LA LIBERA CIRCOLAZIONE DEI DATI PERSONALI NEL MERCATO FINANZIARIO DOPO L'ADEGUAMENTO DELLA NORMATIVA NAZIONALE ALLE DISPOSIZIONI DEL REGOLAMENTO (UE) 2016/679

RAIMONDO MOTRONI

1. I dati personali vengo utilizzati nei processi produttivi delle imprese finanziarie secondo modalità che – da tempo – stanno subendo una significativa trasformazione a causa della globalizzazione dei mercati e delle nuove tecnologie[1] note come «*big data*»[2] e «internet of things»[3]. Le informazioni così raccolte e opportunamente analizzate, consentono alle imprese finanziarie[4] nuove strategie di marketing, l'ingegnerizzazione di prodotti finanziari innovativi, il *profiling* e il *clustering* dei clienti, la valutazione del merito creditizio, analisi e previsioni del rischio assicurativo, solo per fare alcuni esempi.

Inoltre, i mercati finanziari sono stati segnati recentemente dal fenomeno del *Fintech*[5] e dalle criptovalute. I *bitcoin*[6] e alcuni strumenti ad essi connessi quali le *blockchain*[7] e gli *smart*

[1] «La 'rivoluzione' informatica, interessando in modo orizzontale la totalità dei settori economici e sociali, interagisce sulla struttura dei mercati, sulle strategie imprenditoriali, sulle modalità e sui programmi di investimento. Essa sembra destinata a cambiare la stessa logica concorrenziale, stante il mutamento attuale e prospettico dei fattori della domanda»; così F. CAPRIGLIONE, *Non luoghi. Sovranità, sovranismi. Alcune considerazioni*, in *Riv. trim. dir. ec.*, 2018, p. 404.

[2] Il tema dei Big data è affrontato sul piano generale da V. MAYER-SCHÖNBERGER – K. CUKIER, *Big Data*, Milano, 2013, a cui si rinvia per una completa comprensione del fenomeno sul piano tecnologico e delle possibili implicazioni economiche e giuridiche per le persone cui sono riferite le informazioni trattate. Nella dottrina giuridica, tra coloro che pongono in evidenza i rischi per la privacy delle persone derivanti dall'analisi dei Big data, si ricordano, tra gli altri, G. D'ACQUISTO – M. NALDI, *Big data e privacy by design, Anonimizzazione, pseudonimizzazione, sicurezza*, Torino, 2017, p. 23 ss.

[3] Per un'esaustiva descrizione del fenomeno delle IOT e dei rischi da esso derivanti per la privacy degli utenti v. *amplius* G. GIANNONE CODIGLIONE, Internet of things *e nuovo Regolamento privacy*, in *La nuova disciplina europea della privacy*, a cura di S. Sica – V. D'Antonio – G.M. Riccio, Padova, 2016, p. 131 ss.; segnala i rischi peculiari per la privacy nella profilatura degli utenti inconsapevoli che derivano dall'uso dei dati personali raccolti con le IOT E.C. PALLONE, *"Internet of things" e l'importanza del diritto alla "privacy" tra opportunità e rischi*, in *Ciberspazio dir.*, 2016, p. 175 ss.

[4] Con tale terminologia ci si riferisce notoriamente alle imprese che operano nei mercati finanziari costituiti dalla «sommatoria del comparto bancario, finanziario e assicurativo»; così F. ANNUNZIATA, *La disciplina del mercato mobiliare*, Torino, 2015, p. 7.

[5] La forte necessità di adeguamento delle imprese finanziarie tradizionali alle novità derivati dal c.d. *fintech* è sottolineata da R. FERRARI, *L'era del Fintech. La rivoluzione digitale nei servizi finanziari*, Milano, 2016, p. 36 ss.; segnalano il rischio di disintermediazione connesso all'uso delle nuove tecnologie nei mercati finanziari con conseguenti maggiori rischi per i risparmiatori: R. MOTRONI – L. POSOCCO, *La dematerialisation et la desintermediation dans la revolution des «fintech»: premieres considerations*, in *Riv. giur. ec. trasp. amb.*, 2017, p. 151 ss.

contracts[8], comportano l'uso transnazionale di dati personali e sono destinati a modificare i rapporti tra imprese finanziarie e clienti. Il contenuto di alcune categorie di contratti di assicurazione sono sempre più connotati dall'uso di sistemi di geolocalizzazione e di *black box*, di dati biometrici e genetici, nonché di alcuni metodi di indagine sanitaria, basati su un trattamento pervasivo di informazioni personali. Un'ulteriore rivoluzione è attesa poi dall'uso degli smartphone e da apposite *app*, messe a disposizione dei fruitori di social network[9], che, anche attraverso valute virtuali, consentiranno ad una vasta platea di utenti di usare nuovi sistemi di pagamento per *l'e-commerce* e nei rapporti *peer to peer*. Non meno rilevanti appaiono poi le implicazioni connesse all'archiviazione ed all'elaborazione di dati in remoto *on demand*, noti come *cloud computing*[10], usate dalle imprese (non solo) finanziarie per allocare su server (situati anche fuori dal territorio dell'UE) grandi volumi di dati personali.

Le imprese finanziarie come banche e assicurazioni utilizzano queste particolari tecnologie nei rapporti con i clienti per «datizzare»[11] i comportamenti umani ed elaborarli opportunamente al fine di impiegarli nelle diverse attività d'impresa. Tali tecnologie permettono oggi di trarre nuove informazioni da dati apparentemente privi di diretta rilevanza economica[12], attraverso una loro aggregazione e analisi, così da renderli fruibili da parte delle imprese. Il concetto stesso di «informazione economica» può apparire opaco in quanto non presenta più capacità distintiva rispetto ad altre informazioni di diverso contenuto, che posseggono comunque una rilevanza economica ove opportunamente analizzate. Invero, le nuove tecnologie, ed in particolare i big data e i metadati, ci insegnano che l'informazione

---

[6] I bitcoin rappresentano una vasta area di ricerca a cui la dottrina si sta sempre più interessando, in tema, tra i più recenti, v. *amplius* C. PERNICE, *La controversa natura giuridica di Bitcoin: un'ipotesi ricostruttiva*, in *Rass. dir. civ.*, 2018, p. 333 ss.

[7] Per i profili tecnici e le implicazioni giuridiche della *blockchain* si rinvia, da ultimo, a L. PIATTI, *Blockchain, decentralizzazione e privacy: un nuovo approccio del diritto*, in *Ciberspazio dir.*, 2018, p. 179 ss.; A. RAZZINI, *Blockchain e protezione dei dati personali alla luce del nuovo regolamento europeo GDPR*, in *Ciberspazio dir.*, 2018, p. 197 ss.

[8] Per un'illustrazione sintetica dei diversi profili giuridici relativi alle nuove tecnologie in parola, anche con riguardo ai potenziali rischi per la privacy degli utenti, si veda L. PAROLA – P. MERATI – G. GAVOTTI, *"Blockchain e smart contract": questioni giuridiche aperte*, in *Contratti*, 2018, p. 681 ss. Ritiene il settore finanziario un «naturale banco di prova» per la blockchain, con ridotti rischi per la privacy delle persone P. CUCCURU, *"Blockchain" ed automazione contrattuale. Riflessioni sugli "smart contract"*, in *Nuova giur. civ. comm.*, 2017, p. 107 ss.

[9] V. *amplius* C. PERLINGIERI, *Profili civilistici dei social networks,* Napoli, 2014.

[10] Sul tema del *cloud computing* vedi *amplius*: A.G. NOTO LA DIEGA, *Il "cloud computing". Alla ricerca del diritto perduto nel web 3.0*, in *Europa dir. priv.*, 2014, p. 577 ss. Illustrano la nuova disciplina della tutela trattamento dei dati personali con profili di transnazionalità contenuta nel regolamento EU 2016/679 L. VALLE – L. GRECO, *Transnazionalità del trattamento dei dati personali e tutela degli interessati, tra strumenti di diritto internazionale privato e la prospettiva di principi di diritto privato di formazione internazionale*, in *Dir. inf.*, 2017, p. 195 ss.

[11] Il concetto di «datizzazione», inteso come riduzione dei comportamenti umani ad informazioni numeriche analizzabili dai computer, è ben illustrato da MAYER-SCHÖNBERGER – K. CUKIER, *cit.*, p. 130 ss.

[12] Taluni aspetti intimi del soggetto potrebbero essere dedotti attraverso diversi indicatori derivanti dai documenti forniti o creati dallo stesso cliente (es. accredito della pensione di invalidità sul conto corrente bancario; sinistro automobilistico con danno alla salute comunicato all'assicurazione). L'importanza dei dati con rilevanza economica nel mercato sia come strumenti di marketing sia come beni in senso giuridico è posta in evidenza da V. RICCIUTO, *Comunicazione e diffusione dei dati personali e trattamento di dati particolari*, in *Il codice del trattamento dei dati personali*, (a cura di) V. Cuffaro – R. D'Orazio – V. Ricciuto, Torino, 2007, p. 16 ss. Vale ricordare che la Direttiva 2002/58/CE menziona le «informazioni finanziarie» (numeri di carte di credito e di debito, «iban», codici fiscali ed altre) tra quelle per le quali il titolare è obbligato a effettuare una specifica segnalazione al Garante quando esse sia oggetto di trattamento illecito.

economica non è solo quella che ci informa direttamente di un aspetto economico di una persona, ma qualsiasi informazione che possa fornire elementi che, anche combinati con altri, consegnino all'impresa nuova conoscenza che possa essere impiegata in un processo produttivo. Tutte le informazioni che apparivano totalmente irrilevanti sul piano economico e non destavano in alcun modo l'interesse degli operatori finanziari[13] oggi divengono una fonte pressoché inesauribile di nuovi strumenti da utilizzare nei processi produttivi dell'impresa finanziaria.

Con tali premesse, si può affermare che sia divenuto in concreto assai complesso[14] scindere l'uso dei dati personali comuni (anche a contenuto economico) da quello di altre categorie di dati che, per comodità espositiva, possiamo ancora definire «dati sensibili»[15] o «super sensibili» ai fini dell'impiego dei medesimi all'interno dei processi produttivi dell'impresa finanziaria, là dove sono tutti da ritenersi parimenti rilevanti. Tuttavia, considerata la diversità di disciplina di cui ciascuna categoria di dati è destinataria, la corretta applicazione della normativa in materia di trattamento dei dati personali è divenuta un problema prioritario per le imprese finanziarie, che operano ormai a livello globale generando flussi di dati di dimensioni ragguardevoli.

La disciplina del trattamento dei dati personali nei mercati internazionali rimane inevitabilmente frammentaria[16]. Sotto questo profilo, basti ricordare la diversità dell'approccio statunitense da quello europeo rispetto al tema della privacy[17], che ha condotto all'adozione

---

[13] V. R. MORO VISCONTI, *Valutazione dei Big Data e impatto su innovazione e* digital branding, in *Dir. ind.*, 2016, 1, p. 51, il quale ricorda che «gli strumenti digitali acquistano sempre più rilevanza non solo come "luoghi" di espressione e condivisione di rete, ma anche in quanto efficaci veicoli di informazione, sviluppo del *brand*, *marketing* e *business*».

[14] Con riferimento alla disciplina dei Big data è stata ipotizzata la necessità di formulare nuovi paradigmi giuridici, in questo senso G. RESTA – V. ZENO ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ.*, 2018, 460.

[15] La categoria dei dai sensibili menzionata nella Direttiva 95/46/CE e nelle successive normative di attuazione, non coincide perfettamente con il contenuto del nuovo art. 9 del GDPR. Nonostante la diversa terminologia adottata dal GDPR, l'art. 22, par. 2, del d.lgs. 101/2018 ha precisato che "A decorrere dal 25 maggio 2018 le espressioni «dati sensibili» e «dati giudiziari» utilizzate ai sensi dell'articolo 4, comma 1, lettere d) ed e), del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, ovunque ricorrano, si intendono riferite, rispettivamente, alle categorie particolari di dati di cui all'articolo 9 del Regolamento (UE) 2016/679 e ai dati di cui all'articolo 10 del medesimo regolamento".

[16] Taluni segnali di regolazione uniforme di regolazione del fenomeno globale del trattamento dei dati personali si registrano un po' ovunque. Di recente alcuni Paesi africani hanno aumentato significativamente il livello di protezione dei dati come evidenzia S. SLOKENBERGA – J. REICHEL – R. NIRINGIYE – T. CROXTON – C. SWANEPOEL – J. OKAL, *EU data transfer rules and African legal realities: is data exchange for biobank research realistic?*, in *International Data Privacy Law*, ipy010, *https://doi.org/10.1093/idpl/ipy010*. Anche in estremo oriente, là dove la tradizione giuridica dei diritti umani è profondamente diversa da quella europea, si tende a regolare il tema della circolazione delle informazioni personali secondo standard simili alle normative occidentali; sul punto v. I. YAMAGUCHI, *Protecting privacy against emerging "Smart" Big Data surveillance: What can be learned from Japanese law?*, in *Perc. cost.*, 2014, p. 197 ss. Le difficoltà dovuta all'impossibilità di disporre di una regolamentazione globale del trattamento dei dati personali è segnalata da L. VALLE – L. GRECO, *Transnazionalità del trattamento dei dati personali e tutela degli interessati, tra strumenti di diritto internazionale privato e la prospettiva di principi di diritto privato di formazione internazionale*, cit., p. 204 ss.

[17] In particolare, ci sono tre profili principali nei quali si possono cogliere le diversità di approccio al tema della protezione dei dati personali negli USA e nell'UE: a) l'Europa disciplina la privacy come un diritto fondamentale della persona, mentre la tradizione giuridica statunitense è differente; b) l'UE ha come principale

di discipline differenti tra loro, tali da rendere più complessa la circolazione transatlantica delle informazioni, anche in ragione della diversità degli standard di tutela dei dati[18].

Il regolamento (UE) 2016/679[19] (di seguito anche GDPR) ha sostituito le precedenti normative europee e statali ed ha inglobato taluni risultati concettuali dell'elaborazione giurisprudenziale dei giudici nazionali ed europei e dell'attività regolamentare dei Garanti. In tal modo si è venuta a creare una situazione di maggiore certezza del diritto – quantomeno – nel mercato unico, rispetto alle previgenti normative nazionali non del tutto omogenee[20] adottate sulla base della direttiva 95/46/CE. Invero, nello spazio economico europeo sono necessarie quanto più possibile regole certe e uniformi[21], anche con riguardo al trattamento dei dati personali, in quanto le attività economiche non si fondano più solo sulle note

obiettivo la protezione della sfera privata dell'individuo da indebite intromissioni da parte delle imprese, mentre gli USA tendono a garantire i diritti di libertà della persona rispetto ai poteri invasivi del governo; c) l'UE propende per una disciplina dettagliata del fenomeno del trattamento dei dati personali, laddove gli Stati Uniti promuovono l'autoregolamentazione e i processi multi-stakeholder. In questo senso: A. ESTEVE, *The business of personal data: Google, Facebook, and privacy issues in the EU and the USA*, in *International Data Privacy Law*, 2017, p. 36 ss. (anche in *https://doi.org/10.1093/idpl/ipw026*). La distinzione tra l'approccio europeo e quello americano alla tutela della privacy è stato posto in evidenza, da Corte di giustizia dell'Unione Europea del 6 ottobre 2015 relativa alla causa C-362/14, Maximillian Schrems vs. Data Protection Commissioner, in *www.Curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=IT*, secondo la quale gli USA offrono un livello di tutela dei dati personali inferiore rispetto a quello esistente nella UE. Cfr. M. BONINI, *Sicurezza e tecnologia, fra libertà negative e principi liberali. Apple, Schrems e Microsoft: o dei diritti "violabili" in nome della lotta al terrorismo e ad altri pericoli, nell'esperienza statunitense ed europea*, in *AIC*, 2016, 3, p. 30 ss., la quale sottolinea l'importanza di proteggere i diritti fondamentali della persona dalle nuove tecnologie e dalle ingerenze del governative.

[18] Sulle più recenti problematiche di trasferimento dei dati personali in paesi extra UE dopo l'entrata in vigore del regolamento UE 2016/679, v. L. VALLE – L. GRECO, *Transnazionalità del trattamento dei dati personali e tutela degli interessati, tra strumenti di diritto internazionale privato e la prospettiva di principi di diritto privato di formazione internazionale*, cit., p. 201 ss.

[19] Si tratta del c.d. GDPR (*General Data Protection Regulation*) ovverosia del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). Il nuovo regolamento è il più importante atto normativo ad oggi adottato dall'Unione Europea in materia di trattamento di dati personali; tra i primi commenti sui profili generali del regolamento anche con riguardo all'evoluzione normativa precedente si segnalano: M.G. STANZIONE, *Il regolamento europeo sulla "privacy": origini e ambito di applicazione*, in *Europa dir. priv.*, 2016, p. 1249 ss.; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, I, p. 184 ss.; ID., *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, Torino, 2016, II; G. FINOCCHIARO, *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Nuove leggi civ. comm.*, 2017, p. 1 ss.

[20] Ricorda come l'obiettivo principale del GDPR fosse quello di ovviare alla frammentazione della protezione dei dati personali nel territorio della UE S. BONAVITA – R. PARDOLESI, *GDPR e diritto alla cancellazione (oblio)*, in *Danno e resp.*, 2018, p. 271 ss.

[21] Cfr. M.J. BONELL, *Unificazione internazionale del diritto*, in *Enc. Dir.*, XLV, 1992, p. 720 ss.; E. LUCCHINI GUASTALLA, *Il nuovo regolamento europeo sul trattamento dei dati personali*, in *Giustiziacivile.com*, 2017, 8. Già nella Relazione della Commissione, del 15 maggio 2003, intitolata «Prima relazione sull'applicazione della direttiva sulla tutela dei dati» (95/46/CE) – [COM(2003) 265 def.], si poneva in evidenza che gli «obiettivi della politica del mercato interno non sono invece stati pienamente raggiunti. La legislazione in materia di tutela dei dati diverge ancora notevolmente tra gli Stati membri. Queste disparità impediscono alle organizzazioni multinazionali di definire politiche paneuropee in materia di tutela dei dati».

«quattro libertà»[22] (libera circolazione delle persone, dei servizi, delle merci e dei capitali), ma anche sulla «libera circolazione delle informazioni»[23].

Si ricordi però che l'uso del regolamento europeo in questa materia aveva destato alcune perplessità, in quanto, per i diritti della persona il «Trattato prevede un'azione europea volta ad "armonizzare", "ravvicinare", "coordinare" i diritti nazionali mediante direttive» sicché sarebbe «da ritenere illegittimo il ricorso a un regolamento il cui effetto sia quello di "unificare", "rendere identici" tali diritti»[24].

Ma, una lettura gius-economica[25] della normativa conduce a rilevare che, coerentemente con il contenuto della Direttiva 46/95/CE, oggetto del GDPR è il trattamento dei dati personali e non la *privacy* in senso stretto, intesa come diritto fondamentale della persona. Non si tratta, cioè, di una norma volta a disciplinare direttamente ed in via esclusiva un diritto della personalità, ma di una specifica regolamentazione di un rapporto giuridico tra il professionista (o la Pubblica amministrazione) e le persone fisiche con cui viene in contatto, che si instaura tra loro per effetto del semplice "trattamento"[26] di dati personali, che ben può (e nella prospettiva economica, deve) essere disciplinata in modo uniforme[27].

Inoltre, una simile uniformazione della circolazione delle informazioni deve essere letta oggi nel mutato contesto giuridico caratterizzato dal processo di costituzionalizzazione[28] della Carta di Nizza attraverso il Trattato di Lisbona, che implica un'uniformazione dei

---

[22] Sul punto v. S. AMOROSINO, *La "costituzione economica": note esplicative di una nozione controversa*, in *Riv. trim. dir. ec.*, 2014, p. 229.

[23] Ciò, ove le informazioni non siano ontologicamente riconducibili alla categoria dei beni o dei servizi, ma siano strumentali alla circolazione delle merci, dei servizi e dei capitali.

[24] Sull'utilizzo improprio dello strumento del regolamento europeo a fini unificatori, là dove sarebbe consentito solo l'uso della direttiva con finalità di armonizzazioni cfr., con ampi richiami bibliografici in nota, P. FOIS, *Dall'armonizzazione all'unificazione dei diritti interni nell'Unione europea. Valutazione critica di una tendenza in atto*, in *Studi sull'integrazione europea*, VII (2012), p. 237 ss. e, in particolare, p. 253.

[25] Considera i dati personali come possibile «merce di scambio», illustrando le diverse teorie del concetto economico di privacy J. ARPETTI, *Economia della "privacy": una rassegna della letteratura*, in *Riv. dir. media*, 2018, p. 4 ss.

[26] Il concetto di «trattamento» è definito, all'art. 4 regolamento UE 2016/679: «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».

[27] L'esigenza di uniformare ed «europeizzare» la disciplina del trattamento dei dati personali mediante la «circolazione dei modelli giuridici tra i diversi paesi europei» era già sentita con riguardo alla direttiva 95/46/CE; sul punto cfr. N. LUPO, *Le fonti normative della* privacy*, tra esigenze di aggiornamento e ricerca di stabilità*, in V. Cuffaro – R. D'Orazio – V. Ricciuto (a cura di), *Il codice del trattamento dei dati personali*, cit., p. 777 ss. Il considerando 170 del regolamento UE 2016/679 ha affermato che poiché «l'obiettivo del presente regolamento, vale a dire garantire un livello equivalente di tutela delle persone fisiche e la libera circolazione dei dati personali nell'Unione, non può essere conseguito in misura sufficiente dagli Stati membri ma, a motivo della portata e degli effetti dell'azione in questione, può essere conseguito meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea (TUE). Il presente regolamento si limita a quanto è necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo».

[28] Cfr. A. SPADARO, *La "cultura costituzionale" sottesa alla Carta dei Diritti Fondamentali dell'UE. Fra modelli di riferimento e innovazioni giuridiche (Relazione alla giornata di studio su "La Carta dei diritti dell'Unione Europea e le altre Carte (ascendenze culturali e mutue implicazioni)", Messina, 16 ottobre 2015)*, in *Dir. pubb. comm. eur.*, 2016, p. 297 ss.

diritti della persona[29] ivi disciplinati a livello europeo, tra i quali deve essere ricordato proprio il diritto alla protezione dei dati personali. Tali diritti, peraltro, sono ritenuti spesso preminenti rispetto all'attività d'impresa[30], per cui non possono essere in alcun modo pregiudicati dall'uniformità di trattamento derivante dall'adozione di un regolamento europeo sui dati personali.

Le difficoltà connesse all'uniformità della disciplina del trattamento dei dati personali concernono l'individuazione di un bilanciamento tra un diritto introdotto solo di recente negli ordinamenti giuridici contemporanei e gli altri diritti fondamentali preesistenti. Ad esempio, nella patria della privacy, gli USA, il bilanciamento di interessi tra diritto alla riservatezza del cittadino e poteri d'indagine del governo per finalità antiterroristiche[31] ha subito un'ampia rivisitazione a seguito dell'introduzione del *Patriot Act*[32] del 2001. Le esigenze dettate dalla sicurezza nazionale[33] hanno così consentito di comprimere[34] taluni diritti di libertà acquisiti dai singoli cittadini (non solo[35]) americani a beneficio della collettività.

Una problematica meno evidente, ma non dissimile, né meno rilevante, esiste nell'UE con riguardo all'individuazione di un corretto bilanciamento di interessi tra l'attività

[29] Sulle critiche al riduzionismo economico v. P. PERLINGIERI, *Diritto dei contratti e dei mercati,* in *Rass. dir. civ.*, 2011, p. 876 ss.

[30] Con il nuovo regolamento UE 2016/679 si è emancipato il diritto alla «privacy da quella connessione alla dimensione economica propria del consolidamento del mercato interno che invece caratterizzava, almeno *ab origine*, il portato normativo della direttiva 95/46»; così: O. POLLICINO, *Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale*, in *Federalismi*, 2014, p. 6. Una soluzione interpretativa che mantenga la centralità del principio personalistico anche con riferimento all'applicazione della normativa europea sul trattamento dei dati personali è offerta da F. BRAVO, *Sul bilanciamento proporzionale dei diritti e delle libertà "fondamentali", tra mercato e persona: nuovi assetti nell'ordinamento europeo?*, in *Cont. imp.*, 2018, p. 204 ss.

[31] Pone in evidenza le difficoltà di trovare un bilanciamento di interessi tra sicurezza della collettività e diritti della persona F. ROSSI DAL POZZO, *La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona (dal Safe harbour al Privacy shield)*, in *Riv. dir. inter.*, 2016, p. 717 ss.

[32] A seguito dell'attacco terroristico alla «Torri gemelle» dell'11 settembre 2001, il sistema dei «pesi e contrappesi» nella ricerca dell'equilibrio nel rapporto tra sicurezza nazionale e privacy si veda: A. ETZIONI, *How Patriotics is the Patriot Act? Freedom versus Security in the Age of Terrorism, Routledge*, New York-London, 2004, p. 44 ss.; cfr. anche: U. PAGALLO, *La tutela della privacy negli Stati Uniti d'America e in Europa*, Milano, 2008, p. 27 ss.

[33] Anche in Europa, tuttavia, si è reso necessario un nuovo bilanciamento di interessi tra privacy e sicurezza nazionale. Per tale ragione, unitamente al *Regolamento*, è stata emanata la Direttiva (UE) 2016/680 «relativa al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali». Sul tema v. P. TROISI, *La protezione dei dati trattati a fini di prevenzione e accertamento dei reati*, in *La nuova disciplina europea della privacy*, a cura di S. Sica – V. D'Antonio – G. M. Riccio, cit., p. 327 ss.

[34] Tale orientamento è in corso di revisione con taluni interventi normativi segnalati da: E. CHITI, *Verso una riforma dei programmi statunitensi di sorveglianza*, in *Riv. trim. dir. pubb.*, 2014, 2, p. 555 ss.

[35] Diversi problemi relativi la protezione dei dati anche di cittadini anche non statunitensi si sono posti circa la raccolta e lo scambio tra gli Stati UE dei dati riguardanti i passeggeri nel mercato del trasporto aereo (PNR, *Passenger Name Records*). In tale occasione era stata riaffermata l'esigenza del rispetto del principio di proporzionalità. V. Corte di Giustizia 30 maggio 2006, in cause riunite C-317/04 e C-318/04, che ha annullato la decisione del Consiglio 17 maggio 2004, 2004/496/CE, relativa alla conclusione dell'accordo tra la Comunità europea e gli Stati Uniti d'America sul trattamento e trasferimento dei PNR da parte dei vettori aerei all'ufficio doganale e di protezione dei confini del dipartimento per la sicurezza interna degli Stati Uniti, e la decisione della Commissione 14 maggio 2004, 2004/535/CE, relativa al livello di protezione adeguato dei dati personali contenuti nelle schede nominative dei passeggeri aerei trasferiti all'Ufficio delle dogane e della protezione delle frontiere degli Stati Uniti *United States' Bureau of Customs and Border Protection*.

d'impresa e il diritto alla privacy[36] delle persone fisiche, specie là dove il trattamento dei dati personali svolto nell'ambito di attività economiche abbia una rilevanza sistemica nel buon funzionamento dei mercati a tutela dei consumatori o di ampi ceti di utenza, come avviene ordinariamente nelle attività svolte dalle imprese finanziarie.

Invero, l'attività delle imprese finanziarie, soprattutto dopo la stagione del "risparmio tradito", è disciplinata da una densa normativa di matrice europea volta a fissare nuove regole comuni[37] aventi come obiettivo la tutela di interessi collettivi, quali la stabilità e l'efficienza dei mercati, che riverbera i suoi effetti positivi proprio sugli utenti di tali imprese. Il trattamento dei dati personali dei clienti, reso indispensabile e financo obbligatorio nei rapporti con la clientela, diventa, dunque, come si dirà tra breve, un aspetto delle relazioni commerciali attraverso il quale si persegue, nel contempo, il legittimo fine di lucro dell'impresa e l'interesse generale alla stabilità dei mercati.

Il regolamento UE 2016/679, contiene tuttavia oltre ad alcune importanti novità anche talune norme di rinvio alle legislazioni statali[38] alle quali è demandato il compito di compiere specifiche scelte di politica del diritto riguardanti le modalità di applicazione e l'ampiezza dei diritti posti a tutela dell'interessato. Pertanto, le diverse normative nazionali di adeguamento possono ancora tradursi in differenze di regolazione dell'attività delle imprese nei singoli Stati membri – talvolta rilevanti sul piano applicativo – così da rendere più complessa e onerosa la funzione di *compliance* [39]nelle imprese multinazionali e falsare financo i meccanismi concorrenziali[40] all'interno dello stesso mercato unico europeo.

---

[36] Per una critica ai nuovi bilanciamenti di interessi tra persona e mercato introdotti con il regolamento UE 2016/679 dovuta al rischio di lesione del principio personalistico v. F. BRAVO, *Sul bilanciamento proporzionale dei diritti e delle libertà "fondamentali", tra mercato e persona: nuovi assetti nell'ordinamento europeo?*, cit., p. 204 ss.

[37] Ad esempio, il Considerando n. 58 della MiFID II, Direttiva 2014/65/UE, ricorda come «per contribuire all'istituzione di regole uniche per i mercati finanziari dell'Unione, aiutare a rafforzare ulteriormente le condizioni di parità per gli Stati membri e i partecipanti ai mercati, aumentare la tutela degli investitori e migliorare la vigilanza e l'applicazione delle norme, l'Unione si è impegnata a minimizzare, ove possibile, la discrezionalità di cui gli Stati membri dispongono nell'ambito della normativa dell'Unione sui servizi finanziari».

[38] Vi sono alcune norme del regolamento UE 2016/679, come ad esempio l'art. 23 che prevede che il diritto dell'Unione o dello Stato membro possano limitare, mediante misure legislative, la portata degli obblighi e dei diritti riconosciuti all'interessato dagli artt. da 12 a 22. Si veda anche l'art. 9 che consente agli Stati membri di mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute. Del pari si opera un rinvio alle normative nazionali per singole materie come il giornalismo (art. 85) o il lavoro (art. 88) o per specifici compiti come la definizione delle sanzioni (art. 84). Cfr. M. CASTELLANETA, *L'incidenza del regolamento GDPR sul quadro normativo esistente*, in *Notariato*, 2018, p. 259 ss.

[39] M. HINTZE, *Viewing the GDPR through a de-identification lens: a tool for compliance, clarification, and consistency*, in *International Data Privacy Law*, 1 February 2018, p. 86 ss.

[40] La crescente importanza economica dei dati personali rende il livello di protezione della privacy un elemento rilevante nella scelta dei prodotti e dei servizi da parte dei clienti, incidendo, dunque, sulla concorrenza non di prezzo (qualità) nei mercati. Sul tema e con riguardo ai social network professionali si veda: SAMSON Y ESAYAS, *Competition in (data) privacy: 'zero'-price markets, market power, and the role of competition law*, in *International Data Privacy Law*, 1 August 2018, 181 ss. Sul tema della concorrenza si veda anche: REYNA; *The psychology of privacy—what can Behavioural Economics contribute to competition in digital markets?*, in *International Data Privacy Law*, 1 August 2018, p. 240 ss.; per l'importanza della circolazione delle informazioni nel mercato anche nella prospettiva della tutela dei meccanismi concorrenziali v. A. DE NICOLA – D. PORRINI, *Scambio di informazioni e mercato assicurativo analisi economica del diritto antitrust in Italia e USA*, in *Concorrenza e mercato. Rassegna degli orientamenti dell'Autorità Garante*, Milano, 2007, p. 179 ss.

2. Il D.lgs n. 101/2018[41] ha introdotto le disposizioni per l'adeguamento della normativa nazionale alle norme contenute nel regolamento (UE) 2016/679 e conclude, sul versante interno, il complesso[42] *iter* normativo volto a innovare la disciplina del trattamento dei dati personali nell'ordinamento giuridico europeo, rispetto al precedente sistema implementato dalla direttiva 95/46/CE.

Il decreto legislativo in parola ha novellato il D.lgs 196/2003 (c.d. Codice privacy) con un articolato sistema di abrogazioni e di integrazione delle norme preesistenti, rendendone assai complessa[43] la lettura e il coordinamento con le regole europee. Il GDPR in tal modo, vede in parte intaccata la natura esaustiva e la sua vocazione uniformatrice che doveva caratterizzarlo *ab origine*, rendendo prevedibili futuri interventi normativi volti a razionalizzare e coordinare l'ubicazione delle diverse norme ed evitare inutili dispute interpretative.

Si rende, dunque, necessario ricostruire le condizioni di liceità e i limiti dell'utilizzo dei dati personali acquisiti dalle imprese finanziarie nei rapporti con gli utenti[44], considerato che la conoscenza del cliente attraverso i suoi dati personali è divenuta (anche) nelle imprese finanziarie un fattore produttivo indispensabile ad ideare nuove strategie di marketing, ad ingegnerizzare prodotti e servizi finanziari adeguati e a collocarli più efficacemente sul mercato. In tal modo le imprese aumentano la propria capacità penetrativa nel mercato, soddisfano meglio le esigenze di diverse categorie di clientela e possono scongiurare l'acquisto su larga scala di prodotti finanziari inadeguati contribuendo, così, a ridurre i rischi di crisi sistemiche. Per tale ragione ogni nuova disciplina del trattamento dei dati personali costituisce una specifica e stringente regolazione delle attività economiche e incide inevitabilmente sugli adempimenti delle imprese finanziarie nei rapporti con la clientela.

---

[41] Si tratta delle «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)", emanate sulla base della delega contenuta nell'articolo 13 della legge n. 163 del 2017 (legge di delegazione europea 2016-2017) », che ha consentito di emanare provvedimenti legislativi atti ad armonizzare le disposizioni nazionali in vigore prima del 25 maggio 2018 con i contenuti del Regolamento UE 2016/679. Non vede un eccesso di delega nella normativa nazionale di adeguamento al regolamento UE 2016/679 G. DE GREGORIO, *Sull'eccesso di delega del decreto legislativo di adeguamento del Codice "Privacy" alla disciplina del Regolamento (UE) 679/2016*, in *Riv. dir. media*, 2018, p. 1 ss.

[42] L'emanazione del Regolamento è stata preceduta da un lungo dibattito nelle commissioni legislative volto a stabilire le necessità di definizione degli ambiti di regolazione di tale complessa materia. Sul punto v. KROES – V. REDING, *Privacy matters-Why the EU needsnew personal data protection rules*, Brussels, 30 November 2010, in *http://euro-pa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/700.11*; M.G. STANZIONE, *Genesi ambito di applicazione*, in *La nuova disciplina europea della privacy*, a cura di S. Sica – V. D'Antonio – G.M. Riccio, cit., p. 13 ss.

[43] Una critica pienamente condivisibile sulla (in)comprensibilità della nuova formulazione delle norme contenute nel Codice Privacy è espressa da V. CUFFARO, *Quel che resta di un codice: il D.Lgs. 10 agosto 2018, n. 101 detta le disposizioni di adeguamento del codice della privacy al regolamento sulla protezione dei dati*, in *Corr. giur.*, 2018, p. 1183 ss.

[44] I rischi connessi alla mancanza di un valido consenso fornito dagli utenti di imprese che operano sul web a livello globale e che limitano anche l'accesso e il controllo da parte degli utenti alle loro informazioni personali, con specifico riguardo a Google e Facebook, sono ben evidenziati da A. ESTEVE, *The business of personal data: Google, Facebook, and privacy issues in the EU and the USA*, *cit.*, p. 36 ss.

Per quanto qui di interesse, il nuovo complesso di norme che deriva dalla lettura «adeguata» del GDPR e del Codice Privacy non reca particolari novità che connotano l'ordinamento italiano sul piano del trattamento dei dati personali c.d. comuni da parte delle imprese finanziarie. Si può, al più, segnalare l'introduzione, in fase di adeguamento all'art. 2 *ter*, paragrafo 4, D.lgs n. 101/2018, delle definizioni[45] di specifiche attività di trattamento quali la «comunicazione» e la «diffusione» dei dati personali, che si rileva particolarmente utile proprio nei mercati finanziari, là dove la «comunicazione» dei dati è ammessa nei casi consentiti dalla legge o dalla volontà dell'interessato, mentre è tendenzialmente esclusa la loro «diffusione».

Ad esempio, il contenuto di alcune recenti direttive come la MiFID 2[46] e la PSD 2[47], ha evidenziato che nei mercati finanziari la circolazione dei dati personali connessa al collocamento di taluni prodotti o all'erogazione di specifici servizi è indispensabile anche con finalità di tutela del cliente, ma essa può e (in taluni casi deve) avvenire nella forma della «comunicazione», ma non della «diffusione».

Anche in quest'ottica, il consenso[48] espresso dell'interessato quale presupposto di liceità del trattamento dei dati comuni ha perso definitivamente la sua centralità, anche dopo la normativa di adeguamento, per divenire solo uno fra i sei casi di liceità previsti dal regolamento UE 2016/679[49] alternativi e di pari rilevanza (cfr. art. 6)[50]. Tra essi deve essere ri-

[45] Secondo l'art. 2-*ter*, par. 4, del D.lgs 101/2018, si «intende per: a) "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-*quaterdecies*, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione; b) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione».

[46] MiFID II (2014/65/EU) *Markets in Financial Instruments Directive 2*, si tratta della Direttiva europea 2014/65/UE del Parlamento Europeo e del Consiglio del 15 maggio 2014 relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/CE e la direttiva 2011/61/UE.

[47] PSD2 (2015/2366/EU) *Payment Services Directive 2*, si tratta della Direttiva europea del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE.

[48] Il «consenso dell'interessato» è definito dall'art. 4, n. 11, come la «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». Il tema poliedrico della natura e della funzione del «consenso» nella normativa sul trattamento dei dati personali è affrontato da V. CARBONE, *Il consenso, anzi i consensi nel trattamento informatico dei dati personali*, in *Danno e resp.*, 1998, p. 23 ss. S. MAZZAMUTO, *Il principio del consenso e il problema della revoca*, in R. Panetta (a cura di), Libera circolazione e protezione dei dati personali, I, Milano, 2006, p. 1000 ss.

[49] Il consenso aveva perso la sua centralità quale presupposto di liceità per il trattamento dei dati personali sin dall'emanazione delle prime leggi di attuazione della Direttiva 46/95/CE in ragione delle numerose eccezioni in esse previste. Nel regolamento UE 2016/679 il consenso ha perso definitivamente il ruolo di principale criterio di liceità ed ha palesato la sua insufficienza a fornire una tutela adeguata all'interessato, come posto in evidenza da v. M.G. STANZIONE, *Genesi ambito di applicazione*, in *La nuova disciplina europea della privacy*, a cura di S. Sica – V. D'Antonio – G.M. Riccio, cit., 17 ss.; A. THIENE, *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo regolamento europeo*, in *Nuove leg. civ. comm.*, 2017, p. 416 ss.

[50] Pone in evidenza come il consenso sia l'alternativa a una pluralità di casi tutti riconducibili a ipotesi in cui il trattamento è considerato «necessario» dalla legge: E. LUCCHINI GUASTALLA, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Cont. imp.*, 2018, p. 111 ss.

cordato – *in primis* – il caso in cui il trattamento sia «necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso», ai sensi dell'art. 6, par. 1, lett. b). In tal caso il cliente dell'impresa finanziaria non deve esprimere un consenso ulteriore (rispetto alla volontà negoziale) per il trattamento dei dati personali reso necessario dall'adempimento degli obblighi e delle finalità contrattuali.

Ma un chiaro segnale verso una relativizzazione della rilevanza della volontà dell'interessato lo ha fornito il legislatore europeo quando, ha introdotto la lett. f), dell'art. 6, ove l'uso del dato personale (comune) senza il consenso dell'interessato è ammesso quando «è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato (…)».

La fattispecie anzidetta si può riferire certamente alle imprese finanziarie, le quali sono portatrici di un duplice interesse complesso anche di rilevanza pubblica, che può essere scomposto nel diritto di iniziativa economica[51] e nella peculiare funzione di protezione della stabilità e del corretto funzionamento dei mercati finanziari, a fronte dell'uso del dato personale dei clienti, che non leda diritti o libertà fondamentali degli interessati. Il Considerando n. 47 del regolamento UE 2016/679 reputa, infatti, legittimi gli interessi del *titolare* di trattare dati personali, senza il consenso dell'interessato, per finalità ultronee rispetto a quelle contrattuali, quando esista tra loro una relazione pertinente e appropriata come nell'ipotesi in cui il secondo sia un cliente o sia alle dipendenze del primo. In ogni caso, l'esistenza di legittimi interessi del *titolare* richiede un'attenta valutazione basata anche sull'eventuale circostanza, esistente al momento e nell'ambito della raccolta dei dati personali, per la quale l'interessato possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine.

Si deve considerare a questo proposito che, nell'ordinamento italiano, il mercato finanziario è caratterizzato dalla cogenza del «diritto al risparmio» tutelato dall'art. 47 Cost[52], la cui rilettura, coordinata con le norme del TFUE, consente oggi di affermare che «oggetto della tutela dell'art. 47 non è il risparmio in quanto tale, quanto piuttosto quello che grazie all'esistenza e al corretto funzionamento del mercato si risolve in un investimento finanzia-

[51] Riconduce alla libertà di iniziativa economica il diritto di trattare dati personali nelle attività d'impresa: F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Milano, 2018, p. 143 ss.

[52] La dottrina più attenta sul tema ha chiarito che tale norma «va oggi considerata il pilastro sul quale si fondano tutti i pubblici poteri nazionali di regolamentazione e di controllo delle attività finanziarie delle più diverse specie: bancarie, di intermediazione in senso stretto, assicurative e relative alla previdenza complementare, perché tutte hanno in comune la "materia prima", appunto il risparmio. In sintesi: l'art. 47 è divenuto l'"ombrello costituzionale" cui sono riconducibili le regolamentazioni, in senso lato, di tutte le attività finanziarie»; così: S. AMOROSINO, *La "costituzione economica": note esplicative di una nozione controversa*, in *Riv. dir. ec.*, 2014, p. 234 s. La tutela del risparmio non trova un omologo direttamente individuabile nelle fonti costituzionali europee, per cui essa dovrebbe essere desunta da altri principi dell'ordinamento dell'UE, quali la «libertà di stabilimento», la «libera prestazione dei servizi» la «stabilità dei prezzi» ed altri (cfr. M. SEMERARO, *Principio di condivisione degli oneri e tutela del risparmio. Scritto per il Convegno «Salvataggio bancario e tutela del risparmio»*, in *Riv. dir. banc. (dirittobancario.it)*, 2016). Si tratta di principi non immediatamente riconducibili al «diritto al risparmio», ma che appaiono funzionali al raggiungimento delle finalità dell'UE nella «creazione di un mercato comune basato sulla libera concorrenza, all'istituzione di una politica monetaria europea, alla protezione dei consumatori e via dicendo»; così: G. AMATO, *L'informazione finanziaria* price-sensitive, Firenze, 2013, p. 32.

rio. Nella rinnovata convinzione che promuovendo e tutelando quest'ultimo e le aspettative di redditività dell'investitore, oltre che l'interesse individuale, si soddisfi anche un interesse collettivo alla ottimale ed equilibrata distribuzione delle risorse e all'efficienza dell'intero sistema economico»[53].

Il diritto di iniziativa economica e la tutela del risparmio divengono, in concreto, difficilmente distinguibili nell'ambito delle attività svolte dalle imprese finanziarie nei confronti dei clienti. Le diverse attività di trattamento dei dati personali dei clienti potranno così essere finalizzate, ad esempio a profilare il cliente in adempimento della normativa MiFID 2 e – nel contempo – a selezionare il prodotto finanziario da collocare presso il cliente. Si può, quindi, affermare che un'interpretazione troppo stringente delle norme del GDPR con riguardo ai casi che introducano limitazioni[54] del diritto di trattare dati personali possa in concreto comprimere oltre alla libertà d'impresa anche il diritto al risparmio dei clienti delle stesse imprese finanziarie *ex* art. 47 Cost.

Vi è, invece, da ritenere che proprio l'esistenza del «diritto al risparmio» o quantomeno, in chiave comunitaria, della tutela dell'investitore e della stabilità dei mercati finanziari, consenta all'impresa finanziaria di utilizzare i dati personali dei clienti con maggiore libertà rispetto ad altre imprese che non operano in settori di mercato caratterizzati da interesse collettivo di rilevanza strategica per l'economia dei singoli Stati e del mercato unico dell'UE e nei quali l'alienazione di prodotti inadeguati o difettosi – anche su larghissima scala – non può generare crisi sistemiche.

La disciplina del trattamento del dato personale nei mercati finanziari dovrà adeguarsi alla «funzionalizzazione» dei rapporti contrattuali verso interessi ultronei rispetti ai soli interessi (privati) perseguiti dalle parti, per conformarsi ad interessi pubblici secondo una «tendenza a valutare la singola transazione in relazione agli effetti che essa produce sull'intero ordine degli scambi, dove il contratto si configura sempre meno come affare privato dei privati»[55]. Il dato fornito dal cliente, per ragioni contrattuali[56], ad un'impresa finanziaria pare del tutto compatibile con l'uso per fini di *marketing*[57], considerate anche le ricadute positive che possono aversi in termini di migliore soddisfazione delle esigenze di investimento e di risparmio del cliente.

Si deve poi considerare che l'interessato è un soggetto giuridico del mercato fortemente tutelato[58] dalle asimmetrie informative[59] nei rapporti con le imprese, il quale accetta

---

[53] Così: F. GUIZZI, *La tutela del risparmio nella Costituzione*, in *Filangieri*, 2-4, 2005, p. 171 ss.; riconduce al generale principio della stabilità monetaria l'esigenza di fornire una tutela costituzionale al risparmio L. DELLA LUNA MAGGIO, *Il risparmio tra tutele costituzionali e interventi legislativi*, in *AIC*, 2015, 4, p. 7 ss.

[54] Per una descrizione analitica delle condizioni che consentono la limitazione del diritto alla protezione del dato a favore di altri diritti di libertà v. F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, cit., p. 245 ss.

[55] Così: V. RICCIUTO, *Nuove prospettive del diritto privato dell'economia*, in E. Picozza – V. Ricciuto (a cura di), Diritto dell'economia, Torino, 2017, p. 274.

[56] Pone in evidenza i limi di efficacia del contratto rispetto alla circolazione degli attributi immateriali della personalità S. THOBANI, *Diritti della personalità e contratto. Dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Milano, 2018, p. 139 ss.

[57] Lo stesso considerando n. 47 del Regolamento 2016/679 afferma che può «essere considerato legittimo l'interesse a trattare dati personali per finalità di marketing diretto».

[58] È stato opportunamente posto in evidenza che accanto alla (solo parzialmente efficace) tutela civilistica, l'interessato è protetto anche da norme penali che puniscono specifiche ipotesi di uso illecito dei dati, v. sul

di assoggettarsi alle regole operanti nel settore delle contrattazioni dal quale intende ottenere prodotti o servizi. La volontà dell'interessato di accettare il trattamento dei propri dati personali (comuni) da parte di terzi si desume principalmente dal rapporto giuridico che il medesimo instaura con i terzi nel mercato, considerato che ormai una larga parte di beni o di servizi non può essere acquistata senza essere disposti a cedere i propri dati personali, nel quadro delle ampie tutele previste dalla normativa vigente.

In questo contesto, assume un ruolo assai rilevante e, per certi versi, determinante il principio di trasparenza[60] con specifico riguardo all'obbligo di informativa[61] previsto dall'art. 13 del regolamento UE 2016/679. Esso impone di comunicare *ex ante* all'interessato, tra le altre informazioni ivi analiticamente previste, anche le finalità del trattamento cui sono destinati i dati personali e, nell'ipotesi sopra descritta, «i legittimi interessi perseguiti dal titolare del trattamento o da terzi». In tal modo lo stesso conferimento del dato personale, anche se non accompagnato da un consenso al trattamento, può essere considerata una manifestazione di consapevolezza delle conseguenze dell'inserimento delle proprie informazioni personali nel traffico giuridico.

Inoltre, l'intera architettura dei sistemi informativi delle imprese finanziarie deve uniformarsi a tutti i principi contenuti nel regolamento in parola e alla c.d. privacy «by design» e «by default»[62], affinché la circolazione delle informazioni personali possa avvenire in ambiti sicuri e controllati *ab origine*, con conseguente maggiore protezione dei dati dei clienti. Le violazioni più gravi

Si consideri, poi, che nello specifico settore delle imprese finanziarie le informazioni tra le quali si annoverano anche i dati personali sono da sempre assoggettate a trattamenti gestiti sulla base di elevatissimi standard di sicurezza (fisica e logica), cui le imprese finanziarie hanno storicamente ispirato la loro condotta (oggi resa anche più efficiente con l'impiego di nuovi sistemi di cifratura informatica delle informazioni e pseudonimizzazione dei dati personali). Inoltre, i trattamenti «ultracontrattuali»[63] dei dati non comportano con-

---

punto V. ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *Riv. dir. media*, 2018, p. 4. Lo stesso D.P.R. 101/2018 ha introdotto delle fattispecie penali connesse a trattamenti illegittimi di dati personali mediante a riformulazione degli artt. 167 ss. del Codice privacy (D.lgs 196/03).

[59] Già nei primi anni novanta si parlava della rilevanza dell'«asimmetria informativa» nei rapporti economici tra imprese finanziarie e clienti; v. H.E. LELAND – D.H. PYLE, *Asimmetrie informative, struttura finanziaria e intermediazione*, in G. VACIAGO – G. VERGA, *Efficienza e stabilità dei mercati finanziari*, 1995, Bologna, p. 117 ss.; R. MASERA, *Intermediari, mercati e finanza d'impresa*, Roma, 1991, p. 65 ss.

[60] Le condizioni che consentono la limitazione del diritto alla protezione del dato personale previste dall'art. 52 della «Carta dei diritti dell'UE» sono illustrate analiticamente da F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, cit., p. 268 ss. In tema rimangono rilevanti sul punto i provvedimenti dell'Autorità Garante della concorrenza e del mercato del 20 dicembre 2001, nn. 10276, 10277, 10278 e 10279, in *Boll. Sett. AGCM*, n. 51-52, del 7 gennaio 2002, p. 148 ss.

[61] Sul ruolo delle informazioni nelle contrattazioni si possono richiamare gli scritti di S. GRUNDMANN, *L'autonomia privata nel mercato interno: le regole d'informazione come strumento,* in *Eur. dir. priv.*, 2001, p. 295 ss.; A. GENTILI, *Informazione contrattuale e regole dello scambio,* in *Riv. dir. priv.*, 2004, p. 555 ss.

[62] Sul punto v. A. PRINCIPATO, *Verso nuovi approcci alla tutela della* privacy: privacy by design e privacy by default settings, in *Contr. imp. Europa*, 2015, p. 197 ss.

[63] Si ricordi che l'art. 6, par. 4, prevede che qualora «il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, al fine di verificare se il trattamento

seguenze immediate in capo al singolo cliente, ma servono, al più, a creare nuove strategie di marketing destinate alla generalità della (futura) potenziale clientela.

3. Parzialmente differente pare il discorso con riguardo alle «categorie particolari di dati personali», sulla quale grava un generale divieto di trattamento, che però soffre di un rilevante numero di eccezioni analiticamente indicate nell'art. 9[64], tra le quali, per quanto rileva in questa sede, si annoverano i casi in cui l'interessato abbia prestato il proprio consenso specifico ed esplicito all'uso di tali dati o vi sia una norma di legge che ne autorizza il trattamento. Le imprese finanziarie possono, quindi, trattare legittimamente tali dati appartenenti ai clienti e utenti sulla base del consenso espresso da ciascun interessato.

Vale, però, porre in evidenza come nella precedente normativa il consenso dovesse essere rilasciato con atto formale (scritto), mentre il regolamento UE 2016/679 stabilisce che il consenso deve essere espresso in modo "non equivoco", anche mediante un comportamento positivo e sulla base di una completa informativa (ma non necessariamente per iscritto), introducendo così una componente di notevole semplificazione degli adempimenti precontrattuali.

Quand'anche l'operato dell'impresa finanziaria sia indirizzato al perseguimento di un interesse pubblico quale quello sopra evidenziato, esso non pare possa rientrare nell'ipotesi di cui all'art. 9, lett. g). Secondo tale norma il trattamento di particolari categorie di dati (c.d. sensibili) può essere eseguito senza il consenso dell'interessato quando sia necessario per motivi di interesse pubblico ritenuto rilevante sulla base del diritto dell'Unione o degli Stati membri, purché sia proporzionato alla finalità perseguita, rispetti l'essenza del diritto alla protezione dei dati e preveda misure appropriate e specifiche per tutelare l'interessato.

Invero, gli stringatissimi considerando (55-56) del GDPR riferibili a tale norma limitano l'ambito di operatività ai soli soggetti pubblici. Inoltre, in sede di adeguamento l'art. 2-*sexies* del D.lgs 101/2018, concernente il trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante, ha ribadito che tali i trattamenti sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero da norme degli ordinamenti interni. Lo stesso art. 2-*sexies*, in conformità al previgente art. 26 Dl.gs 196/2003, ha previsto che il trattamento possa essere consentito anche da una norma di fonte regolamentare purché essa specifichi i "tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato". Il comma 2

per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro: a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto; b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento; c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10; d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati; e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione».

[64] Sottolinea la rilevanza dell'ampliamento delle «categorie particolari di dati personali» indicate nell'art. 9 rispetto alla previgente nozione di «dati sensibili» M. GRANIERI, *Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679*, in *Nuove leggi civ. comm.*, 2017, p. 167 ss.

dell'art. 2-*sexies* ha limitato le ipotesi di interesse pubblico rilevante a specifici casi tassativi tutti riferibili all'attività dei (soli) soggetti pubblici. In tal modo si è data attuazione ad un assunto – mai compiutamente dimostrato – secondo il quale occorre guardare con sfiducia all'operato del privato (imprenditore), mentre si può presumere la legittimità della condotta del soggetto pubblico.

In altre parole, il caso dell'interesse pubblico perseguito da un soggetto privato mediante il trattamento di dati personali è oggi consentito, senza il consenso dell'interessato, nelle sole ipotesi in cui esso sia espressamente autorizzato da una norma di legge o da una norma UE.

In tal modo si è persa un'occasione per conferire un'interpretazione ampia della norma anzidetta, che permettesse un'adeguata rilevanza agli interessi pubblici di cui sono portatrici le imprese finanziarie, che giustificasse una maggiore libertà nella circolazione dei dati anche "sensibili", sia pure con tutte le garanzie di legge, ove essa riguardi un'attività tesa a preservare il buon funzionamento e la stabilità dei mercati finanziari. In sede di adeguamento poteva anche essere tratto un importante argomento a favore del bilanciamento verso gli interessi collettivi sottesi ai mercati finanziari, da tradursi in termini di semplificazione dell'operato delle attività delle imprese finanziarie, dall'art. 23 del regolamento UE 2016/679, che consente la compressione delle principali tutele offerte all'interessato dallo stesso regolamento da introdursi per legge nei singoli Stati. Ciò è possibile quando la riduzione delle tutele si riveli necessaria per il raggiungimento di «altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria (...)».

4. Alcuni «dati sensibili»[65] mostrano una specifica attitudine ad incidere su aspetti particolarmente intimi della persona, da essi si sono stati tenuti distinti i dati definiti «supersensibili»[66]. In quest'ambito, tra le altre novità[67] introdotte dal regolamento UE 2016/679 vi è l'unificazione delle «categorie particolari di dati personali»[68] *ex* art.9, in cui è contenuta anche la specifica definizione di «dati biometrici» e dei «dati genetici», contenuta nell'art. 4, nn. 13 e 14[69], unitamente ad una disciplina *ad hoc*[70], che li colloca tra le particolari categorie di dati di cui all'art. 9.

[65] Vedi nota 15.

[66] La categoria dei «dati super sensibili» non trova riscontro nel dato normativo ed è di creazione dottrinale. Ci si riferisce ad essa con riguardo a i dati sanitari, ai dati biometrici e ai dati genetici, i quali sono divenuti nel tempo oggetto di una regolamentazione specifica più rigorosa, fondata anche sui provvedimenti del Garante.

[67] Alcune tipologie di dati come i dati «biometrici» e «genetici» – assai rilevanti in campo bancario e assicurativo – erano genericamente ricondotte nell'ampia categoria dei dati personali che «presentano rischi specifici» di cui all'art. 17, D.lgs 196/2003 (Codice per il trattamento dei dati personali), ma non erano considerati «dati sensibili».

[68] In essa rientrano tanto i «dati sensibili» quanto i «dati super sensibili» (quali i «dati genetici» e i «dati biometrici»).

[69] Per la nozione e le specifiche problematiche legate ai «dati super sensibili» v. F. ASTIGGIANO, *Illecito trattamento di dati "supersensibili" e risarcimento del danno (Nota a Cass. Sez. I civ. 19 maggio 2014, n. 10947; Cass. Sez. I civ. 13 maggio 2015, n. 9785)*, in *Famiglia dir.*, 2016, p. 471 ss.

Sulla base di un consolidato orientamento espresso nei provvedimenti del Garante prima dell'emanazione del GDPR si riteneva che alcuni dati «super sensibili» come i dati biometrici e genetici, non potessero essere trattati del tutto liberamente, ancorché il titolare avesse attenuto il preventivo consenso dell'interessato. Essi sono divenuti rilevanti nell'attività delle imprese finanziarie, in quanto possono essere utilizzati come sistemi di identificazione del cliente o come strumento per il calcolo del rischio nei contratti di assicurazione. Per il trattamento di tali dati l'art. 17, D.lgs 196/2003, prevedeva una complessa procedura di interpello preventivo al Garante, il quale doveva fornire specifiche prescrizioni per i trattamenti che presentassero rischi particolari per i diritti e le libertà fondamentali o per la dignità dell'interessato.

La nuova disciplina contenuta nel regolamento in parola si è rivelata meno stringente, in quanto non prevede più l'obbligo di interpello preventivo, salvo specifica regolamentazione introdotta con le diverse normative nazionali di adeguamento, alle quali il menzionato art. 9 fa espresso riferimento. Più precisamente, i legislatori nazionali hanno il potere di mantenere o introdurre limitazioni con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute, e possono, quindi disciplinarne il trattamento in modo più rigoroso[71], sino al punto di sottrarre il trattamento di queste categorie di dati all'autonomia dell'interessato (cfr. anche art. 9[72], lett. a).

Il legislatore italiano ha ritenuto di utilizzare le facoltà demandategli dal GDPR introducendo con l'art. 2-*septies* del D.lgs 101/2018 specifiche limitazioni al trattamento dei dati genetici, biometrici e relativi alla salute. In particolare, il trattamento di tali categorie di dati è stato assoggettato ad un controllo di conformità rispetto alle "misure di garanzia" che il Garante dovrà emanare con specifici provvedimenti cui la norma in parola fa riferimento. Tuttavia lo stesso art. 2-*septies* non determina con esattezza i limiti entro i quali i suddetti dati possano essere legittimamente trattati, ma contiene – come già detto – un mero (ed ulteriore) rinvio al contenuto dei futuri e mutevoli provvedimenti del Garante[73], che dovranno stabilire le misure di garanzia con cadenza almeno biennale sulla base di una pluralità di variabili di natura giuridica, tecnica e tecnologica.

Può già dirsi che, anche in questo caso, la tecnica normativa non pare fornire quel perimetro di certezza e uniformità attesa dai destinatari delle norme, per i quali il buon funzionamento dell'impresa dipende, ormai, dal grado libertà con il quale si possono utilizzare le informazioni necessarie all'espletamento delle loro attività commerciali.

---

[70] Sulle novità relative alla disciplina dei dati genetici e biometrici v. anche M. GRANIERI, *Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679*, cit., p. 167 ss.

[71] Secondo il Considerando n. 53 Regolamento (UE) 2016/679 gli «Stati membri dovrebbero rimanere liberi di mantenere o introdurre ulteriori condizioni, fra cui limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute, senza tuttavia ostacolare la libera circolazione dei dati personali all'interno dell'Unione quando tali condizioni si applicano al trattamento transfrontaliero degli stessi.

[72] L'interessato può rendere lecito il trattamento dei dati sensibili attraverso il proprio consenso esplicito per una o più finalità specifiche, ma il regolamento prevede che questa autonomia possa essere limitata nei casi in cui il diritto dell'Unione o degli Stati membri disponga che l'interessato non possa revocare il divieto al trattamento di tali dati.

[73] Sul ruolo ormai determinate che assume il Garante nell'integrazione del contenuto delle norme del regolamento 2016/679 anche in fase applicativa v. V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali*, in *Cont. imp.*, 2018, p. 1118 ss.

Tuttavia, un piccolo passo in avanti è stato compiuto dal paragrafo 7 dell'art. 2 *septies*, che consente maggiore libertà nel trattamento dei dati biometrici limitatamente alle procedure di accesso fisico e logico ai dati da parte dei soggetti autorizzati, sia pure nel rispetto del quadro normativo posto dal GDPR. In tal modo è stato semplificato nel comparto bancario l'uso di impianti di rilevazione delle impronte digitali o vocali, o basati sulla lettura della topografia della mano, per l'accesso dei clienti e dei dipendenti ad aree ad ingresso controllato quali, ad esempio, i *caveau* o gli ambienti destinati ad ospitare le cassette di sicurezza[74], coerentemente con quanto già disposto in precedenza dai provvedimenti del Garante[75].

Inoltre, con l'avvento delle nuove tecnologie, i «dati biometrici»[76] si sono rivelati particolarmente utili nel fornire nuovi strumenti per il miglioramento dei rapporti contrattuali con la clientela in termini di dematerializzazione[77] degli strumenti e dei servizi finanziari e, in generale, dei documenti anche contrattuali fondati su sistemi ad autenticazione grafometrica di firma elettronica avanzata[78], che può dirsi oggi definitivamente legittima.

Vi è, dunque, da ritenere che in considerazione della previsione di cui al paragrafo 7 dell'art. 2 *septies* e dei numerosi vantaggi che possono derivare alla clientela in termini di qualità, costi, sicurezza ed efficienza dei servizi e dei prodotti, anche l'uso dei dati biometrici nell'ambito appena richiamato debba considerarsi completamente disponibile da parte dell'interessato, e rimesso, pertanto, alla sua volontà da esprimersi in sede contrattuale o attraverso uno specifico consenso, nel rispetto di tutte le garanzie imposte dal regolamento UE 2016/679.

---

[74] Garante per il trattamento dei dati personali, provvedimento, del 27 ottobre 2016, n. 438, relativo alla «Verifica preliminare. Utilizzo di un servizio di riconoscimento biometrico come sistema di autenticazione» (doc. web n. 5763201). Vede, tuttavia, maggiori rischi nel trattamento dei dati personali biometrici eseguito da imprese bancarie, tanto da configurare un'ipotesi autonoma di responsabilità oggettiva nei casi di danni derivati all'interessato per l'illecito trattamento A. MAGNI, *La responsabilità della banca per il trattamento dei dati biometrici*, in *Rass. dir. civ.*, 2018, p. 526.

[75] Garante per il trattamento dei dati personali, provvedimento del 6 febbraio 2014n. 56, relativo ad un «Sistema automatizzato di cassette di sicurezza basato sul rilevamento dell'impronta digitale dei clienti. Verifica preliminare richiesta da Banca degli Ernici di credito coop. ScpA» (doc. web 3000045).

[76] Il trattamento di dati biometrici comporta maggiori rischi in quanto si tratta di dati «direttamente, univocamente e in modo tendenzialmente stabile nel tempo, collegati all'individuo e denotano la profonda relazione tra corpo, comportamento e identità della persona»; in questo senso Provvedimento generale prescrittivo in tema di biometria, del 12 novembre 2014, n. 513 (doc. web n. 3556992).

[77] Tali innovativi servizi sono finalizzati a rendere più semplici, rapidi ed efficienti le contrattazioni con i clienti, aumentando la sicurezza delle singole operazioni bancarie e diminuendone in modo sensibile il costo. Segnala i rischi della dematerializzazione nella contrattualistica nei rapporti con i consumatori S. PAGLIANTINI, *Tutela del consumatore e limiti alla dematerializzazione dei contratti solenni*, in *Rass. dir. civ.*, 2011, p. 213 ss.

[78] Alcuni istituti di credito hanno adottato un servizio di firma digitale remota con autenticazione biometrica o sistema di firma elettronica avanzata con «bio-penna» per la sottoscrizione dei contratti bancari con la clientela. Tali strumenti erano stati ritenuti legittimi in precedenti provvedimenti del Garante (Garante per il trattamento dei dati personali, «Verifica preliminare relativa al trattamento di dati personali connesso all'utilizzo di un servizio di firma digitale remota con autenticazione biometrica - 28 maggio 2015», doc. web n. 4167873; Garante per il trattamento dei dati personali «Sistema di firma elettronica avanzata grafometrica. Verifica preliminare - 4 giugno 2015», doc. web n. 4172308; Garante per il trattamento dei dati personali «Verifica preliminare. Utilizzo di un servizio di firma elettronica avanzata con autenticazione biometrica - 17 dicembre 2015» doc. web n. 4645479).

Fatta eccezione per i casi sopramenzionati di dati biometrici, i dati super sensibili dovranno essere trattati sulla base di quanto periodicamente il Garante stabilirà, con le difficoltà causate dai continui adeguamenti delle policy aziendali e delle architetture interne dei sistemi informatici ed organizzativi delle imprese.

In estrema sintesi, si può, quindi, concludere affermando che la normativa nazionale di adeguamento al Regolamento UE 2016/679 non ha contribuito ad una maggiore chiarezza ed uniformità della disciplina del trattamento dei dati personali complessivamente intesa[79]. Si è, invero, reso più complicato stabilire un adeguato equilibrio sul piano giuridico tra l'interesse dell'impresa, la tutela dei clienti e il corretto funzionamento dei mercati finanziari. Mentre una più attenta considerazione degli interessi collettivi sottesi ai mercati finanziari avrebbe potuto condurre ad una semplificazione della circolazione delle diverse categorie di dati personali fondata su una disciplina uniforme dei presupposti di liceità e delle modalità di trattamento dei dati. Tale disciplina dovrebbe ispirarsi maggiormente al principio di libertà della circolazione delle informazioni e di autodeterminazione dei privati.

[79] Con riguardo alle norme sovrannazionali che dovrebbero consentire un efficace governo dell'economia, vi è chi ha osservato che il «Giudice si trova di fronte ad enunciati normativi riferibili, in via prevalente, ad un legislatore che non appare in grado di armonizzare ed omogeneizzare l'armatura concettuale che offre consistenza ad indirizzi culturali differenti»; così F. CAPRIGLIONE, *Tutela giurisdizionale e processo economico*, in *Riv. trim. dir. ec.*, 2017, p. 387.