UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Università degli Studi di Padova

Dipartimento di Studi Linguistici e Letterari

Dipartimento di Scienze Politiche, Giuridiche ed Internazionali

Corso di Laurea Magistrale in
Strategie di Comunicazione
Classe LM-92

Tesi di Laurea

Il dato personale come corrispettivo in Internet: il problema del consenso

Relatore
Prof. Nicola Brutti

Laureando
Giulia De Bortoli
n° matr.1241484 / LMSGC

Anno Accademico 2021 / 2022

ABSTRACT

Questa tesi analizza il tema del trattamento dei dati personali ed in particolare il ruolo e l'importanza del consenso dell'interessato.

Data l'importanza che la tecnologia e Internet stanno assumendo nella nostra quotidianità, ritengo importante promuovere una consapevolezza riguardo i nostri comportamenti *online* e circa la rilevanza del consenso espresso ogniqualvolta ci si trova a navigare in rete.

Il seguente lavoro, mediante uno studio e un'analisi di diverse fonti giuridiche, manuali ed articoli competenti mostra come la questione del consenso sia collegata ad ogni aspetto della realtà online, dal trattamento dei dati personali ai *cookie*, e rivela come durante il corso degli anni i requisiti siano diventati sempre più inflessibili, con lo scopo di tutelare gli utenti ed offrire la massima protezione dei dati personali.

Inizialmente viene offerta una panoramica generale riguardo l'economia cosiddetta *data driven*, vale a dire guidata dai dati, in cui i dati rappresentano una fonte di ricchezza considerevole, paragonati a delle materie prime che devono essere elaborate per estrarne il valore. Nell'economia dei dati, innovative tecnologie permettono di raccogliere e trattare grandi quantità di dati, che consentono di classificare gli utenti in determinati gruppi con esigenze ed interessi differenti, che saranno oggetto di messaggi di marketing diversificati.

Attraverso lo studio del Regolamento Generale sulla Protezione dei dati (GDPR), la fonte normativa ancora oggi più rilevante in tema di dati personali, vengono offerte alcune definizioni dei principali elementi, come quella di dati personali e dati non personali, di cosa significa trattamento, chi sono le figure del titolare, dell'interessato e del destinatario.

Viene svolto un breve riferimento anche ai big data, le tecnologie che permettono di raccogliere grandi masse di dati, a piattaforme come i social network, a motori di ricerca e servizi di comunicazione digitale, principali fonti di dati.

Nell'economia dei dati si parla di dati personali come controprestazione, dato che gli utenti spesso usufruiscono di un servizio o di un contenuto digitale *online* che

apparentemente sono gratuiti, ma in realtà la “remunerazione” del fornitore del servizio è proprio la messa a disposizione dei nostri dati personali. La raccolta e il trattamento dei dati, se da una parte potrebbe generare dei vantaggi, come lo sviluppo di mercati più competitivi o miglioramenti nell’amministrazione pubblica, comporta anche dei rischi per la privacy degli interessati, in particolare causati da forme illegittime di intrusione nella sfera privata.

Proseguendo, vengono esaminati i principi di liceità, correttezza e trasparenza, di limitazione delle finalità e della conservazione, di necessità e minimizzazione, di esattezza, integrità e di responsabilizzazione, caratterizzanti il trattamento dei dati personali secondo il GDPR. Sempre il GDPR fornisce la definizione di consenso, come «*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*», oltre a stabilire i requisiti che esso deve possedere per essere considerato lecito.

Viene inoltre esaminata l’evoluzione normativa in ambito europeo che ha portato alla stesura del GDPR, con alcuni cenni al contesto internazionale. I provvedimenti più rilevanti del Consiglio d’Europa sono stati la Convenzione europea dei diritti dell’uomo del 1950, la Convenzione 108/1981 “*sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale”* del 1981, la Convenzione di Budapest “*sulla criminalità informatica*”, firmata nel 2001.

Dall’altro lato, i provvedimenti più importanti dell’Unione Europea possono riassumersi con: il Trattato di Lisbona, che comprende la Carta dei diritti dell’Unione proclamata a Nizza; la Direttiva 95/46/CE “*relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché la libera circolazione dei dati”*, ratificata nel 1995; la Direttiva 2002/58/CE *“relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche”* adottata nel 2002; la Direttiva 2009/136/CE *“recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al*

trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori" adottata nel 2009. Ed infine il Regolamento generale sulla protezione dei dati.

Viene poi affrontata la distinzione tra due tesi contrapposte, vale a dire la tesi che sostiene la natura non negoziale del consenso al trattamento dei dati personali, intendendolo esclusivamente come un diritto della personalità, un atto autorizzatorio che tutela la persona dell'invasione della sfera personale; dall'altra parte vi è chi sostiene che il consenso è una manifestazione negoziale di volontà, in cui i dati assumono la natura di beni cedibili, trasferibili e scambiabili. Viene ripresa inoltre la Direttiva UE 2019/770 riguardante i contratti di fornitura di contenuti e servizi digitali, la quale ha generato alcune perplessità e problemi di coordinamento con il GDPR in quanto ha inizialmente qualificato il trasferimento dei dati personali come corrispettivo nei contratti di fornitura e servizi digitali, come un'obbligazione paragonabile al pagamento di un prezzo. Attraverso alcune sentenze della Corte di Cassazione e dell'analisi di confronto tra la Direttiva e il GDPR, in particolare con la questione della revoca del consenso, si giunge però alla conclusione che non si può definire "controprestazione" l'attività del consumatore che presta il consenso al trattamento dei propri dati personali per usufruire del servizio o accedere al contenuto digitale.

Difatti l'obiettivo della Direttiva UE 2019/770 non è quello di sdoganare il pagamento tramite i dati personali ma è quello di allargare le tutele del consumatore comprendendo anche questo tipo di operazioni che ormai sono molto frequenti nel mondo digitale.

In aggiunta, viene affrontato il tema dei *cookie*, vale a dire *file* di testo che il fornitore del sito installa nel dispositivo dell'utente che ha navigato sul suo sito e al quale potrà accedere nuovamente durante un'altra navigazione sul medesimo sito da parte dello stesso utente. Essi sono divisi in due macrocategorie, i *cookie* tecnici installati direttamente dal titolare o dal gestore del sito e hanno esclusivamente funzione strumentale, vale a dire quella di migliorare la navigazione *online,*

e i *cookie* di profilazione possono essere installati dal gestore del sito oppure da soggetti terzi, cioè grandi società tecnologiche; essi hanno lo scopo di verificare e rielaborare tramite l'utilizzo di algoritmi di calcolo, le abitudini, gli interessi e le ricerche operate dall'utente, con l'intento di poter inviare messaggi pubblicitari.

Il presidio di tutela offerto dallo strumento del consenso dell'interessato, che deve essere libero, specifico, informato e inequivocabile, si estende anche a tutte le tecnologie che, come i *cookie*, permettono l'accesso e la raccolta di dati personali durante la sola navigazione *online.*

Viene poi una breve analisi sulla declinazione assunta dai requisiti fondamentali del consenso al trattamento di dati personali che viene effettuato *online*, tramite l'utilizzo di *cookie* di profilazione; l'attenzione viene posta soprattutto sui requisiti di specificità ed inequivocabilità che sono compresi nel modo di manifestazione della volontà, dunque fanno riferimento all'esternazione del consenso, ed i requisiti di libertà ed informazione che invece caratterizzano il cd. consenso interno. In particolare, si fa riferimento all'informativa breve, cioè il *cookie banner*, e all'informativa estesa, e ai requisiti che rendono lecito il trattamento mediante *cookie*.

L'esame dei requisiti e della liceità del trattamento viene effettuato attraverso lo studio di un'importante sentenza della Corte di Giustizia dell'Unione Europea, che ha decretato la non ammissibilità di un'attività di memorizzazione dati e quindi di accesso a informazioni personali già archiviati nel dispositivo di un utente esercitata dal gestore del sito tramite i *cookie* attraverso una casella preselezionata che l'utente, in caso di contrarietà a prestare il consenso, avrebbe dovuto deselezionare.

Infine, la conclusione si sviluppa innanzitutto sul sistema di gestione di qualità dati, che permette alle aziende che operano nel digitale di essere più affidabili e competitive. È di fondamentale importanza per tutte le attività produttive che i dati raccolti siano validi; vale a dire esatti e riconducibili ad una fonte verificabile; è importante dunque trattare dati di alta qualità, adatti per gli obiettivi di business.

Tratta inoltre delle nuove sfide apportate dall'economia dei dati: la tecnologia, infatti, dovrebbe consentire una più libera circolazione dei dati personali

all'interno dell'UE, e il loro trasferimento verso paesi terzi ed organizzazioni internazionali, ma dovrebbe assicurare anche un elevato livello di protezione dei dati personali tramite le *best practices*.

Per questo è importante aggiornare gli strumenti di protezione dei dati personali, che oltre al rispetto dei requisiti per la richiesta di consenso, sono la previsione di regole di trattamento, come limiti o divieti per alcune categorie di trattamento, o maggiori garanzie di anonimizzazione dei dati e regole di tipo tecnico interne al trattamento, come ad esempio la privacy by design e la privacy by default.

Infine, viene esaminato il nuovo Regolamento UE ePrivacy, analizzando le conseguenze sulle imprese operanti nel settore digitale. Viene presa in considerazione la necessità di adottare un Regolamento per sostituire la direttiva ePrivacy del 2002: la direttiva regolava la riservatezza in rete e nelle comunicazioni elettroniche ma gli sviluppi tecnologici degli ultimi vent'anni hanno fatto sì che essa non fosse più sufficiente. La normativa, infatti, non era più adatta a proteggere gli utenti dai rischi attuali.

Il Regolamento ha lo scopo di aumentare la fiducia dei cittadini nei confronti dei servizi digitali, garantendo la massima riservatezza per i dati personali nelle comunicazioni elettroniche.

Trattando diversi temi riguardanti la protezione dei dati personali, questa tesi ha illustrato quante insidie si possono nascondere dietro la realtà online, mostrando quanto sia importante essere consapevoli delle azioni che si compiono e di cosa significa essere pienamente informati sulle conseguenze della prestazione del consenso al trattamento dei nostri dati personali.

INDICE

INTRODUZIONE

Lo sviluppo delle nuove tecnologie ha comportato importanti trasformazioni riguardanti le abitudini quotidiane degli individui, negli andamenti dei mercati e nei diritti degli individui.

È particolarmente rilevante, perciò, il tema della tutela dei dati personali in un mondo come quello di oggi, pervaso dallo sviluppo e della diffusione continua di nuove tecniche in grado di elaborare grandi masse di dati.

I dati personali sono diventati la nuova materia prima, di un'economia cosiddetta *data driven* ed è per questo motivo che la protezione dei dati deve diventare un obiettivo da perseguire con sempre maggiore impegno, in modo da costituire un quadro normativo mondiale armonizzato, in cui i dati possono circolare liberamente e la tutela degli utenti è sempre garantita.

In particolare, un ruolo centrale nella protezione dei dati personali è assunto dal consenso prestato dall'interessato.

Il seguente lavoro esamina quindi principalmente la tematica del consenso prestato per il trattamento dei dati personali; innanzitutto vengono esaminate alcune definizioni riguardanti il campo dei dati personali, per poi proseguire con l'esposizione dell'evoluzione della normativa internazionale, europea e nazionale, concentrandosi maggiormente sul Regolamento generale sulla protezione dei dati elaborato dall'Unione Europea. Viene esaminata poi la distinzione tra il consenso con natura negoziale e consenso come atto autorizzatorio, esaminando varie tesi al riguardo che sostengono l'una o l'altra natura del consenso ed integrandole con alcune importanti sentenze della Corte di Cassazione. L'atto del consenso viene esaminato in tutti i suoi termini, ponendo maggiore attenzione sui requisiti, sulla sua liceità, sulla sua natura, sui diritti dell'interessato.

Viene poi esaminato il consenso al trattamento dei dati personali con riferimento ai *cookie*, implementando le argomentazioni con alcune decisioni della Corte di Giustizia dell'Unione Europea.

Infine, la seguente tesi analizza le risposte dei mercati digitali alle nuove forme di tutela introdotte e le best practice utilizzati per assicurare una tutela sempre maggiore agli utenti che navigano sul web. Viene fornito inoltre un breve focus sul nuovo Regolamento ePrivacy ed in particolare sugli effetti che esso determinerà sulle aziende che operano nel digitale.

CAPITOLO PRIMO - LA RILEVANZA ECONOMICA DEI DATI PERSONALI NELL'ECONOMIA DI INTERNET

1.1 I dati personali: la nuova fonte di ricchezza nell'era di Internet

Le tecnologie digitali hanno comportato un processo di trasformazione che sta dominando i cambiamenti economici e sociali di questo secolo. Non a caso si parla di "società dell'informazione"[1] e di "economia della conoscenza"; la tecnologia digitale ha creato nella società odierna delle trasformazioni di portata epocale che hanno portato allo sviluppo di un vero e proprio "ecosistema digitale"[2]. Al centro di questo processo di trasformazione troviamo nuovi beni, nuove materie prime[3] che sono finite col diventare una fonte di ricchezza estremamente importante nell'era del capitalismo digitale[4].

Questi nuovi beni sono i dati: il sistema di *big data* consente di svolgere diverse operazioni, attraverso tecniche di aggregazione, analisi e gestione è possibile, infatti, riutilizzare grandi masse di dati e sfruttarli per diversi fini. La profilazione dei dati permette di classificare gli utenti in determinati gruppi con diverse esigenze a seconda dei gusti, degli interessi e dei comportamenti[5].

---

[1] A. MANTELERO, *Big Data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Il Diritto dell'Informazione e dell'Informatica*, 2012, p.135

[2] O. POLLICINO, E. BERTOLINI, V. LUBELLO, *Internet: regole e tutela dei diritti fondamentali*, Aracne editrice S.r.l., Roma, 2013, p.11-12

[3] G. MARINO, *Internet e la tutela dei dati personali: il consenso ai cookie*, in *Jusvicile*, (2020) 2, p.398. L'autore scrive che *«Prospera il mercato dei dati personali, imperniato sulla crescente capacità tecnologica degli operatori del web di estrarre valore economico da poderose masse di informazioni e dati personali degli utenti di internet, vere e proprie "materie prime" sul controllo e sfruttamento commerciale delle quali si erige l'egemonia serbatoio dei colossi dell'economia digitale»*

[4] Il valore economico dei dati personali è indubbio, nonostante permangano seri dubbi su quale sia il modo più accurato per misurarlo. V., ad esempio, lo studio effettuato dalla Organisation for Economic Co-Operation and Development, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OEDC Digital Economy Papers No. 220, 2013.

[5] O. POLLICINO, E. BERTOLINI, V. LUBELLO, *Internet: regole e tutela dei diritti fondamentali*, Aracne editrice S.r.l., Roma, 2013, p.33. Gli autori scrivono che la vera ricchezza dei nuovi strumenti di comunicazione telematica si basa sulla profilazione, vale a dire sulla possibilità di

Di fatto ogni giorno lasciamo, senza nemmeno accorgercene, un'infinità di "tracce digitali", o una "scia digitale" che palesano le nostre abitudini, preferenze, gusti, interessi ed emozioni, e solitamente non sappiamo chi ne farà uso e con quali fini[6]. Si parla quindi di un'economia "guidata dai dati" o *data-driven economy*[7].

Basta pensare all'economia di piattaforma che di fatto si sta diffondendo proprio perché in essa si riscontra un meccanismo eccezionale di raccolta, analisi e gestione dati; il vantaggio di questa economia proviene dalla particolare posizione che ricoprono sul mercato le piattaforme digitali: esse infatti si frappongono tra gli agenti economici e i luoghi virtuali nei quali avviene l'interazione, trovandosi quindi nella posizione ideale per raccogliere una notevole mole di informazioni sulle caratteristiche delle parti o sulle loro azioni[8]. Il modello della piattaforma, quindi, è adatto a raccogliere, esaminare e gestire tutte le informazioni che derivano dal processo di produzione, dallo scambio e dall'interazione tra gli utenti. In un'economia che è basata sempre di più sulla raccolta dei dati, il modello di organizzazione della piattaforma risulta più idoneo perché permette di raccogliere e usufruire di dati preziosi in modo più efficace di quanto si faccia con un'organizzazione tradizionale. Attraverso i dati si possono individuare diverse strategie di profitto, dalla pubblicità personalizzata

raccogliere e connettere tra loro un numero crescente di informazioni riguardanti i singoli utenti per ricavarne modelli comportamentali, tramite l'utilizzo di sistemi automatizzati.

[6] C. FOCARELLI, *La privacy. Proteggere i dati personali oggi*, Il Mulino, Bologna, 2015, p.9. L'autore porta un esempio relativo ad un oggetto che ormai tutti possiedono ed utilizzano quotidianamente: basti pensare al proprio smartphone che rivela dove sono in ogni momento, registra i tasti che sto premendo, con chi parlo e per quanto tempo, a chi invio i messaggi e da chi li ricevo, quali foto e quali video condivido, registra le pagine web che visito e la durata della navigazione, gli acquisti online, le strade che percorro, …

[7] *Ivi*, p.45.

[8] A. QUARTA, G. SMORTO, *Diritto privato dei mercati digitali*, Le Monnier Università, Firenze, 2020, p.122-123. Aldilà della ripartizione delle piattaforme in diverse categorie, ciò che tutte hanno in comune è la grande centralità dei dati. Si opera un confronto tra il modello produttivo tradizionale, in cui l'impresa produce beni o fornisce servizi per venderli al consumatore, in cui non l'organizzazione dell'impresa non è pensata per raccogliere dati e il modello della piattaforma in cui la raccolta dei dati è la peculiarità fondamentale. Nel modello tradizionale l'impresa non registra e non conserva i dati del processo di produzione e non è in grado di conoscere come e per quale scopo il consumatore utilizzerà il bene prodotto o il servizio offerto e nemmeno gli eventuali problemi sorti nel suo utilizzo.

all'ottimizzazione di beni e servizi offerti a seconda delle caratteristiche dell'utente.

I dati possono essere paragonati a delle materie prime, in quanto al momento della loro raccolta essi sono grezzi e non organizzati: per estrarne il valore vi è l'esigenza di sottoporli ad un processo di lavorazione e di organizzazione in banche dati e di un software capace di estrarne il valore. Questo conduce ad una considerazione: anche se i costi marginali per la generazione dei dati sono quasi nulli, occorrono però degli investimenti considerevoli per quanto riguarda le attività di elaborazione e conservazione dei dati[9].

L'uso dei dati personali ha di fatto sempre avuto implicazioni economiche, anche in forma indiretta. Si pensi ad esempio ai censimenti, essi sono stati spesso utilizzati per rilevare e misurare la capacità contributiva delle persone; un ulteriore esempio può essere quello della pubblicazione di foto di determinare persone per generare profitti per i giornali che le pubblicano[10].

Uno studio pubblicato dal Fondo Monetario Internazionale[11] ha sottolineato che nel mondo della *digital economy* non ci sia nulla di realmente gratuito: le piattaforme online, infatti, offrono beni e servizi che in apparenza sono gratuiti, ma in cambio richiedono i dati degli utenti, che vengono trasformati in modo da estrarne il valore necessario[12].

---

[9] A. QUARTA, G. SMORTO, *Diritto privato dei mercati digitali*, Le Monnier Università, Firenze, 2020, p.247. La centralità del processo di lavorazione permette di paragonare le informazioni tratte dai dati al petrolio e di ritenerle quindi la nuova fonte di ricchezza alla base dell'economia digitale.

[10] Esempi tratti da C. FOCARELLI, *La privacy. Proteggere i dati personali oggi*, Il Mulino, Bologna, 2015, p.45, in cui l'autore scrive che *«la dimensione economica domina la questione della protezione dei dati personali, sia sotto l'aspetto dello sfruttamento economico dei dati a dispetto della privacy, sia sotto l'aspetto dello sfruttamento economico della privacy stessa».*

[11] W.C.Y. LI, M. NIREI, K. YAMANA, *Value of Data: There's No Such Thing as a Free Lunch in the Digital Economy,* Discussion papers 19022, Research Institute of Economy, Trade and Industry (2019).

[12] S. THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in *Media Laws, Rivista di Diritto dei Media*, (2019) 3, p.132. *«È nota la diffusione del business model di offrire servizi gratuitamente, senza cioè la previsione di un corrispettivo in denaro ma previa acquisizione del consenso al trattamento dei dati personali degli utenti. Si tratta di un modello estremamente diffuso nei rapporti online (anche se non ad essi limitato), sviluppatosi*

Per concretizzare il valore che questi dati possono assumere si pensi all'esempio di Facebook: si stima che gli asset di Facebook avessero un valore di circa 6,3 miliardi di dollari al momento della sua quotazione in borsa nel 2011, ma ben presto la valutazione di mercato della società ha raggiunto un livello decisamente più alto: 104 miliardi di dollari, evidenziando l'enorme contributo delle sue risorse intangibili, tra cui proprio i dati di cui dispone[13].

Un altro esempio ci è offerto dalla società Apple: il colosso dell'economia digitale infatti chiede una commissione pari al 30% sulle vendite agli sviluppatori di applicazioni in cambio proprio dell'accesso ai dati sui consumatori. Da questa operazione ha ricavato in 10 anni, ben 40 miliardi di dollari[14].

Dunque, oggi i flussi globali di dati personali hanno raggiunto livelli senza precedenti sia per quanto riguarda il loro volume, sia per la complessità e sia per ubiquità[15]. Il trasferimento dei dati online è immenso e in continua crescita.

Il processo di digitalizzazione e diffusione delle informazioni è diventato irreversibile. Ma dove sta il problema? Gli utenti possono pensare di poter scambiare alcuni propri dati personali, che a loro non costa nulla, con beni e servizi gratuiti di grande utilità che altrimenti dovrebbero pagare. Inoltre, si pensa di essere comunque arbitri dell'uso dei propri dati personali e di poterlo concedere solo quando conviene anche a noi, ma le cose non stanno esattamente così[16].

---

grazie all'evoluzione delle nuove tecnologie che rendono possibili sempre più pervasive e sofisticate tecniche di raccolta, monitoraggio e sfruttamento dei dati personali».
A. DE FRANCESCHI, *La circolazione dei dati personali tra privacy e contratto,* Edizioni Scientifiche Italiane, Napoli, 2017, p.67 ss.

[13]Disponibile online su *https://www.devita.law/il-valore-dei-dati/* SEC, *Facebook, Inc. 10-K Annual Report for the Fiscal Year Ended December 31, 2012.*

[14] S. FRIER *Is Apple Really Your Privacy Hero*?, in Bloomberg Businessweek, (2018)

[15] C. FOCARELLI, *La privacy. Proteggere i dati personali oggi*, Il Mulino, Bologna, 2015, p.33: il trasferimento dei dati online è enorme e in costante espansione, oggi avviene attraverso reti e non più tramite trasmissioni "da punto a punto" come in passato.

[16] *Ivi*, p.11. L'autore fornisce un interessante esempio di tipo commerciale in merito a ciò. Mettiamo il caso che un utente di Internet voglia acquistare un'auto e sia già orientato verso un determinato modello e marca. Attraverso la connessione ad Internet ha potuto ottenere diverse informazioni, come qualità, dati tecnici, consumi, prezzo di base e prezzo degli optional. Si reca dunque dal concessionario, ottenendo un preventivo; si reca poi da altri concessionari per

Si pensi anche che il singolo utente raramente è in grado di capire il senso che la raccolta di determinate informazioni può assumere in organizzazioni complesse e dotate di mezzi sofisticati per il trattamento dati[17].

1.2 Categorie di dati e "parti in gioco"

Spesso quando si parla di protezione di dati personali si fa riferimento alla protezione della *privacy*[18]; i due concetti però non si equivalgono completamente, anche se sono interconnessi. Da un lato la *privacy* è un concetto più ampio in quanto riguarda anche, ma non esclusivamente, i dati personali. Dall'altro, la protezione dei dati personali è a sua volta più ampia perché i dati sono protetti anche quando non violano la privacy; come ha sostenuto il Garante Europeo per la Protezione dei Dati, la "protezione dei dati" è più vasta della "protezione della privacy" dato che riguarda anche altri diritti e libertà fondamentali e ogni tipo di dati, a prescindere dalla loro connessione alla *privacy*, e allo stesso tempo è più ristretta in quanto riguarda solamente l'elaborazione delle informazioni personali, mentre altri aspetti della *privacy* sono ignorati[19].

---

ottenere altri preventivi che siano magari più convenienti (vantaggio dell'economia di mercato); decide poi di acquistare l'auto dal concessionario che gli ha offerto un preventivo migliore. Vorrebbe però trattare ancora sul prezzo, il venditore non sa che è stato già scelto perché il suo preventivo è stato il migliore; se non ci trovassimo in un mercato concorrenziale, sarebbe a conoscenza degli altri preventivi. Mettiamo caso però che il venditore possa conoscere tutti i segreti dell'utente; l'utente infatti ha rilasciato i suoi dati per i preventivi; incrociando i suoi dati online, il venditore può risalire all'indirizzo IP e può vedere tutte le operazioni che ha effettuato in rete, quando ha visitato il sito del concessionario, come ha configurato l'auto, quali optional ha scelto, su quale fascia di prezzo si è indirizzato. Se fosse così, la strategia negoziale dell'utente di cercare di far abbassare il prezzo, pena il non acquisto, sarebbe inutile. Il venditore sa che acquisterà l'auto da lui e a quale prezzo.

[17] S. RODOTÀ, *Tecnologie e diritti,* Il Mulino, Bologna, 1995, p.35. L'autore mette anche in evidenza il notevole dislivello di potere esistente tra l'individuo isolato e le grandi organizzazioni di raccolta dei dati. In questo modo è completamente illusorio parlare di "controllo".

[18] S. RODOTÀ, *Tecnologie e diritti,* Il Mulino, Bologna, 1995, p.19. L'autore scrive *che «le nuove dimensioni della raccolta e del trattamento delle informazioni hanno provocato la moltiplicazione degli appelli alla privacy».*

[19] C. FOCARELLI, *La privacy. Proteggere i dati personali oggi*, Il Mulino, Bologna, 2015, p.37; M. SOFFIENTINI, *Privacy. Protezione e trattamento dei dati*, Ipsoa, Vicenza, 2018, cit., p.5 *«possiamo aggiungere che, complice il progresso tecnologico, con l'espressione "protezione dei dati personali" si voglia far riferimento anche a tutte le tecniche di tutela proposte alla sicurezza e alla protezione dei sistemi e dei dati personali»*

Prima di addentrarci nello specifico, occorre attuare una precisazione riguardante i dati: essi sono di due tipi, personali e non personali. La definizione e la regolamentazione dei dati personali sono contenute nel Regolamento Generale sulla Protezione dei Dati Personali che sarà trattato meglio in seguito.

Il diritto alla protezione dei dati personali è inteso come un diritto fondamentale delle persone fisiche dal GDPR e consiste nel diritto del soggetto cui i dati si riferiscono di esercitare un controllo, anche attivo, sui tali dati, che si estende dall'accesso alla rettifica[20].

I dati non personali invece non possiedono una definizione specifica ma sono individuati negativamente, indicando tutti quei dati che non sono classificati come dati personali[21]. La loro disciplina e circolazione è stabilita nel Regolamento 2018/1807/UE.

Secondo il Regolamento il dato personale è *«qualsiasi informazione riguardante una persona fisica identificata o identificabile»*, chiamata *"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 o sociale»*[22]. L'analisi di questa definizione consente di individuare due caratteristiche chiave: quella della loro separazione dalla persona cui riguardano, tramite la raccolta, e quella della rilevanza del loro uso e circolazione sulle relazioni, di vario genere, tra interessato e chi usa i dati[23]. Il particolare legame tra dati personali e interessato è testimoniato dalla

[20] G. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Zanichelli Editore, Bologna, 2021, p.1
[21] A. QUARTA, G. SMORTO, *Diritto privato dei mercati digitali*, Le Monnier Università, Firenze, 2020, p.248
[22] Art. 4, Regolamento UE 2016/679 (GDPR).
[23] C. ANGIOLINI, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, G. Giappichelli Editore, Torino, 2020 p.26. L'autrice sottolinea come la disciplina da una parte ha una visione dei dati come oggetti misurabili, del trattamento, raccolti e poi trattati, e dall'altra sancisce un legame persistente con gli interessati, che mette in luce la connessione tra il regime dei dati personali e lo statuto della persona.

previsione di diritti fondamentali che lo tutelano dal e nel trattamento, sia a livello europeo[24] che a livello nazionale[25].

I dati personali sono informazioni che identificano o rendono identificabile una persona fisica, permettendo quindi un'identificazione diretta: dati anagrafici come nome e cognome, immagini, ecc., o indiretta: numero di identificazione come il codice fiscale o l'indirizzo IP, o il numero di targa, e che possono offrire informazioni sulle sue caratteristiche, abitudini, le sue relazioni personali, il suo stato di salute, la situazione economica[26], ecc…

La persona identificata o identificabile è definita "soggetto interessato". Il Regolamento quindi non si limita a includere nelle nozioni che permettono l'identificazione solo nome o indirizzo, ma anche tutte le informazioni che permettono di identificare la persona; dunque, rientrano anche indirizzi IP e i *cookies*, perché combinati con altre informazioni ricevute dai server permettono di costruire il profilo di una persona fisica e di conseguenza di identificarla.

Tra i dati personali vi è una categoria particolarmente importante, cioè quella dei dati sensibili: sono dati idonei a rivelare l'origine razziale o etnica, le convinzioni religiose, le idee politiche, le adesioni sindacali, le informazioni concernenti la salute o la vita sessuale. Sono dunque dati che riguardano la personalità etico-sociale dell'individuo e le sue caratteristiche psico-sanitarie[27]. Rientrano nei dati

[24] Con l'articolo 8 della Carta dei diritti fondamentali dell'Unione Europea. (2000/C 364/01)
[25] Con l'articolo 2 della Costituzione della Repubblica Italiana
[26] Definizione da A. QUARTA, G. SMORTO, *Diritto privato dei mercati digitali*, Le Monnier Università, Firenze, 2020, p.249 *«qualsiasi informazione riguardante una persona fisica identificata o identificabile, definita come il soggetto interessato»*; C. FOCARELLI, *La privacy. Proteggere i dati personali oggi*, Il Mulino, Bologna, 2015, p.30.
[27] G. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Zanichelli Editore, Bologna, 2021, pp.57-58. Occorre segnalare che anche se ka categoria dei dati sensibili sia una categoria chiusa, l'utilizzo dell'espressione "idonei a rivelare" conferisce a questa categoria un carattere di elasticità. Per cui sono dati sensibili anche quelli che potrebbero consentire di individuare la religione di un soggetto, ma che non necessariamente la individuano. Esempio del libro: le scelte alimentari effettuate dal frequentatore di una mensa potrebbero essere idonee a rivelare la religione di questi, ma non necessariamente la rivelano.

sensibili anche i dati biometrici, i dati genetici[28] e quelli relativi all'orientamento sessuale[29].

È da considerare che molte di queste informazioni vengono rivelate dall'utente anche in modo indiretto, per esempio attraverso i "like" su Facebook. Si pensi ad un utente che esprime proprio attraverso i "like" sul *social network* il suo apprezzamento o interesse per un determinato personaggio politico e la sua campagna: in questo modo è possibile compilare una profilazione in modo da renderlo destinatario di messaggi mirati e specifiche comunicazioni elettorali[30].

Per quanto riguarda questi dati il Regolamento non disciplina i diritti del titolare in termini di appartenenza, ma utilizza lo schema dell'informativa della *privacy*, a cui l'interessato può consentire e autorizzare il trattamento dei suoi dati tramite il rilascio del consenso[31]. Il consenso dell'interessato deve essere libero, informato e consapevole, anche grazie alla lettura del testo dell'informativa.

Un'esperienza per capire meglio questo aspetto è fornita dalla decisione 29 luglio 2019 della Corte di Giustizia dell'Unione Europea[32]: in questo caso un'associazione tedesca a tutela dei consumatori aveva agito contro un famoso venditore di abbigliamento online perché i visitatori del sito non erano stati informati che premendo il tasto "like", i loro dati sarebbero stati trasmessi a Facebook. Dunque, la raccolta e il trasferimento dei dati avevano luogo senza il consenso del titolare: l'associazione lamentava quindi una violazione degli obblighi di informazione in riferimento ai dati personali. L'impresa, quindi, è stata ritenuta responsabile[33] delle operazioni di raccolta e comunicazione dei dati

[28] M. SOFFIENTINI, *Privacy. Protezione e trattamento dei dati*, Ipsoa, Vicenza, 2018, p.83. Secondo la Raccomandazione n.R(97) 5 del Consiglio d'Europa, sono considerati dati genetici tutti i dati che fanno riferimento ai caratteri ereditari di una persona o che sono in rapporto con i caratteri che formano il patrimonio di un gruppo di individui affini.
[29] Art. 9 del Regolamento UE 679/2016 (GDPR).
[30] Esempio contenuto in A. QUARTA, G. SMORTO, *Diritto privato dei mercati digitali*, Le Monnier Università, Firenze, 2020, p.253.
[31] *Ibidem*
[32] Corte di giustizia dell'Unione europea, 29 luglio 2019 (Causa C-38/18 - Gambino; Hyka), disponibile online su *http://images.processopenaleegiustizia.it/f/sentenze/documento_imAFh_ppg.pdf*
[33] Insieme a Facebook

personali degli utenti del sito, dato che contribuisce a determinare i motivi e le finalità di tali operazioni. Grazie a questa tattica l'impresa è in grado di ottimizzare la pubblicità dei prodotti offerti e ottenendo di fatto un vantaggio commerciale. Questa corresponsabilità non riguarda però il trattamento dei dati, in quanto si tratta di un'operazione svolta esclusivamente da Facebook dopo aver ricevuto le informazioni. La decisione ha quindi chiarito i profili di responsabilità in materia di trattamento di dati personali nei casi in cui in un sito web siano presenti i pulsanti "like" di Facebook[34].

Infine, un'altra categoria molto importante rientrante nei dati personali è quella dei dati relativi a condanne penali e reati[35]. Si tratta dei dati "giudiziari", quei dati che possono rivelare la presenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale, come la liberazione condizionale, provvedimenti penali di condanne definitive, divieto o obbligo di soggiorno, o la qualità di imputato o di indagato.

L'evoluzione di nuove tecnologie ha inoltre comportato la finizione di altri dati personali con un ruolo significativo: i dati relativi alle comunicazioni elettroniche via Internet o telefono e i dati che permettono la geolocalizzazione, i quali forniscono informazioni sui luoghi frequentati e sugli spostamenti.

Per comprendere meglio il meccanismo del trattamento dei dati personali, è bene fare chiarezza su quelle che sono "le parti in gioco".

L'interessato è *«la persona fisica alla quale si riferiscono i dati»*; per cui ad esempio, se per l'erogazione di un determinato servizio è richiesto l'indirizzo dell'utente Mario Rossi, allora questo costituisce l'indirizzo dell'interessato Mario Rossi[36].

[34] Esempio fornito da A. QUARTA, G. SMORTO, *Diritto privato dei mercati digitali*, Le Monnier Università, Firenze, 2020, p.253.
[35] Art. 10 del Regolamento UE 2016/679 (GDPR)
[36] Art. 4, par. 1, n. 1, del Regolamento UE 2016/679 (GDPR)

Il titolare è *«la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri»*[37]. Il titolare, quindi, è la più importante delle figure in quanto stabilisce finalità e mezzi dei dati personali; la sua condotta deve ispirarsi al principio di responsabilizzazione, introdotto dal GDPR; esso prescrive che il titolare non deve limitarsi a svolgere delle verifiche meramente formali ma deve garantire in modo attivo la tutela dei dati[38]. Il ruolo del titolare può essere ricoperto da una persona fisica o persona giuridica, che può essere sia un ente privato sia un organismo pubblico e può nominare una persona fisica o giuridica responsabile del trattamento dei dati.

Il responsabile del trattamento è «*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento»*[39]. Il titolare deve individuare il responsabile tra soggetti che dispongano di capacità ed esperienza in materia di privacy e sicurezza e deve impartirgli direttive in ordine ai fini, ai mezzi e alle modalità del trattamento[40].

Il Regolamento inoltre ha stabilito la possibilità che un responsabile possa, a sua volta e secondo specifiche condizioni, incaricare un altro soggetto c.d. *"sub-responsabile"* [41].

Il destinatario è *«la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto*

[37] Art. 4, par. 1, n. 8, del Regolamento UE 2016/679 (GDPR)
[38] A. QUARTA, G. SMORTO, *Diritto privato dei mercati digitali*, Le Monnier Università, Firenze, 2020, p.250.
[39] Art. 4 del Regolamento UE 2016/679 (GDPR)
[40] M. SOFFIENTINI, *Privacy. Protezione e trattamento dei dati*, Ipsoa, Vicenza, 2018, p.141
[41] Art. 28, par. 2 del Regolamento UE 2016/679 (GDPR)

dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento»[42].

Per trattamento si intende «*un'operazione o un complesso di operazioni che hanno per oggetto i dati personali*»[43]. Il trattamento, quindi, è un'espressione che raccoglie in sé operazioni diverse come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione o diffusione, la limitazione, la cancellazione o la distruzione[44]. L'articolo 5 del GDPR elenca i principi fondamentali che devono caratterizzare l'attività di trattamento, ovvero i principi di liceità, correttezza e trasparenza; di limitazione delle finalità, di minimizzazione dei dati, di esattezza, di limitazione della conservazione, di integrità e riservatezza e di responsabilizzazione[45]; tra le attività il legislatore ha tenuto conto soprattutto della profilazione, che sta assumendo sempre più importanza nei mercati online[46].

Il trattamento è lecito solo in determinate situazioni, specificate dall'articolo 6 (liceità del trattamento per tutte le categorie di dati) e dall'articolo 9 paragrafo 2 per le categorie particolari[47].

[42] Art. 4 del Regolamento UE 2016/679 (GDPR)
[43] Art. 4, par. 1, n. 2, del Regolamento UE 2016/679 (GDPR)
[44] A. QUARTA, G. SMORTO, *Diritto privato dei mercati digitali*, Le Monnier Università, Firenze, 2020, p.249.
[45] Art.5 del Regolamento UE 2016/679 (GDPR)
[46] A. QUARTA, G. SMORTO, *Diritto privato dei mercati digitali*, Le Monnier Università, Firenze, 2020, p.250. Esempio fornito*: «se Amazon può suggerire i libri da acquistare in base agli ultimi testi visionati o comprati, tale attività è proprio il risultato della profilazione dei suoi utenti, effettuata tramite la raccolta e il trattamento dei dati».*
[47] M. SOFFIENTINI, *Privacy. Protezione e trattamento dei dati*, Ipsoa, Vicenza, 2018, pp.60-61

1.3 Un breve focus sui *big data*

Il fenomeno generale più considerevole per comprendere la dimensione economica dei dati personali è quello dei *big data*[48], ricavati tramite tecniche di data mining relativi a singole persone o per aggregato, e dunque anonimi o de-identificati[49]. Le fonti da cui provengono i dati sono varie, includono i *social media*[50] e gli *open public data*, vale a dire dati personali resi disponibili, solitamente dalla pubblica amministrazione, a chiunque. L'industria dei *big data* è in continua espansione e gli esperti del settore sono molto ricercati, soprattutto *data scientist*, ovvero esperti di analisi dati[51].

Sono presenti diverse definizioni di *big data*, per alcuni sono intesi come «*grandi quantitativi di dati*[52]», oppure come *«dati la cui stessa dimensione diventa parte del problema*[53]*»,* o la cui *«dimensione supera la capacità degli strumenti tipici del software di archiviazione relativa alla cattura, immagazzinamento, gestione ed elaborazione*[54]*».*

---

[48] C. FOCARELLI, *La privacy. Proteggere i dati personali oggi*, Il Mulino, Bologna, 2015, p.45

[49] J. STEIN, *Data Mining: How Companies Now Know Everything about You*, in *Time,* (2011) (online in *http://content.time.com/time/magazine/article/0,9171,2058205,00.html*). «*Every detail of your life, what you buy, where you go, whom you love is being extracted from the Internet, bundled and traded by data-mining companies*».

[50] M. SOFFIENTINI, *Privacy. Protezione e trattamento dei dati*, Ipsoa, Vicenza, 2018, p.488. I social network raccolgono e trattano una gran mole di dati e su questo tema forniscono essi stessi informative privacy dettagliate e complesse, questo però potrebbe non essere sufficiente. Questo basta solo per la creazione e la condivisione di contenuti nella piattaforma, ma se si realizza un'integrazione tra i contenuti di un sito e la corrispondente pagina social occorre integrare anche l'informativa privacy presente sul sito, indicando quali sono le conseguenze per l'utente.

[51] *Professione scienziato del dato*, in *Il Sole 24 Ore*, (2014) online su *https://st.ilsole24ore.com/art/tecnologie/2014-10-26/professione-scienziato-dato-081257.shtml?uuid=ABHDEu6B&fromSearch=,* dove l'autore scrive che *"a quella del data scientist è stata definita dall'economista Hal Ronald Varian «la professione più sexy del futuro», laddove l'aggettivo assume l'accezione di «interessante»".*

[52] T. MCGUIRE, J. MANYIKA e M. CHUI*, Why Big Data Is the New Competitive Advantage*, in *Ivey Business Journal*, luglio-agosto 2012, in *http://iveybusinessjournal.com/publication/why-big-data-is-the-new-competitive-advantage.*

[53] M. LOUKIDES, *What Is Data Science? The Future Belongs to the Companies and People that Turn Data into Products*, 2 giugno 2010, in *http://radar.oreilly.com/2010/06/what-is-data-science.html*

[54] McKinsey Global Institute*, Big Data: The Next Frontier*, rapporto del maggio 2011, in *www.mckinsey.com/insights/business_technology/big_data_the_net_frontier_for_innovation*; E.

La Commissione Europea descrive così il fenomeno dei *big data «Il termine big data (megadati) si riferisce a grandi quantità di tipi diversi di dati prodotti da varie fonti, fra cui persone, macchine e sensori. Alcuni esempi sono i dati sul clima, le immagini satellitari, le immagini e i video digitali, le registrazioni di operazioni o i segnali GPS.»* Quindi con questa espressione si fa riferimento all'insieme di tecnologie e metodi di analisi basati sulla capacità di utilizzare grandi quantità di dati per poterli analizzare e mettere in relazione tra loro, per evidenziarne i legami e ricavarne informazioni utili[55]. I *big data* possono comprendere dati personali, ad esempio informazioni riguardanti una persona, come un nome, una fotografia, un indirizzo e-mail, estremi bancari, messaggi postati sui siti delle reti sociali, informazioni cliniche o l'indirizzo IP di un computer.

Un primo e ricco serbatoio di big data sono le piattaforme digitali come motori di ricerca, *social network*, i servizi di comunicazione digitale, *hosting platforms* etc. Invero, all'utente non è richiesto alcuna controprestazione in denaro per l'offerta di un contenuto o di un servizio digitale da parte del *provider*, ma egli acconsente a fornire i propri dati personali che saranno oggetto di trattamento da parte del *provider* stesso.

L'accesso e dunque lo sfruttamento dei dati personali forniti dall'utente può essere considerato l'interesse primario dell'operatore economico che in questo modo remunera la fornitura di contenuti e servizi digitali.

Questo schema negoziale ha trovato riconoscimento per la prima volta con la direttiva (UE) 2019/770 del 2019, relativa a determinati aspetti dei contratti di

---

DUMBILL, *What is Big Data? An Introduction to the Big Data Landscape*, 11 gennaio 2012, in *http://goo.gl/OrjMIH*

[55] A. QUARTA, G. SMORTO, *Diritto privato dei mercati digitali*, Le Monnier Università, Firenze, 2020, p.19. Gli autori forniscono una spiegazione per comprendere meglio la differenza tra la tecnologia dei big data e quella delle banche dati tradizionali: «*Per descrivere la differenza rispetto alle banche dati tradizionali e delineare le caratteristiche essenziali dei big data, si utilizza comunemente la formula delle tre V: il volume, ossia la quantità di dati generati ogni secondo; la velocità con cui questi dati sono generati e trasmessi in tempo reale, e la varietà dei dati stessi, ovvero sia la loro diversa tipologia. Questa enorme quantità di dati eterogenei e processati in tempo reale ha bisogno di tecniche molto più sofisticate di quelle che sono alla base della gestione delle comuni banche dati, richiedendo modalità nuove di acquisizione, memorizzazione, accesso e gestione dati».*

fornitura di contenuto digitale e di servizi digitali; la direttiva comprende nel proprio ambito oggettivo di applicazione il contratto in cui il consumatore che usufruisce della fornitura di contenuti servizi digitali da parte dell'operatore economico, «*fornisce o si impegna a fornire dati personali all'operatore economico, fatto salvo il caso in cui i dati personali forniti dal consumatore siano trattati esclusivamente dall'operatore economico ai fini della fornitura del contenuto digitale o del servizio digitale [...]»*[56]. L'operatore, quindi, è il titolare del trattamento, che è obbligato a fornire il contenuto o servizio digitale, e che vanterà diritto di accesso e di trattamento di questi dai personali in ragione delle finalità comunicate. I dati personali in genere vengono comunicati al momento della conclusione del contratto[57].

Esiste poi, un altro canale di accesso per la raccolta dei dati personali online, che è operativo ancora prima la conclusione del contratto[58]. Questo canale è consentito dall'evoluzione tecnologica che ha ideato strumenti che consentono ai gestori di siti internet di ricavare le informazioni degli utenti da operazioni elementari come il semplice accesso e la navigazione online. Queste elementari attività sono considerate dagli utilizzatori della rete solitamente molto rapide e impersonali, ma in realtà sono un importantissimo canale di trasmissione e propalazione di informazioni e dati personali, grazie all'utilizzo di *cookie,* di cui si tratterà in seguito[59].

Inoltre, la produzione di processori a basso costo e di facile uso ha permesso che sempre più oggetti della nostra vita quotidiana fossero dotati di piccoli computer

[56] Art. 3 Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio, del 20 maggio 2019, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali, in *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32019L0770*

[57] G. MARINO, *Internet e la tutela dei dati personali: il consenso ai cookie*, in *Jusvicile*, (2020) 2, p.399

[58] Si sta parlando di un contratto di fornitura di un contenuto o di un servizio digitale

[59] G. MARINO, *Internet e la tutela dei dati personali: il consenso ai cookie*, in *Jusvicile*, (2020) 2, p.401. «*Si tratta di un file di testo che il fornitore di un sito Internet installa nel computer dell'utente che lo abbia visitato e al quale potrà accedere durante una nuova navigazione sullo stesso sito da parte di quello stesso utente».*

integrati e connessi alla rete, con lo scopo di inviare e ricevere dati; questi oggetti comuni vengono resi "intelligenti"[60].

La raccolta di grandi quantità di dati e l'elaborazione dei *big data* porta certamente dei benefici, lo stesso rapporto dell'OCSE del 2013, qualifica i *big data* come stimolo di innovazione e di crescita[61], soffermandosi in particolar modo sui benefici apportati al settore della pubblicità online, della pubblica amministrazione, della sanità, delle utenze e dei trasporti, nei quali i big data costituiscono una fonte di ricerca e sviluppo di nuovi beni e servizi e di commercializzazione attraverso una pubblicità mirata e migliori forme di organizzazione dell'economia[62].

Anche la Commissione Europea sottolinea come *«l'innovazione guidata dai dati genererà benefici enormi per i cittadini»*; la Commissione porta l'esempio del miglioramento della medicina personalizzata[63] o quello di nuove soluzioni di mobilità e il contributo che apporterebbe al Green Deal europeo, o una migliore produttività, mercati più competitivi e miglioramenti nell'amministrazione e nei servizi pubblici[64].

---

[60] A. QUARTA, G. SMORTO, *Diritto privato dei mercati digitali*, Le Monnier Università, Firenze, 2020, p.19: nasce così quella che viene chiamata *Internet of Things,* espressione che individua una rete di oggetti fisici muniti di dispositivi elettronici dotati di sensori e gestiti da appositi software che consentono a questi oggetti di essere connessi alla rete, di raccogliere e scambiare dati.

[61] C. FOCARELLI, *La privacy. Proteggere i dati personali oggi*, Il Mulino, Bologna, 2015, p.62. L'autore scrive che «*la migrazione delle attività economiche e sociali su Internet con la corrispondente massa di dati generati per milioni di gigabyte al secondo, nonché la progressiva digitalizzazione delle attività online e la riduzione dei costi di raccolta, trasferimento, immagazzinamento ed elaborazione dei dati, condurrebbero oggi a un modello socioeconomico "guidato dai dati" (data-driven)*»

[62] OCSE, *Exploring Data-Driven Innovation as a New Source of Growth*, in OECDiLibrary, (2013), online in *https://www.oecd-ilibrary.org/science-and-technology/exploring-data-driven-innovation-as-a-new-source-of-growth_5k47zw3fcp43-en*

[63] Comunicazione UE (2020)86, *Una strategia Europea per i Dati,* cit.*,* p.1: «*la medicina personalizzata risponderà meglio alle esigenze dei pazienti permettendo ai medici di prendere decisioni basate sui dati, in modo tale da adeguare la strategia terapeutica giusta alle esigenze della persona giusta al momento giusto, e/o da determinare la predisposizione alla malattia e/o da attuare una prevenzione mirata e tempestiva».*

[64] *Ibidem*. La commissione sottolinea come l'UE possa diventare un modello di riferimento per una società che, grazie ai dati, dispone di strumenti per adottare decisioni migliori, sia nel settore pubblico che per le imprese.

A meno di quattro anni dall'emanazione del GDPR, la Commissione Europea ha emanato questa Comunicazione, intitolata "Una strategia europea per i dati", per dare una spinta ad incentivare il mercato dei dati e a favorire una "sovranità tecnologica europea"[65] viene coniugata con una visione volta a far sempre salvo il principio personalistico[66]. La dimensione economica non viene comunque persa di vista, in quanto *«l'Europa mira a sfruttare i vantaggi di un migliore utilizzo dei dati, compresi una maggiore produttività e mercati competitivi, ma anche miglioramenti in materia di salute e benessere, ambiente, amministrazione trasparente e servizi pubblici convenienti. Le misure illustrate nel presente documento contribuiscono a un approccio globale all'economia dei dati. La presente comunicazione delinea una strategia per le misure politiche e gli investimenti a sostegno dell'economia dei dati per i prossimi cinque anni»*[67]. Difatti le scelte strategiche si concentrano sulla disponibilità e sulla condivisione dei dati, nonché su una maggiore chiarezza riguardante l'utilizzo dei dati, sulla governance dei dati, sull'istituzione di spazi comuni europeo di dati, sull'interoperabilità e sulla qualità dei dati[68].

D'altra parte, si potrebbe incorrere in eventuali rischi, soprattutto per la *privacy*[69]: per analizzarli, profilarli e raccogliere informazioni utili per delineare gusti e opinioni degli utenti, i big data vengono processati mediante trattamenti automatizzati e algoritmi di Intelligenza Artificiale e altre tecniche avanzate. Una

---

[65] *Ivi*, cit., p. 6, ove si trova rimarcato che «Il funzionamento dello spazio europeo di dati dipenderà dalla capacità dell'UE di investire nelle tecnologie e nelle infrastrutture di prossima generazione, come pure nelle competenze digitali, ad esempio l'alfabetizzazione ai dati (data literacy). Ciò contribuirà a sua volta a rafforzare la sovranità tecnologica dell'Europa per quanto riguarda le tecnologie e le infrastrutture abilitanti fondamentali per l'economia dei dati».

[66] *Ivi*, cit., p.5; F. BRAVO, *intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa Europa,* (2021)1, p.202

[67] Comunicazione UE (2020)86, *Una strategia Europea per i Dati*, cit., p.1.

[68] F. BRAVO, *intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa Europa,* (2021)1.

[69] M. GAMBINI, *La protezione dei dati personali come diritto fondamentale della persona: meccanismi di tutela*, in *ESPAÇO JURÍDICO*, (2013), cit., pp.3-4; «*Nella società dell'informazione, la grande quantità di dati personali generati dall'odierno mondo elettronico, combinata con le nuove tecnologie a disposizione, che rendono sempre più sofisticati e meno facili da rilevare gli strumenti di raccolta e trattamento delle informazioni personali, aumentano in modo esponenziale i rischi di esposizione delle persone a forme illegittime di intrusione nella propria sfera privata e di spoglio della propria identità».*

volta inseriti nei sistemi diventano quindi delle gocce nel mare e in questo modo i dati vengono persi di vista dal titolare e dal responsabile del trattamento[70], e questo rappresenta un rischio enorme per la tutela della *privacy* degli utenti, in quanto il titolare del trattamento potrebbe utilizzarli, non intenzionalmente, per finalità differenti rispetto a quanto stabilito nelle informative sulla *privacy* fornite e ai consensi ottenuti[71].

I rischi riguardanti i *big data* possono riferirsi a possibili errori nella raccolta o nell'elaborazione dei dati sulla cui base vengono poi adottate decisioni operative, o nella loro perdita o appropriazione indebita, o dall'abuso nel loro impiego[72]. I rischi non fanno riferimento solo agli individui, ma anche alla reputazione delle imprese che dispongono dei dati, in quanto richiedono risorse gestionali notevoli[73]. Per di più l'elaborazione e l'utilizzo di masse di dati svuotano di significato il requisito del consenso individuale se i dati vengono elaborati per aggregato a prescindere dall'identità dei singoli a cui appartengono. In conclusione, le decisioni derivanti dall'uso di dati di massa devono tener conto di vincoli giuridici ed etici[74].

È necessario chiarire però che i dati di massa non sono dati personali in senso stretto, si tratta di dati aggregati e anonimi e per questo non sembrerebbero influire sulla privacy delle persone. Per applicare la normativa sulla *privacy* occorre dimostrare che i dati sono comunque riconducibili alla persona, attraverso tecniche di reidentificazione o deanonimizzazione, o hanno effetti sulla persona per non essendo personali in senso stretto[75]. Infatti, anche delle informazioni che sono in apparenza anonime possono diventare un rischio perché si può giungere a re-identificare un utente tramite la fusione di banche

[70] Vale a dire il titolare dell'azienda che raccoglie i dati e chi li gestisce
[71] *GDPR e Big Data, la privacy nel trattamento automatizzato di grandi quantità di dati*, in *ITMANAGER.SPACE*, (2020), online su *https://itmanager.space/privacy-gdpr-big-data/*
[72] C. FOCARELLI, *La privacy. Proteggere i dati personali oggi*, Il Mulino, (città), 2015, p.53.
[73] K. KRASNOW WATERMAN E P.J. BRUENING, *Big DATA Analytics: Risks and Responsabilities*, in *International Data Privacy Law*, vol. 4, 2014, n.2, pp. 89-95.
[74] C. FOCARELLI, *La privacy. Proteggere i dati personali oggi*, Il Mulino, Bologna, 2015, pp. 53-54
[75] *Ibidem*

dati diverse. Per cui l'anonimizzazione da sola non basta a garantire la riservatezza dei dati.

Il GDPR, anche se non tratta direttamente la materia dei *big data*, oggi appare lo strumento più efficace, il corpo di norme più completo in fatto di riservatezza dei dati e attento alla difesa della *privacy*, ed è in grado di limitare gli abusi anche nel campo dei *big data*[76].

1.4 Il valore dei dati negli ordinamenti occidentali

Data la rilevanza economica sempre maggiore che stanno assumendo i dati, nel 2017 la Commissione Europea ha promosso uno studio per individuare la dimensione economica di questi ultimi. Da questo studio è nata poi la necessità e la consapevolezza di dover costruire una strategia di gestione della distribuzione economica scaturita dai dati. In quegli anni si era infatti stimato che nell'Unione Europea il valore complessivo derivante dalla "data economy" sarebbe cresciuto da 285 miliardi di euro nel 2015 a 739 miliardi nel 2020[77].

In una comunicazione del 2020 poi, la Commissione Europea ha sottolineato come il volume dei dati prodotti a livello mondiale sia soggetto ad una crescita rapida e costante, dai 33 zettabyte del 2018 ai 175 zettabyte previsti nel 2025[78].

Dato che dalla produzione di dati spesso ne consegue un trasferimento di ricchezza a favore degli stati in cui si trovano le aziende che si occupano di immagazzinare questi dati, si è reso necessario stabilire l'attribuzione della proprietà ai dati prodotti.

Questa esigenza deriva dalla preoccupazione delle autorità europee in quanto le aziende *data driven*, soprattutto statunitensi, realizzano un'acquisizione di risorse

---

[76] *GDPR e Big Data, la privacy nel trattamento automatizzato di grandi quantità di dati*, in *ITMANAGER.SPACE*, (2020), online su *https://itmanager.space/privacy-gdpr-big-data/*
[77] Open Evidence, *European Data Market study*, SMART 2013/0063, 1° febbraio 2017, online su *https://www.key4biz.it/wp-content/uploads/2018/04/SMART20130063_Final-Report_030417_2.pdf*
[78] Comunicazione UE (2020)86, *Una strategia Europea per i Dati*, p.2

che provengono dall'Unione Europea, la quale perde i dati e quindi il valore economico aggiunto[79]. Il controllo dei dati trasferiti, a livello della loro posizione minuto per minuto e della loro elaborazione, è diventata una questione sempre più complicata[80]. Le norme esistenti sulla protezione dei dati si applicano ai "flussi transfrontalieri" di dati personali nel senso che la loro libera circolazione è permessa eccetto quando i dati sono destinati a uno stato nel quale il livello di protezione è inferiore rispetto allo stato di partenza[81]. All'interno dei Paesi UE è ammessa la libera circolazione dei dati, mentre i trasferimenti dei dati verso paesi non appartenenti allo Spazio Economico Europeo o verso un'organizzazione internazionale sono consentiti solo se l'adeguatezza del Paese terzo o dell'organizzazione è riconosciuta tramite decisione della Commissione Europea[82]. In mancanza di tale decisione il trasferimento è consentito se il titolare o il responsabile del trattamento forniscono garanzie adeguate che prevedono diritti azionabili e mezzi di ricorso effettivi per gli interessati[83].

L'esigenza di un intervento legislativo proviene dalla natura dei dati come bene economico: essi, a differenza di altri beni materiali, non sono beni a consumo rivale ed esclusivo[84]. La rivalità dei beni materiali consente che sia più facilmente rivendicabile la loro proprietà, mentre i dati possono essere utilizzati da più persone, allo stesso tempo in copie uguali.

---

[79] F. BANTERLE, *Data Ownership in the Data Economy: A European Dilemma*, in *SSRN Electronic Journal*, gennaio 2018.
[80] C. FOCARELLI, *La privacy. Proteggere i dati personali oggi*, Il Mulino, Bologna, 2015, p.33.
[81] *Ibidem.* L'autore scrive *«è evidente quanto sia difficile su internet definire cosa sia "transfrontaliero". I dati infatti di regola arrivano a destinazione, anche tra computer operanti a poca distanza fisica e all'interno di un singolo stato, attraversando cavi in varie parti del mondo, ed è comunque impossibile per l'utente conoscere il loro percorso fisico e rendersi conto degli stati attraversati dal messaggio nei quali quest'ultimo potrebbe essere intercettato sulla base di norme locali meno protettive della privacy rispetto allo stato di partenza nonostante il destinatario si trovi nello stesso stato dell'inviante».*
[82] Art. 45 del Regolamento UE 2016/679 (GDPR)
[83] Art. 46 del Regolamento UE 2016/679 (GDPR)
[84] La non rivalità indica la circostanza in cui l'uso di un bene da parte di un agente non incide sulla facoltà di goderne completamente da parte di terzi.
La non escludibilità rappresenta invece l'impossibilità di estromettere terzi dal consumo di un determinato bene. *Da www.treccani.it*

Così, nel 1996 con la c.d. “Database Directive” c’è stato il primo tentativo europeo di consentire una proprietà esclusiva sui dati. La direttiva aveva lo scopo di tutelare per un periodo di tempo pari a 15 anni i diritti intellettuali su *database* contenenti dati originali e non originali. In riferimento a questo secondo caso la Direttiva sosteneva che la protezione sarebbe intervenuta se «*il conseguimento, la verifica e la presentazione di tale contenuto attestino un investimento rilevante sotto il profilo qualitativo o quantitativo*» (ex art.7).

D'altronde, la maggior parte dei dati che vengono raccolti ed elaborati non rappresentano produzioni originali dell’intelletto umano, ma piuttosto la rappresentazione di fatti e descrizioni della realtà in linguaggio informatico. Dunque, non è così semplice applicare le norme della proprietà intellettuale alla proprietà dei dati, in quanto viene creata con fini differenti[85]. Di fatto, lo scopo del diritto d’autore è quello di ridurre ed eliminare la pratica sempre più diffusa di copiare libri e altre opere scritte senza il permesso di autore e proprietari.

A seguire, un intervento della Corte di Giustizia dell’Unione Europea ha sottolineato l’inadeguatezza della direttiva rispetto all’evoluzione a cui è andato incontro l’uso dei dati.

L’intervento della Corte era stato in merito alla decisione del caso *The British Horseracing Board Ltd and Others v. William Hill Organization Ltd*, nel 2004[86]. Il contenzioso era nato dall’utilizzo di informazioni nel *database* BHB[87] da parte dell’agenzia di scommesse William Hill e dall’interpretazione degli articoli 7 e 10 della Direttiva. Tutto ciò aveva condotto ad un cambio di prospettiva riguardante la tutela della proprietà dei dati offerta dall’ordinamento europeo.

La conclusione della Corte è stata che l’”investimento rilevante” di per sé non era sufficiente per avere diritto alla protezione menzionata dalla Direttiva. Essa

[85] THE AVALON PROJECT, *The Statute of Anne*; April 10, 1710, online su *https://avalon.law.yale.edu/18th_century/anne_1710.asp*
[86] Causa C-203/02, Sentenza della Corte (grande sezione) del 9 novembre 2004; The British Horseracing Board Ltd e altri contro William Hill Organization Ltd.
[87] The British Horseracing Board Ltd, il Jockey Club e Weatherbys Group Ltd (in prosieguo: «BHB»)

ricopre solo l'investimento effettuato per creare un *database*, ma non riguarda la spesa per ricercare i dati inseriti. Per cui nel caso in questione, l'aver dovuto investire in un call center per la raccolta dei dati sulle corse di cavalli, confluiti poi negli archivi di BHB, non concorre a determinare l'investimento sul database.

Da questa decisione si coglie quindi che la Direttiva tutela esclusivamente l'investimento fatto sul solo *database*. Invece, la fase di raccolta, attuata anche con altri mezzi come dei sensori, non è coperta dalla protezione esistente. Dato che, la quasi totalità dei dati elettronici è ravvolta attraverso dei sensori o altri dispositivi, è concesso qualsiasi riutilizzo di dati, purché esso non leda l'investimento fatto per archiviarli.

Un problema analogo era stato riscontrato dalla Corte Suprema negli Stati Uniti. La Corte in questo caso aveva sottolineato la non compatibilità tra il diritto d'autore e la maggioranza dei dati informatici, soprattutto per la caratteristica citata prima, ossia la natura di descrizione di fatti. Nel caso in questione era stato contestato un mancato rispetto del diritto d'autore per un caso di utilizzo di elenchi telefonici copiati da un'altra azienda[88]. Secondo il Giudice Supremo però, i fatti non possono essere soggetti a *copyright,* quindi la rielaborazione dei dati relativi a tali fatti devono avere almeno un minimo grado di originalità intellettuale.

Questo implica che la tutela potrebbe essere allargata al metodo o al format usato per la raccolta e l'organizzazione di tali fatti, ma non ai fatti in sé considerati.

1.5 La valorizzazione economica e il diritto alla *privacy*

I dati personali sono diventati oggetto di attenzione crescente da parte di istituzione ed imprese, proprio per la notevole capacità di sviluppo che comportano. Di fatto è possibile ottenere enormi vantaggi dalla loro analisi in

[88] U.S. Supreme Court, Feist Publications, Inc. v. Rural Tel. Service Co., 499 U.S. 340, 111 S. Ct. 1282, 113 L. Ed. 2d 358,1991 U.S.

termini di potere e controllo[89] sotto diversi aspetti: quello del mercato (c.d. *business intelligence, behavioural advertisin*g)[90], quello finanziario (*FinTech, TechFin*)[91], quello politico, anche con riferimento alla manipolazione a fini elettorali[92] e quello governativo[93]. Inoltre, i dati personali sono spesso utilizzati in modelli di *business* assai redditizi, frequente è infatti l'accostamento di dati personali al "nuovo petrolio", per indicare appunto le nuove opportunità commerciali che possono derivare dal loro trattamento.

La Commissione Europea ha infatti sottolineato che *«Nel corso degli ultimi anni le tecnologie digitali hanno trasformato l'economia e la società, influenzando ogni settore di attività e la vita quotidiana di tutti i cittadini europei. Nel contempo, il volume crescente di dati industriali non personali e di dati pubblici in Europa, unito ai cambiamenti tecnologici riguardanti le modalità di conservazione ed elaborazione dei dati, costituirà una potenziale fonte di crescita e innovazione che è opportuno sfruttare*»[94].

Tra la costante tensione tra l'interesse economico e il guadagno di competitività nel mercato europeo da un lato, e la tutela della persona dall'altro, sorge una chiara presa d'atto della rilevanza, anche patrimoniale, dei dati personali[95].

---

[89] S. RODOTÀ, *Tecnologie e diritti,* Il Mulino, Bologna, 1995, p.34; A. MANTELERO, *Big Data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Il Diritto dell'Informazione e dell'Informatica, (*2012) 1, pp.135-136.

[90] M. BOURREAU, A. DE STREEL E I. GRAEF, *Big Data and Competition Policy: Market Power, Personalised Pricing and Advertising,* in *SSRN*, (February 16, 2017), online in *https://ssrn.com/abstract=2920301.*

[91] F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa Europa,* (2021)1, p.208

[92] C. FOCARELLI, *La privacy. Proteggere i dati personali oggi*, Il Mulino, Bologna, 2015, pp.13-16; F. BRAVO*, Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa Europa,* (2021)1, p.208

[93] G. RESTA, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/ UE*, in *Diritto dell'Informazione e dell'Informatica*, 2015, pp.697-698; Z. ZENCOVICH, *Intorno al caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in *Diritto dell'Informazione e dell'Informatica*, 2015, pp. 683-684.

[94] Comunicazione UE (2020)86, *Una strategia Europea per i Dati*, cit., p.1.

[95] F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa Europa,* (2021)1, p.210

Oggi l'esposizione online degli utenti e la fruizione dei servizi telematici sono in continua crescita[96], così come sono state potenziate le capacità di raccolta e di calcolo dei dati riferiti agli utenti, che vengono analizzati con tecniche sempre più sofisticate in quanto basate su sistemi di intelligenza artificiale[97].

Alcuni modelli di business si basano appunto su operazioni di "scambio dati", vale a dire operazioni che prevedono la fornitura di servizi a titolo oneroso con controprestazioni non monetarie, ma che si basano sull'accesso, la comunicazione e l'uso di dati personali dell'utente, per fini economici[98]. Come già sottolineato, è molto diffusa quindi la prassi di offrire dei servizi della società

---

[96] Secondo alcune stime fatte nel mercato americano alla fine del secolo scorso *«consumer marketers are currently paying between 10 cents and US$2.50 for profiles of consumers, often based on their zip code and buying habits»*; SULLIVAN, *How Much is Your Playlist Worth?*, in *Wired News*, 1999, 11th March and 3rd November, reperibile online sul sito *www.wired.it*. Il che, rapportato al numero complessivo di persone di cui una data company tratta dati personali, ha fatto stimare, nel 1999, che *«these people digest $75 billion worth of customer information every year»*; SULLIVAN, *How Much is Your Playlist Worth?*, cit.; SCHWARTZ, *Property, Privacy, and Personal Data*, in 117 Harv. L. Rev., 2003-2004, p. 2056, n. 1. Attualmente le stime si aggirano fino a 50 $ circa per ciascun profilo; V. Z. ZENCOVICH, *Do "data markets" exist?*, in *Media Laws*, 2019, cit., p. 23.

[97] Esempio Facebook: se si tiene a mente che la sola Facebook, su scala globale, vanta ora ben *«2.603 bilion monthly active users (MAU)»* (Il numero è ripreso dalle statistiche aggiornate al 1° maggio 2020, riportate da Smith, 250 Amazing Facebook Statistics and Facts for 2020. By the Numbers, in DMR. Business Statistics, 2010, 14th July (last update), consultabile online su https://expandedramblings.com/index.php/by-thenumbers-17-amazing-facebook-stats/#3-facebook-user-statistics-anddemographics). Inoltre, come precisato dall'AGCM in recenti provvedimenti sanzionatori di pratiche commerciali scorrette perpetrate tramite il noto social network, in riferimento proprio all'utilizzo di dati personali degli utenti, dopo aver rimarcato che Facebook Inc. e Facebook Ireland Ltd. sono rispettivamente capogruppo e società operativa a livello europeo, ha evidenziato *che «Il fatturato consolidato di Facebook Inc., al 31 dicembre 2019, risulta pari a 62,931 miliardi di euro (fonte SEC, sulla base del tasso di cambio euro/dollaro al 31 dicembre 2019)»* (AGCM, provv. del 9 febbraio 2021, p. 4, consultabile online all'url www.agcm.it/dotcmsdoc/allegati-news/IP330_chiusura.pdf), mentre *«Il fatturato di Facebook Ireland Ltd., al 31 dicembre 2019, risulta pari a 34,326 miliardi di euro»*. Si tratta di dati particolarmente significativi se confrontanti con l'altra evidenza, emersa in fase di istruttoria nei procedimenti dell'AGCM, ossia che *«i ricavi provenienti dalla pubblicità on line, basata sulla profilazione degli utenti a partire dai loro dati, costituiscono l'intero fatturato di Facebook Ireland Ltd. e il 98% del fatturato di Facebook Inc»* (Cfr. AGCM, provv. del 29 novembre 2018, n. 27432, così come riportato da T.a.r. Lazio, Roma, sentt. 260 e 261 citt., par. 2 delle motivazioni in diritto, su cui v., amplius, F. BRAVO, *La «compravendita» di dati personali?* in *Diritto di Internet*, 2020, 3, p. 521-540.)

[98] M. BOURREAU, A. DE STREEL E I. GRAEF, *Big Data and Competition Policy: Market Power, Personalised Pricing and Advertising*, in *SSRN*, (February 16, 2017), p.31 online in https://ssrn.com/abstract=2920301. «*This is also the new business model of the (often) Internet firms offering products which are supposedly free because they are not paid with money but with data (whose value has increades with the development of big data)».*

dell'informazione senza pretendere un corrispettivo in denaro ma richiedendo la prestazione del consenso al trattamento dei dati personali dell'utente in cambio del servizio.

L'uso di determinati servizi da parte dell'utente genera automaticamente dati sulle preferenze e sui comportamenti, come ad esempio le abitudini di consumo, ma spesso accade che quando si accede ad un servizio, venga chiesto all'utente di consentire il trattamento dei propri dati personali per fini che non riguardano l'erogazione del servizio[99]; molto spesso tale consenso è posto come condizione necessaria per accedere al servizio stesso: si tratta delle c.d. operazioni di *tying.*

In questo modo si compie uno scambio tra il servizio e i dati personali dell'utente che diventano, almeno di fatto, il corrispettivo per usufruire della controprestazione.

Ma perché i dati personali stanno assumendo sempre più importanza?

Nell'introduzione del libro *The Value of Personal Data*, l'autore scrive che *«per preservare il valore inestimabile della nostra persona, abbiamo bisogno di confrontarci con il valore calcolabile dei dati personali, da cui dipende oggi la riuscita di così tante scelte progettuali e strategiche nella pubblica amministrazione e nell'industria»*[100].

Secondo i dati del Cisco Annual Internet Report (2018 – 2023)[101], entro l'anno 2023 gli utenti di Internet saranno 5,3 miliardi, ossia il 66% della popolazione

---

[99] I dati raccolti nell'erogazione del servizio sono di diverso genere: alcuni sono indispensabili per l'erogazione del servizio, ad esempio quando si richiede l'indirizzo dell'utente per la consegna di un bene acquistato online, altri invece non sono strettamente necessari all'erogazione del servizio ma hanno scopi di marketing o di profilazione. Questi ultimi vanno a costituire il "corrispettivo "del servizio" (S. THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in *Media Laws, Rivista di Diritto dei Media*, (2019) 3, p.132)

[100] M.HILDEBRANDT-K. O'HARA-M. WAIDNER, *Digital Enlightenment Yearbook. The value of personal data*, IOS Press, Amsterdam, 2013 p.4. Il fraseggio originale in lingua inglese è il seguente: *«to preserve the invaluable value of our personhood we need to engage with the calculable value of the personal data on which so many business cases in public administration and industry now depend».*

[101] Cisco Annual Internet Report (2018–2023) White Paper, 2020, online su *https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html*

mondiale e si calcola anche che ogni persona sarà in possesso di 3,6 *device* connessi alla rete. Questi dati non sorprendono dato che riflettono una tendenza prevista da tempo, vale a dire la crescita inevitabile degli utenti connessi alla rete. Il dato più stupefacente riguarda infatti le attività che quotidianamente sono svolte online. Secondo il quadro fornito (dalla società Domo), nel 2020 sono caricate su Facebook 147mila foto al minuto, su WhatApp sono condivisi oltre 41 milioni di messaggi, su Instagram postate quasi 350mila storie e infine, su YouTube vengono caricati video della durata di 500 0re complessive. Sempre in 60 secondi, l'app del momento Tik Tok viene installata 2.707 volte mentre Zoom ospita 200mila partecipanti ai vari *meetings*[102].

Si può dunque affermare che la nostra società sia in qualche modo trainata dai dati, nuovi fonti di ricchezza dell'economia, paragonati spesso al petrolio o all'oro nero[103]. Di fatto i dati personali, se da una parte sono rientrano nella sfera soggettiva in quanto riguardano la persona, dall'altra sono oggetto[104] di uso da parte di attori pubblici e privati e spesso vengono qualificati come assets, prodotti e in sede europea anche "fattori di produzione"[105].

Il paragone con l'oro nero o il petrolio può risultare inopportuno se si pensa al fatto che in gioco ci sono principi, valori, libertà e diritti fondamentali, che potrebbero essere svalutati a causa di una mercificazione di difficile inquadramento giuridico. I diritti in questione sono il diritto alla privacy, per cui alla protezione dei dati personali che implica a sua volta il diritto alla riservatezza. Il diritto alla privacy, riconosciuto ad ogni persona, è inviolabile e indisponibile.

«Globally, the total number of Internet users is projected to grow from 3.9 billion in 2018 to 5.3 billion by 2023 at a CAGR of 6 percent. In terms of population, this represents 51 percent of the global population in 2018 and 66 percent of global population penetration by 2023».

[102] R. PANETTA, *Dati personali, sì alla valorizzazione no alla monetizzazione*, in *Corriere Comunicazioni*, 2020, online su *https://www.corrierecomunicazioni.it/privacy/dati-personali-si-alla-valorizzazione-no-alla-monetizzazione/*

[103] Metafore ricorrenti nei documenti di molte istituzioni, tra cui il discorso *The big data revolution,* del vice-presidente della Commissione Europea, del 26 marzo 2013, consultabile all'indirizzo *https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156*

[104] C. ANGIOLINI, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, G. Giappichelli Editore, Torino, 2020 p.2. L'autrice sostiene che i dati personali si collocano al crocevia tra soggetto e oggetto.

[105] Comunicazione UE (2020)86, *Una strategia Europea per i Dati*, p.15.

Questo è ribadito anche dal Regolamento Generale sulla Protezione dei Dati che scrive *«La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale*»[106]. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea stabiliscono che *«ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano».*

Importante per la questione è la Comunicazione n.7[107] sul tema "Scambio e protezione dei dati personali in un mondo globalizzato", che scrive *«Il rispetto della privacy è una condizione necessaria per flussi commerciali stabili, sicuri e competitivi a livello mondiale. La privacy non è una merce di scambio».*

Da sottolineare è il fatto che senza lo specifico intervento del legislatore dell'UE nell'area in comune tra diritto dei consumatori e della protezione dei dati personali, la regolamentazione delle piattaforme online veniva adibita soprattutto agli Stati membri, procurando un'incertezza giuridica degna di nota in ambito nazionale e internazionale. Il Garante Europeo della protezione dei dati ha prima di tutto ritenuto essenziale una rivoluzione nel campo del diritto dei consumatori europeo, del diritto contrattuale e della protezione dei dati.

La primaria questione è stata la cosiddetta "mercificazione dei dati personali". Come detto, i dati personali degli individui sono considerati un valore della personalità da proteggere e preservare e per questo occupano un posto preciso nella zona di salvaguardia delle istituzioni dell'UE. Tuttavia, la realtà può scontrarsi con le intenzioni e la visione del legislatore. Gli accademici hanno cercato di criticare e contestare l'idea di una "non mercificazione" dei dati personali. Nell'attuale quadro legislativo il valore di "merce" per i dati personali è stato escluso, di fatto la Direttiva del 15 aprile 2019 "relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali" ha chiarito la posizione del legislatore in merito: *«Oltre a riconoscere appieno che la protezione*

[106] Art. 1 del Regolamento UE 2016/679
[107] Parere del Comitato economico e sociale europeo sullo «Scambio e protezione dei dati personali in un mondo globalizzato» COM(2017) 7.

dei dati personali è un diritto fondamentale e che tali dati non possono dunque essere considerati una merce, la presente direttiva dovrebbe garantire che i consumatori abbiano diritto a rimedi contrattuali, nell'ambito di tali modelli commerciali». Resta ancora da chiarire però se si possa parlare di "proprietà" nei confronti dei dati.

Gli accademici e almeno uno dei legislatori degli Stati membri[108] sono inclini a valutare i dati come merce negoziabile e a riconoscerne un diritto di proprietà su di essi. Le direttive seguenti[109] però escludono completamente la configurazione di uno schema di "mercificazione dei dati". Esse, le Direttive 770/2019, 771/2019 e 2161/2019 rappresentano anche uno sforzo coraggioso e necessario nelle interazioni tra diritto dei consumatori e protezione dei dati personali.

In particolare, la Direttiva UE 770/2019 relativa a determinati aspetti dei contratti di fornitura di contenuti digitali e di servizi digitali e la Direttiva UE 771/2019 relativa a determinati aspetti dei contratti di vendita di beni hanno l'obiettivo di ottenere una maggiore protezione per i consumatori a livello europeo, attraverso l'instaurazione di un mercato unico digitale e l'aumento della certezza giuridica in merito ai contratti di vendita.

Di fatto i dati personali per la maggior parte delle aziende rappresentano un patrimonio molto prezioso, in grado di trainare mercati interi[110]. Le tecniche di raccolta, monitoraggio e sfruttamento sono entrate a far parte degli asset fondamentali di queste aziende. Secondo la ricerca dell'Osservatorio Big Data Analytics Intelligence della School Management del Politecnico di Milano[111] il

[108] Lussemburgo: come esposto nel "Projet de loi portant modification de l'article 567 du Code de commerce", il legislatore lussemburghese ha chiaramente riconosciuto la piena legittimità nel parlare in termini di "proprietà di dati"
[109] Applicabili dal 1° gennaio 2022
[110] M. BOURREAU, A. DE STREEL E I. GRAEF, *Big Data and Competition Policy: Market Power, Personalised Pricing and Advertising*, in *SSRN*, (February 16, 2017), p.31 online SU *https://ssrn.com/abstract=2920301*.
[111] Politecnico Milano, school of management "*Strategic Data Science: time to grow up!",* 19 novembre 2019, online su *https://www.som.polimi.it/event/osservatorio-big-data-analytics-bi-191119/*
«In questi ultimi anni, i Big Data Analytics, da innovazione di successo per poche aziende proattive, sono diventati una necessità per sopravvivere alla competizione presente sul

valore del mercato dei Big Data Analytics solo in Italia è di 1,7 miliardi di euro[112] e il 93% delle grandi aziende sta investendo proprio in progetto Analytics.

Se questi dati sembrano sorprendenti, basta pensare ad alcune esperienze quotidiane della moderna società dell'informazione riguardante proprio questa rilevanza economica dei dati: uno spazio pubblicitario viene venduto a prezzi diversi in base alle informazioni che si pubblicano; il numero di click, e di conseguenza di introiti pubblicitari, di una notizia cambia in base del protagonista della storia; infine l'offerta di beni e servizi diventa più efficace se si conoscono le abitudini di consumo del cliente.

Per questi motivi il valore economico assunto dai dati personali non deve sorprendere o allarmare. Si tratta di attività lecite, autorizzate e regolamentate dal legislatore e dalle autorità.

La domanda che sorge spontanea è: fin dove può spingersi questa valorizzazione economica dei dati personali senza scontrarsi con il diritto fondamentale alla privacy? Essendo il diritto alla *privacy* un diritto costituzionale[113], esso sancisce il divieto a trasformare il bene giuridico su cui insiste, quindi il dato personale, in mera merce, dato che si tratta di un bene idoneo a rilevare la capacità di godimento dei diritti e delle libertà di un individuo. Questo perché attribuire un prezzo in modo diretto a un proprio dato personale e scambiarlo come un bene in cambio di denaro, renderebbe disponibile un diritto che per definizione deve

mercato. Le aziende hanno portato avanti investimenti tecnologici e internalizzato professionalità qualificate nell'ambito della Data Science, dando vita a nuovi modelli organizzativi per favorire il coordinamento e lo sviluppo di progettualità innovative».

[112] Dato relativo al 2019

[113] «*Il diritto alla riservatezza, quale diritto della personalità, consente di individuare il correlativo fondamento giuridico ancorandolo direttamente all'art. 2 Cost., norma di carattere precettivo e non programmatico*». Corte di Cassazione sent. 5658/1998.
Prima che si giungesse ad una normativa espressa in materia, i primi riferimenti alla privacy si possono far risalire alla Convenzione europea dei diritti dell'uomo e delle libertà fondamentali (CEDU), ratificata dall'Italia nel 1955**,** che prevede all'art. 8 che *«ogni persona ha diritto al rispetto della propria via privata e familiare, del proprio domicilio e della propria corrispondenza».*

essere indisponibile e comporterebbe una monetizzazione e una alienazione di tutti i diritti e le libertà a cui quel dato fa da presidio e ponte.

Dunque, l'accostamento con l'elemento del prezzo condurrebbe a creare un aberrante mercato dei dati personali, caratterizzato da una corsa al ribasso del tutto contraria all'etica pubblica.

Ne deriva che la valorizzazione economica dei dati non dovrebbe andare oltre questi confini giuridici ed anche etici. Il Presidente dell'Autorità Garante Italiana ha ribadito in un'intervista che *«i dati personali, prima che una risorsa economica, costituiscono un bene giuridico, oggetto di un diritto "di libertà" che, come tale, non può essere alienato. Una delle sfide più delicate riguarda proprio la monetizzazione dei dati. Se. Infatti, si legittimasse la remunerazione dei rapporti sociali, ammettendo che per necessità si possa essere disposti a cedere, con i dati, la propria libertà».*

Vi sono per cui alcuni limiti che non dovrebbero essere superati: si tratta di sottoporre il dato personale alle regole del mercato, dunque trattare le informazioni come delle merci o introdurre l'elemento sovversivo del prezzo. Per cui i dati personali non possono essere paragonati al petrolio, come una merce[114] da fornire al migliore offerente. Dunque, se una valorizzazione può essere accettata, una monetizzazione diretta delle informazioni personali non può essere permessa.

Ovviamente la valorizzazione dei dati personali continuerà ad espandersi ed è necessario che il legislatore, sia a livello nazionale che sovranazionale, sia sempre aggiornato sugli ultimi sviluppi tecnologici per consentire sempre un

[114] V. infatti il cons. 24, della direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio del 20 maggio 2019 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali, in cui si precisa che *«Oltre a riconoscere appieno che la protezione dei dati personali è un diritto fondamentale e che tali dati non possono dunque essere considerati una merce, la presente direttiva dovrebbe garantire che i consumatori abbiano diritto a rimedi contrattuali, nell'ambito di tali modelli commerciali»; S. THOBANI, Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente, in Media Laws, Rivista di Diritto dei Media, (2019) 3, p.146; S. RODOTÀ, Tecnologie e diritti, Il Mulino, Bologna, 1995, p.47.*

giusto bilanciamento tra tutela di un diritto fondamentale da una parte ed esigenze di mercato dall'altra.

A differenza degli anni 2000, in cui ci si stupiva ancora del miracolo della rete fondato sull'offerta, apparentemente gratuita, di una grande molteplicità di servizi, oggi i consumatori stanno diventando sempre più consci del fatto che i grandi colossi del *web* ricavano parte dei loro profitti proprio dalla "compravendita" dei dati personali. Per questi motivi si è innescato un meccanismo secondo cui i dati personali vengono percepiti come "merce di scambio" che viene concessa dagli utenti per ottenere determinati servizi, senza dover pagare un corrispettivo in denaro, e che viene acquistata dalle imprese per poter offrire ai consumatori dei servizi ad-hoc, proporre spazi pubblicitari mirati e quindi destinarla al commercio con terzi.

L'interrogativo da cui muovere è la possibile qualificazione dei dati personali come beni e le conseguenze che ne derivano con riguardo alla tutela dell'interessato[115]. In dottrina si è discusso molto riguardo la qualificazione dei diritti dell'interessato, sia secondo la prospettiva delle situazioni giuridiche che vede tali diritti come facoltà che connotano il diritto alla protezione dei dati personali[116], sia in una prospettiva rimediale[117]. Dal punto di vista rimediale, la visione di dati come beni consente di classificare, per quanto riguarda gli effetti, tali diritti rispetto alla ricostruzione della posizione dell'interessato circa il regime d'uso e di circolazione dei dati personali. Queste prerogative, dal punto di vista dei risultati sono destinate a permettere la conoscenza dei trattamenti dei dati personali in atto (diritto di accesso), ad assicurare l'accesso ai dati personali raccolti e il loro possibile utilizzo da parte degli interessati (diritto di copia e diritto

[115] C. ANGIOLINI, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, G. Giappichelli Editore, Torino, 2020 p.133.
[116] C. CASTRONOVO, *Situazioni soggettive e tutela nella legge sul trattamento dei dati personali*, in *Eur. dir. priv*., 1998, p. 653 ss, secondo cui «*la tutela di cui discorriamo è arricchita di una serie di facoltà che al soggetto interessato sono attribuite direttamente (…). In particolare, i diritti previsti (…) compongono una raggiera di tutela interprivata*».
[117]V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, *I dati personali nel diritto europeo*, G. Giappichelli Editore, Torino, 2019, p. 355

alla portabilità), a modificare il regime del bene con riguardo ai trattamenti possibili (diritto alla limitazione del trattamento, diritto di opposizione), a trasformare il bene stesso (diritto di rettifica) e infine ad imporne la distruzione diritto alla cancellazione)[118].

Di fatto, nel nuovo contesto economico e sociale, ogni persona deve essere consapevole della necessità di non impedire che i propri dati circolino, se vuole appartenere pienamente al mondo di oggi, ma deve anche essere messa al corrente dei pericoli derivanti da tale circolazione per i diritti e le libertà individuali. Per cui la questione fondamentale riguardante la tutela dell'interessato è quella di garantirgli un potere di controllo sui dati che lo riguardano. Vale a dire che deve essergli assicurato che i propri dati personali, se trattati da un'altra persona, saranno protetti secondo le modalità e gli standards definiti dalla legge, in modo da concedergli concretamente di mantenere un controllo sulla circolazione delle informazioni a lui riferibili e di determinare le condizioni e i limiti del trattamento delle stesse[119].

[118] C. ANGIOLINI, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, G. Giappichelli Editore, Torino, 2020 pp.134-144.
[119] M. GAMBINI, *La protezione dei dati personali come diritto fondamentale della persona: meccanismi di tutela*, in *ESPAÇO JURÍDICO*, 2013, pp.5-6.

CAPITOLO SECONDO - IL CONSENSO AL TRATTAMENTO DEI DATI PERSONALI E L'EVOLUZIONE DELLA NORMATIVA ALLA LUCE DEL GDPR

2.1 Il consenso e i principi del trattamento dei dati personali

Il trattamento dei dati personali, per essere lecito, deve avere come fondamento una delle basi giuridiche sancite dal Regolamento Generale sulla Protezione dei Dati Personali[120].

La base giuridica è ciò che autorizza il trattamento, in modo che sia rispettato il principio di liceità: in mancanza di essa il trattamento è ritenuto illecito.

È compito del titolare del trattamento giudicare quale sia la base giuridica più adatta per il trattamento che intende eseguire, funzione che deve svolgere prima del trattamento stesso[121]. Il titolare non è libero di scegliere la base giuridica che preferisce, ma deve seguire le indicazioni sancite del GDPR all'art. 6 dove sono elencate le caratteristiche delle basi giuridiche[122].

L'art. 5 del Regolamento inoltre elenca tutti i principi su cui si deve fondare il trattamento: prima di tutto i dati personali devono essere *«trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza")»*[123].

Il trattamento quindi dei dati deve sempre ispirarsi al principio di liceità, trasparenza e correttezza.

Il principio di trasparenza è una delle novità apportate dal Regolamento. Esso stabilisce che le comunicazioni riguardanti il trattamento di dati devono essere

---

[120] Regolamento UE 679/2016 (GDPR)

[121] EDPB, *Linee guida 5/2020 sul consenso ai sensi del Reg (UE) 2016/679*, 4 maggio 2020, p.28. *«L'articolo 6 stabilisce le condizioni per la liceità del trattamento dei dati personali ed elenca sei basi legittime su cui il titolare del trattamento può fondarsi. L'applicazione di una di queste sei basi deve essere stabilita prima di procedere al trattamento e in relazione a una finalità specifica».*

[122] Ogni base giuridica è fondata su condizioni specifiche ed ha conseguenze diverse sui diritti delle persone. Non esiste una gerarchia tra di esse.

[123] Art. 5, par.1, lett. *a)* del Regolamento UE 679/2016 (GDPR)

facilmente accessibili e comprensibili, si deve per cui utilizzare un linguaggio semplice e chiaro.

Esso è strettamente collegato a quello della limitazione delle finalità[124], che prevede che ci sia una corrispondenza tra quanto viene dichiarato dal titolare del trattamento a quanto poi viene realmente eseguito nell'impiego dei dati. Dunque, i dati personali raccolti e trattati devono essere adeguati, pertinenti e limitati a quanto necessario per le finalità dichiarate del trattamento[125].

In ragione del principio della limitazione delle finalità del trattamento[126], i dati personali sono destinati ad usi circoscritti; di fatti, secondo quanto stabilito dall'art. 5 del Regolamento, i dati personali devono essere raccolti per scopi determinati, espliciti e legittimi, e di seguito, trattati in modo che sia compatibile con tali scopi[127]. Le finalità non possono essere ambigue o identificate in modo vago dato che tale formulazione minerebbe la condizione di liceità del trattamento. I criteri per decretare la compatibilità delle finalità sono forniti dall'art. 6, par. 4 del Regolamento; esso privilegia il trattamento che abbia come finalità quella di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici[128].

---

[124] A. PISAPIA, *La tutela per il trattamento e la protezione dei dati personali*, G. Giappichelli Editore, Torino, 2018, cit., pp.44-45. *«Il principio di finalità è particolarmente rilevante nelle operazioni di trattamento svolte da soggetti privati; nel caso in cui sia un soggetto pubblico a essere titolare del trattamento il presupposto della legittimità del trattamento non sarà il consenso dell'avente diritto, ma la base giuridica del trattamento effettuato sarà da riscontrarsi nella legge. È questo, per esempio, il caso dei dati personali trattati per finalità giudiziarie o, come previsto all'art. 10 del GDPR, per il trattamento dei dati personali relativi a condanne penali o reati. Anche qualora il trattamento sia previsto dalla legge, sarà comunque necessario che il titolare informi l'avente diritto della base giuridica obbligatoria applicabile, ma non sarà necessario acquisirne il consenso».*

[125] S. RODOTÀ, *Tecnologie e diritti,* Il Mulino, Bologna, 1995, p.62

[126] Principio menzionato anche dall'art.8 CDFUE

[127] Il considerando 50 del Regolamento UE 679/2016 stabilisce che *«il trattamento dei dati personali per finalità diverse da quelle per le quali i dati personali sono stati inizialmente raccolti dovrebbe essere consentito solo se compatibile con le finalità per le quali i dati personali sono stati inizialmente raccolti»*. Con riguardo alla distinzione tra raccolta e ulteriore trattamento si veda anche GRUPPO DI LAVORO ART.29, Opinion 2/2013 on purpose limitation, 2 aprile 2013, p.21.

[128] C. ANGIOLINI, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, G. Giappichelli Editore, Torino, 2020 pp.159-160. Secondo una parte della dottrina il termine "fini statistici" può avere un'interpretazione estensiva, includendo quindi anche la ricerca a fini

Spesso, la finalità del trattamento è intrinsecamente connessa all'adempimento di un'obbligazione contrattuale, si pensi ad esempio nei contratti bancari o quelli riguardanti un acquisto tramite *e-commerce*. In tali casi, il titolare dovrà comunicare all'utente che la mancanza di consenso al trattamento renderà impossibile eseguire il contratto e dunque anche l'erogazione del servizio annesso. Il consenso informato dato dal titolare sarà strettamente vincolato alla finalità primaria del trattamento, dato che non è obbligatorio fornire il consenso per finalità secondarie come la profilazione o il *marketing*[129]. Nel caso in cui il trattamento avvenga per ulteriori finalità, oltre a quelle dichiarate, questo non comporta necessariamente l'illiceità del trattamento.

È però necessario che ci sia compatibilità tra le finalità dichiarate inizialmente e il successivo trattamento; è compito del titolare giudicare la liceità del trattamento successivo, effettuando la valutazione dei rischi caso per caso e, in applicazione del principio *privacy by design* and *by default*, adotterà le sue decisioni, con la consapevolezza che se le sue scelte violeranno la tutela dei dati personali, dovrà affrontare aspre sanzioni. Se le finalità aggiuntive fossero necessarie per il raggiungimento di quelle iniziali, esse non potrebbero essere ritenute incompatibili e di conseguenza il consenso fornito inizialmente si estenderà come base giuridica anche al trattamento ulteriore.

Un altro principio fondamentale del trattamento dei dati è il principio di necessità e minimizzazione, sancito sempre dall'art. 5 del Regolamento per cui i dati personali devono essere *«adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati»*[130]. Questo significa che non possono essere accumulati senza un preciso scopo e non possono essere conservati per

commerciali, e questa prospettiva sembra essere confermata dai considerando del Reg. UE 2016/679. Per esempio, il considerando 59 prevede che *«il trattamento di dati personali per finalità di ricerca scientifica dovrebbe essere interpretato in senso lato e includere ad esempio sviluppo tecnologico e dimostrazione, ricerca fondamentale, ricerca applicata e ricerca finanziata da privati».*

[129] A. PISAPIA, *La tutela per il trattamento e la protezione dei dati personali*, G. Giappichelli Editore, Torino, 2018, p.45.

[130] Art. 5, par.1, lett. *c)* del Regolamento EU 679/2016 (GDPR)

un tempo eccessivamente lungo senza una specifica motivazione[131]; dunque, la finalità dei dati deve essere la più specifica possibile, limitando la quantità di dati raccolti e la loro collezione in banchi dati[132]. La rilevanza del criterio della necessità è dovuta anche al suo ruolo nella costruzione delle basi giuridiche del trattamento, differenzi dal consenso, come ha recentemente confermato anche la Corte di giustizia in un caso riguardante l'applicazione della base giuridica del legittimo interesse[133]. Va precisato che la valutazione riguardante la necessità del trattamento rispetto alle finalità, non è svolta una volta per tutte, essa al contrario, può cambiare, anche a causa dell'evoluzione tecnologica, che potrebbe far diventare eccessivo il trattamento dei dati a causa dell'impiego di mezzi meno invasivi[134].

Inoltre, il principio di esattezza o accuratezza stabilisce che i dati trattati debbano essere esatti, veritieri, completi ed aggiornati per le finalità del trattamento se

---

[131] A. PISAPIA, *La tutela per il trattamento e la protezione dei dati personali*, G. Giappichelli Editore, Torino, 2018, p.49; l'autrice fornisce un esempio riguardante gli acquisti on-line: il titolare deve raccogliere i dati di fatturazione, quelli relativi al pagamento e quelli relativi al recapito dell'acquisto; tuttavia, non è strettamente necessaria all'esecuzione del contratto di acquisto la tracciatura dei gusti del cliente. Questa operazione è utile al titolare per le sue strategie di marketing che sono lecite solo se presenti tra le finalità previste dall'informativa e ricomprese nel consenso informato già espresso dall'interessato.
G. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Zanichelli Editore, Bologna, 2012, pp.114-116.Nel caso delle applicazioni del cellulare, ogni eventuale funzionalità non necessaria al funzionamento di un'app, come l'accesso al rullino fotografico o la geolocalizzazione, dovrà essere preveduta da un'apposita informativa e dall'acquisizione del consenso dell'utente.

[132] Nell'opinione 1/2014 il Gruppo di Lavoro Articolo 29 interpreta la minimizzazione del trattamento come la non eccedenza dello stesso e la pertinenza dei dati rispetto alle finalità dichiarate.

[133] Nella pronuncia CGUE, *Asociatia de Proprietati bloc M5A-ScaraA, C-708/8,* 11 dicembre 2019, la Corte connette il principio di minimizzazione dei dati e il requisito della necessità del trattamento nell'interpretazione della base giuridica del legittimo interesse, scrivendo che "la condizione attinente alla necessità del trattamento deve essere esaminata unitamente al principio cosiddetto della "minimizzazione dei dati" sancito all'art. 6, par. 1, lett. *c),* della direttiva 95/46/CE, secondo il quale i dati personali devono essere adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e trattati".

[134] C. ANGIOLINI, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, G. Giappichelli Editore, Torino, 2020 pp.161-162. Un esempio del caso è fornito dalla sentenza *Costeja*, dove la Corte di giustizia dell'UE ha evidenziato come un trattamento inizialmente lecito di dati esatti, può diventare incompatibile con le norme in materia di protezione di dati personali "qualora tali dati non siano più necessari in rapporto alle finalità per le quali sono stati raccolti o trattati". CGUE *Google Spain, Google Inc. c. AEPD e Mario Costeja Gonzàles*, C-131/12,13 maggio 2014, p.93.

necessario, *«devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati»*[135].

Il trattamento di dati personali inesatti o non completi potrebbe determinare un'errata rappresentazione dell'individuo interessato che potrebbe subire conseguenza pregiudizievoli[136]; il compito di provvedere alla cancellazione o alla modifica dei dati inesatti o incompleti è del titolare del trattamento, mentre è diritto dell'interessato chiedere l'aggiornamento, l'integrazione o la rettifica, ed infine il titolare dovrà informare l'interessato riguardo alla cancellazione, rettifica o integrazione.

Dopo di che, il principio della limitazione della conservazione stabilisce che i dati personali devono essere *«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»*[137].

Per evitare che siano mantenuti più del necessario, il titolare dovrebbe stabilire un termine per la cancellazione o per una verifica periodica.

Oltre a ciò, il trattamento deve ispirarsi a un principio di integrità e riservatezza, che stabilisce che i dati devono essere sicuri e protetti, per evitarne la perdita e i trattamenti illeciti: *«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»*[138]. Uno degli elementi fondamentali della tutela del

---

[135] Art. 5, par.1, lett. *d)* del Regolamento EU 679/2016 (GDPR)
[136] A. PISAPIA, *La tutela per il trattamento e la protezione dei dati personali*, G. Giappichelli Editore, Torino, 2018, p.48; l'autrice fornisce l'esempio di una mancata attribuzione di titoli e qualifiche legate all'esercizio della professione.
[137] Art. 5, par.1, lett. *e)* del Regolamento EU 679/2016 (GDPR)
[138] Art. 5, par.1, lett. *f)* del Regolamento EU 679/2016 (GDPR)

GDPR è l'uso di adeguate misure di sicurezza, sia tecniche come le password, la pseudonimizzazione o la cifratura, sia misure di tipo organizzativo come la separazione delle informazioni o le procedure di autorizzazione per l'accesso ai dati. Il titolare deve effettuare la valutazione dei rischi ed adottare le misure adeguate; nella valutazione si deve tenere conto dei rischi presentati dal trattamento, come la distruzione accidentale o illegale, la perdita, la modifica, l'accesso di soggetti non autorizzati, che potrebbero provocare un danno fisico, materiale o immateriale[139]. La valutazione d'impatto è prevista all'articolo 35 del Regolamento e ha come obiettivo quello di garantire la sicurezza dei dati ma anche l'individuazione di rischi specifici collegati alle procedure di trattamento di ciascun titolare, con particolare riguardo al trattamento di dati sensibili. Quindi il titolare deve adottare le misure per garantire la sicurezza, effettuare dei test di controllo di anomalie o manomissioni, e nel caso si siano verificate delle violazioni, è tenuto a informare l'interessato[140].

Infine, il principio di responsabilizzazione, una delle novità apportate dal Regolamento, stabilisce che il titolare del trattamento deve garantire il rispetto dei principi applicabili al trattamento dei dati personali.

2.2 Il consenso e le altre basi giuridiche

La condizione più utilizzata per rendere lecito il trattamento è la prestazione del consenso da parte dell'interessato[141].

---

[139] Cons. 83 del Regolamento EU 679/2016 (GDPR)
[140] Art. 34 Regolamento EU 679/2016 (GDPR)
[141] A. QUARTA, G. SMORTO, *Diritto privato dei mercati digitali*, Le Monnier Università, Mondadori Education, Firenze, 2020, p.25; il consenso dell'interessato autorizza il trattamento dei dati. Esso deve essere libero, informato, specifico in relazione alle finalità delle operazioni, autorizzato e deve esprimere in modo inequivocabile la volontà dell'interessato. La prestazione del consenso è un tema che ha preoccupato molto il legislatore europeo, il quale ha introdotto delle cautele normative far sì che l'interessato conosca effettivamente le attività di trattamento per cui sta prestando il consenso. Il GDPR, infatti, stabilisce che la richiesta di consenso dell'interessato che si è prestata con una dichiarazione scritta, in presenza di ulteriori questioni, deve essere presentata in modo chiaramente distinguibile dalle altre materie, in una forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Si veda inoltre A. MANTOVANI, *Questioni relative al trattamento dei dati personali per finalità di*

Oltre a questa, le altre basi giuridiche sono: l'adempimento di obblighi contrattuali o misure precontrattuali, gli obblighi di legge cui è soggetto il titolare del trattamento, interessi vitali della persona interessata o di terzi, il legittimo interesse prevalente del titolare o di terzi cui i dati vengono comunicati[142], l'interesse pubblico o l'esercizio di pubblici poteri. Dunque, il responsabile deve, nel caso in cui non possa giustificare le proprie operazioni di trattamento tramite una espressa base giuridica prevista dal regolamento, acquisire il consenso dell'interessato[143].

È da sottolineare che, se il titolare sceglie il consenso come base giuridica per ogni parte del trattamento, allora egli deve essere pronto a rispettare tale scelta e interrompere la parte del trattamento nel caso in cui l'interessato decida di revocare il consenso. Inoltre, il titolare non può passare dal consenso ad altre basi legittime; sostenere che i dati saranno trattati sulla base del consenso quando in realtà si opta per un'altra base giuridica, sarebbe «formalmente scorretto nei confronti dell'interessato»[144].

---

marketing e profilazione, in *Media Laws, Rivista di Diritto dei Media,* (2019)3, p.2; il consenso rimane la base giuridica più frequente, e spesso imprescindibile.

[142] Con il Regolamento, il legittimo interesse è diventato una base giuridica più facilmente accessibile rispetto a prima; in particolare per quanto riguarda il campo del marketing e della profilazione, il fatto di prescindere dall'obbligo di richiedere il consenso preventivo degli interessati, può comportare consistenti vantaggi operativi per i titolari del trattamento. Per approfondire si veda A. MANTOVANI, *Questioni relative al trattamento dei dati personali per finalità di marketing e profilazione*, in *Media Laws, Rivista di Diritto dei Media,* (2019)3, pp. 2-10. *«Ne discende, infatti, la possibilità di trattare dati personali (in primo luogo, i recapiti utilizzati per contattare i destinatari delle comunicazioni commerciali) per finalità di marketing pur in assenza del consenso di tali destinatari, quando ricorrano le condizioni di cui all'art. 6, comma 1, lett. f) del GDPR. Nello specifico, il trattamento deve essere «necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che», in esito a un bilanciamento fra la posizione di chi vanta l'interesse e quella della persona dei cui dati personali si tratta (c.d. balancing test), «non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore». La possibilità di fondare l'attività di marketing sulla base giuridica del legittimo interesse non è una novità assoluta del GDPR. Prima dell'avvento di tale Regolamento, la base giuridica del legittimo interesse a livello dell'Unione europea era disciplinata dall'art. 7, lettera f), della Direttiva 95/46/CE».*

[143] Cons. 40-42 del Regolamento EU 679/2016 (GDPR)

[144] EDPB, *Linee guida 5/2020 sul consenso ai sensi del Reg (UE) 2016/679*, 4 maggio 2020, cit., p.28. *«Ad esempio, non può ricorrere retroattivamente alla base dell'interesse legittimo in caso di problemi di validità del consenso. Poiché ha l'obbligo di comunicare la base legittima al*

La definizione di consenso è formulata dall'articolo 4 del GDPR[145] come «*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*»[146]. Un requisito essenziale è che il soggetto che presta consenso sia dotato della capacità giuridica per farlo.

Tale base giuridica attribuisce all'interessato il potere di regolare l'estensione del trattamento e di conseguenza di allargare la possibilità di raccolta, uso e circolazione oltre le ipotesi lecite previste dalla legge. Questa facoltà permane in capo all'interessato anche dopo la prestazione del consenso, come testimonia la disciplina riguardante la sua revoca.

La prestazione del consenso è un atto di autonomia privata mediante il quale viene esercitato il diritto alla vita privata e alla protezione dei dati personali: di fatto, in quanto tecnica che permette il trattamento, il consenso può essere considerato come esercizio del diritto alla riservatezza e come una tecnica di tutela e partecipazione dell'interessato rispetto alla costruzione del regime dei dati personali e di conseguenza, come espressione dell'art.8 CDFUE[147], che ne

momento della raccolta dei dati personali, il titolare del trattamento deve aver deciso la base legittima prima della raccolta dei dati».

[145] Art. 4, Par. 11 del Regolamento EU 679/2016 (GDPR).

[146] Il Gruppo di Lavoro Articolo 29 ha fatto notare, nelle *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, cit., p. 5, che la «nozione di consenso rimane sostanzialmente simile a quella della direttiva 95/46/CE». Il considerando 171 del Regolamento (UE) 2016/679 inoltre specifica che i titolari del trattamento che hanno raccolto il consenso degli interessati prima dell'entrata in vigore del Regolamento (UE) 2016/679 non sono sempre tenuti a raccoglierlo nuovamente dato che il «consenso ottenuto continua ad essere valido nella misura in cui è in linea con le condizioni stabilite nel regolamento generale sulla protezione dei dati». Gruppo di Lavoro Articolo 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, 4 maggio 2020, cit., p. 34

[147] Art. 8, Carta dei Diritti Fondamentali dell'Unione Europea (2000/C 364/01); «*Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano».*

fa menzione[148]. Come vedremo in seguito, il Reg. UE 2016/679 lo circonda di una serie di cautele e requisiti[149].

2.3 Requisiti del consenso

Il consenso può rappresentare la base legittima idonea solo se all'interessato vengono concessi il controllo e l'effettiva opportunità di decidere se accettare o meno i termini proposti ed ha quindi la possibilità di rifiutarli senza subire pregiudizio[150]. Pertanto, il titolare che sceglie di basare il trattamento sul consenso è tenuto a verificare che esso abbia determinate caratteristiche[151]; il consenso deve essere:

- Inequivocabile;
- Libero;
- Specifico;
- Informato;
- Verificabile;
- Revocabile.

---

[148] C. ANGIOLINI, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, G. Giappichelli Editore, Torino, 2020, pp.121-122. L'importanza del consenso rispetto all'autodeterminazione del soggetto è messa in evidenza anche dal Gruppo di Lavoro Art.29 che nelle linee guida afferma che questo sia un fondamento valido per il trattamento solo se offre all'interessato «il controllo e l'effettiva possibilità di scegliere se accettare o meno i termini proposti o rifiutarli senza subire pregiudizio»; GRUPPO DI LAVORO ARTICOLO 29*, Linee giuda sul consenso ai sensi del regolamento (UE) 2016/679*, come modificate e adottate il 10 aprile 2018.

[149] *Ivi*, p.22

[150] C. FOCARELLI, *La privacy. Proteggere i dati personali oggi*, Il Mulino, Bologna, 2015, p.70. L'utente deve essere avvisato che saranno raccolti i suoi dati personali, previo il suo consenso. L'autore sostiene che *«il presupposto è che la protezione dei dati personali sia un affare del titolare dei dati e che la sua autonomia sia essenziale alla loro raccolta e uso. L'individuo può scegliere se e fino a che punto i suoi dati possano essere raccolti e usati da altri. Il requisito è sempre più messo in discussione alla luce degli sviluppi tecnologici e sociali dei big data. Si sostiene che nell'era dei big data il valore dei dati personali non emerge al momento della loro raccolta, quando vengono dati l'avviso e il consenso, ma in seguito; che gli avvisi sono ormai così lunghi e complessi che gli utenti non li leggono e comunque non li comprendono, e la raccolta così pervasiva che prestare ogni volta il consenso è un onere troppo gravoso per l'utente, per cui il consenso non è reale».*

[151] Elencate all'art. 7 del Regolamento EU 679/2016 (GDPR)

Il consenso è inequivocabile quando *«il titolare è in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali»*[152]. Una manifestazione inequivocabile di volontà rappresenta una dichiarazione indubitabile[153].

Quindi, per avere la certezza del consenso è necessario che esso si basi su una dichiarazione orale o scritta, eseguita anche per via elettronica[154], ma deve essere un'azione attiva. Ne consegue che l'inattività e il silenzio non possono rappresentare un'indicazione di scelta attiva. L'inerzia non può essere considerata una manifestazione di consenso e nemmeno le caselle precompilate, ma deve esserci una chiara azione positiva come, ad esempio, spuntare una casella o scrivere il proprio indirizzo e-mail in un campo dove è specificato lo scopo per il quale sarà usato[155].

---

[152] Art. 7, Par. 1 del Regolamento EU 679/2016 (GDPR)

[153] A. MANTOVANI, *Questioni relative al trattamento dei dati personali per finalità di marketing e profilazione*, in *Media Laws, Rivista di Diritto dei Media,* (2019)3, p.21

[154] GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, 4 maggio 2020, cit., p. 18 s., dove si sottolinea anche che «*il modo più rigoroso per soddisfare il criterio della "dichiarazione scritta" consiste nell'assicurarsi che l'interessato scriva una lettera o un messaggio di posta elettronica al titolare del trattamento spiegando ciò a cui acconsente esattamente. Tuttavia, spesso ciò non è realistico. Le dichiarazioni scritte possono avere forme e formati diversi che potrebbero essere conformi al regolamento generale sulla protezione dei dati».* Stando alle dichiarazioni del Gruppo di Lavoro Articolo 29, nel contesto dei requisiti di cui al Regolamento (UE) 2016/679, il titolare del trattamento è comunque *«libero di sviluppare un flusso di consenso adatto alla propria organizzazione»,* alcuni esempi possono far scorrere una barra su uno schermo, agitare la mano davanti a una telecamera intelligente, ruotare lo smartphone in senso orario o far compiere ad esso un movimento a otto.

[155] In merito a questo, il Cons. 32 del Regolamento EU 679/2016 (GDPR) sostiene che «*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*

Il consenso può essere anche implicito, ma non tacito, dunque non vale il silenzio, nel momento in cui non vi sia alcun dubbio che col proprio comportamento l'interessato abbia voluto esprimere il proprio consenso.

Vi sono dei casi però in cui esso deve essere necessariamente esplicito: quando vengono trattati categorie particolari di dati, come i dati sensibili, nel caso di trasferimenti di dati verso paesi terza in mancanza di adeguate garanzie stabilite nell'art.46 o quando si tratta di processi decisionali tra cui la profilazione[156]. In questi casi il GDPR stabilisce che il consenso deve essere esplicito, quindi che derivi da una manifestazione di pensiero espressa mediante la forma scritta. Nel mondo online l'interessato può utilizzare diverse modalità: ha la possibilità di fornire un consenso esplicito compilando un modulo elettronico, inoltrando una e-mail, con la scansione di un file che porti la firma dell'interessato, ed infine attraverso la firma digitale o mediante un processo di autenticazione a doppia fase, con una e-mail e un SMS.

Dal Considerando 32 si evince anche che la richiesta di consenso deve essere posta all'inizio del trattamento e deve essere sottoposto un'unica volta; deve essere domandato nuovamente solo se mutano le finalità del trattamento.

Un'ulteriore precisazione da tenere presente è che il consenso non può essere ottenuto attraverso la medesima azione con cui si accetta un contratto o le condizioni generali di servizio. Questa accettazione non può essere considerata come un'azione positiva inequivocabile di consenso all'utilizzo dei dati personali.

Altra caratteristica del consenso è che esso deve essere fornito liberamente, vale a dire che l'interessato deve essere capace di eseguire una scelta effettiva, senza

chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso».

[156] Con il termine profilazione di intende la «*stesura di un profilo, mediante l'identificazione e la raccolta dei dati personali e delle abitudini caratteristiche di qualcuno*» da *www.treccani.it*. Viene inteso quindi l'insieme di attività di raccolta ed elaborazione dei dati degli utenti di un servizio, con lo scopo di suddividerli in gruppi a seconda del loro comportamento. Si attua quindi un processo di segmentazione.

essere soggetto ad intimidazioni o raggiri, e non deve subire conseguenza negative per non aver conferito il proprio consenso.

Il requisito della libertà del consenso può essere letto alla luce dell'art. 8 CDFUE[157] guardando alla prestazione del consenso non come un atto isolato, ma piuttosto analizzando il contesto in cui è prestato, in modo da rendere visibili gli squilibri di potere esistenti[158]. Anche la disciplina normativa sembra confermare quest'impostazione: secondo il considerando 43 del Reg. UE 2016/679, per garantire la libertà di espressione del consenso è opportuno che questo non costituisca un valido presupposto per il trattamento dei dati personali nel caso esista un evidente squilibrio tra l'interessato e il titolare del trattamento[159].

È inoltre particolarmente significativo l'art. 7 del GDPR che stabilisce che «*nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto*».

Inoltre, il considerando 43 Reg. UE 2016/679 prevede una presunzione di non libera espressione del consenso nel caso in cui non sia possibile prestarlo in modo separato per distinti trattamenti di dati personali o qualora l'esecuzione del contratto, inclusa la prestazione di un servizio, sia subordinata al consenso anche se questo non è necessario per l'esecuzione. L'onere della prova è in capo al titolare del trattamento, come confermato dalle recenti linee guida elaborate dal Comitato Europeo per la Protezione dei Dati[160].

---

[157] Art. 8, Carta dei Diritti Fondamentali dell'Unione Europea (2000/C 364/01).
[158] C. ANGIOLINI, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, G. Giappichelli Editore, Torino, 2020 p.126.
[159] EDPB, *Linee guida 5/2020 sul consenso ai sensi del Reg (UE) 2016/679*, 4 maggio 2020, pp.8-9.
[160] *Ivi,* p.11.

Per cui l'interessato dovrà porre particolare attenzione nel caso in cui, assieme ad una finalità per il trattamento dei dati necessari all'esecuzione di un contratto, sia chiesto anche il consenso per altri dati che non sono necessari per l'esecuzione del contratto. Con questa previsione, il legislatore ha voluto garantire che il trattamento dei dati personali per il quale non viene richiesto il consenso, non diventi una controprestazione contrattuale[161].

Ad esempio, per quanto riguarda una pubblicità commerciale, il consenso per la ricezione di pubblicità deve essere differenziato dal consenso per la prestazione contrattuale richiesta dall'utente, dato che all'utente deve essere garantita la possibilità di concludere il contratto senza essere costretto a ricevere pubblicità commerciale.

Questo comporta il rischio che molti dei consensi ottenuti dai servizi online possano essere considerati invalidi. Il Gruppo di Lavoro Articolo 29[162] ne fornisce un chiaro esempio: se un'applicazione mobile per il fotoritocco chiede il consenso per accedere alla geolocalizzazione e in seguito i dati vengono impiegati ai fini di una pubblicità comportamentale, il consenso non è fornito in modo libero perché la geolocalizzazione e la pubblicità non sono necessari per la fornitura del servizio di fotoritocco. Questo rende il consenso illecito.

A proposito di questo, la Corte di Cassazione Italiana, con la sentenza n. 17278/2018[163] ha precisato che il gestore di un sito riguardante un servizio

[161] In questa prospettiva non pare inserirsi quanto stabilito dalla Suprema Corte con sentenza n. 17278 del 2 luglio 2018, in cui si è ritenuto lecito il consenso alla ricezione di comunicazione promozionali imposto agli utenti come condizione necessaria di iscrizione ad un servizio di *newsletter*.

[162] Il Gruppo di lavoro Articolo 29 (Art. 29 WP) era il gruppo di lavoro europeo indipendente che, fino all'entrata in vigore del RGPD, aveva il compito di occuparsi delle questioni relative alla protezione della vita privata e dei dati personali. Il Gruppo Articolo 29, introdotto con la direttiva europea 95/46, è stato sostituito dall'European Data Protection Board (Comitato europeo per la protezione dei dati) col GDPR.

[163] Con la sentenza n. 17278/2018 la Corte di Cassazione nell'accogliere il ricorso dell'Autorità Garante contro una decisione del tribunale di Arezzo riguardo la legittimità del trattamento dei dati personali compiuto per scopi promozionali, violando gli artt. 23 e 130 del Codice privacy, dichiara che la Corte di Arezzo non si è attenuta ai principi fondamentali in materia di consenso al trattamento dei dati personali, con riferimento all'articolo 23 del Codice della privacy, che sancisce che il consenso è validamente prestato solo se espresso liberamente e specificamente in merito ad un trattamento chiaramente individuato, permette al gestore di un

fungibile e rinunciabile può negare l'acceso al servizio se l'utente non presta il consenso per il trattamento dei dati personali a fini commerciali (*cookie wall*[164]), nel caso in cui il sito offre un servizio non essenziale per l'utente[165]. Dunque, il punto chiave sta nella fungibilità e nella rinunciabilità del servizio. Il gestore non potrebbe bloccare l'accesso al sito nel caso in cui si tratti di un servizio essenziale per l'utente. La Corte, infatti, sostiene che è vietato al gestore di «*utilizzare i dati personali per somministrare o far somministrare informazioni pubblicitarie a colui che non abbia la volontà di riceverli*».

Successivamente però il Garante ha stabilito, col provvedimento del 12 giugno 2019[166] che la libertà del consenso «*non è assicurata né quando viene richiesto un unico consenso per più diverse finalità di trattamento, né quando si assoggetta la fruizione di un servizio […] alla previa autorizzazione a trattare i dati conferiti, ai fini di tale servizio, per finalità diverse qual è quella di promozione e quella statistica*». Vi è quindi un contrasto tra la Corte e il Garante.

Un caso particolare riguarda inoltre il consenso dei dipendenti: nel caso in cui il datore di lavoro chieda il consenso all'utilizzo di un dato e vi è un pregiudizio reale o potenziale per il cliente che non acconsente; il consenso non può essere considerato valido perché non sarebbe libero, dato lo squilibrio di potere tra

---

sito Internet, che fornisce un servizio fungibile, a cui l'utente possa rinunciare senza gravoso sacrificio (nella specie servizio di *newsletter* su tematiche legate alla finanza, al fisco, al diritto e al lavoro), di vincolare la fornitura del servizio al trattamento dei dati per finalità pubblicitarie, sempre che il consenso sia singolarmente ed inequivocabilmente prestato in riferimento a tale effetto, il che comporta altresì la necessità, almeno, dell'indicazione dei settori merceologici o dei servizi cui i messaggi pubblicitari saranno riferiti.

[164] Un *cookie wall* è una qualsiasi barriera che non consente l'accesso ad un sito web se l'utente non acconsente all'uso di cookie o altre tecnologie di tracciamento. In generale, *i cookie wall* non presentano un'opzione per il rifiuto. È per cui un mezzo per impedire all'utente l'accesso a un contenuto se questo egli non acconsente all'installazione di *cookie* o all'uso di altri strumenti di tracciamento presenti nel sito che vuole visitare.

[165] La Corte ha ritenuto lecito il consenso perché il servizio per l'accesso al quale era richiesto il consenso, è un servizio a cui l'utente poteva *«rinunciare senza gravoso sacrificio».* Questo ragionamento però non sembra combaciare con la posizione del Gruppo di Lavoro Articolo 29, secondo il quale il consenso non può essere ritenuto prestato liberamente solo perché *«il titolare del trattamento sostiene che esiste una scelta tra il suo servizio che prevede il consenso all'uso dei dati personali per finalità supplementari, da un lato, e un servizio equivalente offerto da un altro titolare del trattamento, dall'altro»*. GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, 4 maggio 2020, cit., p. 10.

[166] Provvedimento n.130 del 12 giugno 2019

datore e dipendente. In casi come questo il consenso non può rappresentare la base giuridica del trattamento.

Il Comitato Europeo per la Protezione dei Dati ha stabilito anche che la prova del requisito della libertà può essere fornita dimostrando che il titolare del trattamento offre, oltre al servizio subordinato alla prestazione del consenso, anche un altro servizio equivalente non "condizionato"[167]. Secondo le linee guida, il consenso non può essere considerato prestato in modo libero se un operatore subordina a questo la prestazione di un servizio e un servizio equivalente e non condizionato è offerto da un altro soggetto. Il motivo sta nel fatto che questa opzione interpretativa imporrebbe al titolare del trattamento di monitorare gli sviluppi del mercato per garantire la validità del consenso nel tempo, dato che l'operatore che fornisce il servizio equivalente potrebbe cambiare le condizioni della propria sfera commerciale[168].

In ambito nazionale, il Garante Italiano per la Protezione dei Dati Personali ha adottato una posizione restrittiva, per cui il consenso non può essere considerato liberamente prestato nel caso in bui la fornitura di un servizio sia a esso subordinato o qualora ci sia un *flag* preimpostato secondo il modello dell'*opt-out*[169].

Il consenso deve essere specifico, vale a dire relativo alla finalità per la quale è eseguito il trattamento. Questo requisito è speculare a quello della "granularità", secondo il quale l'interessato deve essere *«libero di scegliere quale finalità accettare anziché dover acconsentire a un insieme di finalità*[170]». Il requisito della

[167] EDPB, *Linee guida 5/2020 sul consenso ai sensi del Reg (UE) 2016/679*, 4 maggio 2020, p.11.
[168] C. ANGIOLINI, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, G. Giappichelli Editore, Torino, 2020 pp.127-128.
[169] In giurisprudenza si veda Cass., 2 luglio 2018, n.17278, in *Corr. Giur*., 11, 2018, p.1459. estratta da *www.pa.leggiditalia.it*; per una ricostruzione delle diverse posizioni: S. THOBANI, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Eur. Dir. Priv*., n.2, 2016, p.513 ss.
[170] GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, 4 maggio 2020, cit., p. 11, dove di precisa anche che *la «granularità è strettamente correlata alla necessità che il consenso sia specifico […] Quando il trattamento di dati mira a perseguire finalità diverse, la soluzione per soddisfare le condizioni per la validità del*

specificità, infatti, prescrive che il titolare del trattamento debba ottenere un consenso *ad hoc* per ciascuna finalità perseguita[171]. Il Considerando 32 stabilisce di fatto che «*il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o per le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste».*

Non è pertanto lecito raggruppare insieme più finalità in un unico consenso perché l'interessato sarebbe costretto a rifiutare o accettare in blocco tutte le finalità senza altre possibilità di scelta.

In merito a ciò, il Gruppo dei Garanti ha proposto un efficace esempio di un'azienda che con un'unica richiesta di consenso inserisce sia l'autorizzazione a trattare i loro dati, sia la richiesta di inoltrare e-mail pubblicitarie ed infine anche il permesso per comunicare i dati ad altre società.

Anche il Garante italiano ha confermato più volte che le attività di marketing esprimono una finalità diversa dalla comunicazione di dati a soggetti terzi e dalla profilazione: è dunque fondamentale ottenere tre consensi distinti tra loro per le tre diverse finalità.

Un altro caso classico riguarda i cookie: se questi hanno finalità distinte tra loro, allora non può esserci un unico consenso per tutti i cookie.

Come ha affermato svariate volte il Garante per la protezione dei dati personali, non è infatti lecito richiedere un consenso generale, utilizzando generiche dichiarazioni che non consentono all'interessato di rendersi conto della reale portata della sua manifestazione di consenso[172].

---

consenso risiede nella granularità, ossia nella separazione delle finalità e nell'ottenimento del consenso per ciascuna di esse».

[171] A. MANTOVANI, *Questioni relative al trattamento dei dati personali per finalità di marketing e profilazione*, in *Media Laws, Rivista di Diritto dei Media,* (2019)3, p.25

[172] Garante Privacy 28 maggio 1997, in Boll. n. 1, 17 (doc. web n. 40425). Questa decisione del Garante ha lo scopo di fornire alcuni criteri generali riguardanti il tema dell'informativa e richiesta del consenso all'interessato. In particolare, il Garante ha sottolineato come nel caso in esame risultassero espresse in forma molto generica le finalità del trattamento, le modalità e l'indicazione dei soggetti ai quali i dati possono essere comunicati. Inoltre sostiene che è presenta la richiesta di un «consenso generale e incondizionato, proveniente da un soggetto in

Per consenso informato si intende che esso deve essere accompagnato da una valida informativa[173]. L'interessato deve essere messo nelle condizioni di sapere quali dati sono trattati, con quali modalità e quali finalità, i diritti che gli sono riservati dalla legge; deve essere per cui rispettato il principio di trasparenza[174]. Essendo questo un aspetto fondamentale, l'informativa deve essere redatta con un linguaggio semplice e comprensibile, anche colloquiale.

L'informativa deve anche informare l'interessato circa le conseguenze del suo consenso o rifiuto; se ad esempio a causa del mancato consenso l'utente non potrà accedere a specifiche aree del sito web, allora deve essere messo al corrente di ciò.

L'informativa deve essere fornita all'interessato prima di procedere con il trattamento; quindi, prima della raccolta dei dati se questi sono raccolti direttamente dall'interessato; nel caso in cui i dati non sono raccolti direttamente dall'interessato, l'informativa deve essere mostrata entro un ragionevole termine.

Il legislatore specifica al considerando 62 che *«non è necessario imporre l'obbligo di fornire l'informazione se l'interessato dispone già dell'informazione, se la registrazione o la comunicazione dei dati personali sono previste per legge o se informare l'interessato si rivela impossibile o richiederebbe uno sforzo sproporzionato. Quest'ultima eventualità potrebbe verificarsi, ad esempio, nei trattamenti eseguiti a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici».*

posizione nettamente più forte rispetto al destinatario dell´informativa, si risolve in una violazione della libertà contrattuale di quest´ultimo.»

[173] M. SOFFIENTINI, *Privacy. Protezione e trattamento dei dati*, Ipsoa, Vicenza, 2015, cit., p.69; *«Un ruolo fondamentale è svolto dall'informativa».*

[174] L'interessato *«deve essere previamente informato oralmente o per iscritto riguardo a una serie di elementi obbligatori e indefettibili. Fra questi, vanno specificate le modalità che saranno eventualmente utilizzate per il trattamento dati … ossia telefonate automatizzate e modalità assimilate (quali fax, e-mail, sms, mms), oltre che quelle tradizionali come posta cartacea e telefonate con operatore, nonché le finalità del trattamento stesso (ad esempio, ricerca statistica, marketing o profilazione)»* Garante per la protezione dei dati personali, *Linee guida in materia di attività promozionale e contrasto allo spam*, 4 luglio 2013, cit.

Il Regolamento, attraverso gli art. 13 e 14 fornisce alcune indicazioni per poter ritenere che il consenso sia informato; in particolare l'informativa deve contenere almeno l'indicazione di:

- Identità e dati del titolare del trattamento
- Finalità del trattamento e la base giuridica
- Natura dei dati trattati
- Periodo di conservazione dei dati personali
- Possibilità del diritto di revoca
- Esistenza di trasferimenti dei dati in paesi extra UE in mancanza di un intervento di adeguatezza da parte della Commissione
- Presenza di un processo decisionale automatizzato, compresa la profilazione
- Elenco dei destinatari a cui i dati possono essere trasferiti.

Questi elementi possono non essere tutti presenti nell'informativa di riferimento, l'importante è che questa informativa "minima" rimandi ad una più estesa e completa, posizionata in un luogo differente.

Consenso verificabile significa che l'azienda deve essere in grado di dimostrare che l'interessato lo ha accordato in riferimento a quel determinato trattamento, per il periodo di tempo nel quale il trattamento viene attuato. Il Considerando 42 infatti sostiene che *«per i trattamenti basati sul consenso dell'interessato, il titolare del trattamento dovrebbe essere in grado di dimostrare che l'interessato ha acconsentito al trattamento. In particolare, nel contesto di una dichiarazione scritta relativa a un'altra questione dovrebbero esistere garanzie che assicurino che l'interessato sia consapevole del fatto di prestare un consenso e della misura in cui ciò avviene».*

Terminata l'attività di trattamento, la prova del consenso deve essere conservata solo per il tempo necessario *«per l'adempimento di un obbligo giuridico che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è*

soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento»[175].

Infine, il consenso deve essere revocabile[176]; qualsiasi consenso deve poter essere revocato, senza che l'interessato ne subisca un pregiudizio[177]; la revoca deve poter essere esercitata con facilità[178] e senza impedimenti, così come lo è stato dare il consenso e deve poter essere attuata in qualsiasi momento. Possibilmente deve essere utilizzato lo stesso canale con cui si è chiesto il consenso. Si tratta di un'operazione gratuita e a forma libera. L'articolo 7 stabilisce che *«l'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di prestare il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato».*

In alternativa, è possibile chiedere la revoca inviando una comunicazione, attraverso uno specifico punto sul sito o inviando una mail ai contatti indicati nell'informativa (interpello al titolare). Nel caso in cui il titolare non risponda a questa esigenza, ci si può rivolgere al Garante o al tribunale per la tutela dei propri diritti.

Non si è obbligati a motivare la revoca e dopo di essa il trattamento deve essere interrotto. Il titolare del trattamento ha l'obbligo di eliminare i dati o trasformarli in forma anonima, sempre che il trattamento non possa poggiarsi su una diversa base giuridica.

---

[175] Art. 17 del Regolamento EU 679/2016 (GDPR)
[176] A. QUARTA, G. SMORTO, *Diritto privato dei mercati digitali*, Le Monnier Università, Firenze, 2020, p.251
[177] Cons. 42 del Regolamento EU 679/2016 (GDPR)
[178] GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, 4 maggio 2020, cit., p. 25. Il requisito della facilità della revoca a *«è un elemento necessario del consenso valido. Se il diritto di revoca non soddisfa i requisiti del regolamento, il meccanismo di consenso del titolare del trattamento non è conforme al regolamento».*

Una novità interessante introdotta dal GDPR è proprio l'introduzione al diritto di cancellazione. L'interessato ha infatti il diritto di ottenere la cancellazione dei suoi dati personali se è presente uno dei motivi elencati dall'art. 17 par.1[179]. Il regolamento ha quindi introdotto il "diritto all'oblio", vale a dire il diritto a essere dimenticati, rimuovendo dalla rete i contenuti che riguardano l'interessato.

«*L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali».* Sostiene inoltre che *«Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali»[180].*

Inoltre, nel Regolamento i classici diritti dell'interessato sono ridefiniti in modo che siano coerenti con le innovazioni introdotte, sia in base al principio di trasparenza, che in base all'ampliamento del diritto all'informativa. I diritti riconosciuti all'interessato sono il diritto di accesso[181], che permette all'interessato di essere a conoscenza dei trattamenti relativi ai suoi dati, quali sono le finalità, quali categorie di dati sono trattati, se sono stati comunicati a terzi

[179] Art. 17, par.1 del Regolamento UE 2016/679 (GDPR).
[180] Art. 17 del Regolamento UE 2016/679 (GDPR). I paragrafi 1 e 2 non si applicano se il trattamento è necessario:
a) per l'esercizio del diritto alla libertà di espressione e di informazione;
b) per l'adempimento di un obbligo giuridico che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;
d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
[181] Art. 15 del Regolamento UE 2016/679 (GDPR).

e le garanzie di tutela nel caso venissero trasferiti a paesi terzi[182]; il diritto alla rettifica[183] per ottenere la correzione dei dati scorretti e l'integrazione di quelli incompleti; il diritto alla cancellazione o all'oblio (art.17); l'obbligo di notifica (art.19) che stabilisce che quando il titolare accoglie la richiesta di rettifica, cancellazione o limitazione dei trattamenti di dati personali, è tenuto a notificare quanto avvenuto ai destinatari a cui i dati sono stati comunicati. Inoltre, se l'interessato lo richiede, il titolare è tenuto a comunicargli anche quali sono i destinatari in questione. Inoltre il GDPR ha introdotto altri tre diritti dell'interessato, già previsti dalla Direttiva 95/46 ma che nel Regolamento assumono più rilievo: il diritto di limitazione dei trattamenti (art.18), nel caso in cui i dati siano inesatti, oppure nel caso il trattamento sia illecito (invece di chiedere la cancellazione chiede la sospensione), nel caso in cui il titolare voglia interrompere il trattamento ma l'interessato ha interesse alla loro conservazione per esercitare un diritto in sede giudiziaria; il diritto di opposizione, se ad esempio l'interessato non aveva espresso il suo consenso perché il trattamento è avvenuto per motivi di interesse pubblico o sulla base del legittimo interesse del titolare (ad esempio per il marketing diretti); infine il diritto relativo al procedimento decisionale automatizzato e alla profilazione[184]; l'art 22 sostiene che l'interessato ha il diritto a non essere sottoposto "a una decisione automatizzata basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo significativo sulla sua persona".

2.4 Il Regolamento Generale sulla Protezione dei Dati

Il GDPR dell'Unione Europea è stato adottato nel 2016 ed è entrato in vigore due anni dopo, modificando la Direttiva riguardante la protezione dei dati 95/46/CE.

---

[182] F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, G. Giappichelli Editore, Torino, 2018, p.25. *«Merita sottolineare che, conformemente all'obiettivo di favorire lo sviluppo dell'economia digitale nell'ambito dell'Unione, anche il diritto dell'interessato a ottenere copia dei dati che lo riguardano può essere esercitato in forma elettronica, così come il titolare può adempiere alla richiesta utilizzando la stessa forma».*

[183] Art. 16 del Regolamento UE 2016/679 (GDPR).

[184] Diritto già presente nella Direttiva 95/46 ma che assume maggiore importanza con il GDPR;

Questa aveva lo scopo di armonizzare la tutela dei diritti e delle libertà delle persone fisiche nell'attività di trattamento dati e, di conseguenza, di garantire la circolazione dei dati personali tra operatori attivi in Stati membri differenti. Purtroppo, ne è conseguito un processo di frammentazione normativa dato che gli Stati hanno applicato la Direttiva in modi diversi.

Per uniformare le discipline nazionali quindi nel 2009 la Commissione Europea ha dato via a una serie di consultazioni per modificare la Direttiva, con lo scopo di istituire un regolamento che non avesse bisogno di essere trasposto in normative nazionali. L'obiettivo era quello di tutelare la protezione dei dati personali in una realtà modificata dall'evoluzione di Internet e del mercato digitale e dalla diffusione di nuovi attori economici interessati ad accumulare grandi quantità di dati per fondare su di essi un nuovo business[185].

Gli obiettivi e i punti cardine del GDPR sono fissati nel preambolo del regolamento. Vi è innanzitutto la necessità di inquadrare la tutela delle persone fisiche in merito al trattamento dei dati di carattere personale tra i diritti fondamentali, come è sancito anche dalla Carta dei diritti fondamentali dell'Unione Europea (art.8) e dal Trattato sul funzionamento dell'Unione Europea (art. 16). Si ritiene fondamentale inoltre stabilire la necessità di un intervento normativo dato che la portata della condivisione e della raccolta di dati di carattere personale è cresciuta significativamente e che sempre più frequentemente le persone mettono a disposizione al pubblico informazioni che le riguardano.

Lo scopo del GDPR è quello di stabilire un contesto normativo più solido e coerente nel campo della protezione di dati personali nell'Unione Europea, affiancando misure di attuazione che siano efficienti. In questo modo sarà più semplice garantire alle persone il controllo dei loro dati e diffondere un clima di

[185] A. QUARTA, G. SMORTO, *Diritto privato dei mercati digitali*, Le Monnier Università, Firenze, 2020, p.248

fiducia che favorisca lo sviluppo dell'economia digitale nel Mercato europeo comune.

Il Regolamento 2016/679 dunque modifica l'impianto base del trattamento dei dati personali, proprio della direttiva 95/46/CE (cd. Direttiva madre) e della legislazione interna, con riguardo ai modelli organizzativi ed imprenditoriali e agli adempimenti in capo ai responsabili e titolari, trasferendo a questi ultimi il rischio delle attività; di fatto i titolari hanno il dovere di adottare delle misure con carattere tendenzialmente preventivo; ad esempio si parla si *privacy by design* e *privacy by default*[186], intendendo la progettazione di sistemi e applicative che hanno come scopo la minimizzazione dell'uso di dati personali; di misure tecniche e organizzative per minimizzare il rischio per i dati personali, come la

[186] Art. 25 del Regolamento UE 2016/679 (GDPR). *«1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.*
2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica».

pseudominimizzazione[187] o la nomina di una figura di controllo[188], il *Data Protection Officer* o responsabile della protezione dei dati personali[189].

A queste misure poi si affiancano l'affermazione di diritti in capo alle persone fisiche come il diritto all'oblio o la portabilità[190], la regolazione uniforme nel mercato unico europeo del trattamento dei dati di chiunque si trovi sul territorio dell'Unione Europea[191], garantita da un'autorità europea, vale a dire lo *European Data Protection Board[192],* comitato che si affianca al già esistente *European Data Protection Supervisor* e alle autorità garanti nazionali; infine, al di fuori del territorio europeo[193], la limitazione della circolazione dei dati in base alla

[187] Art. 25 del Regolamento UE 2016/679 (GDPR). Già presente in art. 17, Codice Privacy. Con il termine "pseudonimizzazione" si intende un trattamento che si colloca a metà strada tra quello che riguarda i dati personali, dunque riferibili ad un soggetto identificato o identificabile, e quello riguardante dati anonimi. V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, *I dati personali nel diritto europeo*, G. Giappichelli Editore, Torino, 2019, p. 176.
Vedi anche M. MARTORANA, *La privacy al passo con il regolamento UE 2016/679. Esperienze applicative dei principi del GDPR nella governance aziendale,* Key Editore, 2022, p.23: la pseudonimizzazione ai sensi del GDPR è un vero e proprio trattamento dei dati personali, come si intuisce dalla sua definizione contenuta all'articolo 4 del Regolamento Eu n.679/2026 *«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».*
[188] Art. 37 del Regolamento UE 2016/679 (GDPR).
[189] I. A. CAGGIANO, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo (GDPR) e analisi comportamentale. Iniziali spunti di riflessione*, in *Diritto Mercato Tecnologia,* 2017, p.7. Si tratta di una figura che ricopre una posizione terzietà e una funzione di consulenza al responsabile/titolare.
[190] Artt. 19-20 del Regolamento UE 2016/679 (GDPR).
[191] I. A. CAGGIANO, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo (GDPR) e analisi comportamentale. Iniziali spunti di riflessione*, in *Diritto Mercato Tecnologia,* 2017, p.8; *«Quanto all'ambito di applicazione territoriale della normativa (artt. 3 – 5): non si fa più riferimento alla collocazione del terminale nello Stato Membro ma all'offerta dei servizi in stati UE, per cui la nuova disciplina si applica integralmente alle imprese situate fuori dall'Unione europea che offrono servizi o prodotti a persone che si trovano nel territorio dell'Unione europea».*
[192] Art. 68 del Regolamento UE 2016/679 (GDPR). «Il comitato europeo per la protezione dei dati («comitato») è istituito quale organismo dell'Unione ed è dotato di personalità giuridica».
[193] A. MANTOVANI, *Questioni relative al trattamento dei dati personali per finalità di marketing e profilazione*, in *Media Laws, Rivista di Diritto dei Media,* (2019)3, p.4. *«Infatti, al tradizionale criterio dello stabilimento nel territorio dell'Unione di chi tratti i dati personali (già previsto dall'art. 4 dell'abrogata Direttiva 95/46/CE), l'art. 3, comma 2, del GDPR ha aggiunto quelli dell'offerta di beni o prestazione di servizi a interessati che si trovino nel territorio dell'Unione e del monitoraggio del comportamento degli interessati all'interno dell'Unione. Dunque, con l'entrata in vigore del GDPR, la disciplina europea in materia di data protection deve essere*

valutazione di conformità delle misure garantite, per i dati trasferiti extra-UE[194]. Queste novità rivelano un'impostazione con lo scopo di non frenare le prospettive tecnologiche di produzione sempre più massiva di dati, le sfere di utilizzo e le tecniche che consentono la moltiplicazione dei dati stessi, ma sono volte a regolamentare i trattamenti con meccanismi ritenuti "virtuosi", tesi a minimizzare i rischi di perdita, dispersione e diffusione, con lo scopo di proteggere la sfera dei soggetti cui i dati si riferiscono[195].

Attraverso il Regolamento, la tutela dei dati diventa un obiettivo da seguire fin da subito, vale a dire dalla progettazione del trattamento (*"privacy by design"*), anche tramite la definizione di impostazioni predefinite (*"privacy by default"*).

Perciò il principio di *privacy by design* impone che la tutela degli interessati nel trattamento dei dati personali preveda l'attuazione de adeguate misure tecniche e organizzative sia al momento della progettazione, sia a quello dell'esecuzione del trattamento stesso. Mentre il principio di *privacy by default* (o protezione per impostazione predefinita) comporta che per impostazione predefinita le imprese dovrebbero procedere al trattamento esclusivamente dei dati personali necessari e sufficiente per i fini e solamente per il periodo di tempo necessario. Dunque, si deve progettare il sistema di trattamento dati in modo da assicurare la non eccessività dei dati raccolti.

In tale contesto, il consenso è uno dei "fondamenti legittimi"[196] per dare inizio al trattamento dei dati personali, sia per quanto riguarda i dati personali in generale, sia con riguardo a categorie di dati particolari.

---

rispettata anche (e proprio) da coloro che, pur non essendo stabiliti nel territorio dell'Unione, vi indirizzino determinate attività di marketing o di profilazione».

[194] È prescritta l'osservanza di procedure e adeguatezza per il trasferimento dei dati extra-Ue, o, in mancanza, il consenso esplicito dell'interessato o altre particolari condizioni.

[195] A. MANTOVANI, *Questioni relative al trattamento dei dati personali per finalità di marketing e profilazione*, in *Media Laws, Rivista di Diritto dei Media,* (2019)3, p.4.
Dunque il Regolamento ha rafforzato gli strumenti di tutela dell'interessato, sia per quanto riguarda la trasparenza, con l'informazione da fornire agli interessati, sia per quanto riguarda i diritti, come quelli di accesso, portabilità, rettifica e opposizione, che consentono agli interessati di esercitare un controllo sui propri dati.

[196] Secondo la terminologia della Carta di Nizza, o base giuridica.

Nel Regolamento, il consenso è più chiaramente valorizzato in chiave attiva/positiva, anche se non per forza scritta, ma non mancano alcuni contemperamenti per il caso di utilizzo di mezzi elettronici, dove è necessaria comunque un'azione positiva di accettazione[197]. Si pensi ad esempio alla dilagante diffusione di sensori come software di rilevamento del movimento o di rilevamento touch, etc[198].

Le principali novità apportate dal Regolamento si possono sintetizzare nel seguente modo:

1. l'introduzione del diritto alla portabilità dei dati da un titolare del trattamento ad un altro[199], in base all'articolo 20 del Regolamento;
2. nuove procedure e adeguatezza per il trasferimento dei dati in paesi extra-Ue;
3. ampliamento delle sanzioni amministrative di tipo monetario in caso di *data breach* o di violazioni del regolamento, stabilito dall'articolo 83, e l'obbligo di informare l'Autorità nazionale circa le eventuali violazioni dei dati personali, secondo il considerando 85;
4. è stato inoltre introdotto dall'articolo 2 il principio di responsabilizzazione, o *accountability*, tramite la creazione di nuove procedure, figure di garanzie come la valutazione d'impatto, nel caso di trattamenti che comportano rischi elevati, e della *privacy by design*;
5. l'introduzione con l'articolo 37 e seguenti e il considerando 97 di figure di controllo *Data Protection Officer*, vale a dire il responsabile della

[197] Con. 32 del Regolamento UE 2016/679 (GDPR), segnatamente nella parte in cui fa rinvio a *«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 [...] 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».*

[198] I. A. CAGGIANO, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo (GDPR) e analisi comportamentale. Iniziali spunti di riflessione*, in *Diritto Mercato Tecnologia,* 2017, p.10

[199] *Ivi*, p.6. Questo avviene ad esempio nel caso di passaggio di provider e salvataggio dei messaggi di posta elettronica e dei contatti.

protezione dei dati, che ha il compito di assicurare una corretta gestione in imprese ed enti;

6. è stata avviata la promozione di codici di condotta e meccanismi di certificazione rilasciati da un soggetto abilitato o dall'autorità di protezione dati, secondo quanto stabilito nell'articolo 35 e seguenti;
7. istituzione del Comitato Europeo per la protezione dei dati.
8. i fondamenti di liceità del trattamento, elencati nell'art. 6; il consenso deve essere esplicito per i dati sensibili e per decisioni basate su trattamenti automatizzati, compresa la profilazione. (art. 9 e 22 del regolamento) e deve rispettare i requisiti elencati all'art. 7.

2.5 Evoluzione della normativa europea ed internazionale

Come già detto, il Regolamento è entrato in vigore nel maggio del 2018 ed ha introdotto una serie di innovazioni in materia di trattamento di dati personali. Il percorso per l'approvazione del diritto alla protezione dei dati personali inizia il secolo scorso con i primi riconoscimenti dei diritti alla protezione della sfera privata e della riservatezza.

Dal punto di vista internazionale, il diritto alla protezione della sfera privata di una persona è stato riconosciuto per la prima volta con la Dichiarazione Universale dei Diritti dell'Uomo; l'art. 12 infatti stabilisce che *«nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni».* Da queste premesse giuridiche, infatti, deriva la

Convenzione Internazionale sui Diritti Civili e Politici[200], che contiene all'art.17 una disposizione molto simile[201].

La Dichiarazione universale dei diritti dell'uomo è stata approvata il 10 dicembre 1948 dall'Assemblea Generale delle Nazioni Unite e rappresenta un primo tentativo della comunità internazionale di riconoscere il diritto alla riservatezza spettante a ciascun essere umano. Si tratta pur sempre però di un atto non vincolante per gli Stati membri, dato che si tratta di una dichiarazione di principi, ma si tratta ugualmente di una tappa importante da riconoscere.

Occorre specificare però che nel dibattito moderno riguardante i diritti della persona, da una parte vi è il diritto alla privacy inteso come a impedire ogni ingerenza, anche di tipo fisico, nella vita di un'altra persona; poi vi è il diritto alla protezione dei dati personali, come tutela delle persone da ogni raccolta e trattamento di dati che le riguardano, ed infine vi è il diritto della persona a non vedere informazioni che la riguardano diffuse e rese riconoscibili senza il suo consenso[202]; l'oggetto principale della prossima analisi sarà lo sviluppo della normativa riguardante la protezione dei dati personali. Anche se, la prima visione di privacy intesa come il diritto di poter escludere chiunque dalla propria vita privata, è in qualche modo collegata; il diritto alla protezione dei dati personali, infatti, può estendersi fino alla tutela del domicilio o del semplice spazio fisico nel quale una persona si trova[203].

---

[200] Adottato dall'Assemblea Generale delle Nazioni Unite con Risoluzione 2200A (XXI) del 16 dicembre 1966. Entrata in vigore internazionale: 23 marzo 1976, conosciuta anche come il *Patto internazionale sui diritti civili e politici*,

[201] A. PISAPIA, *La tutela per il trattamento e la protezione dei dati personali*, G. Giappichelli Editore, Torino, 2018, p.1

[202] A meno che non prevalga l'interesse pubblico o la comunicazione e la diffusione siano previste da apposite norme. F. PIZZETTI, *Privacy e diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, G. Giappichelli Editore, Torino, 2018, p. 24

[203] F. PIZZETTI, *Privacy e diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, G. Giappichelli Editore, Torino, 2018, cit., p. 25. *«Si pensi ad esempio a qualsiasi perquisizione o ispezione o altro atto di pressione sulla persona che sia finalizzato ad acquisire informazioni o dati che la riguardano, o si pensi al tema delle intercettazioni telefoniche o in genere dei controlli ambientali».*

In questa materia, il diritto europeo è composto da numerosi documenti normativi; quello che oggi viene definito il diritto europeo in materia di protezione dei dati è un sistema quindi davvero complesso, essendo un insieme di regole e principi che incrociano tra loro atti normativi che appartengono a due ordinamenti diversi.

- Il primo ordinamento che concorre a formare il diritto europeo per la protezione dei dati personali è quello del Consiglio d'Europa, istituito nel 1949, il cui atto più rilevante è la Convenzione europea dei diritti dell'uomo, o CEDU[204], firmata nel 1950 a Roma ed entrata in vigore circa tre anni dopo; con l'art. 8 che stabilisce il rispetto della vita privata: *«ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza».*

  Il secondo ordinamento è quello dell'Unione Europea che si fonda sul Trattato di Lisbona firmato nel 2007 en entrato in vigore nel 2009, il quale comprende anche la Carta dei diritti dell'Unione Europea, proclamata a Nizza nel 2000, ma entrata in vigore solo col Trattato di Lisbona.

  Prima si trattava esclusivamente di un documento politico. Col Trattato di Lisbona il diritto alla protezione dei dati personali diventa un diritto fondamentale dei cittadini, e per questo deve essere assicurato a tutti in modo eguale; l'art.8 della Carta di Nizza infatti introduce nuovi diritti, e tra questi anche quello alla protezione dei dati personali[205]. Inoltre, l'articolo 7 stabilisce il rispetto della vita privata e familiare, e di conseguenza il diritto alla privacy[206].

  È con il Trattato di Lisbona, che ha dato alla Carta di Nizza valore giuridico, che il diritto alla protezione dei dati personali diventa un diritto fondamentale autonomo, da cui nasce l'esigenza di redigere un

[204] Convenzione internazionale redatta e adottata nell'ambito del Consiglio d'Europa.
[205] Art. 8, par. 1, Carta di Nizza «*Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano».*
[206] «*Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni».*

regolamento, in modo che questo diritto sia garantito allo stesso modo in tutti gli stati dell'Unione.

Dunque, ciascun ordinamento ha le sue fonti e un proprio sistema di Corti anche se spesso le fonti dei due ordinamenti e le decisioni delle Corti si intrecciano negli effetti che determinano[207].

In particolare, le norme più rilevanti del Consiglio d'Europa e dell'Unione Europea sono:

- La Convenzione 108, o Convenzione di Strasburgo, adottata dal Consiglio d'Europa nel 1981, considerata una dei più rilevanti strumenti legali per la tutela delle persone rispetto al trattamento automatizzato dei dati personali; inoltre è anche l'unico mezzo giuridicamente vincolante a livello mondiale, in quanto possono aderire anche Stati non membri del Consiglio d'Europa. È proprio in questo periodo che comincia a diffondersi l'informatica di massa, le persone cominciano ad avere un personal computer in casa.

  Questa Convenzione si applica a tutti i trattamenti di dati personali eseguiti sia nel settore pubblico che in quello privato, quindi anche a trattamenti esercitati da polizia e autorità giudiziarie. Lo scopo è quello di tutelare gli individui da abusi e regolamentare i movimenti transnazionali dei dati, prende ispirazione proprio dall'articolo 8 della CEDU. L'obiettivo è stabilito dall'articolo 1 che stabilisce quanto segue: «*scopo della presente Convenzione è quello di garantire, sul territorio di ciascuna Parte, ad ogni persona fisica, quali che siano la sua nazionalità o la sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali, e in particolare del suo diritto alla vita privata, in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano («protezione dei dati»)*».

[207] F. PIZZETTI, *Privacy e diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, G. Giappichelli Editore, Torino, 2018, p.27

La Convenzione stabilisce che il trattamento e la raccolta dei dati deve fondarsi su alcuni principi: la correttezza del trattamento, la liceità del trattamento, le finalità del trattamento e la qualità dei dati. Si tratta quindi dei principi fondamentali che regolano l'intera normativa riguardante la protezione di dati personali e che saranno una base importante anche per il GDPR.

Inoltre, essa vieta il trattamento di dati sensibili in mancanza di opportune garanzie giuridiche e sancisce il diritto del cittadino ad avere informazioni riguardanti quali dei suoi dati sono conservati e il diritto di chiederne la rettifica se inesatti.

Per di più stabilisce delle limitazioni alla possibilità di trasferire dati verso Stati in cui non è presente una regolamentazione che fornisca una tutela equivalente. Per quanto riguarda il trasferimento di dati, la Convenzione sancisce il principio della circolazione senza obbligo di autorizzazioni, un principio opposto a quello che stabilirà poi la direttiva 95/46/CE.

Il 18 maggio 2018 il Consiglio ha promulgato un protocollo di modifica della Convenzione 108, vale a dire la Convenzione 108+, con lo scopo di renderla più moderna e fornire un quadro giuridico più adatto all'epoca in cui viviamo, nella quale le violazioni del diritto alla protezione dei dati personali sono sempre più difficili da tutelare.

Inoltre, il protocollo fornisce regole e garanzie più efficaci per disciplinare il flusso di dati attraverso le frontiere. Tra le innovazioni introdotte vi è l'obbligo di comunicare le violazioni dei dati, o *data breach*[208], e il consolidamento del principio di minimizzazione dei dati, e di trasparenza dell'elaborazione, in modo da mantenere un elevato clima di fiducia nell'ambiente digitale. Il Protocollo richiede anche il rispetto del principio

[208] L'art. 4 del Regolamento europeo definisce la violazione dei dati personali (*data breach*) come «*la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*». Dunque, un *data breach* può essere un evento doloso come un attacco informatico o un evento accidentale, come un incidente dovuto a un incendio o una calamità naturale, la perdita di una chiavetta USB o la sottrazione di documenti personali causata dal furto di un pc.

di "*privacy by design*", introducendo nuoce tutele in materia di trattamenti algoritmici, come il diritto di ricevere informazioni riguardanti la logica su cui si basa l'elaborazione dei dati.

La Convenzione 108+ riguarda tutti i tipi di trattamenti, anche quelli che derivano da sicurezza nazionale e difesa[209], tranne i trattamenti operati da persone fisiche nell'esercizio di attività puramente personali e domestiche.

Il nuovo protocollo viene applicato soltanto agli Stati firmatari[210], mentre agli Stati firmatari della sola Convenzione originale si applica quest'ultima.

- Dopo la Convenzione 108 del 1982, nel 1992 il processo di integrazione del Mercato unico europeo arriva all'apice con la firma del Trattato di Maastricht e la conseguente creazione della Comunità Europea.

  Viene così creato anche il sistema di libera circolazione di merci e persone, ossia l'area Schengen. Da questo però nasce una problematica, cioè quello di decretare una normativa europea di riferimento in materia di protezione di dati personali. Di fatti, se è stato istituito un mercato unico, anche i dati devono poter circolare liberamente. Questa è la ragione per cui nel 1995 la Comunità Europea adotta la Direttiva 95/46/CE.

  La scelta di una direttiva è stata giustificata dal fatto che in quel periodo la protezione dei dati era ancora agli inizi e non sarebbe stato facile adottare una normativa uniforme e vincolante per tutti gli Stati. Si è scelto quindi di prediligere una direttiva che fissasse gli obiettivi ma che lasciasse spazio ai legislatori nazionali.

  Dunque, lo scopo principale era quello di armonizzare le norme in merito alla protezione dei dati personali per assicurare un "flusso libero" (*free flow of data*) dei dati e sviluppare un alto livello di tutela dei diritti fondamentali dei cittadini.

[209] A differenza del Regolamento.
[210] L'Italia ha ratificato la nuova Convenzione il 5 marzo del 2019.

Essa però, come le leggi nazionali di recepimento, considerava la protezione dei dati all'interno di una relazione statica tra titolare e interessato, con una visione proprietaria del dato. Se ne promuoveva quindi un'applicazione formalistica, tramite informative e consenso. Il dato apparteneva all'interessato e di conseguenza non poteva essere utilizzato senza il suo consenso. Per questa ragione la Direttiva è stata considerata per molto tempo come un mero adempimento burocratico per raggiungere il diverso obiettivo della Convenzione di Schengen.

Come la Convenzione 108, la Direttiva tutela il diritto alla vita privata e ne accresce le tutele introducendo autorità di controllo dipendenti, chiamate Garanti, per assicurare la corretta attuazione delle norme nel territorio nazionale.

In Italia[211], il Garante per la protezione dei dati personali, chiamato più semplicemente Garante Privacy, è l'autorità di controllo nazionale indipendente istituita dalla legge sulla privacy[212] in attuazione della direttiva 95/46/CE. È stata poi regolamentata dal Codice in materia di protezione dei dati personali[213] o Codice Privacy[214].

Con il Regolamento Europeo che ha sostituito la Direttiva, l'Autorità di controllo interviene soprattutto *ex post,* vale a dire che la sua valutazione avviene successivamente alle valutazioni del titolare del trattamento; si ha inoltre l'eliminazione delle notifiche preventive dei trattamenti che vengono sostituite con l'obbligo di tenere un registro dei trattamenti[215] e con valutazioni di impatto autonome eseguite dal titolare del trattamento. La valutazione di impatto del trattamento[216] è un incarico del titolare del

---

211 G. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Zanichelli Editore, Bologna, 2012, pp. 21-25.

212 Legge del 31 dicembre 1996, n. 675

213 d.lg. del 30 giugno 2003, n. 196

214 Il Codice è stato poi modificato dal decreto legislativo dell'8 agosto 2018, con lo scopo di adeguare la normativa italiana al Regolamento Europeo per la Protezione dei Dati Personali.

215 La tenuta di un registro dei trattamenti è prevista dall'art. 30 del RGPD ed è considerata indice di una corretta gestione dei trattamenti. Il compito di tenere il registro spetta al titolare e, se nominato, al responsabile del trattamento. Il registro deve contenere diverse informazioni, elencate sempre nell'art. 30 del Regolamento.

216 D.P.I.A., cioè Data Protection Impact Assessment.

trattamento, stabilito dall'art. 35 del Regolamento. È lo strumento con cui il titolare esegue l'analisi dei rischi che derivano dai trattamenti posti in essere. Dunque, il titolare deve effettuare una valutazione preventiva, cioè prima che il trattamento abbia inizio, delle conseguenze del trattamento dei dati sulle libertà e sui diritti degli interessati.

In questo scenario, le autorità di controllo ed in particolar modo il Comitato europeo della protezione dei dati[217], erede dell'attuale Gruppo Articolo 29, avranno il compito di garantire uniformità di approccio alla normativa e fornire ausili interpretativi. Di fatto, il Comitato è tenuto a produrre linee-guida e altri documenti di indirizzo sui vari tempi, anche per garantire gli adattamenti se dovessero essere necessari con l'evoluzione delle tecnologie.

Il *prior cheking*, previsto dall'art. 36 del GDPR, si applica *«qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio».*

Quindi il titolare del trattamento chiede un consulto all'autorità di controllo prima di iniziare il trattamento.

Ruolo importante della Direttiva, è stato anche quello di regolamentare il trasferimento dei dati personali all'esterno dello Spazio Economico Europeo, e lo vieta nel caso in cui lo Stato di destinazione non disponga di un livello di protezione adeguato alle norme europee.

La Direttiva è stata applicata a tutto lo Spazio Economico Europeo, oltre quindi il territorio dell'Unione, è stata estesa fino all'Islanda, al Liechtenstein e alla Norvegia.

Il compito di risolvere le questioni legate alla Direttiva e quindi anche quelle legate all'interpretazione, spetta alla Corte di Giustizia Europea (CGUE).

[217] European Data Protection Board (Comitato europeo per la protezione dei dati) che col nuovo Regolamento ha sostituito il Gruppo di lavoro articolo 29, previsto dalla Direttiva 95/46. Il Comitato europeo per la protezione dei dati è il gruppo di lavoro comune delle autorità nazionali di vigilanza e protezione dati.

La Direttiva però ha presentato delle carenze con l'evoluzione della tecnologia ed in particolare dei trattamenti automatizzati; per questo motivo e per garantire il diritto alla protezione dei dati personali a tutti i cittadini allo stesso modo, è nata la necessità di sostituire la Direttiva 95/46 col Regolamento europeo (GDPR)[218].

La Direttiva ha inoltre istituito il Gruppo di lavoro articolo 29, i cui Pareri, Raccomandazioni e Documenti di lavoro fanno parte integrante del materiale che concorre a istituire il diritto europeo per la protezione dei dati personali. Esso ha funzioni consultive e il suo compito fondamentale è di assicurare che le Autorità di controllo seguano interpretazioni comune della Direttiva 95/46 o comunque della normativa europea in generale. È inoltre un organo di consulenza della Commissione, ma può anche emanare Pareri e Raccomandazioni di propria iniziativa[219].

Svolgendo una breve digressione in campo nazionale, si osserva che l'Italia[220] arrivò tra gli ultimi paesi in Europa ad approvare una legge di tutela della privacy di applicazione generale, vale a dire la legge 675 del 1996[221]. Essa è stata poi sostituita dal Codice in materia di protezione dei

[218] Una direttiva rappresenta un'indicazione della Commissione europea, che deve poi essere recepita con provvedimenti nazionali. Questo comporta una possibile differente attuazione dei principi contenuti in essa e col passare del tempo queste differenze possono intensificarsi fino al far venir meno il principio di libera circolazione dei dati in Europa, che è il fondamento giuridico della direttiva. Per questo la Commissione europea ha deciso di adottare un regolamento che deve essere recepito integralmente, senza modifiche, in tutti i paesi europei, garantendo in questo modo omogeneità di trattamento dei dati. A. BIASIOTTI, *ABC del trattamento dei dati personali*, EPC srl, Roma, 2020, p. 1

[219] F. PIZZETTI, *Privacy e diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, G. Giappichelli Editore, Torino, 2018, pp.33-34.

[220] La Costituzione italiana del 1947 all'art. 2 sancisce il rispetto dei diritti inviolabili dell'uomo. Con questo articolo, infatti, si riconosce che la persona è centrale rispetto allo Stato e possiede dei diritti inviolabili che la Repubblica deve tutelare.

[221] Questa legge è stata emanata insieme alla legge 31 dicembre 1996, n.676 «Delega al Governo in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali». La legge delegava il governo ad emanare disposizioni integrative della legislazione in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali. In particolar modo, i decreti legislativi potevano riguardare la disciplina di alcuni tipi di dati, vale a dire i dati utilizzati a fini storici, di ricerca e statistica, i dati sanitari, quelli usati per il *direct marketing*, dati utilizzati per finalità di lavoro, per scopi di sicurezza sociale, i dati detenuti da enti pubblici che dovevano essere comunicati a terzi, i dati riguardanti il settore dei servizi di telecomunicazione, nel rispetto delle raccomandazioni del Consiglio d'Europa. Per di più, i decreti legislativi potevano individuare i presupposti per attribuire un numero di identificazione

dati personali, chiamato anche Codice Privacy. La necessità di creare un testo unico è dovuta alle numerose modifiche che si sono susseguite nel corso degli anni; il Codice, infatti, nasce per riordinare la materia, anche se non è un testo unico puro dato che introduce alcune modifiche e inserisce e sistematizza la giurisprudenza del Garante. L'oggetto del Codice è la protezione dei dati personali anche se viene comunemente chiamato "Codice Privacy". Si tratta piuttosto di una legge sull'utilizzo delle informazioni che detta norme di natura essenzialmente procedurale, sul modo di utilizzare le informazioni[222]; prevede l'adozione di cautele di tipo tecnico ed organizzativo che ognuno deve rispettare per attuare il trattamento dei dati in modo corretto.

La necessità di una revisione della normativa interna e dell'adattamento al nuovo regolamento europeo risulta evidente partendo dall'impostazione di questo Codice, in base al quale il presupposto di legittimità del trattamento è distinto secondo la tipologia di soggetto, pubblico o privato, Distinzione che non si riscontra nel GDPR. Di fatto, nella normativa antecedente al regolamento, il soggetto pubblico individua il presupposto per il trattamento nella legge, mentre quello privato lo riscontra nel consenso espresso dall'interessato[223].

Il Codice successivamente è stato modificato dal decreto legislativo dell'8 agosto 2018, per uniformare la normativa italiana al GDPR. Il Codice è stato modificato e adeguato soprattutto in riferimento ai trattamenti

---

personale; statuire le modalità e i termini per l'aggiornamento dei dati riprodotti su disco ottico e stabilire la semplificazione di alcuni degli adempimenti introdotti dalla nuova legge. In conclusione, la legge delega conteneva una tra le prime disposizioni legislative riguardanti Internet e le reti telematiche. G. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Zanichelli Editore, Bologna, 2021, pp.24-25.

[222] I diritti della personalità di cui tratta il Codice sono essenzialmente tre: il diritto alla protezione dei dati personali, che consiste nel diritto al controllo dei propri dati da parte dell'individuo, i cui dati sono trattati seguendo le regole del Codice; il diritto alla riservatezza, vale a dire il diritto alla protezione della vita intima e familiare della persona; il diritto all'identità personale, che consiste nel diritto del soggetto a vedersi riconosciuto in una determinata immagine e non veder fuorviata la sua immagine. G. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Zanichelli Editore, Bologna, 2021, p.26.

[223] A. PISAPIA, *La tutela per il trattamento e la protezione dei dati personali*, G. Giappichelli Editore, Torino, 2018, p.57

particolarmente complessi e delicati, come ad esempio il trattamento di dati riguardanti la salute, dotando anche l'Autorità di controllo del potere di stabilire specifiche misure di sicurezza.

- Successivamente, la Convenzione 185/2001[224] del Consiglio d'Europa, detta anche Convenzione di Budapest, rappresenta il primo strumento di diritto internazionale riguardante le infrazioni penali commesse attraverso Internet e altre reti informatiche; in particolare si concentra sulle violazioni dei diritti d'autore, sulla frode informatica, la pornografia infantile e le violazioni sulla sicurezza della rete. In aggiunta, prevede diverse misure e procedure, come la perquisizione dei sistemi di reti informatiche e l'intercettazione dei dati. I principi di questa Convenzione sanciscono il rispetto dei diritti umani stabiliti nella Convenzione europea dei diritti umani, oltre al rispetto del principio della proporzionalità tra le misure sanzionatorie e il tipo di reati commessi[225]. L'introduzione di questi principi è avvenuta in seguito ad un intervento del Gruppo dei Garanti europei per la protezione dei dati personali che avevano messo in evidenza come le attività di cooperazione internazionale comportino necessariamente lo scambio di dati personali. Si tratta di un tema di fondamentale importanza dato che la Convenzione è aperta anche a stati che non appartengono all'Unione Europea, le cui leggi nazionali possono differire dalle regole di armonizzazione riguardanti la tutela dei dati personali[226].

- Una tappa molto importante è rappresentata poi dall'emanazione della Direttiva 2002/58/CE[227], chiamata anche direttiva ePrivacy, relativa al

[224] Consiglio d'Europa, Convenzione di Budapest sulla criminalità informatica del 23 novembre 2001
[225] A. PISAPIA, *La tutela per il trattamento e la protezione dei dati personali*, G. Giappichelli Editore, Torino, 2018, p.7
[226] Qualche anno dopo è stato emanato il Protocollo addizionale alla Convenzione n. 185/2001 sulla criminalità informatica relativo all'incriminazione di atti di natura razzista e xenofobica commessi a mezzo di sistemi informatici
[227] Direttiva 2002/58/CE del parlamento europeo e del consiglio del 12 luglio 2002

trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche. La direttiva aveva lo scopo di armonizzare le disposizioni degli stati membri per poter garantire un pari livello di tutela dei diritti e delle libertà fondamentali, con particolare riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche[228]. La Direttiva dunque introduce nuove norme in merito al trattamento dei dati personali nel settore delle comunicazioni elettroniche, come ad esempio l'Art. 5 par 3 che richiede il consenso dell'utente per conservare informazioni come i dati personali nel dispositivo dell'utente finale o per avere accesso a queste informazioni (tramite i cookie ad esempio) e l'Art. 6 che limita in modo esplicito le condizioni alle quali possono essere trattati i dati relativi al traffico, compresi dunque i dati personali e degli abbonati[229]. Il Considerando 6 fa intuire come la Direttiva sia nata dallo sviluppo tecnologico[230], in quanto afferma «*Internet ha sconvolto le tradizionali strutture del mercato fornendo un'infrastruttura mondiale comune per la fornitura di un'ampia serie di servizi di comunicazione elettronica. I servizi di comunicazione elettronica accessibili al pubblico attraverso l'Internet aprono nuove possibilità agli utenti, ma rappresentano anche nuovi pericoli per i loro dati personali e la loro vita privata».*

- L'Unione Europea emana poi la Direttiva 2009/136/CE, che aveva lo scopo di creare maggiore sicurezza e trasparenza per gli utenti che navigano in Internet, prevedendo numerose modifiche alla Direttiva precedente, soprattutto riguardo l'impiego di cookie.
- Nel 2016 l'Unione Europea approva il Regolamento Generale sulla Protezione dei Dati. Esso è entrato in vigore in tutti gli Stati europei proprio per uniformare i criteri per la tutela del trattamento dei dati personali,

[228] Art. 1 della direttiva 2002/58/CE
[229] M. MARTORANA, *La privacy al passo con il regolamento UE 2016/679. Esperienze applicative dei principi del GDPR nella governance aziendale,* Key Editore, 2022, p.194
[230] M. SOFFIENTINI, *Privacy. Protezione e trattamento dei dati*, Ipsoa, Vicenza, 2018, pp.23-24

riconosciuto come un diritto fondamentale della persona. I nostri dati personali venivano inseriti in delle banche dati soprattutto attraverso il rilascio del consenso al trattamento sui siti in cui navighiamo; il Regolamento, e in particolare gli artt. 6 e 7, ha stabilito il diritto ad un consenso libero e specifico proprio per contrastare la diffusa facilità di acquisire il consenso.

Ora, il consenso che viene richiesto per usufruire di un servizio online, lo si concede e lo si manifesta validamente sul piano giuridico, attraverso lo strumento del "segno di spunta" con il *click* o *chechmark*. Questo *click* è da tempo paragonato alla tradizionale sottoscrizione su documenti cartacei. Dunque, l'evoluzione del diritto ha permesso che la tecnologia sia equiparata alla volontà esprimibile con una firma a penna.

Con il Regolamento si introducono regole più chiare riguardanti l'informativa e in consenso. Il concetto di consenso, infatti, si è evoluto molto rispetto alle normative precedenti proprio per adeguarsi meglio ai cambiamenti che le nuove tecnologie stanno apportando nel mondo online.

Col Regolamento è stato adottato un approccio rigido, per la seguente motivazione: nel caso in cui si tenti di "barattare" il consenso con delle controprestazioni o se il consenso viene fornito in situazioni in cui c'è uno sbilanciamento di potere tra le parti, allora lo stesso verrà considerato non valido.

- Inoltre, lo scorso 5 gennaio 2021 il Consiglio dell'Unione Europea ha emanato la proposta del Regolamento ePrivacy che abrogherà la direttiva ePrivacy.

  Il legislatore europeo aveva emanato la direttiva 2002/58/CE del 12 luglio 2002, chiamata anche ePrivacy, con lo scopo di disciplinare il trattamento dei dati personali e tutelare la vita privata nel settore delle comunicazioni elettroniche, come messaggi di testo o e-mail.

  Il Regolamento ePrivacy affiancherà il GDPR e regolerà gli aspetti legati alla comunicazione online.

Tra i due Regolamenti ci sarà un legame stretto perché il Regolamento ePrivacy andrà a precisare ed integrare il GDPR, ne tradurrà i principi in regole specifiche. Inoltre, ci saranno anche norme riguardanti temi non presenti nel GDPR, dato che questo riguarda esclusivamente le persone fisiche mentre il Regolamento ePrivacy tutelerà anche le persone giuridiche.

Per quanto riguarda i cookies, il consenso continuerà ad essere una condizione necessaria ed indispensabile per il tracciamento, in quanto non ci saranno basi giuridiche diverse da quelle contemplate nel GDPR.

Una novità sarà che gli utenti avranno la possibilità di prestare consenso all'uso di determinati tipi di cookie, immettendo uno o più provider in una *whitelist* nelle impostazioni del browser.

In specifici casi, per garantire l'integrità dei servizi di comunicazione o nei casi stabiliti dalla legge, per esempio per il perseguimento di reati o per prevenzione di minacce alla sicurezza pubblica, sarà consentito il trattamento senza il consenso dell'interessato.

Infine, anche i metadati potranno essere raccolti senza il consenso dell'utente se il trattamento è necessario per una migliore gestione della rete o per la sua ottimizzazione, per soddisfare requisiti tecnici di qualità del servizio o altre esigente strettamente correlate alla corretta esecuzione del contratto.

Dunque, i provvedimenti più rilevanti del Consiglio d'Europa sono stati: la Convenzione europea dei diritti dell'uomo del 1950, la Convenzione 108/1981 "*sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale"* firmata a Strasburgo il 29 gennaio 1981, la Convenzione di Budapest "*sulla criminalità informatica*", firmata a Budapest nel 2001; vi sono poi una trentina di Raccomandazioni del Consiglio che riguardano diversi settori della materia.

La Corte istituita dalla Convenzione dei diritti dell'uomo è la Corte europea dei diritti dell'uomo, con sede a Strasburgo; molte volte la Corte è intervenuta in questo campo, dando indicazioni e stabilendo principi che ormai fanno parte del diritto europeo di protezione dei dati personali[231].

Dall'altro lato, i provvedimenti più importanti dell'Unione Europea possono riassumersi con: il Trattato di Lisbona, che comprende la Carta dei diritti dell'Unione proclamata a Nizza; la Direttiva 95/46/CE "*relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché la libera circolazione dei dati"*, ratificata nel 1995; la Direttiva 2002/58/CE *"relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche"* adottata nel 2002; la Direttiva 2009/136/CE *"recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori"* adottata nel 2009. Ed infine il Regolamento generale sulla protezione dei dati. La Corte istituita è la Corte di giustizia dell'Unione Europea, con sede a Lussemburgo. Tale corte è intervenuta più volte in questioni riguardanti la protezione dei dati personali, anche su temi di grande rilevanza come il diritto all'oblio[232].

Infine, a livello internazionale, è importante nominare alcuni provvedimenti rilevanti.

[231] F. PIZZETTI, *Privacy e diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, G. Giappichelli Editore, Torino, 2018, p.29.
[232] Corte di Giustizia dell'Unione Europea, sentenza della Corte (Grande Sezione), 13 maggio 2014 nella causa C-131/12, *Google Spain SL e Google Inc. c. Agencia Espanola de Protectiòn de Datos (AEPD).*

- nel 1980, l'OECD, vale a dire l'Organizzazione per la cooperazione e lo sviluppo economico, emana le linee guida per la protezione della privacy e il flusso transfrontaliero dei dati[233], che saranno aggiornate poi nel 2013.

- Nel 2013 l'assemblea delle Nazioni Unite emana la risoluzione 68/167 sul diritto alla privacy nell'era digitale e nello stesso anno l'OECD modifica le linee guida introducendo un approccio che si basa sulla gestione del rischio e prevedendo le notifiche dei *data breach*.
- Un'ulteriore tappa importante è rappresentata dalle linee guida EDPB 5/2020 del 4 maggio 2020. Si tratta di linee guida in materia di consenso al trattamento di dati personali adottate dal Comitato Europeo, che consistono in un rinnovo delle Linee guida già emanate dal WP29 nel 2018[234], facilita la comprensione dell'effettivo impatto del GDPR. Le Linee guida infatti derivano dalla necessità di avere maggiori chiarimenti sulle modalità di raccolta del consenso all'impiego di cookie e altri strumenti di tracciamento. L'EDPB in particolare chiarisce che per ottenere un consenso valido al trattamento dei dati personali, esso deve essere per forza libero; inoltre, l'accesso a servizi e funzionalità web non può essere condizionato all'accettazione di cookie da parte dell'utente, in quanto si riterrebbe il consenso prestato "non libero" (cd. *cookie wall*); infine specifica che la mera consultazione, vale a dire il cosiddetto *scroll*, del sito non è ritenuto un atto positivo inequivocabile e sufficiente perché da esso si possa ricavare un valido consenso al trattamento dei dati personali in modo implicito[235].

Per concludere, si può sostenere che in un mondo virtuale come quello di oggi è in continua crescita l'utilizzo di dati, specialmente quelli personali che hanno

[233] EDPB, *Linee guida 5/2020 sul consenso ai sensi del Reg (UE) 2016/679*, 4 maggio 2020
[234] Linee guida del Gruppo di Lavo 29 (WP29) sul consenso ai sensi del GDPR, adottate il 28 novembre 2017 come modificate e adottate da ultimo il 10 aprile 2018.
[235] M. MARTORANA, *La privacy al passo con il regolamento UE 2016/679. Esperienze applicative dei principi del GDPR nella governance aziendale,* Key Editore, 2022, p.195.

trovato una forte tutela da parte dell'Unione Europea, in particolare con il Regolamento 679/2016.

CAPITOLO TERZO - IL PROBLEMA DEL DATO PERSONALE COME CORRISPETTIVO NEI CONTRATTI DEI SERVIZI INTERNET: SOVRAPPOSIZIONE TRA REQUISITI DEL CONSENSO NEGOZIALE E REQUISITI DEL CONSENSO AL TRATTAMENTO (CASISTICA IN CASSAZIONE).

3.1 Il dato personale come corrispettivo nella direttiva UE 2019/770

Di recente è tornata in auge la questione di poter utilizzare i dati personali come corrispettivo; questo sembra infatti essere possibile a seguito della Direttiva UE 2019/770[236] riguardante i contratti di fornitura di contenuti e servizi digitali, ma su questa interpretazione va fatta chiarezza alla luce dei problemi di coordinamento con il GDPR e del tormentato percorso di approvazione della Direttiva[237].

Il 29 ottobre 2021 è stato approvato il decreto legislativo che attua la direttiva UE 2019/770. Essa si applica infatti «*a qualsiasi contratto in cui l'operatore economico fornisce, o si impegna a fornire, contenuto digitale o un servizio digitale al consumatore e il consumatore corrisponde un prezzo o si impegna a corrispondere un prezzo»*[238].

L'aspetto innovativo che ha comportato alcune perplessità riguarda l'espressa qualificazione del trasferimento dei dati personali come corrispettivo nei contratti di fornitura e servizi digitali, come un'obbligazione paragonabile al pagamento di un prezzo[239]. Ad un primo sguardo la Direttiva sembrerebbe aprire a questa possibilità[240] per cui, i dati personali possono essere utilizzati come "moneta" per

[236] Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio, del 20 maggio 2019, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali, in *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32019L0770*

[237] L. LADECOLA, *Dati personali come corrispettivo per servizi digitali, da oggi è possibile,* in *Altalex*, 2021; disponibile online in *https://www.altalex.com/documents/news/2021/11/11/dati-personali-come-corrispettivo-per-servizi-digitali-da-oggi-possibile*

[238] Art. 1, Direttiva (UE) 2019/770

[239] L. SIMONA, *Dati personali in cambio di contenuto digitale e di servizi digitali: la Direttiva 2019/770/UE*, in *Diritto di Internet*, 2019.

[240] La versione finale approvata dal legislatore europeo lascia in sospeso molti aspetti relativi alla compatibilità effettiva di questa possibilità con la normativa vigente in tema di protezione dei dati personali.

comprare contenuti e servizi digitali. Questo sarà possibile però solo se l'utente acconsente ad un trattamento eccedente rispetto a quello minimo essenziale per usufruire del servizio.

La Direttiva ha l'obiettivo di allargare la rete di protezione per il consumatore di servizi e contenuti digitali, ma allo stesso tempo descrive anche nuovi modelli contrattuali, in cui il dato personale è inteso come strumento di pagamento[241]. Il Considerando 24 della direttiva elenca una serie di dati personali che possono essere adoperati come strumenti di pagamento, tra questi vi sono l'indirizzo e-mail e il nome che sono forniti dall'utente nel momento dell'iscrizione su un social media oppure contenuti come foto o post che l'utente pubblica on line.

Sempre il Considerando 24 della Direttiva cita anche la protezione dei dati personali definendola come «*un diritto fondamentale e che tali dati non possono dunque essere considerati una merce*», nonostante poi vada oltre questo riconoscimento. Difatti, secondo la Direttiva non si tratta di una vendita di dati, anche se si sta affermando che il dato personale è utilizzabile come corrispettivo, e che ha dunque un valore commerciale; per questo la Direttiva dovrebbe trovare applicazione nei contratti il cui l'operatore economico si impegna a fornire contenuti o servizi digitali al consumatore che a sua volta si impegna a fornire i propri dati personali; questi potrebbero essere comunicati all'operatore economico alla conclusione del contratto, oppure in un momento successivo, ad esempio nel caso in cui l'utente acconsente che l'operatore economico usufruisca degli eventuali dati personali.

Una grande novità della Direttiva è che essa fornisce al consumatore la possibilità di vedersi riconosciuta l'opportunità di attivare i rimedi contrattuali anche nel caso abbia "pagato", trasferendo i suoi dati personali, essendo data per assunta la

[241] Il considerando 24 della Direttiva 2019/770 stabilisce che «l*a fornitura di contenuti digitali o di servizi digitali spesso prevede che, quando non paga un prezzo, il consumatore fornisca dati personali all'operatore economico. Tali modelli commerciali sono utilizzati in diverse forme in una parte considerevole del mercato*».

natura di “corrispettivo contrattuale” dei dati[242]. Il consumatore potrà azionare tali rimedi in caso di mancata fornitura del servizio o del contenuto digitale o in caso di difetto di conformità *«se l’operatore economico ha omesso di fornire il contenuto digitale o il servizio digitale conformemente all’articolo 5, il consumatore invita l’operatore economico a fornire il contenuto digitale o il servizio digitale. Se l’operatore economico omette successivamente quindi di fornire il contenuto digitale o il servizio digitale senza indebito ritardo oppure entro un ulteriore termine espressamente concordato dalle parti, il consumatore ha il diritto di recedere dal contratto»*[243].

3.2 La direttiva UE 2019/770 e il GDPR

Tuttavia, la possibilità di impiegare i dati personali come corrispettivo fa sorgere alcuni problemi di coordinamento con il GDPR. Di fatto il processo di attuazione della Direttiva UE 2019/770 è stato molto travagliato[244].

Già nel 2017 l’European Data Protection Supervisor (EDPS) aveva emanato un parere[245] in cui ribadiva il principio che i dati personali non possono essere paragonati ad una merce di scambio, in quanto sono strettamente legati alla tutela di un diritto fondamentale dell’individuo, per cui non si parla di un semplice interesse dei consumatori.

Ci sono inoltre delle differenze strutturali tra la natura dei dati e la moneta. La differenza maggiore si riscontra proprio nella non rivalità e non escludibilità dei dati personali.

---

[242] L. SIMONA, *Dati personali in cambio di contenuto digitale e di servizi digitali: la Direttiva 2019/770/UE*, in *Diritto di Internet*, 2019.
[243] art 13, par.1 della direttiva 2019/770 (UE)
[244] R. SAVELLA, M. MARTORANA, *Direttiva UE 2019/770: è possibile “pagare con i dati”?,* in *Altalex*, 2021; disponibile online in *https://www.altalex.com/documents/news/2021/10/06/direttiva-ue-2019-770-possibile-pagare-con-dati*
[245] European Dara Protection Supervisor, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content

Invero, se il denaro si “consuma” perché non posso pagare in due negozi differenti, o più volte, con la stessa banconota, questo non si verifica per il dato che può essere raccolto ed utilizzato da più soggetti diversi contemporaneamente e per un periodo di tempo illimitato, dato che si tratta di un’informazione riguardante un individuo, e questo non determina una sua perdita di valore[246].

Infine, si presenterebbero dei problemi di coordinamento tra questo tipo di transazioni e la disciplina prevista dal GDPR, che deve comunque essere applicata al trattamento dei dati personali come stabilito anche dalla Direttiva[247].

Un primo esempio può essere fornito dall’articolo 5 del Regolamento che stabilisce la limitazione delle finalità e della conservazione; il dilemma sta nel come garantire il rispetto di questi principi in una transazione di tipo commerciale in cui l’interessato scambia i propri dati personali per usufruire di un servizio o avere accesso ad un contenuto digitale. Dunque, cosa dovrà scrivere il titolare del trattamento nell’informativo riguardo alle finalità o ai tempi di conservazione? Dovrebbero essere predeterminati?

È da tenere a mente che in questo caso ci si riferisce ai dati non necessari all’esecuzione del contratto; non sono questi ad essere oggetto della transazione di scambio ma sono informazioni aggiuntive, che servono esclusivamente per avere un ritorno economico al fornitore del servizio o del contenuto digitale dallo scambio col consumatore. Dunque, per il GDPR non è ammissibile un’autorizzazione in bianco al trattamento dei propri dati personali anche se questo sarebbe di fatto quello di cui ha bisogno il fornitore.

Un’altra importante problematica riguarda il consenso fornito dal consumatore al trattamento dei dati personali. Ci si chiede infatti se questo possa essere

[246] Aspetto già considerato dall’EDPS nel suo Parere 4/2017.
[247] Il GDPR e in particolare la Direttiva 2019/770 al Considerando 37 prevede che «*i dati personali dovrebbero essere raccolti o altrimenti trattati esclusivamente nel rispetto del regolamento (UE) 2016/679 e della direttiva 2002/58/CE. In caso di conflitto tra la presente direttiva e il diritto dell’Unione in materia di protezione dei dati personali, quest’ultimo dovrebbe prevalere.*»

considerato un consenso libero[248]. L'articolo 7, paragrafo 4 del GDPR specifica, infatti, che «*l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto*». Quindi questo dubbio viene portato alla luce proprio dal Regolamento stesso.

Oltre a ciò, vi è un'altra incognita riguardante il consenso e la sua revoca: il consenso, infatti, deve essere revocabile in qualsiasi momento e con la medesima facilità con cui è stato ottenuto[249]. Ma come si procede se il consumatore revoca il consenso in un momento successivo all'utilizzo del servizio o dopo aver scaricato il contenuto digitale? La domanda più generale è quindi quale sarebbe il collegamento tra il consenso al trattamento dei dati e il consenso al contratto.

La Direttiva conferma inoltre che le condizioni per il trattamento lecito dei dati personali sono disciplinate dal Regolamento 2016/679[250]; di conseguenza, nei casi in cui il trattamento dei dati personali si fondi sul consenso come base giuridica, si applicano le disposizioni del Regolamento[251], comprese le norme riguardanti la valutazione circa la libertà con cui è stato prestato il consenso.

Dunque, la Direttiva non disciplina i casi e le modalità del consenso al trattamento dei dati personali, in quanto rinvia la questione al Regolamento generale sulla protezione dei dati[252].

Per chiarire le perplessità sorte, nella stesura definitiva della Direttiva UE 2019/770 il termine "controprestazione", in riferimento all'attività del consumatore che presta il consenso al trattamento dei propri dati personali per usufruire del

[248] La libertà del consenso è un requisito previsto già dalla Direttiva 95/46/CE (art.2, lett. h), dal Codice della privacy (art. 23) e poi ripreso dal Regolamento (UE) 2016/679.
[249] Art.7, par. 3, del Regolamento (UE) 2016/679
[250] Il Considerando 38 stabilisce che «*La presente direttiva non dovrebbe disciplinare le condizioni per il trattamento lecito dei dati personali, dal momento che tale questione è specificamente disciplinata dal regolamento (UE) 2016/679.»*
[251] Art. 6, par. 1, lett. *a),* del regolamento (UE) 2016/679
[252] L'articolo 16 della Direttiva prevede che in caso di risoluzione o recesso, l'operatore economico deve rispettare quanto stabilito dal GDPR.

servizio o accedere al contenuto digitale, è stato eliminato, dato che il consenso al trattamento dei dati personali non può essere considerato una "controprestazione". Oggi infatti, l'articolo 3 della Direttiva stabilisce infatti che «*La presente direttiva si applica altresì nel caso in cui l'operatore economico fornisce o si impegna a fornire contenuto digitale o un servizio digitale al consumatore e il consumatore fornisce o si impegna a fornire dati personali all'operatore economico, fatto salvo il caso in cui i dati personali forniti dal consumatore siano trattati esclusivamente dall'operatore economico ai fini della fornitura del contenuto digitale o del servizio digitale a norma della presente direttiva o per consentire l'assolvimento degli obblighi di legge cui è soggetto l'operatore economico e quest'ultimo non tratti tali dati per scopi diversi da quelli previsti*».

L'aver eliminato la parola "controprestazione" che era presente nella proposta di Direttiva chiarisce quindi lo scopo della Direttiva, che non vuole stabilire un contratto a titolo oneroso. Così, il legislatore europeo ha tenuto conto del parere dell'EDPS, mantenendo comunque questo tipo di rapporto all'interno della Direttiva, ma non in un'ottica di corrispettività[253].

Lo scopo della Direttiva UE 2019/770 non è dunque quello di sdoganare il pagamento tramite i dati personali ma è quello di allargare le tutele del consumatore comprendendo anche questo tipo di operazioni che ormai sono molto frequenti nel mondo digitale.

Di fatto, svolgendo una breve digressione sul recepimento nel nostro Paese, lo schema del D. Lgs di attuazione introduce un nuovo Capo I-*bis* nel Codice del Consumo, proprio per regolare alcuni aspetti riguardanti i contratti di fornitura di contenuti o servizi digitali attuati tra consumatore e professionista, come la conformità al contratto del contenuto o dei servizio digitale, i rimedi e le modalità dei rimedi in caso di difetti di conformità o di mancata fornitura o la modifica del

[253] L. LADECOLA, *Dati personali come corrispettivo per servizi digitali, da oggi è possibile,* in *Altalex*, 2021; disponibile online in *https://www.altalex.com/documents/news/2021/11/11/dati-personali-come-corrispettivo-per-servizi-digitali-da-oggi-possibile*

servizio o del contenuto digitale. Tutto questo, a prescindere dal fatto che vi sia o meno un pagamento; può trattarsi anche di un rapporto a titolo gratuito, in cui il consumatore presta il consenso all'utilizzo dei propri dati personali non necessari per l'esecuzione del contratto[254].

3.3 Il consenso negoziale e la casistica in Cassazione

Sin dalle prime riflessioni del 1995 intorno alla questione del consenso, si era affermata l'idea che esso non rappresentasse un elemento di una fattispecie negoziale ma piuttosto che raffigurasse un esimente della illiceità del trattamento che il titolare aveva il compito di richiedere all'interessato per evitare le sanzioni previste dalla legge. Questa posizione era in linea con la ricostruzione della nozione di dati personali in termini solo di diritti assoluti e quindi non relativi[255]. Dunque, la tutela dell'interessato è stata collocata interamente nella sfera di tutela dei diritti della personalità, e quindi della responsabilità extracontrattuale, e non della persona, vale a dire dell'interessato, anche come contraente che fornisce i suoi dati personali per ottenere un'utilità economica prendendo parte ad un'operazione economica; l'interessato prestando il proprio consenso, avrebbe concorso a realizzare un'operazione negoziale e avrebbe visto la sua tutela in ambito contrattuale[256].

---

[254] Online in *https://www.ipsoa.it/documents/impresa/contratti-dimpresa/quotidiano/2021/11/29/contratti-fornitura-contenuto-digitale-nuove-disposizioni-vigore-1-gennaio-2022*

[255] V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, *I dati personali nel diritto europeo*, G. Giappichelli Editore, Torino, 2019, p. 35

[256] *Ivi*, pp.35-36. *«se cedo i miei dati ad una banca dati pattuendo un corrispettivo e il soggetto cessionario utilizza, anche correttamente i dati, ma non provvede al pagamento, procederò giudizialmente per inadempimento di quell'obbligo e per il risarcimento del danno patrimoniale eventualmente subito: perché dovrei invocare la tutela della mia personalità morale per il mancato adempimento ed agire per responsabilità extracontrattuale, a fronte di una pura patologia contrattuale (l'inadempimento) che avrebbe poco o nulla a che fare, in una tale fattispecie, con i diritti della personalità?».* Vicenda del tutto diversa da quella in cui il trattamento dei dati venisse effettuato dal titolare senza il consenso dell'interessato, configurandosi quindi come un illecito e comportando la richiesta del danno non patrimoniale.

Dunque, il trattamento illecito dei dati personali, vale a dire eseguito senza il consenso dell'interessato, corrisponde ad un illecito extracontrattuale che lede i diritti assoluti della personalità.

Si è affermata però una tesi che analizza il consenso come fenomeno di natura negoziale, introducendolo quindi nella tematica del diritto delle obbligazioni e del contratto. Ci si trova dunque in un processo di circolazione di ricchezza, secondo i tratti propri di ogni mercato; anche in questo caso però l'interessato avrebbe una serie di tutele riferibili al "diritto alla protezione dei dati personali", riconducibile alla più generale tutela della personalità. Il consenso rimarrebbe comunque in questo caso un elemento negoziale in quanto è condizione essenziale del contratto di trattamento e l'interessato dispone dei suoi dati per uno scopo di arricchimento e spostamento patrimoniale.

Ciò che ha contribuito alla difficoltà della ricostruzione del fenomeno anche in chiave negoziale è la possibilità di revoca del consenso, un diritto dell'interessato che mal si concilia con l'ipotesi di un contratto in cui l'interessato cede i suoi dati al titolare[257]. Questo però non esclude del tutto la possibilità di un rapporto obbligatorio e quindi la negoziabilità dei dati trattati; si pensi ad esempio al d.lgs. 30 giugno 2003, n.196, il c.d. Codice del trattamento dei dati personali, che sancisce il diritto alla protezione dei dati personali che comprende ogni situazione soggettiva, assoluta o relativa, che riguardi la persona in quel fenomeno. È stato costruito come un principio generale ed immanente della disciplina del trattamento, il quale si impone in ogni ambito del fenomeno e di conseguenza anche nelle vicende negoziali aventi ad oggetto quel bene, arrivando a comprendere anche istituti, come quello della revoca del consenso, che

[257] G. RESTA, *Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali* in *Riv. crit. dir. priv.*, n.2, 2000, p.310. *«Lo strumento che permette al soggetto di riappropriarsi nella maniera più completa ed incisiva, del potere di controllo sulla circolazione delle proprie informazioni è costituito proprio dalla revoca del consenso. Il fondamento della facoltà di revoca deve essere ricercato in quello stesso potere di autodeterminazione del soggetto che nella manifestazione del consenso aveva trovato il suo primo e principale atto di esercizio».*

solitamente sono estranei ai tipi contrattuali di disposizione dei beni così come disciplinati nel diritto civile.

Infine, il regime di circolazione del "bene" dato personale è controllato da logiche diverse rispetto a quelle tipiche della trasmissione dei diritti sui beni[258]. Una consistente parte della dottrina ritiene che l'affermazione della natura negoziale dell'atto non sia in contrasto con la definizione di un regime differenziato quanto, ad esempio, alla capacità, ai vizi del consenso e alla sua revocabilità, propendere per una o per l'altra opzione ricostruttiva risulterebbe indifferente sul piano pratico[259]. Alcuni, infatti, sostengono che chi manifesta il consenso, manifesta la sua assenza di interesse alla protezione, vi rinuncia. Ma non è questa la logica a cui sembra ispirarsi la dottrina riguardante il trattamento dei dati personali; innanzitutto, il consenso è solo uno degli strumenti di cui si serve il legislatore per regolare il trattamento dei dati e bilanciare gli interessi in gioco; in secondo luogo, chi presta il consenso non manifesta assenza di interesse ma piuttosto pone in essere un vero e proprio atto di esercizio del diritto all'autodeterminazione nella sfera delle scelte personali[260].

Dunque, il consenso al trattamento è lo strumento attraverso cui l'interessato esercita un ruolo nella determinazione delle possibilità e finalità del trattamento; è uno strumento, infatti, che permette il trattamento, e quindi può essere interpretato come un esercizio del diritto alla riservatezza e come strumento di tutela e partecipazione dell'interessato nella costruzione del regime dei dati personali[261].

C'è anche chi afferma la possibilità di un consenso negoziale che porta alla responsabilizzazione rispetto ai soggetti verso i quali si dirige il consenso. Questo

---

[258] V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, *I dati personali nel diritto europeo*, G. Giappichelli Editore, Torino, 2019, p.38

[259] G. RESTA, *Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali* in *Riv. crit. dir. priv.*, n.2, 2000, p.305.

[260] *Ivi*, p.306. «subordinare la legittimità del trattamento al previo consenso dell'interessato significa in primo luogo riconoscere al soggetto il potere di sottrarre determinate informazioni alla raccolta e all'elaborazione da parte di terzi».

[261] C. ANGIOLINI, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, G. Giappichelli Editore, Torino, 2020 p.122

punto di vista mantiene strutturalmente intatto lo schema dell'esclusività in un rapporto costruito come bene-soggetto. Si sostiene dunque che la riservatezza, che sta alla base della tutela dei dati personali, agisce rispetto alla persona come opera il concetto di esclusività con riguardo ai beni. Inoltre, c'è chi ha anche sostenuto che il consenso esegue una funzione dispositiva nei confronti della sfera privata dell'individuo-interessato. La divisione del consenso in due momenti non tiene però presente che quando si qualifica il consenso come autorizzazione, è già il momento in cui si determinano le finalità e i destinatari della comunicazione dei dati personali[262]. Tenendo quindi uniti il momento della prestazione del consenso e quello della determinazione delle finalità, il consenso si potrebbe configurare come atto di autonomia privata, tramite cui l'interessato esercita il diritto alla vita privata e alla protezione dei dati personali[263].

La questione riguardante la qualificazione del consenso come atto negoziale è di fatto molto complicata; se da una parte infatti la volontà dell'interessato rileva sotto il profilo della determinazione delle finalità del trattamento, dall'altra però l'effetto di rendere lecito il trattamento deriva da una disposizione di legge, vale a dire l'art. 6, par. 1, lett. *a)* Reg. UE 2016/679 o dall'art. 9, par.2, lett. *a)* nel caso di dati sensibili. Di fatto parte della dottrina ha qualificato il consenso come atto non negoziale[264].

L'interessato ha però il potere di permettere la creazione del bene in senso giuridico o di regolare l'estensione del trattamento, esercitando in questo modo il diritto alla protezione dei dati di cui è titolare. Non si può quindi escludere del tutto

[262] Pena la mancanza di un consenso specifico. Il Considerando 43 del Reg. UE 2016/679, prevede una presunzione che il consenso non sia liberamente prestato «se non è possibile prestare un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso»; EDPB, *Linee guida 5/2020 sul consenso ai sensi del Reg (UE) 2016/679*, 4 maggio 2020, pp.12-13 secondo cui il consenso non può essere considerato libero e specifico se non è prestato per ogni singola finalità e quindi se non è "granulare".
[263] G. RESTA, *Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali* in *Riv. crit. dir. priv.*, n.2, 2000, p.307. Il consenso è "vero e proprio atto di esercizio di quel diritto di autodeterminazione nella sfera delle scelte personali che trova nella orma costituzionale (art.2) il più generale "precetto di tutela" e nella disciplina sulla protezione dei dati una diretta e immediata concretizzazione".
[264] C. ANGIOLINI, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, G. Giappichelli Editore, Torino, 2020 p.125

il carattere negoziale dell'atto, dato che gli effetti sono pur sempre determinati dalla decisione del soggetto.

Secondo il giurista Stefano Rodotà, al quale non sfuggiva certo la qualificazione della privacy come diritto fondamentale, dato che aveva contribuito a definirlo nell'art. 8 della Carta Europea dei diritti fondamentali dell'Unione Europea, questo era possibile una configurazione di tipo negoziale del consenso; dopo l'entrata in vigore della prima legge nazionale in materia di privacy egli affermava ciò*: «Io credo che noi dobbiamo lavorare molto nella dimensione negoziale, non ho nessun dubbio. Negoziale vuol dire per esempio: il consenso può essere oneroso, può essere condizionato, può essere a termine? Io come risposta generale direi di sì, e perché no? Posso negoziare, e badate alcune forme improprie di negoziazione già ci sono. Quando si dice che se tu riempi questo questionario riceverai un campione del prodotto, non è un prodotto in omaggio, perché io cedo qualcosa che per il soggetto che mi darà il prodotto ha un valore aggiunto molto maggiore di ciò che mi viene dato; quindi, ci sono già delle transazioni economiche su questa base, di difficile definizione, ma certamente ci sono»*[265].

Recentemente, anche la Corte Suprema di Cassazione sembra sia giunta alla medesima conclusione in quanto ha affermato che subordinare la fornitura di un servizio, nel caso in esame si trattava di una newsletter finanziaria, alla prestazione del consenso da parte dell'utente al trattamento dei suoi dati personali per finalità di marketing, non è sufficiente a invalidare l'efficacia del consenso che conserva i requisiti stabiliti dalla disciplina privacy. Secondo i giudici questo era possibile almeno quando il servizio o il contenuto digitale elargito dal fornitore che esige il consenso, sia un servizio fungibile e/o rinunciabile per l'utente[266].

[265] S. RODOTÀ, *Conclusioni, in Trattamento dei dati personali e tutela della persona*, a cura di V. CUFFARO-V. RICCIUTO-V. ZENO ZENCOVICH, cit., p.308.
[266] Cass. Civ. 17278/2018 – Newsletter, e-mail pubblicitarie e consenso

Con questi presupposti i giudici scrivono che *«non può allora essere condiviso l'argomento svolto dal giudice di merito secondo cui, dando credito alla tesi sostenuta dal Garante, si finirebbe per «delineare una sorta di obbligo tout court, per il gestore del portale, di offrire comunque le proprie prestazioni, a prescindere dalla prestazione del consenso al trattamento dei dati personali da parte dell'utente»: e, in buona sostanza, per obbligare così il gestore del portale a rinunciare al tornaconto economico dell'operazione che egli compie, proveniente dall'attività pubblicitaria realizzata tramite l'impiego dei dati personali acquisiti. Nulla, infatti, impedisce al gestore del sito — beninteso, si ripete, in un caso come quello in questione, concernente un servizio né infungibile, né irrinunciabile —, di negare il servizio offerto a chi non si presti a ricevere messaggi promozionali, mentre ciò che gli è interdetto è utilizzare i dati personali per somministrare o far somministrare informazioni pubblicitarie a colui che non abbia effettivamente manifestato la volontà di riceverli. Insomma, l'ordinamento non vieta lo scambio di dati personali, ma esige, tuttavia, che tale scambio sia frutto di un consenso pieno ed in nessun modo coartato».*

Da questo si evince che la Cassazione sembra ammettere la qualificazione del consenso al trattamento di dati personali come corrispettivo non pecuniario di una prestazione, a condizione però che questa prestazione sia fungibile e rinunciabile per l'interessato.

In questo modo secondo i Giudici di legittimità non ci sarebbe nessun contrasto con l'art. 7, comma 4 del GDPR, il quale stabilisce che *«Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto».*

Si tratta però di una posizione che difficilmente si concilierebbe con la posizione dei Garanti per la protezione dei dati personali europei che nelle loro linee guida

del 4 maggio 2020[267], sul consenso nel GDPR hanno indicato che *«Se il consenso è un elemento non negoziabile delle condizioni generali di contratto/servizio, si presume che non sia stato prestato liberamente. Di conseguenza, il consenso non sarà considerato libero se l'interessato non può rifiutarlo o revocarlo senza subire pregiudizio»* suggerendo un esempio che si contrappone al caso all'origine della decisione dalla Corte di Cassazione.

Lo stesso Comitato, nelle medesime linee guida, ritorna sul concetto e interpreta il comma 4 dell'art. 7 del GDPR, nel senso di ritenere che con questo articolo il Regolamento intende garantire *«che il trattamento dei dati personali per cui viene richiesto il consenso non possa trasformarsi direttamente o indirettamente in una controprestazione contrattuale»*[268].

Nelle linee guida sono proposti altri esempi sul tema, uno di questi ribadisce il concetto dicendo che *«Una banca chiede ai clienti il consenso per consentire a terzi di utilizzare i dettagli di pagamento per finalità di marketing diretto. Questa attività di trattamento non è necessaria per l'esecuzione del contratto stipulato con il cliente e la prestazione di servizi ordinari di conto bancario. Qualora il rifiuto del cliente a prestare il consenso per tale finalità di trattamento porti alla negazione di servizi bancari, alla chiusura del conto bancario o, a seconda dei casi, a un aumento della commissione, il consenso non può considerarsi espresso liberamente»*[269].

---

[267] EDPB, *Linee guida 5/2020 sul consenso ai sensi del Reg (UE) 2016/679*, 4 maggio 2020, p.8.
L'esempio è il seguente: *«Un'applicazione mobile per il fotoritocco chiede agli utenti di attivare la localizzazione GPS per l'utilizzo dei suoi servizi. L'applicazione comunica agli utenti che utilizzerà i dati raccolti per finalità di pubblicità comportamentale. Né la geolocalizzazione né la pubblicità comportamentale online sono necessarie per la prestazione del servizio di fotoritocco e vanno oltre la fornitura del servizio principale. Poiché gli utenti non possono utilizzare l'applicazione senza acconsentire a tali finalità, il consenso non può essere considerato liberamente espresso».*

[268] *Ivi*, p.11. Dunque, nelle Linee Guida si chiarisce che «le due basi legittime per la liceità del trattamento dei dati personali, ossia il consenso e l'esecuzione di un contratto, non possono essere riunite e rese indistinte»

[269] *Ivi*, p.12-13. Un altro esempio riguardante i cookie wall sostiene*: «Un fornitore di un sito web predispone uno script che blocca la visualizzazione del contenuto e fa apparire solo la richiesta di accettare i cookie, le informazioni sui cookie che verranno installati e le finalità per le quali i dati saranno trattati. Non è possibile accedere al contenuto senza cliccare sul pulsante "Accetto*

Nonostante ciò, neppure il comitato dei Garanti giunge alla conclusione di escludere completamente che il consenso al trattamento dei dati personali possa essere classificato come controprestazione, in quanto ricorda che tale conclusione è "solo" una "presunzione forte" con la conseguenza che "in un numero molto ristretto di casi"[270] subordinare la fornitura di un servizio alla prestazione del consenso potrebbe non valere a rendere invalido il consenso.

Trattandosi però di una presunzione forte, in queste limitate ipotesi, in caso di contestazione, sarà compito del titolare del trattamento fornire prova della circostanza che il consenso può ritenersi liberamente espresso, anche se condizionato.

Sembra dunque difficile classificare il trattamento di dati personali come controprestazione di un servizio.

Un caso concreto riguardante questo tema è offerto dalla Sentenza[271] con la quale lo scorso 29 marzo 2021 il Consiglio di Stato ha comprovato la sostanziale legittimità del provvedimento adottato dall'Autorità Garante per la concorrenza e il mercato (AGCM) nei confronti di Facebook, il 29 novembre 2018[272]. Facebook era stato accusato di aver fatto intendere ai suoi utenti che il servizio offerto fosse gratuito, anche se in realtà, veniva fornito con la messa a disposizione dei dati personali dei consumatori[273].

i cookie". Poiché all'interessato non è offerta una scelta effettiva, il suo consenso non è espresso liberamente. In questo caso il consenso non è valido, in quanto la prestazione del servizio è subordinata al fatto che l'interessato clicchi sul pulsante "Accetto i cookie". Non è offerta una scelta effettiva».

[270] *Ibidem*

[271] Cons. St. sentenza 29 marzo 2021, n.2631

[272] AGCM, provvedimento 29 novembre 2018, n.27432

[273] Ivi, cit, p.2. «*In sede di avvio veniva ipotizzata l'ingannevolezza della pratica a), descritta sub sezione II), in quanto il Professionista non informerebbe adeguatamente e immediatamente l'utente, in fase di attivazione dell'account, dell'attività di raccolta dei suoi dati a fini commerciali ovvero finalizzata alla loro monetizzazione, rendendolo edotto della sola gratuità della fruizione del servizio, così da indurlo ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso (registrazione al social network e permanenza nel medesimo)».*

Si pone quindi una questione di fondamentale importanza, vale a dire se il trattamento dei dati personali da parte di una società può essere considerato il corrispettivo di un servizio offerto dalla società stessa ai propri utenti.

Da un lato, di fronte ai giudici amministrativi, la società di Facebook ha sostenuto di no, affermando anche che «*I dati personali di ciascun individuo costituiscono un bene extra commercium, trattandosi di diritti fondamentali della persona che non possono essere venduti, scambiati o, comunque, ridotti a un mero interesse economico*[274]*».* Ha inoltre aggiunto che *«Non può immaginarsi possibile come erroneamente ha inteso rappresentare il giudice di primo grado (il TAR Lazio*[275]*), che gli utenti cedano i propri dati a Facebook quale 'corrispettivo' per la fornitura del servizio né che la trasmissione di dati personali possa attenere ad una attività economicamente valutabile, se non invece e al più, ad un mero profilo di tutela di alcuni diritti fondamentali».*

Dall'altro il Consiglio di Stato ha sostenuto che se *«si volesse aderire alla tesi della odierna parte appellante (Facebook) secondo la quale il dato personale costituisce una res extra commercium, la patrimonializzazione del dato personale, che nel caso di specie avviene inconsapevolmente (ad avviso dell'Autorità nel momento in cui accusa una informazione ingannevole nell'esercizio della pratica in questione), costituisce il frutto dell'intervento delle società attraverso la messa a disposizione del dato – e della profilazione dell'utente – a fini commerciali».*

In pratica i Giudici amministrativi non ritengono fondamentale rispondere in modo diretto al problema della qualificabilità del trattamento di dati personali come "corrispettivo" del servizio fornito da Facebook, ma credono sia sufficiente la

[274] M. FERRARI, *Facebook non è gratis: l'utente "paga" il servizio con i propri dati personali*, in *Altalex*, 14/04/21, online su *https://www.altalex.com/documents/news/2021/04/14/facebook-non-e-gratis-utente-paga-servizio-con-i-propri-dati-personali.*
Facebook avrebbe adottato questa linea difensiva per dimostrare l'inapplicabilità delle norme del Codice del Consumo in caso di pratiche commerciali scorrette, per escludere la sussistenza di una pratica commerciale; non può esserci una pratica scorretta nel caso in cui non ci sia una pratica commerciale.
[275] Tar Lazio, Sez. I, 10 gennaio 2020, n.260

circostanza che i dati personali degli utenti formano oggetto di "patrimonializzazione da parte di Facebook" a considerare scorretta e ingannevole la presentazione del servizio come gratuito. I giudici hanno confermato il provvedimento sanzionatorio solo in relazione alla pratica commerciale scorretta[276] ed ingannevole, dato che Facebook, al momento dell'iscrizione informa l'utente solo della gratuità dell'iscrizione e non comunica che i dati personali saranno ceduti ed usati a scopi commerciali, vale a dire per la profilazione[277].

Come è già stato detto, questo business model delle più influenti piattaforme, è ormai diffusissimo nel mercato digitale, diventando proprio una delle sue peculiarità: i servizi sono erogati senza pretendere un pagamento in denaro ma con la precedente raccolta dei dati personali degli utenti.

In questo modo, come sottolineano i Giudici del Consiglio di Stato, sono destinati a formare oggetto di "patrimonializzazione" nell'ambito di un'attività commerciale[278].

Tuttavia, anche se il fornitore del servizio digitale ricava profitto dai dati dei propri utenti, questo non vuol dire necessariamente che gli utenti paghino il servizio fornito con i loro dati personali, almeno in una dimensione di analisi giuridica.

---

[276] In merito alla qualificazione di una pratica commerciale scorretta, l'art. 20 del Codice del Consumo considera scorretta una pratica se: 1. È contraria alla diligenza professionale, 2. È falsa o idonea a falsare in misura apprezzabile il comportamento economico del consumatore medio. La pratica ingannevole adottata da Facebook è stata quella di non informare subito i propri utenti circa l'utilizzo dei loro dati che sarebbero stati utilizzati per finalità commerciali.

[277] M. FERRARI, *Facebook non è gratis: l'utente "paga" il servizio con i propri dati personali*, in *Altalex*, 14/04/21, online su *https://www.altalex.com/documents/news/2021/04/14/facebook-non-e-gratis-utente-paga-servizio-con-i-propri-dati-personali.*
Secondo l'AGCM il 98% del fatturato della società deriva proprio dalla pubblicità online, che si basa sulla profilazione degli utenti.

[278] Facebook ha contestato l'applicazione del Codice del Consumo, invece che del GDPR, dato che la condotta contestata non riguarda l'acquisto di un prodotto. Il Consiglio di Stato ha ritenuto però che la non commerciabilità dei dati non ostacoli la disciplina consumeristica e allo stesso tempo non rende applicabile il GDPR. Questo perché anche se il dato personale non è commerciale, è evidente che lo stesso abbia subito una patrimonializzazione da parte di Facebook.

Infatti, se si presume che tutti i dati personali raccolti siano davvero indispensabili al fornitore del servizio per l'esecuzione del contratto e quindi permettano l'utilizzo del servizio da parte degli utenti, in questi casi i dati personali non possono essere considerati una prestazione o un corrispettivo per il servizio ma rappresentano piuttosto una condizione necessaria per la sua esecuzione.

D'altro canto, se il fornitore del servizio dichiarasse di raccogliere e trattare solo i dati necessari per la fornitura del servizio ma raccogliesse anche dati ulteriori o trattasse quelli raccolto per finalità diverse, questa sarebbe considerata una pratica illecita ai sensi della disciplina in materia di protezione dei dai personali.

La pratica della raccolta o del trattamento di dati personali per finalità diverse da quelle dichiarate potrebbe essere classificata infatti come corrispettivo occulto, vale a dire versato inconsapevolmente, del servizio[279].

Tuttavia, in questo caso non si potrebbe propriamente parlare di fornitura di dati personali come corrispettivo di un servizio in quanto un corrispettivo non è una controprestazione se viene versato inconsapevolmente.

Vi è poi un'altra ipotesi, cioè quella in cui il fornitore del servizio chieda all'utente il consenso al trattamento dei medesimi o ulteriori dati personali per finalità diverse rispetto alla mera esecuzione del contratto.

Ricordiamo che il consenso è sempre comunque revocabile. Dunque, secondo tale principio, non sembra possibile parlare di corrispettività del consenso rispetto alla fornitura del servizio, dato che la prestazione del consenso sarebbe solo eventuale, perciò può essere revocata, e il servizio è destinato a essere fornito anche qualora l'utente non presti tale consenso.

[279] EDPB, *Linee guida 5/2020 sul consenso ai sensi del Reg (UE) 2016/679*, 4 maggio 2020, cit. p. 7. «L'articolo 5, paragrafo 1, lettera b), del RGPD stabilisce il principio della limitazione delle finalità, che impone che i dati personali siano raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità»

Il consenso è quindi sempre revocabile ma l'eventuale revoca non incide sull'obbligo del fornitore a continuare ad adempiere alle proprie obbligazioni.

Inoltre, se il consenso viene fornito, si pone la questione della sua classificazione nella dimensione negoziale, dato che l'utente in sostanza consegna al fornitore un'importante utilità economica senza però ricevere in cambio nulla in più o differente rispetto al servizio del quale potrebbe avvalersi se negasse il consenso.

Per questo motivo, la prestazione del consenso potrebbe essere considerata come liberalità dell'utente nei confronti del gestore della piattaforma. Ma si tratta comunque di una qualificazione insoddisfacente sul piano negoziale.

Non si può però affermare che ci sia una corrispettività se i dati sono forniti esclusivamente per la fornitura del servizio.

In nessuno dei casi visti infatti, il fornitore del servizio subordina l'utilizzo di tale servizio alla raccolta dei dati personali non necessari alla semplice esecuzione del contratto, paragonandoli quindi ad una controprestazione in denaro.

Per cui, nessuno dei precedenti scenari pare conciliare con la fattispecie pure già entrata in vigore nell'Ordinamento europeo con l'articolo 3 della Direttiva (UE) 2019/770 secondo il quale la Direttiva viene applicata anche *«nel caso in cui l'operatore economico fornisce o si impegna a fornire contenuto digitale o un servizio digitale al consumatore e il consumatore fornisce o si impegna a fornire dati personali all'operatore economico, fatto salvo il caso in cui i dati personali forniti dal consumatore siano trattati esclusivamente dall'operatore economico ai fini della fornitura del contenuto digitale o del servizio digitale a norma della presente direttiva o per consentire l'assolvimento degli obblighi di legge cui è soggetto l'operatore economico e quest'ultimo non tratti tali dati per scopi diversi da quelli previsti».*

È proprio l'analisi di questa disposizione che conferma che non c'è corrispettiva quando i dati personali sono concessi al fornitore del servizio solo per scopi legati alla fornitura del servizio stesso; il consumatore potrebbe vedersi riconosciuta la

medesima tutela consumeristica che gli spetterebbe se la prestazione fosse di tipo monetario.

Il Garante ha stabilito l'illiceità di questo trattamento di dati personali ed ha quindi emanato un provvedimento inibitorio in quanto «*la società non ha consentito agli interessati di esprimere uno specifico consenso per la ricezione di messaggi promozionali via e-mail essendo stato […] obbligatorio prestare il consenso alla ricezione degli stessi per potersi iscrivere al servizio di newsletter, salvo la possibilità di servirsi dell'opt-out»*[280]*.*

Il Tribunale di Arezzo, tuttavia, ha accolto l'opposizione apportata dalla società, ritenendo che il Codice per la protezione dei dati personali non obbligasse il gestore di un portale di offrire le proprie prestazioni anche se l'utente non avesse prestato il consenso e che comunque gli utenti; ritenne inoltre che gli utenti avessero comunque prestato il proprio consenso in modo libero. Per di più, il Tribunale sostenne che, attraverso le Linee Guida contro lo spam del 2013, il Garante aveva indebitamente integrato gli obblighi stabiliti dall'articolo 23 del Codice Privacy.

Quindi il Garante per la Protezione dei dati personali ha interpellato la Corte di Cassazione[281] impugnando la sentenza del Tribunale di Arezzo, reclamando una diversa natura delle proprie Linee Guida che *"recavano invece soltanto la corretta interpretazione del dato normativo, alla luce del quale occorreva che il consenso al trattamento dei dati personali fosse espresso liberamente e specificamente, mancando nel caso di specie una specifica manifestazione di volontà volta alla ricezione di messaggi promozionali via ma/l, essendo obbligatorio prestare il consenso alla loro ricezione per potersi iscrivere al servizio di newsletter offerto dalla società".*

È da premettere che, sebbene la vicenda si sia sviluppata prima dell'entrata in vigore del GDPR, i principi esposti erano già vigenti nella normativa europea: di

[280] *Ivi*, p.2
[281] Cass. Sentenza del 2 luglio 2018, n. 17278

fatto l'art. 23 del D.Lgs. n. 196/03[282] già richiedeva un consenso libero che, stando alle indicazioni fornite dal Garante per la protezione dei dati personali, si declinava nell'assenza di condizionamenti da parte del titolare del trattamento. Dunque, sia il GDPR e quindi le linee guida del WP29 si pongono in continuità con principi già consolidati in tema di consenso libero. Infatti la stessa Corte di legittimità, in questa sentenza, opera un richiamo al GDPR per meglio definite la portata dell'art. 23 citato.

La Cassazione ha accolto il ricorso dell'autorità Garante e ha analizzato la nozione di consenso adottata dal legislatore con l'articolo 23 del Codice Privacy, prendendo in considerazione anche la nozione offerta dall'articolo 4 del GDPR. La Corte di Cassazione ha messo in evidenza diversi aspetti tra cui:

- Il fatto che la nozione di consenso all'interno di un processo di trattamento di dati personali non può essere paragonata a quella del consenso genericamente necessario a fini negoziali e commerciali: il consenso al trattamento di dati personali deve essere *"rafforzato",* come il consenso *"informato*" necessario a fini sanitari e *«dettato dall'esigenza di rimediare alla intrinseca situazione di debolezza dell'interessato, sia sotto il profilo della evidente «asimmetria informativa », sia dal versante della tutela contro possibili tecniche commerciali aggressive o suggestive»;* dunque la Corte cerca di delineare i contorni della definizione di consenso ai fini della normativa sulla protezione dei dati personali, precisando appunto che non a questa definizione non può essere attribuita semplicemente lo stesso significato che assume il consenso nella disciplina negoziale del codice civile. Ai fini privacy, infatti, è richiesto che il consenso sia prestato da un soggetto informato a cui devono essere comunicate tutte le informazioni necessarie, indicate ad oggi negli articoli 13 e 14 del GDPR.

[282] Articolo successivamente abrogato dal D.Lgs. n. 101/2018

- Il consenso in materia di dati personali ha un ruolo *«tale da non ammettere compressioni di alcun genere e non sopporta di essere sia pure marginalmente perturbato non solo per effetto di errore, violenza o dolo, ma anche per effetto dell'intero ventaglio di possibili disorientamenti, stratagemmi, opacità, sotterfugi, slealtà, doppiezze o malizie comunque adottate dal titolare del trattamento. In tal senso va inteso il dato normativo alla luce del quale deve trattarsi di un consenso libero, ossia pienamente consapevole ed informato e non già frutto di alcun condizionamento, e specifico, ossia inequivocabilmente riferito a ciascun particolare effetto del trattamento»*[283].

Dunque, fin qui possiamo dire che la posizione dei giudici di legittimità sembra essere accordo con le linee guida del WP29.

Tuttavia, la Cassazione sostiene che l'esistenza di un condizionamento non possa essere presunta a priori, ma questa deve essere rilevata tenendo in considerazione la fungibilità e l'irrinunciabilità del servizio richiesto[284].

Infatti, nel caso in esame i giudici hanno ritenuto che il servizio informativo derivante dalla newsletter fosse fungibile, dato che è possibile giungere alle stesse informazioni per altre vie, anche a pagamento. Quindi un'eventuale rinuncia a tale servizio non comporterebbe un gravoso sacrificio per l'interessato, secondo la Cassazione.

- Riguardo al requisito della libertà del consenso, la Corte sottolinea che l'articolo 7, paragrafo 4 del GDPR prescrive di tenere *«nella massima considerazione l'eventualità […] che l'esecuzione di un contratto,*

[283] Cass. Sentenza del 2 luglio 2018, n. 17278
[284] *Ivi*, cit, p.9. *«Ritiene la Corte, nel quadro di applicazione del citato articolo 23, che la risposta al quesito non possa essere univoca e, cioè, che il condizionamento non possa sempre e comunque essere dato per scontato e debba invece essere tanto più ritenuto sussistente, quanto più la prestazione offerta dal gestore del sito Internet sia ad un tempo infungibile ed irrinunciabile per l'interessato»*

compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto»[285]*;* però, secondo la Cassazione, il fatto che il gestore di un sito subordini l'offerta del servizio che offre e dunque l'accesso al sito al consenso all'utilizzo dei dati personali per l'invio di messaggi promozionali da parte di terzi, non implica una tale repressione della libertà dell'interessato da rendere il consenso non libero; di fatto ci sarà tanto più un condizionamento tale da rendere il consenso non conforme all'articolo 23 «*quanto più la prestazione offerta […] sia ad un tempo infungibile ed irrinunciabile per l'interessato, il che non può certo dirsi accada nell'ipotesi di offerta di un generico servizio informativo del tipo di quello in discorso»*[286]*.*

L'interessato, infatti, poteva tranquillamente rinunciare al servizio offerto, senza andare in contro ad un "gravoso sacrificio". Per di più, il gestore del sito poteva negare il servizio fornito a chi non prestava il consenso alla ricezione di messaggi pubblicitari, dato che non si trattava di un servizio né infungibile né irrinunciabile; d'altra parte, però non poteva trattare i dati personali per l'inoltro di comunicazioni promozionali senza un'effettiva e chiara manifestazione di volontà da parte dell'interessato.

- C'è un altro requisito da tenere in considerazione, vale a dire quello della specificità del consenso: esso è indissolubilmente connesso con il requisito della libertà di consenso perché ha a che vedere con la *"produzione di effetti che l'utente abbia preventivamente avuto modo di rappresentarsi, singolarmente, con esattezza*[287]*";* dunque, nel caso siano presente diverse finalità del trattamento che necessitano del consenso dell'interessato, è doveroso che egli possa prestare il consenso in

[285] *Ibidem*
[286] *Ibidem*
[287] *Ivi*, p.11

riferimento a ciascuna finalità, singolarmente. Per cui il generico riferimento vicino alla *checkbox* non ha rispettato questo principio.

- Infine, secondo la Cassazione anche l'aver indicato come finalità l'invio di messaggi pubblicitari non ben definiti potrebbe costituire un'azione non sufficientemente precisa: di fatto, per far sì che il consenso possa essere riferito ad un trattamento specifico, è necessario che vengano precisati i settori merceologici o i servizi a cui si riferiscono i messaggi promozionali in questione. Questo era già stato sottolineato dal Garante nelle Linee Guida contro lo spam che richiedono appunto al titolare di includere nell'informativa almeno la categoria merceologica dei terzi a cui vengono trasferiti i dati personali per compiere le loro attività promozionali.

In conclusione, la Corte di Cassazione ha evidenziato definitivamente che il gestore di un sito Internet che offre un servizio fungibile di cui l'utente può fare a meno senza incorrere in un gravoso sacrificio, può subordinare la fornitura del servizio stesso al trattamento dei dati personali per scopi di tipo commerciale, a condizione che il consenso sia singolarmente e inequivocabilmente prestato per tutte le diverse finalità; questo quindi comporta l'obbligo di specificare i settori merceologici o i servizi cui saranno riferititi le comunicazioni promozionali.

La Suprema Corte inoltre sottolinea che se si avvalorasse la tesi del Garante della privacy, secondo cui il gestore del sito informativo non potrebbe condizionare l'erogazione del servizio al consenso al trattamento di dati personali per fini commerciali, si finirebbe per *«delineare una sorta di obbligo tout court, per il gestore del portale, di offrire comunque le proprie prestazioni, a prescindere dalla prestazione del consenso al trattamento dei dati personali da parte dell'utente e, in buona sostanza, per obbligare così il gestore del portale a rinunciare al tornaconto economico dell'operazione che egli compie, proveniente dall'attività pubblicitaria realizzata tramite l'impiego dei dati personali acquisiti».* La Corte precisa, inoltre, che «*l'ordinamento non vieta lo scambio di dati*

personali, ma esige tuttavia che tale scambio sia frutto di un consenso pieno ed in nessun modo coartato»[288].

Quindi riassumendo:

- Il consenso al trattamento di dati personali non necessari ad un servizio fungibile e rinunciabile di cui si domanda la prestazione non è necessariamente condizionato, nonostante il consenso sia una condizione per poter beneficiare del servizio stesso;
- Lo scambio di dati personali come "corrispettivo" per il servizio, fungibile e rinunciabile, è ammissibile, a condizione che questo derivi da un *"consenso pieno e in nessun modo coartato".*

Le conclusioni della Corte sembrano dunque in contrasto con le indicazioni fornite dalle linee guida nelle quali è stabilito che la richiesta di un consenso al trattamento di dati personali non necessari al servizio domandato, come condizione necessaria per l'erogazione del servizio stesso, è segno di un consenso non libero, anche nel caso di un servizio fungibile e rinunciabile che potrebbe quindi essere richiesto altrove.

L'apparente contrasto tre le due posizioni ha dato vita ad una situazione di incertezza tra gli addetti ai lavori che può però essere superata tramite una lettura coordinata di entrambe le parti.

L'articolo 7, paragrafo 4 del Regolamento Europeo stabilisce che nel giudicare la libertà del consenso, si deve tenere in massima considerazione l'eventualità che l'esecuzione di un contratto o la prestazione di un servizio siano condizionate alla prestazione del consenso all'utilizzo di dati personali non necessari.

Il legislatore europeo ha perciò sì introdotto un criterio per valutare la libertà del consenso, ma questo criterio non è di per sé decisivo, anche se ha una rilevanza importante nel processo valutativo; di fatto la norma non individua una

[288] *Ivi*, p.10

presunzione assoluta ma rimanda all'operatore la valutazione della fattispecie in concreto.

La valutazione in concreto richiede quindi che chi interpreta il caso deve bilanciare tutti gli elementi della fattispecie, senza considerazioni a priori e astratte; di conseguenza, la previsione di una prestazione subordinata al consenso al trattamento di dati non essenziali per il servizio o trattati per finalità diverse, anche se deve comunque essere presa in considerazione, non è per forza decisiva per ritenere intaccata la libertà del consenso.

Ragion per cui la Suprema Corte determina un criterio per stabilire in quali casi il processo volitivo dell'interessato sia di fatto condizionato: questo si verifica nei casi in cui il servizio di interesse sia allo stesso tempo infungibile e irrinunciabile. I giudici della Corte non specificano cosa si intende per "fungibilità" e "irrinunciabilità", né se queste condizioni debbano sussistere congiuntamente o no, ma dall'esame della sentenza in questione si deduce che tali non sono i servizi che possono essere usufruiti per altre vie, senza dover incorrere in un gravoso sacrificio.

Dunque, analizzando il ragionamento della Cassazione, è giusto ritenere che la fungibilità non va intesa in senso letterale e oggettivo come insostituibilità assoluta del servizio con un altro, ma va indicata tenendo presente il carattere rinunciabile o meno del servizio che può essere sostituito con un altro senza incorrere in un gravoso sacrificio da parte dell'interessato.

Dunque, la valutazione in merito alla libertà del consenso deve prendere in considerazione, congiuntamente, i caratteri di infungibilità e irrinunciabilità della prestazione, accedendo ad un'interpretazione soggettiva delle stesse.

Quindi, un servizio soggettivamente infungibile e irrinunciabile sarebbe in grado di condizionare il processo volitivo dell'interessato, condizionandone di conseguenza il consenso.

In tali condizioni il consenso prestato per l'erogazione del servizio concernente dati non necessari, non può essere ritenuto libero poiché diventa uno strumento di pressione che lede l'autodeterminazione dell'interessato.

Quindi, il principio stabilito dalla Corte di Cassazione sembra essere in contrasto con il considerando del GDPR[289] e con le linee guida del WP29 che, come già detto, ritengono un consenso non liberamente prestato quello al trattamento di dati non necessari al servizio come condizione per l'erogazione di tale servizio.

Per quanto riguarda il considerando 43 però c'è da precisare che i considerando delle norme europee non sono vincolanti, ma sono solo un ausilio per l'interpretazione delle norme cui si riferiscono; per questo motivo un considerando non può differire dal contenuto della norma o richiamare elementi che la norma non contempla.

Nella fattispecie in esame, l'art. 7, par. 4, indica di tenere nella massima considerazione i casi come quello in esame, senza però insinuare alcuna presunzione legale; dunque, il considerando 43 va interpretato in conformità con la disposizione regolamentare e deve essere inteso nel senso che specifiche circostanze costituiscono un indicatore di assenza di libertà che però deve comunque essere vagliata nel caso concreto. Per lo stesso motivo, le linee guida del WP29, e ora dell'European Data Board, non possono entrare in contrasto con i principi dettati dal GDPR, introducendo una presunzione che il Regolamento non contempla, ma possono solo esplicitarne il contenuto semplificando la comprensione e l'applicazione, anche tramite l'indicazione di indici che rivelano un possibile condizionamento del consenso.

In conclusione, si può notare come il contrasto tra i principi stabiliti dalla Corte di Cassazione e quelli delle linee guida è in realtà solo apparente; entrambi, infatti,

[289] Considerando 43 del Regolamento (UE) 2016/679, *«Per assicurare la libertà di espressione del consenso, è opportuno che il consenso non costituisca un valido presupposto per il trattamento dei dati personali in un caso specifico, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento»*

sono volti a garantire la piena libertà del consenso, in assenza di effettivi e concreti condizionamenti.

Nel valutare questo, non vanno comunque condannati quei fornitori di servizi che offrono prestazioni gratuite a fronte del consenso al trattamento dei dati personali per finalità commerciali, anche tramite il trasferimento dati a terzi; soggetti per i quali il trattamento dei dati rappresenta in sostanza un corrispettivo per il servizio offerto; di fatto l'ordinamento non vieta l'utilizzo di dati come corrispettivo per una determinata prestazione e anzi sono molti diffusi casi in qui imprese che offrono diversi servizi gratuiti in cambio del consenso dell'interessato al trattamento dei suoi dati personali per diverse finalità.

Molti dei servizi offerti sono comunque reperibili da altri fornitori; quindi, l'interessato è comunque libero di decidere se prestare il suo consenso e usufruire gratuitamente delle prestazioni offerte oppure se rivolgersi altrove anche pagando un corrispettivo economico. In questo modo non ci riscontra alcun condizionamento, dato che nessuno può pretendere l'erogazione gratuita di un servizio e comunque la rinuncia a tale servizio non costituisce un "gravoso sacrificio" idonea a condizionare il consenso dell'interessato.

Ovviamente, l'interessato deve essere a conoscenza di tutte le finalità e le modalità del trattamento per valutare se prestare il consenso o meno. Quindi ci è una sorta di gap informativo dato che il titolare del trattamento si trova in una posizione di forza rispetto al soggetto interessato; è per questo motivo che il GDPR impone una serie di obblighi informativi[290] per rendere consapevo e informato l'interessato circa le conseguenze del suo consenso.

3.4 Due tesi contrapposte

La disciplina non sempre sembra fornire indicazioni univoche riguardo a una delle più controversie questioni sollecitate dall'ordinamento europeo, ovvero la natura del consenso dell'interessato. Vi sono due tesi distinte:

[290] Art. 13 e 14 del Regolamento (UE) 2016/679

a) la tesi della natura non negoziale del consenso: sostiene che il consenso non sia altro che un atto giuridico in senso stretto con valore autorizzatorio[291]. Il consenso avrebbe una funzione autorizzatoria rispetto al dovere generale di astensione nella sfera della riservatezza, uno strumento quindi che intende tutelare la persona dall'invasione altrui nella propria sfera personale.

   Questa tesi si fonda sul fatto che il diritto alla riservatezza del dato personale rappresenta un diritto indisponibile, dato che costituisce un diritto della personalità, rispetto al quale il consenso è un'autorizzazione scriminante di un'attività che altrimenti sarebbe illecita.[292]

   Secondo questa prospettiva, il consenso è interpretato come uno strumento di "autodeterminazione", come un'espressione della personalità umana e di conseguenza non può essere valutato in termini patrimoniali. Di fatto è la persona che presta il consenso che sceglie se e cosa mettere a disposizione di terzi, di quali informazioni della propria identità personale mettere a conoscenza. Dunque, gli effetti delle sue azioni non possono essere qualificabili in termini di arricchimento dei due soggetti che prendono parte al processo di trattamento[293]. Con queste basi quindi il consenso non prende parte ad un fenomeno di negoziabilità dei dati, ma piuttosto rappresenta un'autorizzazione della persona all'adozione di comportamenti e azioni che coinvolgono la propria identità personale[294].

---

[291] PARENZO, *Dati personali come "moneta". Note a margine della sentenza TAR Lazio n.260/2020*, in *Juscivile*, (2020)5, p.1374

[292] D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv*., 1998, pp. 339 ss; S. PATTI, *Il consenso dell'interessato al trattamento dei dati personali*, in *Riv. dir. civ*., 1999, pp. 466 s

[293] Vale a dire l'interessato, il soggetto a cui i dati si riferiscono e il soggetto che tratta i dati, il titolare.

[294] V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, *I dati personali nel diritto europeo*, G. Giappichelli Editore, Torino, 2019, p.37. *«Si pensi, ad esempio, al consenso prestato al trattamento dei propri dati personali al fine di poter accedere alle cure mediche. In tal caso le informazioni (non solo quelle più strettamente e direttamente attinenti alla salute, quali la presenza di patologie, gruppo sanguigno, stile di vita, ecc., ma altresì quelle più generiche, quali età, status genitoriale, tipologia di lavoro, preferenze alimentari, ecc.) sono trattate non per ricavare un'utilità economica ma per consentire di riconoscere la presenza di eventuali patologie e disporre le cure più adeguate».*

Come detto nel capitolo precedente, il Regolamento Generale sulla Protezione dei Dati stabilisce che i dati personali sono trattati in modo lecito solo se ogni trattamento è conforme a uno dei legittimi presupposi per il trattamento dei dati, indicati dall'art. 6 per i dati personali "normali" e all'art. 9 per le categorie particolari di dati, vale a dire i dati sensibili.

Dunque, il consenso prestato dall'interessato nel Regolamento ha una posizione diversa rispetto a quella che detiene nel Codice Privacy, nel quale il consenso rappresentava la condizione di liceità del trattamento, sufficiente per i dati comuni oppure seguita da un'autorizzazione del Garante per la protezione dei dati personali di natura sensibile.

Il Regolamento ha dunque eguagliato il consenso dell'interessato ad ogni altro fondamento legittimo indicato dalla legge, stabilendo che «s*i tratta di condizioni tra loro equipollenti e pari ordinate, essendo sufficiente che ve ne sia almeno una per poter ritenere superato il primo stadio del processo valutativo in ordine alla liceità del trattamento»*[295].

Nonostante ciò, però, il consenso rappresenta tuttora un presupposto di liceità del trattamento di grande importanza. Come abbiamo visto, il tema riguardante la sua natura è stato ampiamente dibattuto nella dottrina.

Un filone dottrinale sostenitore della tesi che sostiene la natura non negoziale del consenso, inoltre, tende a fare ricorso alla nozione di consenso con valore scriminante[296]; per cui la manifestazione del consenso rappresenterebbe l'atto attraverso il quale l'interessato rimuove l'antigiuridicità del trattamento, rendendo di conseguenza il trattamento un'attività lecita che altrimenti sarebbe vietata.

Questo e altri filoni dottrinali però partivano da un presupposto che oggi è stato superato, di fatto essi reputano che il trattamento di dati personali sia

[295] G. FINOCCHIARO, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017, p.126.
[296] Modello riconducibili all'articolo 50 del Codice Penali nell'ordinamento giuridico italiano.

un'attività intrinsecamente illecita, anche se dal GDPR emerge in maniera chiara ed evidente la configurabilità di un vero e proprio diritto al trattamento dei dati personali di un soggetto spettante al titolare del trattamento, sempre che le attività del trattamento siano permesse ai sensi dell'articolo 5 del Regolamento europeo.

La visione che vede dell'illeceità nel trattamento se non vi è il consenso dell'interessato, non tiene presente dell'esistenza di ulteriori presupposti che conferiscono liceità al trattamento e che lo rendono conforme al diritto.

b) tesi opposta è quella della natura negoziale del consenso: i sostenitori di questa tesi infatti ritengono il consenso una manifestazione negoziale di volontà. Essi valutano le informazioni oggetto si trattamento come protagonista di un processo di reificazione, alla fine del quale assumono le fattezze di beni giuridici, rispetto ai quali il consenso assumerebbe funzione dispositiva[297]. Secondo tale tesi, in questo modo si valorizzerebbe l'autodeterminazione individuale, sottostante ad esempio all'atto di accesso al web che parrebbe *«tradursi in un comportamento concludente attraverso il quale l'interessato manifesta la propria disponibilità affinché altri raccolgano ed elaborino le proprie informazioni"*[298]. Questa tesi risulta molto criticata in quanto attribuisce un valore patrimoniale al consenso.
   Vi è chi sostiene che il consenso sia un atto di disposizione negoziale; in tal caso si vede nel consenso un atto di autonomia negoziale con cui si dispone dei dati personali dell'interessato, senza eseguire alcun atto di tipo traslativo; si ammetterebbero quindi altri nella propria sfera personale, instaurando un rapporto di durata, per cui il consenso non si esplicherebbe

[297] C. ANGIOLINI, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, G. Giappichelli Editore, Torino, 2020 p.122
[298] V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, *I dati personali nel diritto europeo*, G. Giappichelli Editore, Torino, 2019, p. 255.

in un effetto una tantum, definitivo ed irrevocabile ma piuttosto porterebbe all'instaurazione di un rapporto continuativo, che si crea inter partes[299].

L'inquadramento come negozio quindi di rinvenirvi un atto che *«già per il suo significato socio-giuridico, veicola qualcosa di ulteriore, non immanente all'atto stesso…Ora, il consenso al trattamento, nel permettere l'utilizzo di questo bene[300], non è volto alla semplice rimozione di un limite e, soprattutto, non corrisponde a un'autorizzazione fattuale cui giuridicamente segue la disattivazione di una certa disciplina (quella che proibisce il trattamento laddove difetti una base); piuttosto il consenso al trattamento mira alla creazione di una situazione giuridica in capo a un altro soggetto. E un simile effetto non è imminente alla fattualità della dichiarazione o del comportamento; esso, al contrario, deriva dall'attivazione di una convenzione socio-giuridica direttamente volta ad approvarlo. Di conseguenza, nell'atto di consenso deve rinvenirsi un negozio»[301].*

La qualificazione del consenso come negozio impone di rinvenirvi un atto di disposizione: un negozio unilaterale volto al trasferimento costitutivo di un diritto; tale diritto a sua volta ha ad oggetto un bene personale; il diritto però *«sfugge alla distinzione tra personalità e patrimonialità, finendo per innestarsi nella specifica libertà o nello specifico diritto cui di volta in volta è più legato (ora alla libertà di espressione, ora alla potestà pubblica e così via). Solo nel caso in cui tale libertà non è altro che quella economica, come nei casi in cui il trattamento dei dati serve per finalità di marketing o simili, potrebbe ipotizzarsi che il diritto assuma dal lato del titolare del trattamento un valore patrimoniale e, di riflesso, che così connoti (almeno in parte) pure il suo soggetto: ciò che, conseguentemente, imporrebbe di*

[299] G. OPPO, *Sul consenso dell'interessato*, in CUFFARO, RICCIUTO, ZENO-ZENCOVICH (a cura di), *Trattamento dei dati e tutela della persona*, Giuffrè, 1999.
[300] Col il termine "bene" ci si riferisce al dato personale che l'interessato cede con il consenso.
[301] *Anuario 2021, Osservatorio Giuridico sulla Innovazione Digitale*, (a cura di) S. ORLANDO, G. CAPALDO, Università La Sapienza, 2021, cit, p.137

rinvenire nel negozio l'atto di disposizione di un bene (anche) patrimoniale»[302]*.*

Chi sostiene questa seconda tesi insiste sul concetto di "reificazione" dei dati personali, che diventano "beni" suscettibili di autonoma considerazione di tipo economico e dunque in quanto tali, destinati a circolare sul mercato, senza che tutto ciò infierisca col carattere indisponibile riconosciuto ai diritti della personalità.

Sono diffuse perciò due diverse visioni: da una parte i sostenitori della natura autorizzativa del consenso, qualificato dunque come atto non negoziale, e come elemento facente parte di una fattispecie legale i cui effetti vengono meno solo se l'interessato manca della volontà di manifestare l'atto di consenso sulla base dei presupposi specifici richiesti dalla legge, senza che alcuna rilevanza «possa essere attribuita ai motivi che hanno indotto l'interessato a prestare il consenso, tra i quali può ipotizzarsi quello di ottenere un compenso»[303]. Dall'altra ci sono invece i sostenitori della natura negoziale del consenso, che si basano sulla natura dei dati come beni cedibili, trasferibili e scambiabili, oppure sulla nozione di appartenenza, in quanto sarebbero "elementi della sfera del soggetto" che "gli appartengono a questo titolo, senza che sia necessario stabilire se il titolo sia "proprietario" o meno". Proprio in quest'ultima prospettiva si posizionano coloro hanno sostenuto che il consenso può essere considerato a tutti gli effetti come «consenso negoziale, manifestazione di volontà in ordine alla circolazione dei dati»[304] dato la diffusione dell'operazione economica per cui l'utente, nell'aderire ad un servizio, acconsente al fatto che i suoi dati personali siano utilizzati dal

[302] *Ivi*, p.139
[303] Per l'Autorità Garante della Privacy il consenso è libero «solo se si presenta come manifestazione dell'autodeterminazione informativa, e dunque al riparo da qualsiasi pressione» (Provvedimento del 28 maggio 1997, Istituti di credito Criteri generali in materia di informativa e richiesta del consenso dell'interessato, in *Corr. Giur*., 1997, pp.915-917); pressione che invece potrebbe esservi nel caso in cui la prestazione del consenso venga subordinata alla conclusione del contratto.
[304] RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Dir. inf. inform*., 2018, cit, p.722

fornitore del servizio per scopi estranei alla mera fornitura del servizio stesso, dunque scopi generalmente di tipo commerciale, ceduti a soggetti terzi per fini pubblicitari. Dunque, la prestazione di rilascio del consenso al trattamento coincide con il momento in cui l'utente-interessato aderisce al contratto per la prestazione del servizio, come se il consenso divenga "merce di scambio" per la fornitura del servizio[305].

È inequivocabile che la revoca del consenso rappresenti una propensione per la prima tesi e mal si concilia con la qualificazione negoziale che vede nel consenso dell'interessato la cessione del dato al titolare, dato che il vincolo una volta sorto sarebbe irritrattabile dalle parti.

D'altra parte, però vi è un movimento in atto che chiede un'apertura all'autonomia privata anche per i diritti della personalità, tralasciando quindi quel tradizionale carattere dell'indisponibilità, veicolando in questo modo forme di patrimonializzazione del diritto della persona e di sfruttamento ad opera del titolare, conciliabili quindi con la tesi che sostiene la natura negoziale del consenso.

Ricordando le riflessioni di Stefano Rodotà il quale osservava che *«dobbiamo lavorare molto nella dimensione negoziale, non ho nessun dubbio. Negoziale vuol dire per esempio: il consenso può essere oneroso, può essere condizionato, può essere a termine? Io come risposta generale direi di sì (...) Il controllo non viene perduto, i motivi legittimi per i quali si può impedire la comunicazione di dati pur legittimamente raccolti, pertinenti o assentiti in tutto o in parte, dimostrano quindi che c'è una scelta dell'interessato che definisce l'area della protezione»*[306].

---

[305] C. IRTI, Consenso "negoziato" e circolazione dei dati personali, Giappichelli Editore, Torino, p.2021, p.76. Si pensi ad esempio ai social network in cui la maggior parte delle volte non è possibile distinguere tra l'atto di accettazione dei termini d'uso de servizio (condizioni generali di contratto) e la prestazione del consenso al trattamento del dato per le finalità indicate dal titolare. Al momento della registrazione l'utente viene informato che cliccando sul "pulsante elettronico" che conclude l'iscrizione egli dichiara di accettare i "termini d'uso" del servizio, dunque le condizioni d'uso dei social network e, contemporaneamente, manifesta il suo consenso al trattamento dei dati personali.

[306] S. RODOTÀ, Conclusioni, in Trattamento dei dati personali e tutela della persona, (a cura) di V. CUFFARO-V. RICCIUTO-V. ZENO ZENCOVICH, Giuffrè, 1999, cit., 308, c

Dalle sue parole sembra quindi che anche se il consenso rivestisse un carattere negoziale, non costituirebbe necessariamente l'adesione ad una visione improntata alla piena disponibilità di dati personali, ma avrebbe il fine di valorizzare quel controllo dell'atto di autonomia privata in funzione della salvaguardia dei valori della persona che vengono coinvolti.

Le considerazioni svolte assumono particolare importanza proprio per lo sviluppo della data economy, nella quale l'asset cardinale è proprio la raccolta e lo sfruttamento dei dati personali degli utenti da parte di operatori commerciali; mano amano che la circolazione di dati personali si avvicina al rapporto contrattuale di fornitura di beni e servizi digitali, sembra inevitabile un percorso di intersezione tra la legge della tutela dei dati personali e quella del mercato e del contratto. Dunque l'utente si trova ad esprimere un consenso sia in veste di interessato al trattamento dei propri dati personali, sia come consumatore che vuole concludere il contratto di fornitura di un certo contenuto o servizio digitale[307].

Le due fattispecie però hanno diversa natura giuridica: il consenso richiesto per scopi commerciali è espressione del principio di autonomia contrattuale dei privati, e perciò deve essere fornito da un soggetto che abbia la capacità di intendere e di volere e non deve essere viziato da errore, violenza o dolo, da pericolo o da bisogno; quindi se sussistono perturbazioni che si trovano al di sotto di questa soglia di rilevanza giuridica predisposta dal codice civile, si tratta di una volontà che sussiste validamente. La formazione del consenso negoziale è sottoposta a regole definite dall'ordinamento, che descrivono il se, il come e il quando del perfezionamento dell'accordo tra le parti; perciò, il consenso negoziale giunge alla sua completezza solo nell'accordo tra le parti, nell'ottica della mediazione tra le volontà e tra gli interessi opposti di cui il contratto è la massima espressione.

[307]Per questo assume particolare importanza il principio del consenso separato. G. MARINO, *Internet e tutela dei dati personali: il consenso ai cookie,* in *Jus Civile,* 2020,2*,* p. 416

Diversa è la figura del consenso al trattamento dei dati personali, espressione del potere di autodeterminazione e della libertà di dominare gli aspetti personali dell'individuo a cui viene riconosciuto un diritto fondamentale. L'individuo è in questo caso protagonista e unico autore delle sue scelte. Esso deve essere libero, specifico, inequivocabile ed informato; dunque si tratta di un consenso caratterizzato da una tutela rafforzata rispetto al diritto comune[308].

A fronte della difficoltà e della diversità delle tesi proposte, è stato suggerito di tralasciare del tutto questa "ansia catalogatoria"; la soluzione proposta è quella di intervenire sotto il profilo metodologico: «*alla domanda se sia possibile ricostruire un "sistema" della privacy e del consenso al trattamento dei dati, la risposta è nel senso che il sistema, se c'è, è instabile per definizione e non presenta i caratteri tradizionali della compiutezza e della necessaria correlazione di ciascun elemento […]. Se proprio si dovesse scegliere un nomen iuris, il consenso in questione potrebbe essere definito elemento di una fattispecie legale a contenuto e disciplina composita: ergo, non "il" ma "i" consensi. Bisogna rassegnarsi all'idea che siamo di fronte a "materiali" nuovi, né soltanto italiani, né esclusivamente stranieri, bensì europei e sovranazionali*»[309].

[308] Si veda sul punto Cass. civ., Sez. I, 2 luglio 2018, n. 17278. In questo caso la Suprema Corte ribadisce la diversità di disciplina tra le due diverse figure, non ritenendo di sovrapporre il consenso finalizzato al trattamento dei dati personali a quello richiesto a fini negoziali.
[309] S. SICA, *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in *Riv. Dir. Civ*., 2001, p.90

CAPITOLO QUARTO - IL CONSENSO AL TRATTAMENTO DEI DATI PERSONALI E I COOKIE: ESPERIENZA DELLA CORTE DI GIUSTIZIA DELL'UE

4.1 I *cookie*: definizione e suddivisione

Come sostenuto nei capitoli precedenti, una ricca fonte di *big data* sono sicuramente le piattaforme digitali, come motori di ricerca o *social network*, basate su un modello che prevede la fornitura di un servizio o di un contenuto digitale da parte di un *provider* all'utente, che non deve ricambiare con alcun corrispettivo in denaro ma fornisce i propri dati personali che saranno poi oggetto di trattamento da parte del *provider* stesso. I dati personali dell'utente solitamente vengono trasmessi nel momento della conclusione del contratto, pertanto nella fase attuativa del rapporto[310].

Inoltre, vi è un altro canale di accesso e raccolta *online* di dati personali, che è operativo prima ancora e a prescindere dalla conclusione o meno del contratto di fornitura del contenuto o servizio digitale. Si tratta di strumenti che, grazie allo sviluppo tecnologico, permettono ai gestori dei siti internet di ottenere informazioni di tipo personale da attività elementari degli utenti, come l'accesso e la navigazione in rete[311]. Queste attività sono percepite come rapide ed impersonali da parte degli utenti ma in verità sono un potente veicolo di

---

310 Un esempio di tale rapporto è fornito dal considerando 24 della Direttiva UE 2019/770: *«ad esempio, la presente direttiva dovrebbe applicarsi nel caso in cui il nome e l'indirizzo email forniti da un consumatore al momento della creazione di un account sui social media siano utilizzati per scopi diversi dalla mera fornitura di contenuti digitali o servizi digitali o non conformi agli obblighi di legge».*

311 G. MARINO, *Internet e tutela dei dati personali: il consenso ai cookie,* in *Jus Civile,* 2020,2*,* pp.398 ss.

trasmissione di dati personali, grazie all'utilizzo dei *cookie*[312], diffusi in modo capillare nel *web*[313].

Il GDPR stabilisce che *«Le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, marcatori temporanei (cookies) o identificativi di altro tipo, quali i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle*[314]*».*

Essi sono dei *file* di testo che il fornitore del sito installa nel dispositivo[315] dell'utente che ha navigato sul suo sito e al quale potrà accedere nuovamente durante un'altra navigazione sul medesimo sito da parte dello stesso utente. È un messaggio trasmesso da un *web server* ad un *browser* e viene memorizzato sull'*hard disk* dell'utente e poi trasmesso al *server* ogni qualvolta che il *browser* richiederà nuovamente una pagina allo stesso *server*[316]. Sono definiti dei "marcatori temporanei" dal GDPR[317] e consentono di raccogliere dati e parametri di ricerca riguardanti l'interessato[318].

---

312 La paternità viene attribuita ad un ingegnere di Nescape, Lou Montulli. Li creò nel 1994 originariamente solo per riconoscere l'indirizzo IP del computer dell'internauta nel momento in cui riempiva un cestino di acquisti, navigando tra le varie pagine di un sito. L'uso invece nel campo pubblicitario da parte delle grandi piattaforme di diffuse verso la fine degli anni '90 e inizio degli anni 2000.

313 Gli utenti forniscono i propri dati agli operatori per poter fruire in modo gratuito di prodotti o servizi digitali o per condividere contenuti come foto, video, messaggi (come succede nei *social network*) o li rilasciano in maniera più o meno consapevole nel *web* tramite i *cookie*. Annuario 2021, Osservatorio Giuridico sulla Innovazione Digitale, (a cura di) S. ORLANDO, G. CAPALDO, Università La Sapienza, 2021, p.206

314 Considerando 30 del Regolamento UE 2016/679 (GDPR)

315 Ci si riferisce per esempio a un computer, un tablet, uno smartphone, e ad ogni altro dispositivo capace di archiviare informazioni. Ci si riferisce anche ai cd. Dispositivi IoT (*Internet of Things*), progettati per connettersi alla rete. Garante per la protezione dei dati personali, *Linee guida cookie e altri strumenti di tracciamento*, n. 231, 10 giugno 2021

316 Cookie, letteralmente "biscottino", è un insieme di informazioni testuali, che viene memorizzato in uno specifico file come cookie.txt sul disco fisso dell'utente. A. R. POPOLI, I *cookies e il commercio elettronico: indagine sulla effettiva conoscenza delle problematiche connesse alla privacy,* in *Bocconi Legal Papers*, online su *http://bocconilegalpapers.org*

317 Considerando 30 del Regolamento UE 2016/679 (GDPR)

318 A. LORIO, L. AMBROSI, *E-commerce. Risvolti e implicazioni giuridiche e fiscali,* in *Il Sole 24 ore,* luglio 2020, 3, p.46

Vengono distinte due grandi categorie, i *cookie* "tecnici" e i *cookie* "di profilazione", in base ai soggetti che se ne avvalgono e dunque alle finalità di utilizzo connesse.

I *cookie* tecnici sono installati direttamente dal titolare o dal gestore del sito e hanno esclusivamente funzione strumentale, vale a dire quella di migliorare la navigazione *online*. Hanno il solo scopo di "*effettuare la trasmissione di una comunicazione su una reta di comunicazione elettronica*".[319]

Questi poi possono essere suddivisi in altre tre micro-categorie: *cookie* di navigazione o di sessione che permettono la normale navigazione e fruizione di un sito *web*[320]; i *cookie* di funzionalità che consentono all'utente di poter navigare su un sito applicando una serie di criteri selezionati, come la lingua, per migliorare il servizio del sito; infine i *cookie analytics* che sono assimilabili ai *cookie* tecnici se vengono impiegati direttamente dal gestore per raccogliere informazioni sul numero degli utenti che visualizzano il sito e sul modo in cui ci navigano[321].

D'altra parte, i *cookie* di profilazione possono essere installati dal gestore del sito oppure da soggetti terzi, cioè grandi società tecnologiche; essi hanno lo scopo di verificare e rielaborare tramite l'utilizzo di algoritmi di calcolo, le abitudini, gli interessi e le ricerche operate dall'utente, con l'intento di poter inviare messaggi pubblicitari coerenti con le preferenze dell'utente nel corso della navigazione[322]. Hanno quindi un grado di invasività molto alto[323].

---

319 Ivi, p.47

320 I *cookie* di navigazione permettono ad esempio di realizzare un acquisto *online* o di autenticarsi per accedere ad aree riservate.

321 Provvedimento n. 229 dell'8 maggio 2014 del Garante per la protezione dei dati personali. *Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie*. Secondo il Garante della Privacy italiano è bene fare un'ulteriore precisazione per i *cookie analytics*, assimilabili ai *cookie* tecnici solo se utilizzati per ottimizzare il sito direttamente dal titolare del sito stesso, che potrà raccogliere informazioni in forma aggregata sul numero degli utenti e su come visitano il sito.

322 Nell'art. 4 del GDPR la "profilazione" è intesa come *«qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati 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».*

323 A. LORIO, L. AMBROSI, *E-commerce. Risvolti e implicazioni giuridiche e fiscali,* in *Il Sole 24 ore,* luglio 2020, 3, p.47. Inoltre, vi è un'altra categoria comprendente i *cookie* di terze parti, che vedono l'installazione di cookie appartenenti a terzi soggetti che vengono utilizzati

L'utente può ricevere sul suo dispositivo anche *cookie* di siti o di *web server* diversi, chiamati cookie di "terze parti"; questo si verifica quando nel sito *web* in cui si sta navigando sono presenti immagini, mappe, suoni o determinati *link* a pagine web di altri domini che si risiedono su altri server rispetto a quello in cui si trova la pagina visitata[324].

Grazie all'archiviazione e alla successiva possibilità di utilizzazione dei *cookie* sui dispositivi degli utenti, i *provider* possono accedere a informazioni personali del singolo soggetto in modo da creare un profilo che fingerà da *target* per le operazioni di *marketing* comportamentale e diretto e promozionale di prodotti e servizi[325].

Ci si trova in questo caso quindi in una prima fase di approccio tra l'utente e il gestore del sito in cui un *browser* consente l'accesso e la successiva navigazione *online.* Queste possono sembrare operazioni molto distanti dalla conclusione di un contratto di fornitura di beni e servizi digitali ma in realtà ne rappresentano un presupposto fondamentale[326].

Tale situazione in cui il trattamento di dati personali avviene tramite l'uso di *cookie* di profilazione, è un'operazione distinta da quella del trattamento situato nell'ambito di un'operazione contrattuale che prevede lo scambio tra dati personali e fornitura di contenuti e servizi digitali. Questa traiettoria sembra essere seguita anche dal legislatore europeo che nei considerando della DCSD scrive che «*la presente direttiva non dovrebbe applicarsi ai servizi di accesso a Internet*[327]*»,* e nemmeno nelle situazioni in cui l'operatore economico raccoglie solo i metadati, vale a dire come informazioni sul dispositivo dell'utente o la cronologia internet[328].

---

anch'essi per scopi di profilazione e tracciamento dell'utente. Un esempio di questa categoria sono i *social cookie*, vale a dire quelli guidati tramite i *plugin* dei *social network*.

[324] F. SALMI, F. SAPORITI, *GDPR e sanzioni. Guida ai principali provvedimenti dei garanti europei: come evitare le contestazioni*, Key Editore, Milano, 2021, p. 54

[325] G. MARINO, *Internet e tutela dei dati personali: il consenso ai cookie,* in *Jus Civile,* 2020,2*,* pp. 401-402

[326] *Ibidem*

[327] Cons. 19 della Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio, del 20 maggio 2019

[328] Cons. 25 della Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio, del 20 maggio 2019. Nel medesimo considerando la Direttiva non esclude uno spazio di

Dunque, nel mondo virtuale la sola navigazione e l'utilizzo delle funzionalità di un sito non comporta la conclusione di un contratto tra *provider* e utente in quanto non sono presenti i presupposti minimi di un accordo[329]; eppure grazie ai *cookie* di profilazione l'utente potrebbe già aver permesso l'accesso a informazioni personali da parte del gestore del sito che potrà sfruttare per fini commerciali.
Si verifica quindi una sorta di violazione della sfera privata dell'individuo, causata da *cookie* che permettono l'ingerenza sui dispositivi dell'utente e la caratterizzazione della sua identità digitale tramite algoritmi di profilazione, che verrà poi sfruttata per scopi economici.
Tali attività rappresentano una prima relazione tra i soggetti del *web*, che non può essere configurata come un contratto, ma non può nemmeno non avere alcuna rilevanza dal punto di vista giuridico, dato che sono in gioco i dati personali dell'individuo[330].
Vediamo quindi prima di tutto come si sviluppa il quadro normativo di riferimento in materia di *cookie*, in cui un ruolo centrale è ricoperto dal consenso prestato dal soggetto interessato, e successivamente si farà riferimento alla declinazione assunta dai requisiti fondamentali e dalle modalità di manifestazione del consenso quando il trattamento dei dati personali è eseguito *online* tramite l'utilizzo di strumenti tecnologici come i *cookie*.

---

discrezionalità del legislatore nazionale, in quanto nei singoli ordinamenti municipali le fattispecie descritte possono essere qualificate come contratti di prestazione di servizi ai quali estendere le previsioni della direttiva stessa.

329 G. MARINO, *Internet e tutela dei dati personali: il consenso ai cookie,* in *Jus Civile,* 2020,2*,* p. 403. *«Invero, come nel mondo reale non si sosterrebbe che il passeggiare tra gli scaffali di una libreria, il consultare un volume o chiedere informazioni al libraio implichino la conclusione di un contratto tra il negoziante e il (potenziale) cliente, così nel mondo virtuale la semplice navigazione e utilizzazione delle funzionalità di un sito internet non postula, in quanto tale, la conclusione di un contratto tra provider e utente».*

330 È degno di nota il considerando 24 della Direttiva 2002/58 secondo cui *«le apparecchiature terminali degli utenti di reti di comunicazione elettronica e qualsiasi informazione archiviata in tali apparecchiature fanno parte della sfera privata dell'utente, che deve essere tutelata ai sensi della convenzione europea per la protezione dei diritti dell'uomo e delle libertà fondamentali».*

Con entrambe queste situazioni si è confrontata la Corte di Giustizia dell'Unione Europea, attraverso un'importate decisione che rivela l'attualità della questione[331].

Per l'utilizzo di *cookie* e di altri identificatori di tipo tecnico, il titolare del trattamento dovrà solamente fornire una specifica informativa, senza avere l'obbligo quindi di richiedere il consenso dell'interessato; diversamente i *cookie* e gli altri strumenti di tracciamento che abbiano scopi diversi da quelli tecnici, potranno essere utilizzati solo previa acquisizione del consenso informato dell'utente[332].

4.2 Il quadro normativo europeo in materia di cookie

Il quadro normativo, non solo relativo ai *cookie*, ma a tutte le tecnologie che permettono la memorizzazione e l'accesso a informazioni di tipo personale archiviate nel dispositivo dell'utente, è in continuo mutamento, a causa anche delle innovazioni tecnologiche.

Un posto rilevante è occupato dalla direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche, che è stata oggetto di importanti modifiche da parte della direttiva 2009/136/CE; le attività di accesso e di navigazione *online, dunque,* rientrano nella categoria di "servizio di comunicazione elettronica".

La direttiva, perciò, regola il trattamento di dati personali estrapolati dallo svolgimento di queste semplici operazioni con lo scopo di garantire la riservatezza delle comunicazioni di tipo elettronico[333].

---

331 Corte di Giustizia dell'Unione Europea, sentenza della corte (Grande sezione),1° ottobre 2019, causa C-673/17, disponibile online sul sito della CGUE, *http://curia.europa.eu.*

332 Garante per la protezione dei dati personali, Linee guida cookie e altri strumenti di tracciamento, n. 231, 10 giugno; F. SALMI, F. SAPORITI, *GDPR e sanzioni. Guida ai principali provvedimenti dei garanti europei: come evitare le contestazioni*, Key Editore, Milano, 2021, p. 54

333 Art. 5 della Direttiva 2002/58/CE; G. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Zanichelli Editore, Bologna, 2012, pp. 241 ss. L'autrice si concentra sul tema delle comunicazioni elettroniche a fini commerciali.

Tale disciplina è basata sul presupposto che il consenso deve essere precedentemente prestato dall'interessato per l'utilizzo da parte del gestore del sito di un *cookie* che quindi permette la memorizzazione e l'accesso ai dati sul dispositivo dell'utente[334].

Per rinforzare la tutela dell'utente la direttiva 2009/136 ha apportato delle modifiche rilevanti ai requisiti del consenso stabiliti dall'art. 5, par. 3 della direttiva 2002/58. Di fatto prima delle modifiche era sufficiente che gli utenti fossero informati in modo chiaro e completo dell'atto di memorizzazione di informazioni nel dispositivo dell'utente o dell'accesso alle informazioni archiviate, con particolare riferimento agli scopi del trattamento e doveva essere offerta la possibilità di rifiutare quest'ultimo.

La direttiva 2009/136 ha sostituito l'obbligo di informazione relativo al diritto di rifiuto stabilendo che *«l'abbonato o l'utente in questione dev'aver espresso preliminarmente il proprio consenso*»; in questo modo il sistema di *opt-out*, quindi di rifiuto informato, è stato rimpiazzato da un sistema di *opt-in* di consenso informato.

Data l'evoluzione tecnologica nel campo delle comunicazioni elettroniche, il legislatore si è accorto ben presto dell'inadeguatezza della direttiva 2002/58 e ha avviato un processo di profondo cambiamento dell'orizzonte normativo.

Una tappa fondamentale è rappresentata dalla Proposta di Regolamento E-Privacy[335]; questo, dopo un lungo iter legislativo ancora in corso, abrogherà la direttiva 2002/58/CE, introducendo importanti cambiamenti integrando le nuove tecnologie nel suo quadro giuridico.

---

334 Il par.3, art.5 della Direttiva offre però un'eccezione relativa ai cookie tecnici che sono indispensabili all'erogazione di un servizio di comunicazione elettronica da parte del provider, a partire proprio dal servizio primario di navigazione sul sito.
Anche per quanto riguarda la disciplina nazionale interna vi è questa distinzione tra cookie tecnici e cookie di profilazione, con l'art. 122 del codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196, infra cod. priv.). Inoltre, il Garante della Privacy ha sottolineato la distinzione col provvedimento n.229 dell'8 maggio 2014.

335 Proposta di Regolamento del Parlamento Europeo e del Consiglio del 10 gennaio 2017, relativa al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (Regolamento sulla vita privata e le comunicazioni elettroniche).

Oltre a questo, un significativo intervento riguardante la disciplina generale di protezione dei dati personali, rimane il Regolamento Generale sulla Protezione dei Dati[336].

Vi è un collegamento tra questi due atti normativi che sta nell'individuazione dei requisiti del consenso al trattamento dei dati personali nelle comunicazioni elettroniche in generale, e in particolare con riguardo ai *cookie*.

Di fatto l'art. 2, lett. f) della direttiva 2002/58 che dichiara che il consenso dell'utente *«corrisponde al consenso della persona interessata di cui alla direttiva 95/46/CE[337]»* stabilisce una relazione di equivalenza tra il consenso richiesto per l'archiviazione di *cookie* di profilazione e il consenso del soggetto interessato al trattamento dei dati personali regolamentato nel GDPR[338], che, come abbiamo già visto, prescrive una serie di requisiti necessari a conferire liceità al trattamento[339].

Un'altra correlazione tra i due corpi normativi è individuata nel punto di regolamentazione degli obblighi informativi; di fatto l'art. 5, par.3 della direttiva 2002/58 stabilisce che l'utente deve essere informato in modo chiaro e completo con riguardo ai fini dell'utilizzazione di *cookie* da parte del *provider*, prima che esprima il suo consenso. La direttiva rinvia esplicitamente agli obblighi di informazione della disciplina in materia di dati personali, oggi stabiliti dall'art. 13 del GDPR.

Inoltre, più in generale, la vasta portata delle definizioni contenute nel GDPR riguardanti i dati personali e il trattamento, porta a ritenere che l'archiviazione sui

---

336 Regolamento UE 2016/679 (GDPR)

337 Oggi questo rinvio è da intendersi al GDPR

338 Anche il considerando 17 della Direttiva 2002/58 afferma ciò in quanto si legge che *«ai fini della presente direttiva il consenso dell'utente o dell'abbonato, senza considerare se quest'ultimo sia una persona fisica o giuridica, dovrebbe avere lo stesso significato del consenso della persona interessata come definito ed ulteriormente determinato nella direttiva 95/46»,* oggi con riferimento al GDPR.

339 Sul tema dei requisiti del consenso si veda tra gli altri C. ANGIOLINI, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, G. Giappichelli Editore, Torino, 2020 pp.126 ss; C. FOCARELLI, *La privacy. Proteggere i dati personali oggi*, Il Mulino, Bologna, 2015, p.70; G. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Zanichelli Editore, Bologna, 2012, p. 194 ss;

dispositivi degli utenti, e dunque la possibilità di accedere ai dati personali di quel soggetto attraverso l'uso di *cookie* di profilazione da parte de *provider*, integra un'attività di trattamento di dati personali descritta nel GDPR[340].

Esso stabilisce che il consenso per essere lecito deve essere libero, specifico, informato e inequivocabile, ne deriva che il presidio di tutela offerto dallo strumento del consenso dell'interessato, si estende anche a tutte le tecnologie che, come i *cookie*, permettono l'accesso e la raccolta di dati personali durante la sola navigazione *online*, dunque durante una diffusa e quotidiana attività, spesso compiuta distrattamente, senza che l'utente si renda conto di quanto si annidino molte insidie alla protezione dei suoi dati personali[341].

Dunque, siamo di fronte ad un quadro normativo che si articola su diverse fonti, comprendenti la disciplina in materia di comunicazioni elettroniche e quella relativa alla protezione dei dati personali; tuttavia, è tenuto insieme da un filo conduttore individuato nella regola generale del consenso prestato dall'interessato come strumento per tutelare le informazioni e i dati personali degli utenti.

D'altra parte però le due parti non si sovrappongono in materia di principi e valori generali su cui sono fondati: la direttiva 2002/58 si pone come obiettivo la tutela della riservatezza delle comunicazioni economiche e dei dati personali che da queste possono essere ricavati attraverso l'intrusione nei dispositivi degli utenti; essa si fonda sull'art. 7 della Carta dei diritti fondamentali dell'UE che tutela il diritto fondamentale al rispetto della vita privata e familiare, del domicilio e delle comunicazioni dell'individuo; d'altra parte il GDPR è un'attuazione dell'art. 8 della medesima Carta e dell'art. 16 del Trattato sul funzionamento dell'Unione Europea, che sanciscono il diritto di ogni persona alla protezione dei propri dati personali e ne ammettono il trattamento solo se fondato sul consenso o su altre basi giuridiche stabilite dalla legge.

---

340 In questi termini si esprime la menzionata sentenza della Corte di Giustizia dell'Unione Europea dell'1° ottobre 2019, C-673/17.

341 G. MARINO, *Internet e tutela dei dati personali: il consenso ai cookie,* in *Jus Civile,* 2020,2*,* pp. 408-409.

Il GDPR, per di più, non si basa su una prospettiva tradizionale di non divulgazione degli aspetti privati di una persona, ma bensì adotta la prospettiva di un mercato globale che si fonda sulla raccolta e sulla libera circolazione di ingenti masse di dati resa possibile dalle nuove tecnologie[342].

4.3 Declinazione assunta dai requisiti del consenso nel trattamento effettuato mediante i *cookie.*

È interessante svolgere una breve analisi sulla declinazione assunta dai requisiti fondamentali del consenso al trattamento di dati personali che viene effettuato *online*, tramite l'utilizzo di *cookie* di profilazione.

In merito a questo tema, assume particolare importanza una decisione della Grande Sezione della Corte di Giustizia dell'Unione Europea[343].

Essa si è rivelata particolarmente considerevole in quanto vieta definitivamente la richiesta di consenso degli utenti all'installazione di *cookie* attraverso caselle di spunta preselezionate.

Il caso riguarda un prestatore di servizi digitali, precisamente di giochi *online*, che nel proprio sito *internet* chiedeva una duplice manifestazione di consenso dell'utente per poter partecipare ai giochi[344]. Dunque l'utente si trovava di fronte a due caselle da selezionare prima di poter accedere al gioco; la prima casella, non preselezionata, chiedeva il consenso per essere contattato da una serie di aziende *partner* del prestatore del servizio digitale per ricevere offerte di tipo commerciale[345]; la seconda casella, che al contrario era già preselezionata di

---

342 *Ibidem*

343 Corte di Giustizia dell'Unione Europea, sentenza della corte (Grande sezione),1° ottobre 2019, causa C-673/17

344 Il caso riguarda un gioco a premi organizzato dalla Planet49.

345 La didascalia della prima casella digitava *«Acconsento a ricevere informazioni per posta, per telefono, per posta elettronica o via SMS da sponsor e partner sulle offerte del loro rispettivo settore commerciale. È mia facoltà stabilire qui autonomamente i soggetti legittimati ad inviarmi dette offerte, in caso contrario la scelta spetta all'organizzatore. Posso revocare il consenso in qualsiasi momento. Ulteriori informazioni al riguardo si trovano qui».* Era presente poi un link che rinviava ad un elenco di 57 imprese con i rispettivi indirizzi, il settore commerciale che sarebbe stato pubblicizzato e la modalità di comunicazione utilizzata per la pubblicità che poteva essere per posta elettronica, posta o telefono. Inoltre,

default, chiedeva il consenso per l'installazione di *cookie* sul dispositivo dell'utente, per poter esaminare le sua navigazioni sul *web* e le visite ai siti *Internet* dei partner commerciali del gestore del sito, in modo da poter inoltrare pubblicità mirata sugli interessi dell'utente stesso[346].

Le questioni pregiudiziali vertono sull'interpretazione delle previsioni stabilite in materia di consenso sia nell'ambito della direttiva 2002/58/CE sulla protezione della vita privata nelle comunicazioni elettroniche sia della direttiva 95/46/CE che del Regolamento europeo per la protezione dei dati personali, in particolar modo sui requisiti della specificità, dell'inequivocabilità e dell'informazione del consenso del soggetto interessato.

Innanzitutto, la Corte Suprema tedesca ha posto l'attenzione sull'ammissibilità o meno di un'attività di memorizzazione dati e quindi di accesso a informazioni personali già archiviati nel dispositivo di un utente esercitata dal gestore del sito tramite i *cookie* attraverso una casella preselezionata che l'utente, in caso di contrarietà a prestare il consenso, avrebbe dovuto deselezionare. Quindi la questione riguarda se il consenso dell'interessato a *cookie* di profilazione e, di conseguenza, al trattamento di dati personali può ritenersi valido ed efficace anche se questo deriva dalla mancata deselezione di una casella preselezionata dal *provider*[347].

---

dopo il nome di ogni singola impresa compariva il termine "eliminare"; l'elenco era preceduto da questo avviso: *«Cliccando sul link "eliminare" stabilisco che non può essere comunicato al menzionato partner/sponsor il consenso a fini pubblicitari. Ove io non abbia eliminato alcun partner/sponsor o non ne abbia eliminato un numero sufficiente, la Planet49 compirà la scelta dei partner/sponsor per mio conto a sua discrezione (numero massimo: 30 partner/sponsor)».*

346 La seconda casella riportava la seguente descrizione: *«Acconsento a sottopormi al servizio di analisi web Remintrex. Di conseguenza, l'organizzatore del gioco a premi, a seguito dell'approvazione della mia registrazione al gioco, installa cookie al fine di analizzare tramite Remintrex le mie navigazioni sul web e le mie visite ai siti Internet dei partner commerciali e di inviarmi pubblicità centrata sui miei interessi. Posso cancellare i cookie in ogni momento. Per ulteriori dettagli si legga qui».*

347 Le questioni pregiudiziali che sono state presentate dalla Corte Suprema tedesca alla CGUE sono formulate nel seguente modo: *«1) Se sussista un consenso efficace ai sensi dell'articolo 5, paragrafo 3, e dell'articolo 2, lettera f), della direttiva 2002/58, in combinato disposto con l'articolo 2, lettera h), della direttiva 95/46, nel caso in cui la memorizzazione di informazioni ovvero l'accesso a informazioni già archiviate nell'apparecchiatura terminale di un utente siano consentiti tramite una casella preselezionata che l'utente deve deselezionare per negare il suo consenso. b) Se, ai fini dell'applicazione dell'articolo 5, paragrafo 3, e dell'articolo 2, lettera f), della direttiva 2002/58, in combinato disposto con*

La questione riguarda soprattutto il requisito di inequivocabiltà del consenso al trattamento dei dati personali; la Corte alla fine ha negato la validità del consenso prestato in tale modo, vale a dire ottenuto dalla mancata deselezione della casella già preselezionata dal gestore del sito; la decisione viene giustificata tenendo in considerazione alcune fonti europee in materia; prima di tutto il giudice europeo ha richiamato il considerando 17 della direttiva 2002/58 dal quale deriva che il consenso che da l'utente ai *cookie* può essere prestato secondo qualsiasi modalità appropriata, anche tramite la *«selezione di un'apposita casella nel caso di un sito Internet».*

Per di più, anche se si ritiene di per sé neutra sul piano letterale la formulazione dell'art.5, par. 3 che prevede che l'utente deve avere *«espresso preliminarmente il proprio consenso»*, la Corte ha richiamato un argomento storico, sottolineando l'origine della disposizione in parola: la versione attuale è il risultato di una modifica sostanziale, attuata dalla direttiva 2009/136, mentre quella originaria si limitava a pretendere che l'utente avesse solo la possibilità di rifiutare l'installazione dei *cookie* nel proprio dispositivo, la nuova versione afferma che l'utente deve aver espresso prima il suo consenso.

Dunque, il giudice europeo ne ricava che il legislatore non avrebbe ritenuto idonea una manifestazione del consenso presunta data dalla mancanza di rifiuto dell'utente ma avrebbe voluto invece un comportamento attivo del soggetto.

La decisione della Corte inoltre mette in evidenza la sostanziale eguaglianza tra la nozione di consenso prevista dalla direttiva 2002/58 e quella definita dalla disciplina di protezione di dati personali; per di più, da questa prospettiva, il giudice europeo sottolinea come il termine "manifestazione" di volontà, già

---

l'articolo 2, lettera h), della direttiva 95/46, la situazione differisca nel caso in cui le informazioni archiviate o consultate consistano in dati personali. c) Se, in presenza delle circostanze indicate nella prima questione pregiudiziale, [lettera a),] sussista un consenso efficace ai sensi dell'articolo 6, paragrafo 1, lettera a), del regolamento 2016/679. 2) Quali informazioni debbano essere comunicate dal fornitore di servizi all'utente, affinché quest'ultimo sia informato, in termini chiari e completi ai sensi dell'articolo 5, paragrafo 3, della direttiva 2002/58. Se in tali informazioni rientrino altresì la durata della funzione dei cookie e il fatto che terzi abbiano accesso ai cookie stessi».

nell'ambito della direttiva 95/46[348], deve essere espressa in modo inequivocabile, evocando quindi un'azione attiva e non solamente passiva[349].

Infine, la Corte sottolinea che, tenendo presente quanto espresso dal GDPR, queste conclusioni diventano ancora più decisive; di fatto l'articolo 4 definisce il "consenso dell'interessato" ai fini dell'art. 6, par.1, lett. a), pretende una manifestazione di volontà da parte dell'interessato che deve essere "libera, specifica, informata e inequivocabile", che deve comprendere una dichiarazione di assenso oppure un'"azione positiva inequivocabile".

Inoltre, il considerando 32 del GDPR stabilisce che la manifestazione del consenso potrebbe anche includere la selezione di una casella nel sito *internet*, mentre non comprende "Il silenzio, l'inattività o la preselezione di caselle".

Dunque, dopo aver esaminato questi elementi, la Grande Sezione della Corte di Giustizia, è giunta alla conclusione che una dichiarazione predisposta dal gestore del sito e caratterizzata da una casella preselezionata, rispetto alla quale l'utente non si è opposto, non è idonea a rilevare una manifestazione di volontà inequivocabile come richiesta dalle norme richiamate in tema di protezione di dati personali[350].

Pertanto, da questa decisione si può ricavare che per ritenere valido il requisito di inequivocabilità, l'interessato deve esprimere un consenso "attivo" al trattamento dei propri dati personali in un ambiente digitale. Per cui il suo silenzio o un'omissione o una mera inerzia non possono integrare una manifestazione di

---

348 Art. 7 della direttiva 95/46

349 Questa linea è stata adottata anche dall'Avvocato generale, al punto 81 della conclusione, quando richiama i concetti elaborati dal Gruppo di lavoro "Articolo 29" per la protezione dei dati personali (nel parere 2/2010 sulla pubblicità comportamentale online), secondo il quale il consenso implica una precedente azione attiva da parte degli utenti finalizzata all'accettazione della memorizzazione dei cookie e del loro utilizzo. Il Gruppo di lavoro indica che la stessa nozione di "manifestazione" comporta la necessità di un'azione.

350 Il giudice europeo ha infatti dichiarato che *«a tal riguardo, risulta praticamente impossibile determinare in modo oggettivo se, non deselezionando una casella preselezionata, l'utente di un sito Internet abbia effettivamente manifestato il proprio consenso al trattamento dei suoi dati personali, nonché, in ogni caso, se tale consenso sia stato manifestato in modo informato. Non può, infatti, essere escluso che detto utente non abbia letto l'informazione che accompagna la casella preselezionata, o addirittura che lo stesso non abbia visto tale casella, prima di continuare la propria attività sul sito Internet che visita».* (CGUE, 1° ottobre 2019, causa C-673/17, par. 55).

volontà idonea per la prestazione del consenso in quanto potrebbero condurre ad ambiguità ed incertezze riguardo all'effettivo volere dell'interessato.

Invece, la manifestazione del consenso espresso tramite un *click* su una casella in un sito internet è da inquadrare nella categoria della dichiarazione espressa; di fatto pur non utilizzando un linguaggio scritto o verbale, l'utente esteriorizza la sua volontà mediante un gesto che, secondo l'uso comune e la convenzione degli utenti nel *web*, si identifica come strumento per indicare assenso. Non può invece considerarsi tale la mancata deselezione di una casella preselezionata di *default* dal gestore del sito[351].

Oltre ad aver quindi vietato l'uso di caselle di spunta preselezionate per richiedere il consenso, la decisione ha rafforzato anche i requisiti di informativa riguardanti l'installazione di *cookie*. I gestori dei siti internet dovranno quindi verificare la compatibilità delle proprie *policy* con la decisione della Corte, dato che le autorità garanti della *privacy* saranno tenute a seguirla[352].

Inoltre, la decisione della Corte ha influenzato i negoziati svolti sul testo del nuovo Regolamento ePrivacy dato che si sono registrate maggiori divergenze di pensiero proprio sul tema dei *cookie*.

---

[351] *«Quest'orientamento si pone peraltro in linea con l'insegnamento tradizionale di teoria generale del contratto 41 e con l'elaborazione giurisprudenziale predominante 42, secondo cui in seno al procedimento di formazione della volontà negoziale il silenzio, l'inerzia, non possono che essere considerati contegni neutri, ambigui, privi in quanto tali di un autonomo significato».* G. MARINO, *Internet e tutela dei dati personali: il consenso ai cookie,* in *Jus Civile,* 2020,2*,* pp. 412-413.

[352] L. TOSONI, *Cookie: l'impatto della sentenza della Corte UE che bandisce le caselle di spunta preselezionate*, in *Agenda Digitale,* 3 ottobre 2019, online su *https://www.agendadigitale.eu/sicurezza/privacy/cookie-limpatto-della-sentenza-della-corte-ue-che-bandisce-le-caselle-di-spunta-preselezionate/*

4.4 Il principio del consenso separato: il requisito della specificità

Un'altra significativa questione riguardante la manifestazione del consenso al trattamento dei dati personali attraverso i *cookie*, riguarda il profilo della specificità[353].

A riguardo, alcune interessanti conclusioni interpretative sono fornite dalla decisione della CGUE nel caso già citato e nelle convulsioni dell'Avvocato generale.

Nel caso in esame il gestore del sito dichiarava che l'interessato aveva fornito un consenso efficace per aver "cliccato" sul pulsante di partecipazione al gioco a premi *online* istituito dal gestore stesso, compiendo quindi un'azione attiva e non per non aver deselezionato la casella comprendente la dichiarazione di consenso. Nel cliccare il pulsante di partecipazione al gioco *online* quindi l'utente allo stesso tempo aveva acconsentito all'installazione di *cookie* nel suo dispositivo, aventi finalità commerciali. Secondo la Corte però questo non rispetterebbe il principio di specificità del consenso al trattamento dei dati personali[354], il quale prevede che il consenso deve riferirsi precisamente al trattamento e dunque non può essere desunto da una manifestazione di volontà che detiene un oggetto distinto, come in questo caso quella dell'attivazione del pulsante di partecipazione al gioco[355].

Questo requisito della specificità espresso dal GDPR, conduce ad un altro principio generale che governa la manifestazione del consenso al trattamento dei dati personali *online*, vale a dire il principio del consenso separato.

---

353 In dottrina sul profilo della specificità del consenso al trattamento di dati personali si vedano, tra gli altri, S. THOBANI, *Operazioni di tying e libertà del consenso*, in *Giur. it*., 2018, 537.

354 Espresso dall'art. 4, n.11, del Regolamento UE 2016/679 (GDPR)

355 Secondo la Corte, «la manifestazione di volontà di cui all'articolo 2, lettera h), della direttiva 95/46 deve, in particolare, essere «specifica», nel senso che deve riferirsi precisamente al trattamento dei dati interessati e non può essere desunta da una manifestazione della volontà avente un oggetto distinto. Nel caso di specie, contrariamente a quanto sostenuto dalla Planet49, il fatto che l'utente attivi il pulsante di partecipazione al gioco a premi organizzato da detta società non può essere, pertanto, sufficiente per ritenere che l'utente abbia validamente espresso il suo consenso all'installazione di cookie» (CGUE, Grande Sezione, 1° ottobre 2019, par. 58-59).

Secondo questo principio la volontà contrattuale e il consenso all'installazione di *cookie*, e perciò alle attività di trattamento di dati personali che ne consegue, non possono confondersi in una sola ed unica manifestazione di volontà[356].

Anche l'Avvocato generale si è espresso in tale modo, sostenendo che *«l'attività che un utente svolge su Internet (leggere una pagina web, partecipare a un gioco a premi, guardare un video, ecc.) e la prestazione del consenso non possono far parte dello stesso atto. In particolare, dal punto di vista dell'utente, la manifestazione del consenso non può apparire di natura accessoria rispetto alla partecipazione al gioco a premi. Entrambe le azioni devono, specialmente sotto il profilo visivo, essere presentate su un piano di parità[357]».*

L'adozione del requisito della specificità porta a ritenere che il consenso al trattamento tramite *cookie* non sia validamente espresso per mezzo di "comportamenti concludenti"[358], vale a dire dalla condotta dell'utente che ha manifestato la volontà di concludere un contratto in internet premendo un pulsante; questo vale anche per tutti quei casi in cui il *web* adotta svariate formule come "proseguendo nella navigazione l'utente accetta", nelle quali il consenso all'installazione di cookie di profilazione viene ricavato dal comportamento dell'utente che si limita a proseguire nella navigazione sul sito.

Quindi non si può ritenere valido il consenso ai *cookie* prestato semplicemente proseguendo a navigare in una pagina web[359].

Dunque, il quadro normativo della protezione dei dati personali viene rafforzato attraverso il potenziamento dei caratteri costitutivi del consenso al trattamento, in particolare sulle modalità di manifestazione del consenso, tramite i requisiti di specificità ed inequivocabilità.

---

356 G. MARINO, *Internet e tutela dei dati personali: il consenso ai cookie,* in *Jus Civile,* 2020,2*,* p.415

357 Punto 66

358 *«Rileggendo la fattispecie alla stregua delle infrastrutture concettuali tradizionali va segnalato uno scostamento rispetto ai pilastri della teoria generale del contratto, per la quale, com'è noto, la manifestazione della volontà negoziale può essere ricavata non soltanto per mezzo di una dichiarazione (espressa o tacita), bensì anche dall'adozione di "comportamenti concludenti"».* G. MARINO, *Internet e tutela dei dati personali: il consenso ai cookie,* in *Jus Civile,* 2020,2*,* cit*,* p.416

359 *Annuario 2021, Osservatorio Giuridico sulla Innovazione Digitale*, (a cura di) S. ORLANDO, G. CAPALDO, Università La Sapienza, 2021, p.128.

Come si è già detto, la *data economy*, basata sul potere di raccolta e sfruttamento dei dati personali, si sta sviluppando sempre di più, e per questo è inevitabile un processo si intersezione tra la legge di tutela dei dati personali e quella del mercato e del contratto; in questo contesto assume particolare rilevanza il principio del consenso separato il quale ha il fine di delineare un confine tra il consenso prestata dal soggetto in veste di interessato che fornisce il consenso al trattamento dei suoi dati personali, e quello del consenso prestato dall'utente/consumatore che vuole concludere un contratto di fornitura di un determinato servizio o contenuto digitale.
Ovviamente, la natura giuridica delle due figure è differente, e così anche le regole che concorrono alla formazione delle due volontà e *rationes* che le caratterizzano[360].

4.5 I requisiti di libertà e informazione del consenso al trattamento di dati personali via *cookie*

Specificità ed inequivocabilità fanno parte del modo di manifestazione della volontà, dunque fanno riferimento all'esternazione del consenso, i requisiti di libertà ed informazione invece caratterizzano il cd. consenso interno e concorrono a formare il processo di formazione del volere nel "foro interiore"[361] dell'interessato.
Dato che il consenso degli utenti al trattamento di informazioni personali rappresenta la chiave per l'estrazione di un importante valore economico tramite l'uso di tecnologie a disposizione dell'operatore economico, come i *cookie*, di

[360] Il consenso richiesto a scopi commerciale è espressione del principio di autonomia contrattuale dei privati e deve essere prestato da un soggetto che sia capace di intendere e di volere e non deve essere viziato da errore, violenza o dolo, oppure da pericolo o bisogno. Dunque, quando non sussistono tali condizioni, si tratta di una volontà che sussiste validamente. Il consenso negoziale trova la sua interezza dolo nell'accordo tra le volontà, nella dimensione della mediazione e della composizione di interessi confliggenti di cui il contratto è massima espressione. Al contrario, il consenso al trattamento dei dati personali è solo espressione del potere di autodeterminazione dell'individuo. G. MARINO, *Internet e tutela dei dati personali: il consenso ai cookie,* in *Jus Civile,* 2020,2*,* cit*,* p.417.

[361] *Ibidem, cit.*

conseguenza aumentano anche le possibili minacce alla libertà e alla consapevolezza del medesimo.

Il requisito di libertà ha lo scopo di rafforzare la tutela dei dati personali; anche in questo caso, nel trattamento di dati personali esercitato attraverso *cookie* di profilazione, non è ritenuto libero il consenso dell'utente ricavato per "comportamenti concludenti", come ad esempio dal solo fatto che egli prosegua nella navigazione in una certa pagina *web*; molti gestori di siti *web* utilizzano questa strategia perché tentano di ottenere il consenso dell'utente che non ha del tutto compreso il contenuto della sua manifestazione di volontà o è anche ignaro di averla manifestata; oppure viene indotto ad accettare l'uso dei *cookie* in modo da poter continuare la navigazione; queste modalità di manifestazione del consenso diffuse in rete però ledono il requisito della libertà[362].

Inoltre, un altro problema riguardante la libertà di consenso si verifica quando la fornitura di un contenuto o servizio digitale è subordinata al rilascio del consenso dell'interessato[363].

---

[362] L'EDPB ne fornisce un chiaro esempio ai punti 40 e 41 nel parere n. 5/2020, del 4 maggio 2020: «*Un fornitore di un sito web predispone uno script che blocca la visualizzazione del contenuto e fa apparire solo la richiesta di accettare i cookie, le informazioni sui cookie che verranno installati e le finalità per le quali i dati saranno trattati. Non è possibile accedere al contenuto senza cliccare sul pulsante "Accetto i cookie". Poiché all'interessato non è offerta una scelta effettiva, il suo consenso non è espresso liberamente.In questo caso il consenso non è valido, in quanto la prestazione del servizio è subordinata al fatto che l'interessato clicchi sul pulsante "Accetto i cookie". Non è offerta una scelta effettiva.*»

[363] Abbiamo già notato come ci sia una diversità tra gli orientamenti del Garante della Privacy italiano e della Suprema Corte di Cassazione; il Garante ha sostenuto che non può ritenersi libero il consenso prestato per finalità promozionali, quando il titolare subordina il godimento dei suoi servizi al rilascio del consenso; la Corte invece ha affermato la possibilità di distinguere l'ipotesi in cui la prestazione offerta del titolare consiste in un servizio fungibile e rinunciabile senza gravoso sacrificio, da quella in cui il servizio risulta essere infungibile e irrinunciabile: in questo secondo caso solamente, si verifica un condizionamento tale da minare la libertà del consenso. Così Cass., 2 luglio 2018, n. 17278, cit., secondo cui *«in tema di consenso al trattamento dei dati personali, la previsione dell'art. 23 del d.lgs. n. 196/2003, nello stabilire che il consenso è validamente prestato solo se espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, consente al gestore di un sito Internet, il quale somministri un servizio fungibile, cui l'utente possa rinunciare senza gravoso sacrificio (nella specie servizio di newsletter su tematiche legate alla finanza, al fisco, al diritto e al lavoro), di condizionare la fornitura del servizio al trattamento dei dati per finalità pubblicitarie, sempre che il consenso sia singolarmente ed inequivocabilmente prestato in riferimento a tale effetto, il che comporta altresì la necessità, almeno, dell'indicazione dei settori merceologici o dei servizi cui i messaggi saranno riferiti».*

Sul tema dell'acquisizione del consenso per i *cookie* si è espresso anche il EDPB[364] sostenendo che il semplice scrolling non può essere ritenuto idoneo a manifestare compiutamente la volontà dell'interessato indirizzata ad acconsentire alla ricezione di *cookie* nel proprio terminale, diversi da quelli tecnici.

Anche il Garante Italiano ha condiviso questa interpretazione sostenendo che lo *scrolling* non può costituire una valida manifestazione di volontà dell'interessato, tuttavia indica la possibilità che esso possa prendere parte al processo di acquisizione del consenso costituendo una delle componenti di un più articolato procedimento, non l'unica.

Un'altra modalità non concessa per ottenere il consenso è il cosiddetto "cookie wall"[365] con il quale si fa riferimento ad un meccanismo vincolante in cui l'utente è costretto ad esprimere il proprio consenso alla ricezione di *cookie* e altri strumenti di tracciamento, senza potersi rifiutare, altrimenti non gli sarà possibile accedere al sito[366].

Questo meccanismo non permette di identificare la validità dei requisiti che devono caratterizzare il consenso secondo il GDPR, con particolare riferimento al requisito della "libertà".

Di fatto il *cookie wall* viola la libertà del consenso in quanto i vizi che incidono su questo requisito sono le situazioni di squilibrio, la condizionalità e gli effetti pregiudizievoli[367]. Infatti, il considerando 43 del Regolamento sostiene che il consenso non può ritenersi liberamente prestato «*qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento […] e ciò rende pertanto improbabile che il consenso sia prestato liberamente in tutte le circostanze di tale situazione specifica*». Il considerando comprende non solo le autorità pubbliche,

---

364 EDPB, parere n. 5/2020, del 4 maggio 2020

365 Meccanismo chiamato "take it or leave it". F. SALMI, F. SAPORITI, *GDPR e sanzioni. Guida ai principali provvedimenti dei garanti europei: come evitare le contestazioni*, Key Editore, Milano, 2021, p. 55.

366 I *cookie wall* sono stati vietati già dalla versione del regolamento e-Privacy approvata il 26/10/2017 dal Parlamento UE in prima lettura; è stato accolto con favore anche dall'EDPB con le linee guida 05/2020.

367 R. I. D'AFFLITTO, Rapporto Privacy 2021, Temi e dibattiti sulla protezione dei dati personali, Key Editore, Milano, 2022, p.68

ma anche tutte le società che si trovano in una posizione di mercato dominante[368].

Si verifica condizionalità quando la fornitura di un servizio è subordinata al rilascio del consenso. Il considerando 43 del GDPR, sostiene che il consenso non è libero *«se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione».* Infine, nel *cookie wall* il soggetto non può rifiutare o revocare il consenso senza subire un pregiudizio[369], dunque si verifica un esempio di effetto pregiudizievole. Dopo versioni precedenti intermedie del Consiglio che avevano eliminato l'esplicitazione di tale divieto, la proposta finale, approvata il 10 febbraio 2021, ritorna di nuovo sul tema richiamando ancora una volta i considerando 42 e 42 del Regolamento.

Il nuovo Considerando contenuto nella versione approvata dal Consiglio stabilisce che «*Contrariamente all'accesso al contenuto del sito web fornito dietro pagamento in denaro, dove l'accesso è fornito senza pagamento monetario diretto ed è subordinato al consenso dell'utente finale alla memorizzazione e alla lettura dei cookie per scopi aggiuntivi, richiedere tale consenso normalmente non sarebbe considerato privare l'utente finale di una scelta autentica se l'utente finale è in grado di scegliere tra servizi, sulla base di informazioni chiare, precise e di facile utilizzo circa le finalità dei cookie e tecniche simili, tra un'offerta che include il consenso all'utilizzo dei cookie per finalità ulteriori da un lato, e dall'altro un'offerta equivalente da parte dello stesso fornitore che non comporta il consenso al trattamento dei dati per finalità ulteriori. Al contrario, in alcuni casi, si può ritenere che l'accesso ai contenuti del sito web dipenda dal consenso all'uso di tali cookie, in presenza di un chiaro squilibrio tra l'utente finale e il fornitore del servizio, in quanto priverebbe l'utente finale di una scelta autentica. Questo sarebbe normalmente il caso dei diti web che forniscono determinati servizi, come quelli forniti dalle autorità pubbliche. Allo stesso modo, tale squilibrio potrebbe esistere quando l'utente finale ha solo poche o nessuna alternativa al*

[368] Per esempio Facebook nel campo dei servizi *social networking*.
[369] Considerando 42 del Regolamento UE 2016/679 (GDPR)

servizio, e quindi non ha una scelta reale sull'uso dei cookie, ad esempio nel caso di fornitori di servizi in posizione dominante[370]*».*

Un'altra modalità sembra poter ledere il requisito della libertà del consenso: si tratta del caso in cui vi sia un'eccessiva riproposizione del *banner* per ottenere il consenso quando l'utente ha già in precedenza negato la prestazione del consenso; in tale caso, infatti, si induce l'utente a prestare il consenso per poter continuare a navigare sul sito libero dalla comparsa del banner con l'informativa breve e la richiesta di prestazione del consenso.

Il Garante italiano inoltre ha fornito delle linee guida contenenti le indicazioni per un banner correttamente costruito[371]. Il Garante fa riferimento anche agli obblighi informativi dettati dal Regolamento, con particolare riferimento all'art. 25 il quale

---

[370] Considerando 20aaaa della versione del Consiglio.

[371] Il *banner*, infatti, dovrebbe contenere «oltre alla X in alto a destra di cui è stata già illustrata la funzione, almeno le seguenti indicazioni ed opzioni:

i) l'avvertenza che la chiusura del banner mediante selezione dell'apposito comando contraddistinto dalla X posta al suo interno, in alto a destra, comporta il permanere delle impostazioni di default e dunque la continuazione della navigazione in assenza di cookie o altri strumenti di tracciamento diversi da quelli tecnici;

ii) una informativa minima relativa al fatto che il sito utilizza – se così è ovviamente - cookie o altri strumenti tecnici e potrà, esclusivamente previa acquisizione del consenso dell'utente da prestarsi con modalità da indicarsi nella medesima informativa breve (cfr. punto iv che segue), utilizzare anche cookie di profilazione o altri strumenti di tracciamento al fine di inviare messaggi pubblicitari ovvero di modulare la fornitura del servizio in modo personalizzato al di là di quanto strettamente necessario alla sua erogazione, cioè in linea con le preferenze manifestate dall'utente stesso nell'ambito dell'utilizzo delle funzionalità e della navigazione in rete e/o allo scopo di effettuare analisi e monitoraggio dei comportamenti dei visitatori di siti web;

iii) il link alla privacy policy, ovvero ad una informativa estesa posizionata in un second layer – che sia accessibile con un solo click anche tramite un ulteriore link posizionato nel footer di qualsiasi pagina del dominio cui l'utente accede - ove vengano fornite in maniera chiara e completa almeno tutte le indicazioni di cui agli artt. 12 e 13 del Regolamento, anche con riguardo ai predetti cookie o altri strumenti tecnici (cfr., al riguardo, il successivo paragrafo 8);

iv) un comando attraverso il quale sia possibile esprimere il proprio consenso accettando il posizionamento di tutti i cookie o l'impiego di eventuali altri strumenti di tracciamento;

v) il link ad una ulteriore area dedicata nella quale sia possibile selezionare, in modo analitico, soltanto le funzionalità, i soggetti cd. terze parti - il cui elenco deve essere tenuto costantemente aggiornato, siano essi raggiungibili tramite specifici link ovvero anche per il tramite del link al sito web di un soggetto intermediario che li rappresenti - ed i cookie, anche eventualmente raggruppati per categorie omogenee, al cui utilizzo l'utente scelga di acconsentire».

Garante per la protezione dei dati personali, *Linee guida cookie e altri strumenti di tracciamento*, n. 231, 10 giugno 2021

stabilisce che *«Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità …».*

Per adempiere a tale prescrizione, il titolare deve perciò garantire, con un'impostazione predeterminata, che siano trattati esclusivamente i dati necessari a conseguire ciascuna finalità del trattamento e che la quantità di dati raccolti e la durata della loro conservazione «*non eccedano il minimo necessario per il conseguimento delle finalità perseguite»*[372].

Inoltre aggiunge che il consenso può essere considerato validamente prestato solo se deriva da un intervento attivo e consapevole dell'utente; per questo stabilisce che *«qualora i gestori dei siti web decidano di conformarvisi, dovranno implementare un meccanismo in base al quale l'utente, accedendo per la prima volta alla home page (o ad altra pagina) del sito web, visualizzi immediatamente un'area o banner le cui dimensioni siano, al tempo stesso, sufficienti da costituire una percettibile discontinuità nella fruizione dei contenuti della pagina web che sta visitando, ma anche tali da evitare il rischio che l'utente possa far ricorso a comandi e dunque compiere scelte indesiderate o inconsapevoli».*

Anche l'EPDB[373] concorda sul fatto che il presupposto della libertà del consenso viene a mancare se il soggetto è effettivamente obbligato a prestare il suo consenso perché vuole ottenere un bene o un servizio o perché il rapporto in cui di trova ad agire è squilibrato; *l'European Data Protection Board* fa riferimento alla cosiddetta *tying practices;* in merito il GDPR adotta una posizione piuttosto equivoca all'art.7, par.4 e al considerando 43[374]; si può dedurre probabilmente che la necessità di fornire il consenso per beni o servizi essenziali lo rende

---

372 *Ibidem*

373 Linee guida dell'EPDB *5/2020* che aggiornano le linee guida del Gruppo di lavoro Articolo 29

374 Sostengono che va tenuta nella "massima considerazione" l'eventualità che l'esecuzione del contratto sia condizionata al consenso, "presumendosi" la mancanza di libertà se il trattamento dei dati non è necessario a tale esecuzione.

inevitabilmente invalido; viceversa se si tratta di beni o servizi non essenziali il consenso può essere richiesto e prestato validamente; per esempio sarebbe possibile subordinare uno sconto al consenso ma non condizionare l'accesso a una app già scaricata al consenso per il trattamento di dati non necessari per l'esecuzione del servizio o l'accesso ad una pagina *web* al consenso ai *cookie*, come accade con i *cookie walls*[375].

Infine, il requisito che è messo più in crisi dagli sviluppi sul mercato di tecnologie capaci di tracciare e rielaborare informazioni personali per scopi commerciali, è quello dell'informazione.

Il legislatore infatti ha cercato di potenziare le previsioni che impongono agli operatori economici di fornite un'informazione chiara e completa riguardante il trattamento di dati personali degli utenti e si è occupato di definire in modo preciso i contenuti indefettibili; la direttiva 2002/58 in materia di comunicazioni elettroniche indica i punti essenziali dell'informazione che deve fornire il gestore che consistono nell'individuare la natura dei dati sottoposti a trattamento, gli scopi e la durata del trattamento[376]; la normativa inoltre rinvia alla disciplina europea di protezione di dati personali che stabilisce che l'informazione deve essere somministrata in modo chiaro e completo, prima della manifestazione di volontà dell'interessato per poter formare un consenso consapevole[377]. Inoltre, deve essere rispettato il principio generale di correttezza e trasparenza nel trattamento di dati personali[378].

Di conseguenza, con il GDPR, ogni sito internet deve informare l'utente riguardo all'eventuale raccolta di dati personali ed ottenerne il consenso; in particolare, la

---

375 *Annuario 2021, Osservatorio Giuridico sulla Innovazione Digitale*, (a cura di) S. ORLANDO, G. CAPALDO, Università La Sapienza, 2021, pp.125-126.

376 Considerando 23 e 26 della direttiva 2002/58

377 Le informazioni devono riguardare le finalità del trattamento cui sono destinati i dati personali e la base giuridica (art. 13, par. 1, lett. c), GDPR), eventuali destinatari (art. 13, par. 1, lett. d), periodo di conservazione o criteri utilizzati per determinarne la durata (art. 13, par. 2, lett. a), l'esistenza del diritto di accesso, rettifica o cancellazione dei dati, alla portabilità dei dati (lett. b), del diritto di revoca (lett. c) e di reclamo a un'autorità di controllo (lett. d).

378 art. 5 del Regolamento UE 2016/679 (GDPR)

normativa richiede che sia fornita un'informatica completa, redatta su due livelli: un'informativa breve o *Cookie Banner* e un'informativa estesa o *Cookie Policy*.
L'informativa breve si presenta come un *banner* mostrato all'accesso di una qualsiasi pagina del sito contenente i pulsanti di accetta e rifiuta e la possibilità di fornire un consenso granulare, mentre l'informativa estesa risiede in una determinata area del sito chiamata *Cookie Policy* che dovrà essere accessibile da qualsiasi pagine del sito. Quest'ultima informativa deve essere conforme ai requisiti di trasparenza imposti dagli art. 12 e 13 del GDPR[379].
Nonostante tutti questi obblighi informativi, l'utente medio non è in grado di comprendere a pieno la complessità tecnica dei *cookie*; inoltre, la costante predisposizione di internet ad una crescente rapidità e intuitività d'uso[380] contribuiscono ad aggravare il divario di conoscenze creatosi tra *provider* e *user*[381].
Tra questi due soggetti, gli obblighi di informazione riguardanti il trattamento di dati personali operato attraverso strumenti di tecnologia complessi come i *cookie*

[379] Recentemente (2019-2020) è successo che la proprio la Corte di Giustizia, dunque l'organo di massima tutela della giustizia dei diritti e delle libertà dei cittadini, ha violato la normativa sui cookie: l'EDPS, infatti, che ha anche il compito di controllare il rispetto della normativa *data protection* da parte delle istituzioni comunitarie, ha ripreso la CGUE per inadempimento circa l'utilizzo dei cookie sul proprio sito internet. Il sito web in questione è https://curia.europa.eu, usato in genere per fare ricerche riguardanti le decisioni della Corte. Un cittadino che stava visitando il sito si è reso conto della non regolarità del banner dei cookie e lo ha segnalato all'EDPS. Esso ha dunque interpellato la Corte, rilasciando una serie di raccomandazioni su come reimpostare il sito stesso; la CGUE ha quindi modificato la cookie policy, prevedendo l'installazione dei *cookie analytics* solo con il consenso e non negando più l'uso del sito in sua mancanza, implementando un meccanismo di revoca del consenso attraverso la *cookie policy*. Sono state poi riscontrate altre violazioni a cui la CGUE si è prontamente attivata per risolvere, su segnalazione dell'EDPS.

[380] il consenso ai cookie per sua natura è assai particolare; la fattispecie presenta soprattutto problemi di regolazione peculiari, causati dalla natura della navigazione sul web, vale a dire dalla sua velocità e complessità. *Annuario 2021, Osservatorio Giuridico sulla Innovazione Digitale*, (a cura di) S. ORLANDO, G. CAPALDO, Università La Sapienza, 2021, p.146

[381] l'Avvocato generale, nelle conclusioni a margine della richiamata decisione della Corte di Giustizia dell'Unione Europea, Grande Sezione, 1° ottobre 2019, causa C-673/17, attribuisce una rilevanza fondamentale agli obblighi informativi, sostenendo che «l'informazione chiara e completa implica che un utente sia in grado di stabilire agevolmente le conseguenze di eventuali consensi prestati. A tal fine, l'utente stesso dev'essere in grado di valutare gli effetti delle proprie azioni. Le informazioni fornite devono essere chiaramente comprensibili e non soggette ad ambiguità o interpretazione e devono essere sufficientemente dettagliate, in modo da consentire all'utente di comprendere il funzionamento dei cookie effettivamente impiegati» (punti 114-115 delle Conclusioni).

di profilazione, provocano il rischio di risultare inefficaci o comunque insufficienti al conseguimento dell'obiettivo della formazione di una volontà realmente consapevole dell'interessato.

Per evitare ciò, si dovrebbe allargare l'obiettivo sul generale modo di operare delle grandi compagnie tecnologiche nell'accesso, nella condivisione e nello sfruttamento dei dati personali sul mercato digitale; il mercato dei dati personali dovrebbe sempre ispirarsi ai principi di trasparenza, specie in relazione alle informazioni sulle finalità, sui destinatari e sui mezzi tecnologici che permettono l'elaborazione, e di correttezza delle operazioni di trattamento[382].

Per migliorare la disciplina riguardante il consenso ai *cookie*, inoltre, si dovrebbe eliminare quella asimmetria che fa sì che gli utenti abbiano a disposizione solo pochi secondi per fornire il consenso ad una notevole moltitudine di *cookie*.

La soluzione che renderebbe anche meno "ingombrante" la richiesta di consenso per i cookie potrebbe essere quella di unire le singole e specifiche scelte, che devono essere eseguite da capo per ogni sito, in una sola decisione precedente alla navigazione e diversa a seconda di macro-categorie di *cookie*, che sarebbero suddivisi in base alla finalità dello specifico trattamento[383].

---

[382] *«Si pensi alla manifesta ritrosia delle compagnie tecnologiche della Silicon Valley nel divulgare al mercato e all'opinione pubblica informazioni relative ai circuiti di destinatari e alle modalità con cui si svolge lo sfruttamento dei dati personali degli utenti, sovente celate dietro agli assunti (indimostrati) della complessità dell'algoritmo e dell'idea per cui una tecnologia libera da regole eteronome "massimizza" il benessere degli individui. Questa "mitologia" aziendale, riassunta infine nel refrain del too big to fail, non può non riportare drammaticamente alla mente le parole dei "sacerdoti" della finanza che, prima della crisi dei mutui subprime, pretendevano di giustificare il difetto di trasparenza del mercato finanziario sotto il parafulmine della complessità dei suoi prodotti e della rassicurazione che la cd. deregulation perseguisse il bene della società».*G. MARINO, *Internet e tutela dei dati personali: il consenso ai cookie,* in *Jus Civile,* 2020,2*,* cit*,* p.423.

[383] *Annuario 2021, Osservatorio Giuridico sulla Innovazione Digitale*, (a cura di) S. ORLANDO, G. CAPALDO, Università La Sapienza, 2021, pp. 154-155.

CAPITOLO QUINTO – FEEDBACK DEI MERCATI DIGITALI E BEST PRACTICES

La velocità, la costante crescita dell'evoluzione tecnologica e la globalizzazione comportano sicuramente nuove sfide per la protezione dei dati personali[384]. Di fatto si parla di un'economia *data driven* in cui i dati sono diventati le nuove materie prime; la portata e la condivisione della raccolta dei dati personali sta crescendo significativamente proprio perché la tecnologia oggi permette sia alle imprese private sia alle autorità pubbliche di sfruttare i dati personali nello svolgimento delle loro attività.

La tecnologia dovrebbe consentire una più libera circolazione dei dati personali all'interno dell'UE, e il loro trasferimento verso paesi terzi ed organizzazioni internazionali, ma dovrebbe assicurare anche un elevato livello di protezione dei dati personali.

Molto importante per tutte le attività produttive è che i dati raccolti siano validi; quindi, esatti e riconducibili ad una fonte verificabile, è fondamentale dunque trattare dati di alta qualità, adatti per gli obiettivi di *business*[385].

Infatti, dei dati di bassa qualità potrebbero causare una seria violazione del GDPR ed anche una inefficacia dei processi decisionali, con gravi effetti in termini di affidabilità e competitività delle imprese e delle amministrazioni pubbliche.

5.1 Sistema di gestione di qualità dei dati: affidabilità e competitività

Dunque, per poter essere competitivi è molto utile utilizzare un *Data Quality Management* (DQM), ovvero un processo di gestione della qualità dei dati per poter sempre avere dati personali affidabili per raggiungere gli obiettivi di business.

[384] Cons. 6 e 7 del Regolamento UE 2016/679 (GDPR)
[385] G. ALVERONE, *Gestione della qualità dei dati: best practice per garantire affidabilità e competitività aziendale*, in *Cybersecurity360*, 20 settembre 2021, online su https://www.cybersecurity360.it/soluzioni-aziendali/gestione-della-qualita-dei-dati-best-practice-per-garantire-affidabilita-e-competitivita-aziendale/

L’alta qualità dei dati personali che deriva proprio dal rispetto di principi stabiliti dal GDPR, crea sistemi produttivi attendibili, in quanto basati su valori essenziali di integrità, affidabilità, disponibilità, riservatezza e trasferibilità[386]; e affidabili perché degni di fiducia, centrale nelle relazioni commerciali.

Il GDPR e alcuni standard internazionali forniscono utili indicazioni per implementare e creare un processo di gestione della qualità dei dati.

Per costituire un DQM efficace, la persona fisica che pratica le funzioni di titolare del trattamento, supportato dal DPO, deve:

- Statuire un quadro chiaro dei ruoli e delle responsabilità, dunque “chi” fa “che cosa” ed entro quale tempo;
- Indicare le funzioni aziendali che hanno il compito di sviluppare il processo;
- Individuare un responsabile di processo;
- Dotarsi della tecnologia appropriata come piattaforme o applicazioni idonee;
- Determinare una chiara procedura per la gestione dei dati, che comprenda la raccolta, l’analisi, l’archiviazione, la filtrazione, l’aggregazione e la conservazione;
- Effettuare una valutazione riguardante il rischio per diritti e libertà fondamentali;
- Determinare gli indicatori chiave per la qualità (KPI);
- Istituire un documento che provi l’effettiva esecuzione di tutti i precedenti passaggi[387].

[386] Artt. 5, 20 e 32 del Regolamento UE 2016/679 (GDPR)
[387] G. ALVERONE, *Gestione della qualità dei dati: best practice per garantire affidabilità e competitività aziendale*, in *Cybersecurity360*, 20 settembre 2021, online su https://www.cybersecurity360.it/soluzioni-aziendali/gestione-della-qualita-dei-dati-best-practice-per-garantire-affidabilita-e-competitivita-aziendale/

La norma che fornisce un modello di riferimento per costituire un DQM è la ISO 8000-61: 2016 che può essere anche utilizzata in combinazione con la norma ISO 9001:2015.

La norma fissa i principi essenziali della gestione della qualità dei dati che sono: l'approccio per processi, secondo cui la gestione della qualità è assicurata dalla definizione e dallo sviluppo di specifici procedimenti che possono essere ripetibili ed affidabili; il miglioramento continuo derivante dall'analisi, dal tracciamento e dall'eliminazione dei fattori che causano scarsa qualità dei dati ed infine il coinvolgimento delle persone. Tale principio prevede che ad ottenere il maggiore effetto diretto sulla qualità dei dati siano gli utenti finali.

Infine, il processo di implementazione comprende quattro passaggi basati sul ciclo di Deming, secondo il modello PDCA[388]:

1. Data quality planning: per stabilire la strategia iniziale
2. Data quality control: garantisce che i dati ricavati dalle attività rispettino i requisiti necessari
3. Data quality assurance: per esaminare i livelli di qualità dei dati
4. Data quality improvement: per offrire miglioramenti sostenibili della qualità dei dati.

Una domanda che sorge spontanea è come poter bilanciare le esigenze del mercato con la tutela e la protezione dei dati personali. Di fatto, quando si tratta di circolazione dei dati personali, la normativa a protezione dei consumatori e quella riguardante la protezione della privacy tendono a scontrarsi[389].

Ovviamente, il consenso assume un ruolo fondamentale. L'utente ha il diritto di manifestare liberamente la propria volontà, ed ha anche la possibilità di revocarla in qualsiasi momento.

---

[388] Modello *plan-do-check-act*

[389] A. STURABOTTI, *Consenso al trattamento dei dati: come bilanciare privacy ed esigenze del mercato?,* in *Agenda Digitale*, 12 aprile 2022, online su *https://www.agendadigitale.eu/sicurezza/privacy/consenso-al-trattamento-dei-dati-come-bilanciare-privacy-ed-esigenze-del-mercato/*

Alcuni strumenti efficaci, che vanno al di là della prestazione o meno del consenso, per la protezione dei dati personali e quindi per una loro diffusione incontrollata, potrebbero essere: la previsione di regole di trattamento, vale a dire di limiti o divieti per alcune categorie di trattamento, previo inizio del trattamento stesso, oppure delle maggiori garanzie di anonimizzazione dei dati e regole di tipo tecnico interne al trattamento[390]. Difatti il rispetto dei requisiti di *protection by design*, quindi fin dalla progettazione, e *by default*, vale a dire per impostazione predefinita, rappresenta un punto essenziale nella promozione della tutela della privacy e della protezione dei dati personali.

L'EDPB ha elaborato delle raccomandazioni operative per poter correttamente applicare tali principi, adottando la versione finale delle Linee Guida riguardanti il tema della *data protection by design e by default*[391].

Per il Comitato innanzitutto è essenziale che i *data controllers* prendano seriamente la loro responsabilità in quanto i requisiti di protezione di dati personali *by design e by default* costituiscono un ruolo determinante nel processo di protezione di dati personali; essi, quindi, devono attuare gli obblighi stabiliti dal GDPR fin dalla fase di progettazione delle operazioni relative ai trattamenti di dati personali.

Le Linee Guida elaborate dall'EDPB hanno lo scopo di fornire un orientamento generale riguardante l'obbligo di attuare tali requisiti, come previsto dall'art. 25 del GDPR. L'obbligo riguarda la totalità dei titolari del trattamento, senza considerare dimensioni e complessità del trattamento. Di conseguenza è importante che il *data controller* colga tali principi, vale a dire la loro portata, i diritti e le libertà concesse ai *data subjects*; l'obbligo prioritario è rappresentato dall'adozione di

---

[390] I.A. CAGGIANO, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo (GDPR) e analisi comportamentale. Iniziali spunti di riflessione*, in *Diritto Mercato Tecnologia,* 2017.
Regole tecniche sono previste già nel GDPR, con la cosiddetta privacy by design (art.25 del Regolamento e art. 33, 34, 35 e 36 del Codice Privacy) e con la promozione di meccanismi e organismi di certificazione della privacy (art. 42 del Regolamento). Gruppo di lavoro articolo 29 per la Protezione dei dati, Parere 05/2014 sulle tecniche di anonimizzazione, 10 aprile 2014.
[391] EDPB, Guidelines 4/2019 on Article 25, Data Protection by Design and by Default, 20 ottobre 2020.

misure tecniche ed organizzative idonee e di garanzie che hanno lo scopo di assicurare *by design e by default* una adeguata attuazione dei principi di *data protection* e dunque i diritti e le libertà dei soggetti interessati[392].

Come stabilisce l'art. 25 del GDPR, infatti, il titolare del trattamento ha il dovere di attuare misure tecniche ed organizzative adeguare, come ad esempio la pseudonomizzazione, e a integrare nel trattamento garanzie utili a soddisfare i principi in materia di protezione dei dati personali previsti dal GDPR, tutelando i diritti e le libertà dell'interessato.

Facendo riferimento al principio di *accountability*, il titolare del trattamento deve poter dimostrare di aver adottato misure di sicurezza idonee. Inoltre, egli ha il dovere di istituire misure tecniche ed organizzative per far in modo che solo i dati personali necessari per ogni determinata finalità del trattamento, siano trattati tramite impostazione predefinita. Questo vincolo riguarda la quantità di dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità.

Tali misure tecniche ed organizzative appropriate e garanzie necessarie possono essere considerate in senso lato come qualunque metodo o mezzo che può essere utilizzato dal titolare nel trattamento; esse devono essere "appropriate" nel senso che devono essere idonee a raggiungere lo scopo di assicurare i principi di protezione dei dati.

Dunque, una misura tecnica e organizzativa può essere di vari tipi, come l'adozione di soluzioni tecniche avanzate, la formazione del personale, la pseudonomizzazione dei dati personali, la memorizzazione dei dati in un formato strutturato e comunemente leggibile da un computer, l'uso di sistemi di rilevamento *malware*, ecc.

---

[392] F. MISTRETTA, *Data protection by design e by default, best practice e raccomandazioni operative*, in *Cybersecurity360*, 11 novembre 2020, online su *https://www.cybersecurity360.it/legal/privacy-dati-personali/data-protection-by-design-e-by-default-best-practice-e-raccomandazioni-operative/*

Per cui gli *standard*, le *best practice* e i codici di condotta che vengono riconosciuti da associazioni ed altri organismi rappresentanti le categorie di *data controllers*, possono fornire un aiuto per stabilire le misure appropriate. Ovviamente è poi essenziale che il titolare del trattamento verifichi l'adeguatezza delle misure che intende adottare, tenendo in considerazione il trattamento in questione.

L'art. 25 del GDPR deve essere letto in combinazione con l'art. 5 dello stesso Regolamento che stabilisce i principi generali che si applicano al trattamento dei dati personali. Si ricorda infatti che i dati personali devono essere:

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»).»

Dunque, l'adozione di misure tecniche ed organizzative appropriate è finalizzata all'effettiva attuazione di ogni principio citato dall'art.5.

Il *data controller* deve poter dimostrare, secondo il principio di *accountability*, di avere posto in essere tutte le misure tecniche d organizzative che hanno lo scopo di garantire il rispetto dei principi sanciti dal GDPR. Per tale scopo il data controller può promuovere la raccolta dei cosiddetti *key performance indicators* (KPI) per provare l'efficacia con cui si assicura la protezione dei dati.

Questi indicatori possono essere quantitativi, come la diminuzione di reclami o il minor tempo di risposta nel caso in cui gli interessati esercitino i loro diritti, o qualitativi, per esempio la valutazione di prestazioni o le valutazioni di esperti. Essi sono essenziali per il disegno di un buon DQM[393]; fanno riferimento innanzitutto all'unicità del dato; inoltre riguardano anche la completezza e l'integrità del dato, la tempestività e la disponibilità dei dati quando sono necessari, la coerenza per assicurare che durante la trasmissione tra applicazioni e reti i dati mantengano il medesimo valore, ed infine l'accuratezza, quindi il livello di corrispondenza del dato teorico con il dato reale.

Oltre a questi mezzi, il *data controller* può mostrare il rispetto dei principi fornendo la logica che si trova alla base dell'*assessment* dell'efficacia delle misure e delle garanzie selezionate[394].

---

[393] G. ALVERONE, *Gestione della qualità dei dati: best practice per garantire affidabilità e competitività aziendale*, in *Cybersecurity360*, 20 settembre 2021, online su https://www.cybersecurity360.it/soluzioni-aziendali/gestione-della-qualita-dei-dati-best-practice-per-garantire-affidabilita-e-competitivita-aziendale/

[394] All'art. 25, comma 1 del GDPR vengono elencati gli elementi che il titolare del trattamento deve considerare quando determina le misure di un trattamento specifico

Tutti gli elementi riportati concorrono a determinare l'idoneità di una misura ad attuare in modo efficace i principi stabiliti dal GDPR. Il *data controller* innanzitutto deve tenere presente i progressi della tecnologia disponibile sul mercato per scegliere le misure più efficaci; deve perciò possedere una conoscenza approfondita e aggiornata riguardanti i progressi tecnologici per comprendere come la tecnologia può avere effetti sulle operazioni di trattamento dati e per capire come migliorare le misure di sicurezza che garantiscono i principi e i diritti degli interessati[395].

Un altro elemento che il *data controller* deve tenere presente nella scelta delle misure è fornito da "la natura, l'ambito di applicazione, il contesto e le finalità del trattamento". Mentre il concetto di "natura" fa riferimento alle caratteristiche intrinseche del trattamento, "l'ambito di applicazione" riguarda le dimensioni e la gamma del trattamento. Il "contesto" rappresenta le circostanze che contrassegnano il trattamento e che potrebbero avere effetti sulle aspettative dell'interessato; infine, le "finalità" concernono i fini del trattamento.

Quarto elemento stabilito sempre dall'art. 25 è rappresentato dai "rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche derivanti dal trattamento". Quindi il *data controller* ha il dovere di identificare i rischi che una potenziale violazione dei principi causerebbe ai diritti degli interessati, e deve stabilire quindi la loro probabilità e gravità per poter utilizzare le misure finalizzate a ridurre o eliminare i rischi[396].

Il quinto elemento è l'aspetto temporale; il GDPR prevede infatti che la protezione dei dati venga eseguita "sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso"[397]. Quindi nel determinare i mezzi si fa

[395] Criterio dello stato dell'arte. L'assenza di conoscenza e di aggiornamento degli sviluppi tecnologici attuali potrebbe tradursi in un mancato rispetto dell'articolo 25.
[396] A tale riguardo, si ricorda che le Linee Guida dell'EDPB si focalizzano sul se un'operazione di trattamento può comportare o meno un rischio elevato per l'interessato e forniscono orientamenti su come valutare i potenziali rischi emersi.
[397] Con "all'atto del trattamento stesso" il legislatore intende sottolineare che, quando il trattamento è cominciato, il *data controller* ha il dovere di garantire la protezione dei dati sia *by design* sia *by default,* rivalutando il livello di rischio; questo perché la natura, la portata, il contesto ed il rischio possono mutare durante il trattamento, motivo per cui il *data controller*

riferimento al periodo in cui il data controller individua le modalità in cui il trattamento sarà eseguito e le misure di sicurezza più idonee.

Gli obblighi di mantenere, rivedere ed aggiornare il trattamento si devono applicare anche ai sistemi posti in essere prima dell'entrata in vigore del GDPR.

Il GDPR, come già anticipato, prevede anche la protezione *by default* dei dati, vale a dire per impostazione predefinita. L'art. 25, comma 2 specifica infatti che «*il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento*». Per "impostazione predefinita" si intendono le scelte riguardanti le opzioni di configurazione impostati in un *processing system* come *software, device* o procedure di elaborazione manuale.

Il *data controller* ha il compito di scegliere ed essere responsabile della realizzazione delle impostazioni predefinite in un trattamento in modo che sia lecito solamente il trattamento strettamente necessario al raggiungimento delle finalità predeterminate. Dunque, per impostazione predefinita, il titolare del trattamento non può raccogliere, trattare ed infine conservare dati più dello stretto necessario e dei fini prestabiliti.

Per identificare i soli dati necessari al raggiungimento dello scopo delineato, sono utili le Linee Guida riguardanti la "valutazione della necessità e della proporzionalità delle misure che limitano il diritto alla protezione dei dati personali"[398].

Le autorità di controllo detengono una serie di poteri correttivi in base all'art. 58 del GDPR, per verificare il rispetto dell'art. 25. Esse hanno il potere di:

a. emettere degli avvertimenti al titolare del trattamento o al responsabile del trattamento;
b. emettere degli ammonimenti;

deve riesaminare il trattamento attraverso revisioni e valutazioni periodiche per poter confermare l'efficacia delle misure e delle garanzie adottate.

[398] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.

c. ingiungere un ordine per garantire il rispetto dei diritti dei soggetti interessati;
d. imporre una limitazione provvisoria o definitiva al trattamento (incluso il divieto di trattamento);
e. infliggere una sanzione amministrativa pecuniaria i sensi dell'articolo 83;
f. ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

5.2 Le linee guida dell'EDPB

L'EDPB ha elaborato una serie di raccomandazioni ai *data processor* e ai *data controllers* per rendere più facile e per migliorare la concretizzazione dei principi di protezione dei dati *by design* e *by default*.

Innanzitutto, sottolineano come sia importante che il titolare del trattamento pensino alla protezione dei dati fin dalle prime fasi di pianificazione di un trattamento; inoltre nel caso il titolare usufruisse d DPO, l'EDPB suggerisce un coinvolgimento attivo dello stesso per poter integrare la protezione *by design* e *by default* anche nelle procedure di procurement e sviluppo e non solo nel corso del trattamento. L'EDPB, per di più, suggerisce al producer di dimostrare che la *data protection* by design e by default è assicurata, attraverso una certificazione; la sua presenza, infatti, potrebbe influenzare i *data subjects* nelle loro scelte tra i diversi beni e servizi. Ottenere un trattamento certificato rappresenta quindi un vantaggio competitivo per i produttori, per i responsabili e i titolari del trattamento. Inoltre, può anche far aumentare la fiducia dei soggetti interessati nei confronti del trattamento di dati personali.

I *data controllers* dovrebbero scegliere solo quei sistemi che gli permettono di rispettare l'art. 25, dato che sono appunto i data controllers ad essere responsabili della mancata attuazione dell'articolo.

Inoltre, i producers e i data processors, dovrebbero garantire in modo attivo che i criteri per lo "stato dell'arte" siano rispettati e far presente ai *data controllers* le

potenziali modifiche dello stato dell'arte dato che potrebbero influire sull'efficacia delle misure adottate.

Il Comitato raccomanda ai data controllers di pretendere che produttori e data processors provino in che modo i loro hardware, software, servizi o sistemi permettano di rispettare i requisiti di responsabilità stabiliti per la protezione *by design* e *by default* dei dati, ad esempio utilizzando specifici *key performance indicators* per verificare l'efficacia delle misure scelte.

Infine, l'EDPD chiede ai titolari del trattamento di essere leali nei confronti degli interessati e di mostrare in modo trasparente il modo in cui essi valutano e assicurano la *data protection by design e by default*, rispettando quindi il principio di accountability stabilito dal GDPR[399].

5.3 Il Regolamento UE sulla ePrivacy: i cambiamenti per il marketing digitale

Ancora oggi gli obiettivi prestabiliti dal GDPR non si sono compiuti a pieno, esso ha comportato nuovi adempimenti e modelli di gestione di dati personali per imprese ed istituzioni che hanno modificato i precedenti assetti.

In campo digitale stanno per aggiungersi ulteriori tasselli con l'entrata in vigore del Regolamento ePrivacy. Di fatto negli ultimi anni il GDPR ha cercato di colmare alcune lacune lasciare dalla direttiva ePrivacy del 2002; la direttiva regolava la riservatezza in rete e nelle comunicazioni elettroniche ma gli sviluppi tecnologici degli ultimi vent'anni hanno fatto sì che essa non fosse più sufficiente. La normativa, infatti, non era più adatta a proteggere gli utenti dai rischi attuali.

Il GDPR non ha potuto provvedere completamente a colmare queste lacune perché la materia in questione richiede una legge apposita; il 10 febbraio del (2021) finalmente, dopo circa quattro anni di lavori, il Consiglio UE ha approvato il testo

[399] F. MISTRETTA, *Data protection by design e by default, best practice e raccomandazioni operative*, in *Cybersecurity360*, 11 novembre 2020, online su *https://www.cybersecurity360.it/legal/privacy-dati-personali/data-protection-by-design-e-by-default-best-practice-e-raccomandazioni-operative/*

finale del nuovo Regolamento UE che andrà a sostituire la direttiva e-Privacy. Il Regolamento tutelerà tutti gli utenti che si trovano nel territorio UE, inoltre si estenderà anche a tutte le OTT, anche estere, che comprendono nelle proprie attività quegli utenti.

I settori che saranno maggiormente interessati sono quello del digital marketing, dell'*Internet of Things*, dell'intelligenza artificiale, il *Machine-to-machine*, la messaggistica istantanea e le applicazioni[400].

Dunque, cosa stabilisce il nuovo Regolamento UE? Esso si è posto lo scopo di aumentare la fiducia dei cittadini nei confronti dei servizi digitali, garantendo la massima riservatezza per i dati personali nelle comunicazioni elettroniche. Questo si verificherebbe impedendo a soggetti diversi dai diretti destinatari di ascoltare, monitorare o trattare tali dati.

Questi diritti però devono trovare un punto di equilibrio con la libera circolazione dei dati e dei servizi di comunicazione elettronica nell'UE, per questo motivo sono presenti delle eccezioni permette per il trattamento di dati che possono agevolare fornitori e utilizzatori di questi servizi.

Di fatto i dati personali potranno essere sottoposti a trattamento se fosse necessario per la realizzazione della trasmissione della comunicazione oppure per «mantenere o ripristinare la sicurezza delle reti e dei servizi di comunicazione elettronica o rilevare problemi e/o errori tecnici nella trasmissione di comunicazioni elettroniche»[401]; ovviamente questo esclusivamente per la durata necessaria a tali finalità. Inoltre, il trattamento dei metadati[402] è consentito esclusivamente

---

[400] S. CORSI, *Il nuovo Regolamento UE sulla e-privacy. Cosa cambierà per il marketing digitale,* in *Cyberlaw*s, 17 febbraio 2021; online su *https://www.cyberlaws.it/2021/nuovo-regolamento-ue-e-privacy-marketing-digitale/*

[401] Art. 6, punto 1, lett. b) della Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche).

[402] Art. 4 punto 3 lett. C «*metadati delle comunicazioni elettroniche: i dati trattati in una rete di comunicazione elettronica per trasmettere, distribuire o scambiare il contenuto delle comunicazioni elettroniche compresi i dati usati per tracciare e identificare la fonte e il destinatario di una comunicazione, i dati relativi alla localizzazione del dispositivo generati nel*

per obblighi giuridici, di fatturazione o prevenzione di uso fraudolento o abusivo dei servizi di comunicazione elettronica, o dopo aver ottenuto il consenso dell'utente per determinate e specifiche finalità.

Infine, il contenuto delle comunicazioni elettroniche potrà essere sottoposto a trattamento a fini dell'erogazione di un servizio all'utente finale, se egli presta il consenso per determinate finalità o se tutti gli utenti finali interessati acconsentono a uno o più fini specifici, che non potrebbero essere conseguiti attraverso il trattamento anonimizzato delle informazioni, con precedente consultazione del fornitore con l'autorità di controllo di competenza.

Dunque, cosa comporta per chi si occupa di marketing digitale?

Tra i casi appena citati, nelle specifiche finalità a cui l'utente può acconsentire, rientra anche quello del trattamento per fini commerciali. In questo caso però si pone un requisito fondamentale, presente già anche nel GDPR, ma che col nuovo Regolamento acquista maggiore importanza. Si tratta dell'anonimizzazione delle informazioni. Questo significa che per poter trattare i dati che scorrono in rete e nelle comunicazioni elettroniche, è necessario munirsi di strumenti che permettano di anonimizzarli; altrimenti il trattamento dovrà essere subordinato al consenso dell'utente ma anche essere sottoposto ad una specifica consultazione con le autorità di controllo[403]. Dunque, per non appesantire la mole di lavoro, sarebbe meglio avvalersi fin da subito di strumenti per anonimizzare i dati, in modo da poter continuare le campagne di marketing digitale ed offrire maggiore tutela agli utenti.

Il testo finale del Regolamento è preceduto da una relazione, la quale sottolinea l'importanza di un intervento sulla "centralizzazione del consenso" della *cookie technology*. Lo scopo è quello di liberare gli utenti dalla cosiddetta "stanchezza

contesto della fornitura di servizi di comunicazione elettronica nonché la data, l'ora, la durata e il tipo di comunicazione».

[403] Nel caso non ci possa essere una profilazione anonimizzata dei dati, chi compie tale operazione dovrebbe consultarsi con il Garante (come previsto dall'art. 36 del GDPR).

da *cookie banner*"[404], in modo da appesantire meno la navigazione degli utenti tra i siti web. Per raggiungere questo fine viene quindi suggerito di impostare una white list, un sistema di protezione della vita privata sempre attivo e preimpostato. Ovviamente gli utenti che vorrebbero partecipare a questa opportunità, devono essere informati chiaramente e precisamente in modo da poter effettuare una scelta consapevole e libera che possono comunque modificare in qualsiasi momento.

Una problematica potrebbe però riscontrarsi nel fatto che l'istituzione non sarà un obbligo ma solamente una libera scelta. Inoltre, non è chiarito quale soggetto, tra i browser, i motori di ricerca, i singoli siti web o gli utenti deve prendere in carica l'implementazione della *white list*.

Dal punto di vista di un'azienda, questo potrebbe comportare degli ostacoli in ambito digitale e dei rallentamenti nella realizzazione degli obiettivi di *marketing*.

D'altra parte, dal punto di vista degli utenti, essi potrebbero ottenere livelli di tutela differenti tra loro, in base alle singole giurisdizioni nazionali e ai diversi browser e motori di ricerca impiegati.

Dunque, le giurisdizioni nazionali dovrebbero scegliere se far diventare la white list un obbligo o una semplice best practice. Potrebbe quindi venire a mancare un'armonizzazione in tal senso a livello europeo. Ci si troverebbe in presenza di un quadro estremamente diversificato, a livello statale e tecnologico; di conseguenza verrebbero a mancare i principi di semplificazione e proporzionalità a cui si ispira il Regolamento.

C'è da sottolineare anche che quella della white list che potrebbe apparire a prima vista come una semplificazione a vantaggio e tutela dell'utente, potrebbe comunque trasformarsi in un nulla di fatto: infatti se l'utente decidesse di non inglobare nella sua *white list* i *cookie* di marketing o di terze parti[405], il

[404] S. CORSI, *Il nuovo Regolamento UE sulla e-privacy. Cosa cambierà per il marketing digitale,* in *Cyberlaw*s, 17 febbraio 2021; online su *https://www.cyberlaws.it/2021/nuovo-regolamento-ue-e-privacy-marketing-digitale/*

[405] Si tratta di una scelta che probabilmente effettuerebbe la maggioranza degli utenti.

Regolamento permetterebbe comunque al sito web di proporre il cookie banner per chiedere il consenso.

Dunque, l'utente si ritroverebbe nuovamente una costante riproposizione dei banner, situazione che il Regolamento avrebbe voluto evitare.

Per di più, mettiamo caso che l'utente decidesse di default di acconsentire ai cookie con scopi di marketing, allora il titolare del sito web dovrebbe ritenere reale l'interesse per finalità di marketing dell'utente che sta navigando? In questo modo, il dato di tracciamento impostato che è fondamento di specifiche campagne di marketing, non potrebbe essere considerato del tutto affidabile e si finirebbe per indirizzare risorse ed energie verso utenti che non sono realmente interessati.

Quando si effettua un bilancio dei possibili costi e benefici sull'effetto della nuova normativa nell'economia digitale è necessario tenere a mente tutto ciò.

Per superare queste problematiche relative ai cookie, alcuni soggetti come Google, Firefox e Safari stanno sperimentando delle tecniche alternative di tracciamento rispetto ai *cookie*.

Queste tecnologie si fonderanno su un sistema di tracciamento anonimizzato e machine learning, che avrà lo scopo di ottenere risultati di profilazioni equiparabili a quelli realizzabili coi i *cookie*, considerati ormai una tecnologia obsoleta e poco rispettosa della protezione dei dati personali.

Come già sottolineato, l'anonimizzazione dei dati contribuirebbe ad ottenere una maggiore riservatezza dei dati personali nel mondo digitale, come richiesto dal Regolamento ePrivacy, in modo più efficace e bilanciandoli anche con le esigenze dell'economia digitale.

CONCLUSIONI

Possiamo affermare quindi che la rete Internet ha pervaso le nostre vite, modificando le abitudini quotidiane di ciascuno di noi, si è imposta con prepotenza nella nostra quotidianità costringendoci a rimettere in discussione alcuni valori, morali ed economici, della nostra società.

Le tecnologie digitali hanno determinato un processo di trasformazione che sta dominando i cambiamenti economici e sociali di questo secolo; la tecnologia digitale ha dato il via nella società odierna a delle trasformazioni di portata epocale che hanno comportato lo sviluppo di un vero e proprio "ecosistema digitale". Al centro di questo processo di trasformazione si trovano le nuove materie prime, vale a dire i dati personali, che sono diventate una nuova fonte di ricchezza molto importante nell'epoca del capitalismo digitale.

Ecco perché è diventato così importante assicurare la tutela dell'interessato che presta il consenso al trattamento dei suoi dati.

Questa tesi ha illustrato quante insidie si possono nascondere dietro questa realtà, mostrando quanto sia importante essere consapevoli delle azioni che si compiono e di cosa significa essere pienamente informati sulle conseguenze della prestazione del consenso al trattamento dei nostri dati personali.

La tecnologia, che sta sviluppando tecniche sempre più innovative, dovrebbe da una parte permettere una più libera circolazione dei dati personali all'interno dell'UE, e il loro trasferimento verso paesi terzi ed organizzazioni internazionali, ma, dall'altra dovrebbe anche assicurare anche un elevato livello di tutela dei dati personali.

Tale obiettivo è perseguito con costante impegno da parte dell'Unione Europea, che nel corso degli anni ha istituito regole e normative sempre più coerenti con lo scopo di proteggere e tutelare i dati personali dei cittadini, tenendo conto dei nuovi sviluppi digitali.

D'altra parte, però sta anche ai cittadini che navigano in rete comprendere le conseguenze delle loro azioni e capire quanto importante sia l'atto di prestazione

del proprio consenso e quanto impegno giuridico si nasconde nelle operazioni di richiesta del consenso per il trattamento di dati personali.

È da tenere presente che il diritto alla protezione dei dati personali è un diritto fondamentale dell'individuo, sancito dall'articolo 8 della Carta dei Diritti Fondamentali dell'Unione Europea, e per questo deve essere tutelato con il massimo impegno.

Negli ultimi anni è stato posta l'attenzione sulle difficoltà che il processo di integrazione giuridica europea sta percorrendo, ma con riferimento al tema della protezione dei dati personali, tale affermazione non può trovare un riscontro.

Infatti, lo sviluppo e la diffusione di un sistema integrato di tutela e salvaguardia dei dati rimane un obiettivo primario dell'Unione. Specialmente negli ultimi anni in Europa sono stati messi in atto progressi evidenti nel campo del diritto alla protezione dei dati personali, in particolar modo con il Regolamento generale sulla protezione dei dati. L'adozione, infatti, di una disciplina generale, mediante un atto vincolante come un regolamento, è parsa a molti la soluzione più adeguata alle dinamiche di oggi, caratterizzato dall'incessante evoluzione del contesto in cui si trova il diritto alla protezione dei dati.

Esso aveva lo scopo di offrire un'adeguata garanzia giuridica, una semplificazione amministrativa, oltre che alla maggiore tutela nel trattamento e nel trasferimento di dati personali. Si può sostenere che a differenza della normativa degli anni precedenti, il Regolamento pone al centro della protezione dei dati personali soprattutto il trattamento e le relative misure di sicurezza, con un importante ruolo svolto dalla prestazione del consenso dell'interessato e del rispetto dei requisiti di liceità.

Di fatto vi sono ancora alcuni limiti da superare, specialmente riguardanti la possibilità di interpretare i dati personali come un corrispettivo diverso dal denaro.

La presente tesi chiaramente non può mostrare un punto di arrivo della materia, ma ha l'obiettivo di mostrare un percorso in continua evoluzione, tutt'oggi in corso.

Le sfide future da affrontare riguardano sicuramente gli sviluppi tecnologici e di conseguenza anche le nuove frontiere che potrebbero determinare nel campo

dei dati per scopi di marketing o pubblicità. Altro aspetto problematico concerne l'allargamento dei confini di flusso di dati all'intero mondo, vale a dire la globalizzazione dell'informazione.

Se esistono ancora molti dilemmi da affrontare, è pur vero che il legislatore europeo è attento e pronto a rispondere alle nuove sfide apportate dai cambiamenti tecnologici, con l'obiettivo principale di garantire prima di tutto la protezione dei dati dei cittadini.

BIBLIOGRAFIA

Manuali:

- A. BIASIOTTI, *ABC del trattamento dei dati personali*, EPC srl, Roma, 2020
- A. DE FRANCESCHI, *La circolazione dei dati personali tra privacy e contratto,* Edizioni Scientifiche Italiane, Napoli, 2017
- A. PISAPIA, *La tutela per il trattamento e la protezione dei dati personali*, G. Giappichelli Editore, Torino, 2018
- A. QUARTA, G. SMORTO, *Diritto privato dei mercati digitali*, Le Monnier Università, Firenze, 2020
- *Annuario 2021, Osservatorio Giuridico sulla Innovazione Digitale*, (a cura di) S. ORLANDO, G. CAPALDO, Università La Sapienza, 2021
- C. ANGIOLINI, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, G. Giappichelli Editore, Torino, 2020
- C. FOCARELLI, *La privacy. Proteggere i dati personali oggi*, Il Mulino, Bologna, 2015
- C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Giappichelli Editore, Torino, 2021
- F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, G. Giappichelli Editore, Torino, 2018
- F. PIZZETTI, *Privacy e diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, G. Giappichelli Editore, Torino, 2018
- F. SALMI, F. SAPORITI, *GDPR e sanzioni. Guida ai principali provvedimenti dei garanti europei: come evitare le contestazioni*, Key Editore, Milano, 2021
- G. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Zanichelli Editore, Bologna, 2012

- G. OPPO, *Sul consenso dell'interessato*, in CUFFARO, RICCIUTO, ZENO-ZENCOVICH (a cura di), *Trattamento dei dati e tutela della persona*, Giuffrè, 1999
- M. MARTORANA, *La privacy al passo con il regolamento UE 2016/679. Esperienze applicative dei principi del GDPR nella governance aziendale,* Key Editore, 2022
- M. SOFFIENTINI, *Privacy. Protezione e trattamento dei dati*, Ipsoa, Vicenza, 2018
- O. POLLICINO, E. BERTOLINI, V. LUBELLO, *Internet: regole e tutela dei diritti fondamentali,* Aracne editrice S.r.l., Roma, 2013
- R. I. D'AFFLITTO, Rapporto Privacy 2021, Temi e dibattiti sulla protezione dei dati personali, Key Editore, Milano, 2022
- S. RODOTÀ, *Conclusioni, in Trattamento dei dati personali e tutela della persona*, a cura di V. CUFFARO-V. RICCIUTO-V. ZENO ZENCOVICH, Giuffrè, 1999
- S. RODOTÀ, *Tecnologie e diritti,* Il Mulino, Bologna, 1995
- V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, *I dati personali nel diritto europeo*, G. Giappichelli Editore, Torino, 2019

Articoli di riviste:

- A. MANTELERO, *Big Data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Il Diritto dell'Informazione e dell'Informatica, (*2012)1
- A. MANTOVANI, *Questioni relative al trattamento dei dati personali per finalità di marketing e profilazione*, in *Media Laws, Rivista di Diritto dei Media, (2019)3*
- A. R. POPOLI, I cookies e il commercio elettronico: indagine sulla effettiva conoscenza delle problematiche connesse alla privacy, in Bocconi Legal Papers, online su http://bocconilegalpapers.org

- A. STURABOTTI, *Consenso al trattamento dei dati: come bilanciare privacy ed esigenze del mercato?,* in *Agenda Digitale*, 12 aprile 2022
- B. PARENZO, *Dati personali come "moneta". Note a margine della sentenza TAR Lazio n.260/2020,* in *Juscivile*, (2020)5.
- D. BERGEMANN, A. BONATTI, *Markets for Information: An Introduction*, Cowles Foundation Discussion paper no. 2142, August 2018
- F. BANTERLE, *Data Ownership in the Data Economy: A European Dilemma*, in *SSRN Electronic Journal*, gennaio 2018
- F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa Europa,* (2021)1
- F. MISTRETTA, *Data protection by design e by default, best practice e raccomandazioni operative*, in *Cybersecurity360*, 11 novembre 2020
- G. ALVERONE, Gestione della qualità dei dati: best practice per garantire affidabilità e competitività aziendale, in Cybersecurity360, 20 settembre 2021
- G. MARINO, *Internet e la tutela dei dati personali: il consenso ai cookie*, in *Jusvicile*, (2020)2
- G. RESTA, *Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali* in *Riv. crit. dir. priv.*, n.2, 2000, p.307.
- https://www.devita.law/il-valore-dei-dati/ SEC, *Facebook, Inc. 10-K Annual Report for the Fiscal Year Ended December 31, 2012.*
- I.A. CAGGIANO, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo (GDPR) e analisi comportamentale. Iniziali spunti di riflessione*, in *Diritto Mercato Tecnologia,* 2017
- L. LADECOLA, *Dati personali come corrispettivo per servizi digitali, da oggi è possibile,* in *Altalex*, 2021
- L. SIMONA, *Dati personali in cambio di contenuto digitale e di servizi digitali: la Direttiva 2019/770/UE*, in *Diritto di Internet*, 2019.

- L. TOSONI, *Cookie: l'impatto della sentenza della Corte UE che bandisce le caselle di spunta preselezionate*, in *Agenda Digitale,* 3 ottobre 2019
- M. FERRARI, *Facebook non è gratis: l'utente "paga" il servizio con i propri dati personali*, in *Altalex*, 14 aprile 2021
- M. GAMBINI, *La protezione dei dati personali come diritto fondamentale della persona: meccanismi di tutela*, in *ESPAÇO JURÍDICO*, (2013)
- Politecnico Milano, school of management "Strategic Data Science: time to grow up!", 19 novembre 2019
- *Professione scienziato del dato*, in *Il Sole 24 Ore*, (2014)
- R. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. Priv*., 1998
- R. SAVELLA, M. MARTORANA, *Direttiva UE 2019/770: è possibile "pagare con i dati"?,* in *Altalex*, 2021
- S. CORSI, *Il nuovo Regolamento UE sulla e-privacy. Cosa cambierà per il marketing digitale,* in *Cyberlaw*s, 17 febbraio 2021
- S. FRIER *Is Apple Really Your Privacy Hero?,* in Bloomberg Businessweek, 2018
- S. PATTI, *Il consenso dell'interessato al trattamento dei dati personali*, in *Riv. dir. Civ*., 1999
- S. SICA, *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in *Riv. Dir. Civ*., 2001
- S. THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in *Media Laws, Rivista di Diritto dei Media*, (2019) 3
- S. THOBANI, *Operazioni di tying e libertà del consenso*, in *Giur. it*., 2018, p.537.
- SULLIVAN, How Much is Your Playlist Worth?, in Wired News, 1999
- V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Dir. inf. inform*., 2018
- V. Z. ZENCOVICH, *Do "data markets" exist?*, in *Media Laws*, 2019

- W.C.Y. LI, M. NIREI, K. YAMANA, *Value of Data: There's No Such Thing as a Free Lunch in the Digital Economy*, Discussion papers 19022, Research Institute of Economy, Trade and Industry, 2019

Fonti normative:

- AGCM, provv. del 29 novembre 2018, n.27432
- Carta dei diritti fondamentali dell'Unione Europea (CDFUE)
- Cass. Civ., provv. 17278/2018
- Causa C-203/02, St. della Corte (grande sezione) del 9 novembre 2004; The British Horseracing Board Ltd e altri contro William Hill Organization Ltd.
- Cisco Annual Internet Report (2018–2023) White Paper, 2020
- Comunicazione UE (2020)86, *Una strategia Europea per i Dati*
- Cons. St. sentenza 29 marzo 2021, n.2631
- Consiglio d'Europa, Convenzione di Budapest sulla criminalità informatica del 23 novembre 2001
- Convenzione europea dei diritti dell'uomo e delle libertà fondamentali (CEDU), ratificata dall'Italia nel 1955
- Corte di Giustizia dell'Unione Europea, sentenza della Corte (Grande Sezione), 13 maggio 2014
- Corte di Giustizia dell'Unione Europea, sentenza della corte (Grande sezione),1° ottobre 2019, Causa C-673/17
- Corte di giustizia dell'Unione europea, sentenza della corte, 29 luglio 2019, Causa C-38/18 - Gambino; Hyka
- D.Lgs. n. 101/2018
- Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio, del 20 maggio 2019
- Direttiva 2002/58/CE del Parlamento europeo e del consiglio del 12 luglio 2002

- EDPB, Guidelines 4/2019 on Article 25, Data Protection by Design and by Default, 20 ottobre 2020.
- EDPB, *Linee guida 5/2020 sul consenso ai sensi del Reg (UE) 2016/679*, 4 maggio 2020
- European Dara Protection Supervisor, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content
- Garante per la protezione dei dati personali, *Linee guida cookie e altri strumenti di tracciamento*, n. 231, 10 giugno 2021
- Garante per la Protezione dei Dati Personali, provvedimento del 25 settembre 2014, n.427
- GRUPPO DI LAVORO ARTICOLO 29, Linee-guida sui responsabili della protezione dei dati (RPD), 13 dicembre 2016
- Parere del Comitato economico e sociale europeo sullo «Scambio e protezione dei dati personali in un mondo globalizzato» COM(2017) 7
- Proposta di Regolamento del Parlamento Europeo e del Consiglio del 10 gennaio 2017, relativa al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE
- Provvedimento del 28 maggio 1997, Istituti di credito Criteri generali in materia di informativa e richiesta del consenso dell'interessato, in *Corr. Giur*., 1997
- Provvedimento n. 229 dell'8 maggio 2014 del Garante per la protezione dei dati personali, *Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie*.
- Regolamento UE 2016/679 (GDPR)
- Tar Lazio, Sez. I, 10 gennaio 2020, n.260

SITOGRAFIA

- *http://bocconilegalpapers.org*
- *http://bocconilegalpapers.org*
- http://content.time.com/time/magazine/article/0,9171,2058205,00.html
- http://images.processopenaleegiustizia.it/f/sentenze/documento_imAFh_ppg.pdf
- http://radar.oreilly.com/2010/06/what-is-data-science.html
- *https://curia.europa.eu/jcms/jcms/j_6/it/*
- *https://ec.europa.eu/info/index_it*
- *https://edpb.europa.eu/edpb_it*
- *https://european-union.europa.eu*
- *https://european-union.europa.eu/index_it*
- https://st.ilsole24ore.com
- *https://www.agcm.it/*
- *https://www.agendadigitale.eu*
- *https://www.altalex.com/documents/news/2021/10/06/direttiva-ue-2019-770-possibile-pagare-con-dati*
- *https://www.cortedicassazione.it/corte-di-cassazione/*
- *https://www.devita.law/il-valore-dei-dati/ SEC*
- *https://www.garanteprivacy.it/*
- *https://www.ipsoa.it/documents/impresa/contratti-dimpresa/quotidiano/2021/11/29/contratti-fornitura-contenuto-digitale-nuove-disposizioni-vigore-1-gennaio-2022*
- *www.treccani.it*

RINGRAZIAMENTI

Ringrazio innanzitutto la mia famiglia per avermi sempre sostenuta. In particolare ringrazio i miei genitori, i miei pilastri, per il loro costante sostegno, per tutto ciò che mi hanno insegnato e messo a disposizione nel corso della vita, permettendomi di arrivare fino a qui. Li ringrazio per la loro capacità di ascoltarmi e per essere sempre stati al mio fianco.

Grazie ad Andrea, la persona che più di tutte è stata in grado di capirmi e di essermi accanto anche nei momenti più difficili, la mia isola felice, il mio rifugio e il mio sostegno.

Un grazie speciale alle mie amiche, alle mie pazze complici, Beatrice, Irene, Jessica, Laura e Margherita, per aver condiviso con me questi anni, tra gioie e dolori, sacrifici e ricompense. Le ringrazio per aver costruito insieme i ricordi più belli e divertenti che mi accompagneranno sempre, sperando di poterne condividere tanti altri. Siete le compagne di viaggio migliori che potessi desiderare.