UNIVERSITA' DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE ECONOMICHE ED AZIENDALI "M.FANNO"

DIPARTIMENTO DI DIRITTO PRIVATO E CRITICA DEL DIRITTO

CORSO DI LAUREA IN ECONOMIA

PROVA FINALE

"IL MERCATO DEI DATI PERSONALI. IN PARTICOLARE: IL CASO MEDIAWORLD"

RELATORE:

CH.MA PROF.SSA CHIARA ABATANGELO

LAUREANDA: MARTINA RAVAROTTO

MATRICOLA N. 1163998

ANNO ACCADEMICO 2019 – 2020

Il/La candidato/a, sottoponendo il presente lavoro, dichiara, sotto la propria personale responsabilità, che il lavoro è originale è che non stato già sottoposto, in tutto in parte, dal/dalla candidato/a o da altri soggetti, in altre Università italiane o straniere ai fini del conseguimento di un titolo accademico. Il/La candidato/a dichiara altresì che tutti i materiali utilizzati ai fini della predisposizione dell'elaborato sono stati opportunamente citati nel testo e riportati nella sezione finale 'Riferimenti bibliografici' e che le eventuali citazioni testuali sono individuabili attraverso l'esplicito richiamo al documento originale.

INDICE

INTRODUZIONE

Nel presente elaborato si andrà a trattare il tema sempre più attuale e complesso del mercato dei dati personali inteso come scambio di un bene o servizio contro la prestazione del consenso al trattamento dei dati personali dell'utente. L'evoluzione tecnologica degli ultimi anni ha permesso la rapida diffusione di questo fenomeno, nonostante vi siano diversi dubbi circa la sua liceità.

Nel primo capitolo si esaminerà, nelle sue parti più rilevanti, il Regolamento UE relativo alla protezione dei dati personali entrato in vigore il 25 maggio 2018 con l'obiettivo di armonizzare le normative degli Stati membri in materia di privacy. Si vedrà che, tra le finalità del Regolamento, vi è anche la libera circolazione dei dati, promuovendo così lo sviluppo di un mercato unico delle informazioni.

Nel secondo capitolo si entrerà nel vivo della trattazione e si parlerà del mercato dei dati personali, analizzando la corrispettività, di fatto esistente, tra il consenso al trattamento dei dati e l'accesso a un bene o servizio. Attraverso lo studio della normativa a tutela dei consumatori e delle norme in materia di protezione dei dati personali, si cercherà di capire quando lo scambio dei dati è ammesso e secondo quali principi debba essere effettuato.

Nel terzo e ultimo capitolo si prenderà in considerazione la prassi assai diffusa di rilasciare carte fedeltà, quali strumenti di raccolta dei dati personali. L'attenzione sarà rivolta, in particolar modo, al noto marchio di elettronica di consumo "MediaWorld", che è stato oggetto nel 2019 di un importante provvedimento da parte del Garante per la protezione dei dati personali a causa dell'uso non corretto delle fidelity card.

CAPITOLO 1

TRATTAMENTO DEI DATI PERSONALI: IL REGOLAMENTO UE 679/2016

1.1 Oggetto, finalità e ambito di applicazione materiale

Il Regolamento UE n. 679 del 2016, noto anche con l'acronimo inglese GDPR (General Data Protection Regulation), è la nuova normativa relativa alla protezione dei dati personali che abroga la precedente direttiva 95/46/CE con l'obiettivo di armonizzare definitivamente la regolamentazione in materia di protezione dei dati personali all'interno dell'Unione Europea. Il Regolamento è funzionale allo sviluppo digitale dell'Unione e, come vedremo lungo la trattazione, tutela anche la libertà di circolazione dei dati personali.

Andando ad analizzare nello specifico il testo normativo, l'articolo 1 afferma che il Regolamento "stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati". Si può quindi osservare il duplice oggetto del Regolamento: protezione dei dati personali da un lato e libera circolazione degli stessi dall'altro. Da questo si può dedurre un importante profilo, ovvero che i due ambiti di regolamentazione sono posti sullo stesso piano senza che l'uno possa considerarsi prevalente sull'altro. Negli ultimi anni, infatti, l'innovazione tecnologica e la globalizzazione hanno fatto sì che la raccolta e la condivisione dei dati personali siano aumentate in modo considerevole, rendendo gli individui sempre più tracciabili. A tal proposito, il Regolamento 679/2016 dichiara: "la tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che le riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali."[1]

Continuando la lettura dell'articolo 1, al comma 2 si parla di "diritto alla protezione dei dati personali": si tratta di un diritto fondamentale dell'individuo ai sensi della Carta dei diritti

[1] Considerando 6 del Regolamento UE 679/2016.

fondamentali dell'Unione Europea (articolo 8) e che costituisce una specificazione ed un ampliamento del diritto alla libertà e alla vita privata, entrambi riferibili agli esseri umani. Tuttavia, il diritto alla protezione dei dati personali è un diritto distinto ed autonomo rispetto al diritto alla riservatezza (privacy) in quanto estende la tutela dell'individuo oltre la sfera privata e in particolar modo nelle relazioni sociali, garantendo così il controllo sulla circolazione dei propri dati e la possibilità per l'interessato di richiedere la loro cancellazione o rettifica.

Un profilo importante da sottolineare è che il diritto alla protezione dei dati personali, così come il diritto alla circolazione dei dati, non è un diritto assoluto, "ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità"[2]. Il GDPR ha come soggetti d'interesse le sole persone fisiche viventi, escludendo così dal suo campo di applicazione le persone fisiche decedute e le persone giuridiche. I dati personali di quest'ultime, infatti, sono disciplinate da altre normative che non sono oggetto di analisi in questo elaborato.

L'articolo 2 del Regolamento si occupa dell'ambito di applicazione materiale della normativa. Il GDPR si applica sia al trattamento automatizzato dei dati sia al trattamento manuale dei dati personali contenuti in un archivio o destinati a figurarvi. A tal riguardo si dice che il Regolamento protegge i dati personali a prescindere dalla tecnologia usata per trattare tali dati e quindi è una normativa neutrale sotto il profilo tecnologico. L'articolo 4 comma 6 definisce l'archivio come "qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico". "Tale definizione contribuisce in maniera significativa a connotare come "generale" la portata del Regolamento giacché diventa difficile anche solo immaginare un trattamento di dati personali svolto al di fuori di un "archivio" così definito." [3]

Tuttavia, il legislatore europeo esclude dal campo di applicazione materiale alcuni ambiti:

1) normativa extra-UE: trattamento di dati per finalità estranee al diritto dell'Unione. Per tali ambiti ciascuno Stato si regolerà autonomamente;

2) politica estera e sicurezza: trattamento di dati nell'esercizio di attività rientranti nella politica estera e di sicurezza comune (capo 2 del titolo V del Trattato dell'Unione);

3) scopi personali: trattamento di dati effettuati da una persona fisica per l'esercizio di attività esclusivamente personale o domestico

[2] Considerando 4 del Regolamento UE 679/2016.

[3] RICCIO G. M., SCORZA G., BELISARIO E., a cura di, 2018. *GDPR e normativa privacy. Commentario,* p. 12.

4) sicurezza pubblica e giustizia: trattamento di dati effettuato dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati, esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica.[4]

1.2 Dato personale

Elemento fondamentale della disciplina in oggetto è senza ombra di dubbio il concetto di dato personale. Il Regolamento UE 679/2016 lo definisce all'articolo 4 come "qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".

È interessante notare come la nozione ponga particolare attenzione alle nuove forme di identificazione "tecnologica", come i dati di ubicazione all'interno di un sistema di geolocalizzazione o gli identificativi on line (si pensi per esempio agli indirizzi IP). Questo perché oggigiorno viene scambiata una mole sempre più elevata di informazioni tramite le nuove tecnologie e l'individuo, utilizzando dispositivi e applicazioni, lascia tracce utili alla sua identificazione.

La definizione di dato personale contiene quattro elementi fondamentali:

1. "qualsiasi informazione"
2. "riguardante"
3. "persona fisica"
4. "identificata o identificabile"

L'espressione "qualsiasi informazione" rappresenta la volontà del legislatore europeo di definire un concetto ampio di dati personali allo scopo di ottenerne un'interpretazione altrettanto estesa. È importante precisare che non è necessario che l'informazione sia di natura riservata o intima: anche informazioni generalmente disponibili, come i dati pubblici, sono dati personali. Inoltre, perché l'informazione diventi un "dato personale" non è necessario che sia vera o dimostrata. Essenziale è, invece, il giudizio prognostico di prossimità, che si fonda sulla

[4] CICCIA MESSINA A. e BERNARDI N., 2017. *Privacy e regolamento europeo,* p. 26.

nozione di “collegamento” tra l’informazione e la persona fisica: l’informazione suscettibile di essere definita come “dato personale”.[5]

Di conseguenza, si possono includere nella definizione informazioni oggettive come dati anagrafici, codice fiscale, indirizzi e-mail e referti di analisi cliniche, ma anche informazioni soggettive come valutazioni e opinioni.

“Riguardante” è il secondo elemento fondamentale nella definizione di dato personale in quanto è molto importante stabilire le relazioni esistenti tra informazioni e persone fisiche. Si può dire che un’informazione “riguarda” una persona quando può essere stabilito in modo semplice un collegamento. A titolo chiarificatore si riportano alcuni esempi: le informazioni contenute in un referto medico riguardano chiaramente il paziente, oppure i dati contenuti in un fascicolo sotto il nome di un determinato cliente riguardano senza ombra di dubbio quel cliente.

Continuando la trattazione si è già visto che il Regolamento 679/2016 si riferisce alle “persone fisiche” a prescindere dalla loro nazionalità e residenza e che non sono oggetto della normativa i dati personali relativi alle persone fisiche decedute. Tuttavia, visto che i dati dei defunti possono, in alcuni casi ,essere meritevoli di protezione, il legislatore europeo al considerando 27 precisa che “gli stati membri possono prevedere norme riguardanti il trattamento dei dati personali delle persone decedute”. A tal proposito, la normativa italiana prevede che “i diritti di cui agli articoli da 15 a 22 del Regolamento riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione.”[6]

L’ultimo elemento fondamentale che troviamo nella definizione di dato personale è di persona fisica “identificata o identificabile". Un individuo è “identificato” quando è possibile distinguerlo da qualsiasi altro soggetto o all’interno di una determinata categoria; una persona è “identificabile” quando non è ancora identificata ma è possibile distinguerla da tutte le altre ricorrendo ad ulteriori elementi. Si può quindi affermare che il concetto di dato personale è un concetto dinamico che va riferito all’interno di un contesto: se vi è un’informazione isolata che non porta all’identificazione di un soggetto, questa può comunque assumere la natura di dato personale se può essere usata per l’identificazione tramite altri dati. L’identificazione avviene normalmente attraverso degli “identificatori” come colore dei capelli, altezza, aspetto ma anche la professione.

[5] RICCIO G.M., SCORZA G., BELISARIO E., a cura di, 2018. *GDPR e normativa privacy. Commentario*, p. 37.

[6] Dlgs. 10 agosto 2018, n.101, art.2-terdecies.

Inoltre, come stabilito nel considerando 26 del GDPR, una persona può essere identificata direttamente attraverso il nome anagrafico, ad esempio, oppure indirettamente attraverso la targa dell'automobile, il numero di telefono o il numero del passaporto.
Nell'articolo 4 il Regolamento 679/2016 procede con una classificazione di dati personali in dati genetici, dati biometrici e dati relativi alla salute su cui non ci si soffermerà nel presente elaborato.
Ciò che risulta importante esaminare, in vista del prossimo capitolo, è il concetto di dato personale inteso come diritto della personalità o come bene immateriale. I dati personali rientrano nella categoria dei diritti della personalità in quanto si riferiscono alla persona umana e rappresentano delle entità idonee a soddisfare un interesse non economico dell'individuo (espressione del diritto alla riservatezza). Tuttavia, i diritti della personalità presentano alcune caratteristiche fondamentali, come l'indisponibilità e la non patrimonialità, che non sono proprie dei dati personali. Questi sono delle informazioni che "diventano estrinsecazioni immateriali della persona in grado di circolare autonomamente e lo sviluppo tecnologico determina un salto non solo quantitativo ma anche qualitativo di tale circolazione."[7]
Alla luce di ciò, i dati personali possono essere qualificati anche come beni giuridici economicamente valutabili e quindi oggetto di scambio. Da queste brevi considerazioni si deduce la natura ambivalente del dato personale, inteso in parte come diritto della personalità, in parte come diritto patrimoniale e quindi suscettibile di valutazione economica.
Questa doppia natura è riconosciuta anche dal GDPR che, ribadendo quanto già detto, disciplina non solo la protezione dei dati personali ma anche la libera circolazione degli stessi in un'ottica di mercato comune nell' Unione Europea.

1.3 Trattamento dei dati personali e principi applicabili

Il legislatore europeo ha affidato all'articolo 4 comma 2 il significato di "trattamento" inteso come "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, 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, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione". Si tratta di un'elencazione esemplificativa che non distingue tra

[7] THOBANI S., 2018. *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali,* p. 15.

strumenti automatizzati e non. Inoltre, dall'analisi del comma in questione si può affermare che qualunque operazione che coinvolga un dato personale rappresenta un'attività di trattamento.
Il Regolamento riserva poi all'articolo 5 la definizione dei principi applicabili al trattamento dei dati personali, ovvero quelli di liceità, correttezza e trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza, responsabilizzazione.
Per liceità si intende innanzitutto rispetto delle norme: è lecito il trattamento che non violi norme generali e norme specifiche dell'ordinamento. Il GDPR specifica poi che "perché sia lecito, il trattamento di dati personali dovrebbe fondarsi sul consenso dell'interessato o su altra base legittima prevista per legge dal presente regolamento o dal diritto dell'Unione o degli Stati membri […]"[8]. All'articolo 6, il Regolamento elenca quali sono questi presupposti che permettono di qualificare un trattamento come lecito:

- consenso dell'interessato
- contratto
- obbligo legale
- salvaguardia di interessi vitali dell'interessato o di altra persona fisica
- compiti di interesse pubblico connesso all'esercizio di pubblici poteri
- legittimo interesse del titolare

È specifico dovere del titolare del trattamento valutare quale tra esse è la base giuridica più idonea per il trattamento che intende realizzare. È importante sottolineare come le condizioni di liceità siano trattate tutte insieme senza distinguere tra i titolari del trattamento (enti pubblici o soggetti privati). Inoltre, come specificato nell'articolo in questione, è sufficiente che vi sia uno solo dei citati presupposti per configurare lecito il trattamento.

Procedendo con l'analisi dei principi applicabili al trattamento dei dati, la correttezza è sinonimo di lealtà e buona fede nel comportamento del titolare lungo tutto l'arco del trattamento, dalla fase della raccolta fino a quelle successive dell'elaborazione, archiviazione e delle operazioni connesse. Il principio di trasparenza ha invece come obiettivo essenziale quello di rendere l'interessato consapevole delle caratteristiche del trattamento che riguarda i propri dati anche al fine di consentirgli, nel caso, l'esercizio del diritto di revoca. Per la comprensione del citato principio bisogna ricorrere al considerando 39, dove il GDPR afferma che "dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che le riguardano nonché la misura in cui i dati

[8] Considerando 40 del Regolamento UE 679/2016.

personali sono o saranno trattati". E ancora "il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro. Tale principio riguarda, in particolare, l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento corretto e trasparente con riguardo alle persone fisiche interessate e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che le riguardano."

Continuando la lettura si può notare come sia riconducibile a tale principio l'esigenza di sensibilizzare e proteggere le persone con riferimento "ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento."

1.4 Consenso dell'interessato e informativa

Come già detto nel paragrafo precedente, una delle basi legittime del trattamento dei dati personali è il consenso dell'interessato che è strettamente legato al principio di liceità. Il concetto di consenso si è evoluto rispetto alla precedente normativa per tenere conto dei cambiamenti avvenuti nell'Unione Europea in seguito all'uso sempre più massiccio delle nuove tecnologie. La normativa in vigore definisce il 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". A tal proposito il considerando 32 specifica che l'interessato deve manifestare il consenso attraverso una dichiarazione scritta, anche con l'ausilio di mezzi elettronici, o orale. Non basta quindi il silenzio (consenso tacito) o l'inattività del soggetto, ma si rende necessario un comportamento attivo da parte dell'interessato (come, ad esempio, spuntare una casella o inserire la mail in un campo dove è specificata la finalità per la quale sarà usato il dato). Il consenso deve, invece, essere necessariamente espresso nel caso di trattamento dei dati sensibili (art. 9 del Regolamento) e per decisioni basate su trattamenti automatizzati, compresa la profilazione. Inoltre, sempre secondo il considerando 32, se il trattamento presenta più finalità, il consenso deve essere prestato per ognuna di queste. Il consenso non può ritenersi libero se l'interessato non è in grado di scegliere liberamente (in quanto soggetto a intimidazioni o raggiri) o non può rifiutare o revocare il consenso senza subire un danno. Il GDPR specifica poi che "per assicurare la libertà di prestare il consenso, è opportuno che il consenso non costituisca un valido fondamento

giuridico per il trattamento dei dati personali in un caso specifico, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato prestato liberamente in tutte le circostanze di tale situazione specifica".[9] Questo squilibrio di potere esiste anche nel rapporto fra datore di lavoro e lavoratore e per questo sarebbe preferibile trattare i dati su base giuridica differente.

Affinché il consenso si possa ritenere informato, l'interessato dovrebbe conoscere almeno l'identità del titolare del trattamento e le finalità del trattamento, cioè deve essere rispettato il principio di trasparenza.

Infine, il consenso deve essere revocabile in qualsiasi momento senza alcun obbligo di motivare la revoca, a seguito della quale il trattamento deve interrompersi. Con la revoca si innesca il diritto di cancellazione, per cui il titolare del trattamento deve cancellare i dati dell'utente.

Tornando al concetto di consenso informato, l'informativa è una comunicazione che deve essere fornita all'interessato prima di effettuare il trattamento, quindi prima della raccolta dei dati, se questi sono raccolti direttamente presso l'interessato. Nel caso di dati personali non raccolti direttamente presso l'interessato, l'informativa deve essere fornita entro un ragionevole termine. Questa comunicazione è dovuta ogni qual volta vi sia un trattamento di dati e, se il consenso è richiesto come base giuridica del trattamento, l'informativa diventa anche una condizione di legittimità del consenso.

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."

Per quanto riguarda i contenuti, questi vengono tassativamente indicati negli articoli 13 e 14 del Regolamento 679/2016 e sono fondamentali per il rispetto dei principi di trasparenza e correttezza. L'informativa deve essere coincisa, chiara e facilmente comprensibile e accessibile per l'interessato, eventualmente anche utilizzando immagini o icone; deve essere data per iscritto e preferibilmente in formato elettronico (soprattutto nei servizi online). Sono comunque ammesse altre modalità, tra cui la forma orale.

[9] Considerando 43 del Regolamento UE 679/2016.

1.5 Profilazione

Il Regolamento UE 679/2016 definisce la profilazione all'articolo 4, comma 4, come "qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica". Questi aspetti possono riguardare la situazione economica, la professione, la salute, gli interessi, le preferenze personali, il comportamento e gli spostamenti della persona fisica. Questa tecnica può implicare una serie di deduzioni statistiche ed è utilizzata in un numero crescente di settori, sia pubblici che privati, come banche e assicurazioni, assistenza sanitaria, fiscalità, pubblicità e marketing. I progressi nella tecnologia e le capacità in materia di intelligenza artificiale hanno reso più facile l'affermarsi di processi decisionali automatizzati, con potenziali effetti sui diritti e le libertà delle persone fisiche.

La profilazione viene applicata diffusamente in ambito commerciale per segmentare meglio i mercati e personalizzare i prodotti e i servizi con l'obiettivo di rispondere più efficacemente alle esigenze dei consumatori. Questo processo presenta vantaggi, tra cui il risparmio di risorse e una migliore efficienza, e svantaggi. La profilazione può essere poco trasparente e non completamente chiara. L'individuo, infatti, potrebbe non sapere di essere profilato. Inoltre, l'interessato potrebbe ritrovarsi in una categoria in cui non si riconosce ed essere sottoposto a qualche forma di discriminazione.

Per cercare di evitare questi rischi e rendere la profilazione conforme alla normativa, il legislatore europeo prevede:

- "requisiti specifici di trasparenza e correttezza;
- maggiori obblighi in termini di responsabilizzazione;
- basi giuridiche specifiche per il trattamento;
- il diritto delle persone fisiche di opporsi alla profilazione, segnatamente alla profilazione per finalità di marketing;
- qualora siano soddisfatte determinate condizioni, la necessità di effettuare una valutazione d'impatto sulla protezione dei dati"[10].

In sintesi, tornando all'articolo 4 del GDPR, si ha profilazione in presenza di tre elementi:

1. un trattamento automatizzato
2. eseguito su dati personali

[10] Gruppo di lavoro Articolo 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679,* p. 6.

3. con lo scopo di valutare aspetti personali di una persona fisica

Con questa procedura si raccolgono informazioni su un individuo o un gruppo di individui, si analizzano le sue caratteristiche e i suoi comportamenti e si inserisce il profilo in una determinata categoria o segmento per effettuare valutazioni o previsioni riguardanti certi aspetti.

Il Regolamento sancisce all'articolo 22 un generale divieto di sottoporre un individuo a processi decisionali automatizzati, compresa la profilazione, quando il processo produce effetti giuridici, oppure incide in modo significativo sulla persona dell'utente e la decisione è basata interamente sul trattamento automatizzato dei dati.

Al comma 2 sono previste delle eccezioni al divieto, per cui un soggetto può essere sottoposto ad un processo decisionale automatizzato, compresa la profilazione, quando:

- la decisione è necessaria per concludere o eseguire un contratto
- la decisione è autorizzata da una legge
- vi è il consenso esplicito (e non desunto da comportamento concludente) dell'interessato

CAPITOLO 2

IL MERCATO DEI DATI PERSONALI

2.1 Il valore economico dei dati personali

Quando si parla di mercato dei dati personali si fa riferimento alla prassi sempre più diffusa, soprattutto nei contratti stipulati online, di offrire beni e servizi in cambio del consenso al trattamento dei dati personali degli utenti, senza quindi richiedere un corrispettivo in denaro. Questa "gratuità" del contratto viene, tuttavia, smentita dal valore economico dei dati personali raccolti.

Riprendendo quanto già affermato in precedenza, i dati personali presentano una duplice natura: sono considerati sia diritti della personalità, sia beni immateriali ed è compito del legislatore assicurare il giusto bilanciamento tra di essi. Risulta, infatti, importante tutelare da un lato il dato come diritto fondamentale della persona, e dall'altro affermare che il dato è anche una risorsa economica che può essere scambiata.

A proposito del valore economico dei dati personali, "la stessa giurisprudenza – che a livello declamatorio è usa negare la natura contrattuale del consenso allo sfruttamento degli attributi immateriali della propria persona – riconosce esplicitamente che i diritti della personalità hanno un contenuto anche patrimoniale".[11]

Se si pensa all'odierna era digitale, l'evoluzione delle nuove tecnologie ha permesso la raccolta e il trattamento sempre più massicci di dati personali, il cui sfruttamento genera benefici ed utilità economiche.

Si consideri, per esempio, i social network quali Facebook, Instagram e Twitter: queste applicazioni apparentemente sembrano gratuite ma, in realtà, fondano il proprio business sulla raccolta e monetizzazione dei dati personali degli utenti.

Proprio per questo è importante sottolineare il valore intrinseco delle informazioni raccolte, soprattutto in un'ottica di scambio dei dati personali tra soggetti.

[11] THOBANI S., 2018. *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, p. 85.

2.2 Il nesso di corrispettività tra il consenso al trattamento dei dati personali e l'accesso a un bene o servizio

Lo sviluppo di nuove tecniche di raccolta, monitoraggio e sfruttamento dei dati personali ha permesso la diffusione delle operazioni cosiddette di tying, ovvero situazioni in cui, per accedere a un servizio, viene richiesto all'utente di prestare il consenso al trattamento dei dati personali per finalità ulteriori rispetto a quelle necessarie per l'esecuzione del contratto, come scopi di profilazione e marketing, e questo consenso si considera necessario per accedere al servizio. Questi dati raccolti per finalità aggiuntive (o, per meglio dire, il consenso al trattamento) rappresentano il corrispettivo del servizio, in quanto il fornitore del bene (gratuito) trae un vantaggio economico dal loro utilizzo.

Tuttavia, ciò che risulta importante chiedersi è se sia lecito offrire beni e servizi in cambio della cessione dei dati personali. In altre parole, è ammesso un mercato dei dati personali? Per rispondere alla domanda è utile analizzare la questione sotto diversi punti di vista.

Innanzitutto, risulta fondamentale il richiamo al requisito di libertà del consenso al trattamento. Nel capitolo precedente si è affrontato il tema del consenso dell'interessato quale base giuridica per il trattamento dei dati personali e si è giunti alla conclusione che il suddetto consenso rappresenta un atto giuridico meramente autorizzatorio senza il quale si configura un illecito extracontrattuale lesivo dei diritti (assoluti) della personalità. Tuttavia, nel caso in esame dei dati personali offerti come controprestazione, il consenso dell'interessato assume una natura negoziale in quanto necessario per accedere al servizio posto in essere dal contratto.

A proposito della validità delle operazioni di tying, si è espresso il Garante per la protezione dei dati personali affermando che, "qualora il consenso non sia necessario per adempiere a obblighi di legge o per dare esecuzione al contratto, l'interessato debba poter scegliere se prestarlo o meno, senza che una scelta di segno negativo possa influire sulla instaurazione del rapporto."[12]

Secondo l'Autorità garante, chi ha intenzione di richiedere il consenso al trattamento dei dati in occasione della fornitura di un bene o servizio deve prevedere come facoltativa la prestazione di tale consenso. Da questo ne deriva che il consenso non può considerarsi libero se viene posto come condizione per accedere a un bene o servizio: il trattamento dei dati che ne consegue sarà, in questo caso, illecito.

Alla luce di quanto emerso, il Garante privacy sembra porre un limite alle operazioni di tying e quindi allo sviluppo di un mercato basato sullo scambio dei dati personali. Infatti, se gli utenti

[12] THOBANI S., 2016. *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*. In Europa e diritto privato, fasc. 2, p. 533.

devono essere liberi di accedere al servizio scegliendo se prestare o meno il consenso al trattamento dei dati, è possibile che molti interessati decidano di negare il consenso.

Anche il Gruppo di lavoro Articolo 29 sembra essere a sfavore di un mercato dei dati personali, affermando che "l'obbligo di acconsentire all'uso di dati personali aggiuntivi rispetto a quelli strettamente necessari limita la scelta dell'interessato e ostacola l'espressione del libero consenso. Poiché la legislazione in materia di protezione dei dati mira a tutelare i diritti fondamentali, è essenziale che l'interessato abbia il controllo sui propri dati personali; inoltre sussiste una presunzione forte secondo cui il consenso a un trattamento di dati personali non necessario non può essere considerato un corrispettivo obbligatorio dell'esecuzione di un contratto o della prestazione di un servizio."[13]

Secondo il punto di vista del Regolamento UE 679/2016 non si riscontra, invece, un netto divieto alla prassi di subordinare l'accesso a un bene o servizio alla prestazione del consenso al trattamento dei dati. In particolar modo, l'articolo 7, comma 4, del GDPR 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."

Come si può notare, il legislatore europeo pone particolare attenzione alla condizionalità come presunzione di mancanza di libertà di esprimere il consenso. La norma non deve essere intesa in senso assoluto perciò, in alcuni casi, tale condizionalità potrebbe non rendere invalido il consenso.

Alla luce di ciò, si può affermare che non sono vietate le operazioni di tying, ma si tratta di circostanze da tenere nella "massima considerazione" allo scopo di valutare la libertà del consenso e tutelare come fine ultimo la persona.

Richiamando quanto già detto nel paragrafo 1.4, si deve verificare che il consenso dell'interessato non sia stato prestato a seguito di raggiri o intimidazioni, bensì in condizioni di serenità, consapevolezza e trasparenza. Affinché l'interessato possa scegliere liberamente se prestare o meno il consenso, chi fornisce un servizio chiedendo il consenso al trattamento dovrebbe offrire all'utente due versioni del servizio: una condizionata alla prestazione del consenso e l'altra no.[14]

[13] Gruppo di lavoro Articolo 29, *Linee guida sul consenso ai sensi del regolamento (UE) 679/2016,* p. 9.

[14] THOBANI S., 2019. *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*. In MediaLaws – Rivista di diritto dei media, fasc. 3, p. 140.

Le due alternative non sono identiche, ma devono presentare effettivamente lo stesso valore e le stesse caratteristiche e, se l'utente opta per il servizio senza la prestazione del consenso, dovrà pagare una somma di denaro congrua.

Il problema sorge quando le alternative presenti sul mercato sono offerte da operatori diversi. A tal proposito il Gruppo di lavoro stabilisce che "il consenso non possa considerarsi prestato liberamente se 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. In tal caso la libertà di scelta dipenderebbe dagli altri operatori del mercato e dal fatto che l'interessato ritenga che i servizi offerti dall'altro titolare del trattamento siano effettivamente equivalenti."[15]

Questa prospettiva fa nascere non pochi problemi in quanto il titolare del trattamento deve controllare costantemente l'evoluzione del mercato per garantire che il consenso continui ad essere valido.

Per chiarire meglio la questione circa la validità delle operazioni di tying, si prende in considerazione un'importante sentenza della Suprema Corte di Cassazione. In particolare, nel caso in esame, il gestore di un sito web offriva un servizio di newsletter su tematiche di finanza, fisco e diritto condizionando l'iscrizione alla prestazione del consenso al trattamento dei dati personali. Secondo la Corte, non è lecito subordinare l'accesso a un bene o servizio alla prestazione del consenso al trattamento dei dati se la prestazione è infungibile e irrinunciabile per l'interessato. Questo, "non può certo dirsi accada nell'ipotesi di offerta di un generico servizio informativo del tipo di quello in discorso, giacché all'evidenza si tratta di informazioni agevolmente acquisibili per altra via, eventualmente attraverso siti a pagamento, se non attraverso il ricorso all'editoria cartacea, con la conseguenza che ben può rinunciarsi a detto servizio senza gravoso sacrificio."[16]

Analizzando le caratteristiche che deve avere il servizio, per infungibilità si intende l'impossibilità di trovare nel mercato un servizio equivalente senza, nel caso in oggetto, acconsentire al trattamento dei dati. L'irrinunciabilità fa riferimento, invece, all'essenzialità del servizio per l'interessato. Per evitare problemi di interpretazione, è diffusa la convinzione secondo cui se un servizio è effettivamente infungibile è anche irrinunciabile.

---

[15] Gruppo di lavoro Articolo 29, *Linee guida sul consenso ai sensi del regolamento (UE) 679/2016,* pp. 10-11.

[16] Cass. Civ., Sez. I, 2 luglio 2018, n. 17278.

Il gestore del sito, nel caso presentato alla Corte di servizio fungibile e rinunciabile, può liberamente negare l'accesso al servizio di newsletter a chi non intende ricevere messaggi pubblicitari.
Alla luce di ciò, l'ordinamento non vieta lo scambio di dati personali ma pretende che lo scambio derivi da un consenso libero, pieno e in nessun modo forzato.
La conseguenza più evidente derivante dalla decisione della Suprema Corte è, collegandosi al paragrafo precedente, il riconoscimento di un valore economico dei dati degli interessati che, prestando il consenso libero e informato al trattamento dei dati personali in cambio di un determinato servizio, effettuano uno scambio.

2.3 Tutela dell'utente e tutela dell'interessato: uno sguardo alle normative

Il mercato dei dati personali si presenta come un concetto estremamente complesso in quanto chi accede a un servizio prestando il consenso al trattamento dei propri dati è sia un utente, e quindi un consumatore, sia un interessato, cioè il soggetto a cui si riferiscono le informazioni.
Si ritiene necessario, quindi, prendere in considerazione non solo la normativa in materia di protezione dei dati personali, ma anche le norme a tutela dei consumatori.
Attraverso una breve analisi si vedrà che la normativa a tutela dei consumatori definisce come lo scambio debba essere attuato, garantendone la trasparenza e assicurando ai consumatori alcuni rimedi in caso di clausole vessatorie, mentre le norme in materia di protezione dei dati personali stabiliscono quando tale mercato è ammesso e quindi lecito.
Quando si accede ad un bene o servizio e in cambio si presta il consenso al trattamento dei propri dati personali, si instaura un rapporto di consumo tra il fornitore del servizio e l'utente-consumatore. Il contratto che si va a configurare non è gratuito in quanto, come si è già ribadito più volte, i dati raccolti presentano un valore economicamente rilevante. Uno degli obiettivi della normativa a tutela dei consumatori è quello di garantire la trasparenza e l'adeguatezza delle condizioni presenti nei contratti tra il professionista e l'utente.
Infatti, l'articolo 2 del Codice del Consumo[17] prevede che ai consumatori sia riconosciuto il diritto ad un'adeguata informazione e a una corretta pubblicità; all'esercizio delle pratiche commerciali secondo principi di buona fede, correttezza e lealtà; alla correttezza, alla trasparenza ed all'equità nei rapporti contrattuali.

[17] Dlgs. 6 settembre 2005, n. 206.

Da questo ne deriva che il contratto, se prevede l'offerta di beni o servizi in cambio della cessione dei dati personali, non può essere definito gratuito nonostante il consumatore non sia chiamato a versare un corrispettivo.

Anche l'Autorità garante della concorrenza e del mercato è intervenuta più volte sulla questione sanzionando come scorretta la pratica di un famoso social network di non informare in modo chiaro gli utenti del servizio delle finalità remunerative dello stesso, attraverso la raccolta e il trattamento di dati personali, ma anzi di pubblicizzarne la gratuità.[18]

Secondo Thobani (2019, p.135) è necessario riconoscere il nesso sinallagmatico che si crea tra la fornitura del bene o servizio e la prestazione del consenso al trattamento dei dati personali da parte degli utenti. In questo modo, si vogliono evitare pratiche commerciali scorrette garantendo la trasparenza del mercato e si vuole riconoscere all'utente-interessato gli stessi rimedi previsti per il consumatore, anche se il servizio non prevede il pagamento di una somma di denaro.

A tal proposito, un importante traguardo si è raggiunto con la 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.

L'articolo 3, comma 1, stabilisce 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". L'ambito di applicazione, in sostanza, non è solo il contratto che prevede il pagamento di un corrispettivo, ma anche il servizio per così dire "gratuito".

Al considerando 24 viene specificato che il legislatore riconosce la protezione dei dati personali quale diritto fondamentale del soggetto e che, nell'ambito di questi contratti, si dovrebbe garantire ai consumatori il diritto a rimedi contrattuali.

L'obiettivo è fare in modo che gli utenti, considerati parte debole del rapporto di consumo, siano adeguatamente informati circa le operazioni che mettono in pratica e tutelati in caso di inadempimento o in presenza di pratiche commerciali scorrette.

Parlando invece della normativa in materia di protezione dei dati personali, si è già ampiamente detto nel paragrafo precedente che bisogna fare riferimento al requisito di libertà del consenso contenuto nell'articolo 7 del GDPR per stabilire i confini di liceità del mercato dei dati personali.

[18] Autorità garante della concorrenza e del mercato, *Facebook – condivisione dati con terzi*. Provvedimento del 29 novembre 2018, n. 27432.

2.4 Limiti al mercato dei dati personali

I limiti allo sviluppo di un mercato dei dati personali sono da collegarsi agli interessi che il legislatore europeo intende tutelare. Dalla lettura del paragrafo dedicato al nesso di corrispettività tra il consenso al trattamento dei dati personali e l'accesso a un bene o servizio, si può notare come il requisito di libertà del consenso rappresenti una limitazione al mercato dei dati. Sono previsti, infatti, requisiti molto stringenti per la sua validità che possono rappresentare un ostacolo per lo scambio di dati.

Come si è già visto, il Regolamento UE 679/2016 si pone due obiettivi: la libera circolazione dei dati personali da un lato, e la protezione degli stessi quale diritto fondamentale riconosciuto dall'Unione Europea, dall'altro.

Questo diritto "non ha un contenuto omogeneo ed è anzi volto in via strumentale a tutelare interessi eterogenei, che vanno oltre quelli dei singoli interessati di volta in volta coinvolti".[19]

Il fine ultimo è, quindi, proteggere gli interessi della collettività per evitare che il trattamento in massa dei dati personali effettuato con l'ausilio delle nuove tecnologie possa portare all'adozione di comportamenti discriminatori o di decisioni basate su informazioni non pienamente corrette.

L'obiettivo di voler tutelare interessi collettivi e generali è confermato anche dal fatto che il titolare del trattamento utilizza le informazioni degli interessati per finalità ulteriori, come attività di profilazione e invio di comunicazioni commerciali, in cui l'individuo è parte di una collettività. Come si può notare, risulta poco rilevante considerare i dati di un soggetto nella sua individualità, nonostante il condizionamento di un servizio al consenso al trattamento dei dati riguardi i singoli rapporti.

Alla luce di questa breve analisi, "lo scopo delle limitazioni poste al mercato dei dati personali pare dunque essere quello di evitare che grazie alla mole di informazioni raccolte si pongano in essere condotte pregiudizievoli per la società in generale".[20]

[19] THOBANI S., 2019. *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente.* In MediaLaws – Rivista di diritto dei media, fasc. 3, p. 144.

[20] Op. cit.

CAPITOLO 3

STRUMENTI DI RACCOLTA DEI DATI PERSONALI: ALCUNE QUESTIONI

3.1 Le carte fedeltà: regole e finalità del trattamento dei dati

Le carte e i programmi di fidelizzazione sono sempre più diffusi tra la popolazione e coinvolgono non solo il settore della grande distribuzione, come i supermercati, ma anche l'erogazione di servizi nei trasporti, nel credito, nella telefonia e nel noleggio.
Attraverso le fidelity card vengono concessi ai clienti diversi vantaggi sottoforma di sconti per l'acquisto di una determinata quantità di prodotti, premi e servizi accessori con l'obiettivo di creare un rapporto duraturo e profittevole con la clientela. Questo implica la raccolta e il trattamento di dati personali dei clienti come dati anagrafici, indirizzi e-mail e recapiti telefonici. Tuttavia, accanto a questi dati, vengono spesso raccolte altre informazioni che non sono necessarie per attribuire i vantaggi al cliente, come ad esempio titolo di studio, professione, stato civile, interessi, preferenze. Il problema sta nel fatto che queste informazioni vengono frequentemente utilizzate anche per scopi di profilazione, senza che gli interessati siano pienamente consapevoli e possano acconsentire al loro uso.
I programmi di fidelizzazione, in sostanza, offrono vantaggi in cambio di informazioni che consentono alla società che rilascia le carte fedeltà di creare profili, studiare propensioni al consumo, orientare campagne di marketing, ecc.
A tal proposito si è espresso il Garante per la protezione dei dati personali con il provvedimento del 24 febbraio 2005 denominato "Fidelity card e garanzie per i consumatori" in cui vengono fissati i criteri per il trattamento dei dati personali raccolti attraverso le carte fedeltà.
È importante sottolineare che, in seguito all'entrata in vigore del Regolamento UE 679/2016, le tutele previste per il trattamento dei dati personali in tale ambito devono ritenersi ulteriormente rafforzate: esso dovrà avvenire nel rispetto dei principi di liceità, correttezza, trasparenza, limitazione delle finalità, limitazione del trattamento, minimizzazione, esattezza, integrità e riservatezza stabiliti all'articolo 5 del GDPR.
Ritornando al provvedimento del Garante, le regole riguardano le tre principali finalità per le quali i dati personali dei clienti vengono raccolti ed utilizzati: la *fidelizzazione*, realizzata attribuendo vantaggi al cliente; la *profilazione*, mediante l'analisi delle abitudini e delle scelte di consumo; il *marketing diretto*.

Chi rilascia carte fedeltà deve innanzitutto informare i clienti in modo chiaro e completo sull'uso che verrà fatto dei dati che li riguardano, tenendo conto delle diverse finalità perseguite. L'informativa fornita al cliente deve essere evidenziata all'interno dei moduli di sottoscrizione ed essere facilmente individuabile rispetto alle altre clausole presenti. "In particolare, devono essere poste in distinta e specifica evidenza le caratteristiche dell'eventuale attività di profilazione e/o di marketing, come pure l'intenzione di cedere a terzi specificamente individuati i dati per finalità da indicare puntualmente."[21]

Questo passaggio del provvedimento merita particolare attenzione in quanto, mentre il trattamento di dati per programmi di fidelizzazione può essere svolto senza l'acquisizione del consenso dell'interessato, le informazioni raccolte con carte fedeltà che hanno anche finalità di profilazione e marketing diretto possono essere trattate solo con il consenso esplicito dell'interessato, che comunque è libero e facoltativo.

Il Garante stabilisce poi che le aziende devono ridurre al minimo l'uso dei dati personali e devono comunque utilizzare solo informazioni pertinenti e non eccedenti, nel rispetto del principio di minimizzazione dei dati.

Analizzando nello specifico le tre principali finalità per le quali i dati vengono raccolti, con la fidelizzazione possono essere trattati solo dati necessari per attribuire vantaggi connessi all'uso della carta, cioè dati che consentono di identificare l'intestatario e dati riguardanti il volume di spesa globale effettuato. Ribadendo quanto già detto, per questa attività non è necessario acquisire il consenso dell'interessato perché il trattamento dei dati si considera svolto per finalità contrattuali.

Per quanto riguarda la profilazione, non è lecito utilizzare i dati sensibili, in particolar modo quelli che riguardano lo stato di salute. Con l'attività di marketing, invece, possono essere raccolti i dati necessari all'invio di materiale pubblicitario o di comunicazioni commerciali.

Questa parte dell'elaborato serve da introduzione al prossimo paragrafo incentrato sulla catena di distribuzione MediaWorld, che è stato oggetto di un provvedimento da parte del Garante privacy.

[21] Garante privacy, *'Fidelity card' e garanzie per i consumatori. Le regole del Garante per i programmi di fidelizzazione.* Provvedimento del 24 febbraio 2005 [doc. web n. 1103045].

3.2 Il caso "MediaWorld"

Nel paragrafo precedente si è specificato che il trattamento di dati personali raccolti con carte fedeltà per scopi di profilazione e marketing diretto non è lecito senza un consenso libero e specifico dell'interessato. Per approfondire meglio la questione si prende in esame il noto marchio "MediaWorld", appartenente a Mediamarket S.p.A., catena specializzata nell'elettronica di consumo presente in modo capillare in tutta Europa.

La Società è stata oggetto di un provvedimento[22] da parte del Garante per la protezione dei dati personali con cui vengono imposte una serie di misure per garantire la tutela della privacy dei consumatori.

Nello specifico, sono arrivate al Garante diverse segnalazioni da parte di una cliente del brand "MediaWorld" circa la continua ricezione mediante posta elettronica di offerte commerciali, senza il necessario consenso e nonostante l'interessata abbia chiesto più volte alla società, e con diversi mezzi, di cessare l'invio di posta indesiderata. In seguito, anche un secondo cliente si è lamentato di non riuscire a cancellarsi dalla mailing list e di aver contattato più volte la società senza successo.

I fatti contestati dalla prima cliente risalgono tra il 2007 e il 2009 e i dati sarebbero stati raccolti con la sottoscrizione di due carte fedeltà "Saturn", marchio che poi è stato inglobato dal brand "MediaWorld". Come afferma l'Autorità nel provvedimento in esame, "non è stata fornita dalla Società documentazione relativa alla raccolta dei dati personali della segnalante (asseritamente effettuata mediante i coupon relativi alle menzionate carte fedeltà), né la prova del consenso al trattamento per finalità di marketing dei dati (anch'esso asseritamente) richiesto alla segnalante nelle suindicate circostanze temporali". E ancora, "la Società non aveva richiesto agli interessati, limitatamente al modulo a marchio "Saturn", un consenso specifico per le finalità promozionali, bensì un unico consenso per tali finalità nonché per finalità diverse e riconducibili alla gestione contrattuale e para-contrattuale (quale in particolare la comunicazione ad aziende terze per la valutazione del grado di soddisfazione della clientela e la gestione dei premi)".

Alla luce di quanto emerso, il Garante ha disposto un accertamento ispettivo presso la Società nel febbraio 2018 durante il quale la stessa si è giustificata affermando di avere avuto, nel periodo in questione, una serie di problemi legati alle banche dati causati dall'aggiornamento dei sistemi informatici e per questo non è stata in grado di bloccare l'invio di e-mail pubblicitarie.

[22] Provvedimento del 20 giugno 2019 [doc. web n. 9124420].

Dall'ispezione sono emersi, inoltre, problemi ulteriori relativi al trattamento dei dati personali dei clienti e questo ha portato il Garante ad applicare il Regolamento UE 679/2016.

In primo luogo, è stato accertato che il consenso al trattamento dei dati per scopi pubblicitari non si può ritenere valido in quanto i clienti sono stati costretti a rilasciarlo per poter usufruire dei vantaggi derivanti dalla carta fedeltà. Vi è stato, in altre parole, un trattamento illecito dei dati raccolti, poiché la Società non ha acquisito il consenso libero, specifico e inequivocabile dell'interessato per una o più finalità.[23]

In secondo luogo, è risultato che "MediaWorld" ha commesso un ulteriore illecito inviando comunicazioni commerciali ad alcuni clienti che si erano opposti al trattamento dei dati per finalità di marketing. La Società ha così violato l'articolo 21 del GDPR.

Nel provvedimento, l'Autorità ha quindi ammonito la Società a non effettuare alcun trattamento per scopi di marketing di dati personali raccolti mediante la carta fedeltà "Saturn" senza un consenso libero e specifico dell'interessato. Ha vietato, inoltre, l'utilizzo, per gli stessi fini, dei dati di qualunque interessato, in assenza di un consenso avente le caratteristiche già citate in precedenza. Infine, ha imposto alla Società di adottare una serie di misure organizzative e tecniche adeguate al fine di garantire la gestione corretta dei diritti degli interessati, in particolar modo il diritto di opposizione, e per assicurare anche il tracciamento tempestivo delle richieste dei clienti.

[23] Secondo quanto imposto dagli articoli 4, 6 e 7 del Regolamento UE 679/2016.

CONCLUSIONI

Con l'emanazione del Regolamento UE 679/2016 il legislatore europeo ha voluto dimostrare la sempre più crescente attenzione verso il trattamento dei dati personali posto in essere con le nuove tecnologie. Attraverso una serie di strumenti come siti web e social network si possono raccogliere quantità elevate di informazioni, con conseguenti rischi in tema di privacy da non sottovalutare.

A tal riguardo, il GDPR continua a porsi come obiettivo la protezione dei dati personali, prevedendo una serie di principi per il loro trattamento, ma intende anche instaurare un'area in cui tali dati possano circolare liberamente.

In quest'ottica si è discusso del concetto di mercato dei dati personali, giungendo alla conclusione che l'offerta di un bene o servizio contro la prestazione del consenso al trattamento dei dati è ammessa nei limiti imposti dalla norma in materia di libertà del consenso al trattamento. L'obiettivo del legislatore pare dunque quello di ammettere lo scambio ma con dei requisiti molto stringenti in modo da tutelare la parte debole del rapporto, cioè l'utente.

Inoltre, se l'interessato non ha intenzione di prestare il consenso, deve comunque avere la possibilità di accedere ad un servizio equivalente (ovvero un'alternativa), nel rispetto del principio di libero consenso.

Per capire le modalità con cui lo scambio dei dati debba essere effettuato, è necessario fare ricorso alla normativa a tutela dei consumatori, mentre le norme in materia di protezione dei dati personali ne stabiliscono la legittimità sostanziale.

Con riferimento all'uso sempre più massiccio delle carte fedeltà, il noto brand "MediaWorld" rappresenta un chiaro esempio di violazione del Regolamento UE 679/2016, in quanto non sono stati rispettati i requisiti fondamentali del consenso prestato dall'interessato.

Alla luce dell'analisi fatta nel presente elaborato, il mercato dei dati personali si presenta come un fenomeno complesso e in continua crescita e risulta importante, per questo, mantenere la normativa costantemente aggiornata per evitare trattamenti illeciti dei dati personali.[24]

[24] Conteggio parole: 8372.

BIBLIOGRAFIA

CICCIA MESSINA A. e BERNARDI N., 2017. *Privacy e regolamento europeo*, II edizione, Milano: IPSOA.

NUCCI G., 2018. *Protezione dei dati personali e GDPR: dai precetti giuridici ai processi organizzativi*, Milano: IPSOA.

RESTA G. e ZENO-ZENCOVICH V., 2018. *Volontà e consenso nella fruizione dei servizi in rete.* In Rivista trimestrale di diritto e procedura civile, fasc. 2, Milano: Giuffrè Editore.

RICCIO G. M., SCORZA G., BELISARIO E., a cura di, 2018. *GDPR e normativa privacy. Commentario,* I edizione, Milano: IPSOA.

SOFFIENTINI M., 2018. *Privacy. Protezione e trattamento dei dati*, IV edizione, Milano: IPSOA.

THOBANI S., 2016. *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*. In Europa e diritto privato, fasc. 2, Milano: Giuffrè Editore.

THOBANI S., 2018. *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Milano: Ledizioni.

THOBANI S., 2019. *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente.* In MediaLaws – Rivista di diritto dei media, fasc. 3. Disponibile su http://www.medialaws.eu/rivista/il-mercato-dei-dati-personali-tra-tutela-dellinteressato-e-tutela-dellutente/ [Data di accesso: 10/03/2020]

ZORZI GALGANO N., a cura di, 2019. *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano: CEDAM.

NORMATIVA

Autorità garante della concorrenza e del mercato, *Facebook – condivisione dati con terzi*. Provvedimento del 29 novembre 2018, n. 27432. Disponibile su https://www.agcm.it/dotcmsdoc/allegati-news/PS11112_scorr_sanz.pdf

Carta dei diritti fondamentali dell'Unione Europea.

Direttiva del Parlamento europeo e del Consiglio n. 770/2019 del 20 maggio 2019 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali.

Dlgs. 6 settembre 2005, n. 206 (Codice del consumo).

Dlgs. 10 agosto 2018, n. 101.

Garante privacy, *'Fidelity card' e garanzie per i consumatori. Le regole del Garante per i programmi di fidelizzazione.* Provvedimento del 24 febbraio 2005 [doc. web n. 1103045]. Disponibile su https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1103045

Garante privacy, Provvedimento del 20 giugno 2019 [doc. web n. 9124420]. Disponibile su https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9124420

Gruppo di lavoro Articolo 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679.*

Gruppo di lavoro Articolo 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai sensi del regolamento (UE) 2016/679.*

Regolamento del Parlamento europeo e del Consiglio n. 679/2016 del 27 aprile 2016.

GIURISPRUDENZA

Cass. Civ., Sez. I, 2 luglio 2018, n. 17278.

SITOGRAFIA

https://protezionedatipersonali.it/profilazione

https://www.privacy.it/2017/11/02/decisioni-automatizzate-profilazione-wp29/

https://www.altalex.com/documents/altalexpedia/2018/05/28/profilazione

https://www.altalex.com/documents/altalexpedia/2018/02/28/diritti-della-personalita

https://www.cybersecurity360.it/legal/privacy-dati-personali/la-corretta-individuazione-dei-dati-personali-regole-e-norme-per-il-pieno-rispetto-del-gdpr/

https://protezionedatipersonali.it/consenso

https://www.garanteprivacy.it/home/doveri#2

https://protezionedatipersonali.it/informativa

https://www.garanteprivacy.it/regolamentoue/informativa

https://www.cybersecurity360.it/legal/privacy-dati-personali/gdpr-il-garante-ammonisce-mediamarket-niente-pubblicita-senza-consenso-a-chi-ha-carte-fedelta/

https://www.altalex.com/documents/news/2018/07/03/consenso-newsletter