolario Garzanti online.
- (voce)Statistica, in Vocabolario Treccani online