Giusella Finocchiaro * e Laura Greco **

FinTech e protezione dei dati personali

SOMMARIO: 1. FinTech: i dati al servizio della tecnologia finanziaria – 2. La protezione dei dati personali nel settore FinTech – 2.1. Il diritto alla protezione dei dati personali e il Regolamento (UE) 2016/679 – 3. Le norme del Regolamento applicate a FinTech – 3.1. Il principio di *accountability* – 3.2. Il principio di trasparenza – 3.3. Il diritto alla portabilità dei dati personali – 4. Le criticità nell'attuazione concreta del Regolamento nel settore FinTech – 5. Conclusioni.

1. FinTech: i dati al servizio della tecnologia finanziaria

Nel 2014 la Commissione europea affermava già: "è in atto una nuova rivoluzione industriale trainata dai dati digitali, dall'informatica e dall'automazione" [1].

Questa rivoluzione [2] è collegata in particolare allo sfruttamento delle nuove tecnologie al servizio delle attività finanziarie e prende oggi comunemente il nome di "FinTech" [3].

---

* Professore ordinario di Diritto privato e di Diritto di Internet e dei *Social Media* presso l'Alma Mater Studiorum, Università di Bologna. Avvocato del foro di Bologna.

** *Research fellow* presso l'Alma Mater Studiorum, Università di Bologna. Avvocato del Foro di Bologna.

[1] Commissione europea, COM(2014)442 final, *Verso una florida economia basata sui dati*, 2 luglio 2014, p. 2.

[2] Sulla "quarta rivoluzione industriale", si veda, *inter alia*, Parlamento Europeo, *Industry 4.0. Digitalisation for productivity and growth*, 2015, disponibile sul sito https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/568337/EPRS_BRI(2015)568337_EN.pdf, consultato il 29 aprile 2021; BUTERA, *Lavoro e organizzazione nella quarta rivoluzione industriale: la nuova progettazione socio-tecnica*, in *L'industria*, 3, 2017; per i profili di diritto del mercato e dell'innovazione, FALCE-GHIDINI-OLIVIERI (a cura di), *Informazione* e Big Data *tra innovazione e concorrenza*, Milano, 2018.

[3] Il termine Fintech descrive, in particolare, il fenomeno in base al quale si assiste ad una offerta di servizi di finanziamento, di pagamento, di investimento e di consulenza ad alta intensità tec-

L'innovazione nel settore finanziario non è certo una novità. Il 2009 è infatti l'anno in cui viene convenzionalmente fissata l'origine del FinTech. È allora che la crisi finanziaria e la conseguente sfiducia nei confronti degli operatori tradizionali del settore fornirono la spinta *disruptive* per l'incontro tra attività finanziarie e tecnologia [4]. Basti pensare che la prima transazione in *bitcoin* risale al 12 gennaio 2009 [5].

Soltanto oggi, però, agli investimenti nella tecnologia (comunque incrementati rispetto al passato) si aggiunge la possibilità di sfruttare un'ingente quantità di dati dal valore incalcolabile.

"Is data the new oil?" si domanda il Parlamento europeo in apertura del *briefing* sulla *digital economy* [6] e la risposta è senz'altro positiva. I dati – personali e non [7] – rappresentano l'*asset* più prezioso dell'economia moderna.

---

nologica. Tale innovazione finanziaria, resa possibile dalla tecnologia, riverbera i suoi effetti sia nel campo dei servizi finanziari sia bancari, modificandone la struttura. La Commissione europea, nella COM(2018) 109 final, *Piano d'azione per le tecnologie finanziarie: per un settore finanziario europeo più competitivo e innovativo*, 8 marzo 2018, definisce "le tecnologie finanziarie (*fintech*), ossia l'innovazione nel settore dei servizi finanziari resa possibile dalla tecnologia" come "il punto di incontro dei servizi finanziari e del mercato unico digitale" (p. 2). Sul punto, cfr. anche FINOCCHIARO-FALCE (a cura di), *Fintech: diritti, concorrenza, regole. Le operazioni di finanziamento tecnologico*, Bologna, 2019; FINOCCHIARO-FALCE *La digital revolution nel settore finanziario. Una nota di metodo*, in *Analisi Giuridica dell'Economia*, 1, 2019, 313-326.

[4] Secondo ARNER-BARBERIS-BUCKLEY, *FinTech, RegTech, and the Reconceptualization of Financial Regulation,* in *Northwestern Journal of International Law & Business*, 2017, vol. 37(3), 371-413, "Regulatory and technological developments are changing the nature of financial markets, services, and institutions in ways completely unexpected prior to the 2008 Global Financial Crisis". Sul punto si veda anche ID., *The evolution of fintech: new post-crisis paradigm,* in *Georgetown Journal of International Law*, 2016, vol. 47(4), 1271-1320, dove secondo gli autori, sebbene Fintech sia spesso considerato "a uniquely recent marriage of financial services and information technology", in realtà, "the interlinkage of finance and technology has a long history. In fact, financial and technological development have long been intertwined and mutually reinforcing. The Global Financial Crisis of 2008 was a watershed and is part of the reason FinTech is now evolving into a new paradigm".

[5] Cfr. GAMBINO-BOMPREZZI, *Blockchain e criptovalute*, in FINOCCHIARO-FALCE (a cura di), *Fintech: diritti, concorrenza, regole. Le operazioni di finanziamento tecnologico*, Bologna, 2019, 267-290. In tema di connessione tra Fintech e servizi di pagamento aventi ad oggetto (anche) monete virtuali, cfr. SCHENA-TANDA-ARLOTTTA-POTENZA, *Lo sviluppo del Fintech. Opportunità e rischi per l'industria finanziaria nell'era digitale*, in *Quaderni Fintech*, 1, 2018.

[6] Parlamento europeo, *Is data the new oil? Competition issues in the digital economy*, 8 gennaio 2020, disponibile *on line* al *link* https://*www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI(2020)646117_EN.pdf*, consultato il 2 maggio 2021.

[7] I dati non personali sono oggetto della disciplina dettata dal Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio del 14 novembre 2018 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea. Questo Regolamento, adottato "per potenziare ulteriormente lo scambio transfrontaliero dei dati e promuovere l'economia dei dati", si è affiancato al Regolamento (UE) 2016/679 in materia di protezione dei dati personali. A

Sono l'*input* a fondamento di tecnologie rivoluzionarie, come l'intelligenza artificiale, e di molti servizi *on line*. La detenzione e l'utilizzo dei dati agiscono inevitabilmente anche sulle dinamiche competitive e concorrenziali del mercato, fungendo da parametro concorrenziale tra le imprese. Ma sono anche una risorsa fondamentale per la creazione di modelli di *business* innovativi (come il processo di *servitization* sempre più diffuso tra le imprese [8]) e mercati completamente nuovi, come appunto il FinTech.

La grande accessibilità e disponibilità di dati, oltre che il potere computazionale attualmente disponibile, rappresentano quindi elementi cruciali per lo sviluppo delle tecnologie e, in particolare, del settore FinTech.

Dunque, il fenomeno FinTech, unitamente alle opportunità da questo create ma anche ai rischi da esso derivanti, non può che essere analizzato nel più ampio contesto della *data-driven economy* e in particolare in relazione all'utilizzo dei dati, personali e non personali.

2. La protezione dei dati personali nel settore FinTech

In un mercato finanziario europeo supportato dalla tecnologia è necessario il pieno rispetto di alcune garanzie fondamentali. Le tecnologie finanziarie possono infatti offrire nuove opportunità e benefici, ma pongono anche delle sfide legate alla *cybersecurity*, alla protezione dei dati, alla tute-

---

tal proposito, la Commissione europea, COM/2019/250 final, *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, 29 maggio 2019, p. 2, rileva che "ora esiste un quadro globale per uno spazio comune europeo dei dati e per la libera circolazione di tutti i dati all'interno dell'Unione europea".

[8] Il termine "servitizzazione", dall'inglese *servitization*, indica il passaggio da un modello di *business* incentrato sulla vendita di un prodotto ad uno basato sull'offerta di un servizio che comprenda il prodotto. In altre parole, si tratta di un processo di trasformazione di un'impresa che, attraverso la modifica della propria struttura, dei propri processi e della propria organizzazione, riesce a trasformare il proprio *core business* dalla vendita di un prodotto in un sistema in grado vendere servizi a valore, integrati e legati al prodotto stesso. Sebbene si parli di "servitization" sin dal 1988, questo modello di *business* assume una nuova portata oggi grazie allo sviluppo tecnologico che consente di beneficiare della disponibilità di mezzi di comunicazione sempre più pervasivi e performanti e capacità elaborative significative rispetto il loro costo di acquisto. Sul tema cfr. ARDOLINO-RAPACCINI-SACCANI-GAIARDELLI-CRESPI-CARLO-RUGGERI, *The role of digital technologies for the service transformation of industrial companies*, in *International Journal of Production Research*, 2018, vol. 56, *issue* 6, 2116-2132; CAVALIERI-OUERTANI-ZHIBIN-RONDINI, *Service transformation in industrial companies*, in *International Journal of Production Research*, 2018, vol. 56, issue 6, 2099-2102; PORTER-HEPPELMAN, *How smart, connected products are transforming competition*, in *Harvard Business Review*, 2014, vol. 92, *issue* 11, 64-88.

la dei consumatori e all'integrità del mercato. In questo contributo saranno esaminati in particolare i profili emergenti dall'interazione delle nuove tecnologie finanziarie con la protezione dei dati personali.

2.1. Il diritto alla protezione dei dati personali e il Regolamento (UE) 2016/679

Occorre anzitutto offrire qualche cenno sul diritto fondamentale alla protezione dei dati personali e quindi inquadrare brevemente il contesto normativo in cui oggi intervengono le tecnologie finanziarie.

Il diritto alla protezione dei dati personali consiste nel diritto del soggetto al quale i dati si riferiscono di esercitare un controllo, anche attivo, su tali dati. Esso è riconosciuto dalla Carta dei diritti fondamentali dell'Unione europea [9] dove, all'art. 8, si afferma che i dati personali devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o ad un altro fondamento legittimo previsto dalla legge e che ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.

Il diritto alla protezione dei dati personali si configura, dunque, come il diritto di un soggetto di controllare l'insieme delle informazioni che allo stesso si riferiscono e che quindi costituiscono il suo riflesso e delineano lo stesso suo essere nella società dell'informazione [10]. Tale diritto ha quindi un oggetto molto ampio, come rivela la stessa definizione di "dato personale": "qualsiasi informazione riguardante una persona fisica identificata o identificabile ('interessato'); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo *on line* o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale" [11].

---

[9] La Carta dei diritti fondamentali dell'Unione europea approvata il 7 dicembre 2000 è stata pubblicata nella G.U.C.E. 200/C-364/01. In dottrina, RESCIGNO, *La Carta dei diritti fondamentali dell'Unione europea,* Torino, 2003; sul successivo progetto di Trattato istitutivo della Costituzione europea, MANZELLA-MELOGRANI-PACIOTTI-RODOTÀ, *Riscrivere i diritti in Europa. Introduzione alla Carta dei diritti fondamentali dell'Unione europea,* Bologna, 2001 e BARBERA, *La Carta europea dei diritti e la Costituzione italiana*, in AA.VV., *Le libertà e i diritti nella prospettiva europea*, Padova, 2002, 107.

[10] Così RODOTÀ, allora Presidente dell'Autorità Garante per la protezione dei dati personali, sulla nozione di "corpo elettronico", in Relazione 2002; ID., *Tecnologie e diritti*, Bologna, 1995.

[11] V. art. 4, 1° comma, n. 1 del Regolamento.

Distinto dal diritto alla protezione dei dati personali è invece il diritto alla riservatezza, anch'esso riconosciuto dalla Carta dei diritti fondamentali, ma da intendersi come libertà negativa di non subire interferenze nella propria vita privata [12]. Mentre il diritto alla protezione dei dati personali costituisce il fondamento della libertà positiva di esercitare un controllo sul flusso delle proprie informazioni, il diritto alla riservatezza è un diritto a contenuto negativo, quello di non fare conoscere e di mantenere riservate alcune informazioni. Inoltre, a differenza del diritto alla protezione dei dati personali, non ha ad oggetto le informazioni, di qualunque natura esse siano, ma soltanto le vicende riservate.

È il diritto alla protezione dei dati personali ad essere oggetto 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 [13] (di seguito, "Regolamento") che, come è noto, abrogando la previgente Direttiva 95/46/CE, ha innovato la disciplina sui dati personali.

La riforma della normativa in materia di protezione dei dati personali costituiva d'altronde un passaggio obbligato per il legislatore europeo nell'*iter* di creazione di un mercato unico digitale. La Direttiva infatti non risultava più al passo coi tempi. Essa era il frutto di un dibattito culturale e di un pensiero dottrinale sviluppatosi nei decenni precedenti e delineava un modello statico di trattamento dei dati personali, ormai superato. Diversa all'epoca

---

[12] Cfr. BUSNELLI, *Nota introduttiva al commento della l. 31 dicembre 1996, n. 675. Spunti per un inquadramento sistematico*, in *Tutela della privacy. Commentario alla l. 675/96*, (a cura di) BIANCA-BUSNELLI-BELLELLI-LUISO-NAVARETTA-PATTI-VECCHI, Padova, 1999, 228-233. Per un inquadramento sistematico del diritto alla riservatezza, AULETTA, *Riservatezza e tutela della personalità*, Milano, 1978; RESTA, *Autonomia privata e diritti della personalità*, Napoli, 2005, 209.

[13] In generale, sul Regolamento ALPA, *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contr. e impr.*, 2017, III, 723-733; BUSIA-LIGUORI-POLLICINO (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali*, Roma, 2016; CALIFANO-COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017; CUFFARO-D'ORAZIO-RICCIUTO, *I dati personali nel diritto europeo*, Torino, 2019; FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019; PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice privacy)*, Milano, 2019; PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, Torino, 2016; RICCIO-SCORZA-BELISARIO (a cura di), *GDPR e Normativa Privacy. Commentario*, Milano, 2018; SICA-D'ANTONIO-RICCIO (a cura di), *La nuova disciplina europea della privacy*, Padova, 2016; TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019; ZORZI-GALGANO (a cura di), *Persona e mercato dei dati: riflessioni sul GDPR*, Padova, 2019.

anche la tecnologia: era un mondo privo di *smart phone*, *social network* e motori di ricerca. Il modello normativo individuava un unico scambio di dati: dall'interessato al titolare del trattamento di dati personali. Oggi invece la realtà è ben diversa e si basa su un modello di condivisione e di cogestione di dati e informazioni, destinati fin dall'origine ad una circolazione globale.

Alla luce del nuovo contesto socio-economico e delle nuove esigenze del mercato, il Regolamento si è quindi posto un obiettivo, tanto importante quanto difficile: il bilanciamento tra la libera circolazione dei dati e la loro protezione. Come anticipato, infatti, il bene sul quale si fonda l'economia moderna è costituito dalle informazioni, delle quali il legislatore europeo non può che favorire la circolazione, per sostenere il mercato europeo. Il diritto alla protezione dei dati personali non è dunque concepito come "una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ottemperanza al principio di proporzionalità" [14]. Allo stesso tempo, tuttavia, i dati personali devono essere protetti.

Il legislatore europeo si è quindi impegnato in un esercizio molto complesso volto a non trascurare né l'esigenza di tutelare il diritto fondamentale alla protezione dei dati personali, né l'urgenza di costruire e rafforzare il mercato unico digitale europeo [15].

---

[14] V. considerando n. 4 del Regolamento. In questo senso, già alcune decisioni della Corte di Giustizia europea, tra cui *Promusicae*, *Volker und Markus Schecke e Eifert* e *ASNEF e FE–CEMD*. Il considerando citato riporta alla mente alcune affermazioni della Corte di Cassazione italiana, in particolare quella contenuta nella sentenza n. 10280/2015 della Sezione III della Corte di Cassazione, ove si afferma che il diritto alla protezione dei dati personali, qualificato come pretesa ad esigere una corretta gestione dei propri dati personali, pur rientrando nei diritti fondamentali della persona, non è un "*totem* al quale possano sacrificarsi altri diritti altrettanto rilevanti sul piano costituzionale" e, conseguentemente, la disciplina in materia "va coordinata e bilanciata da un lato con le norme che tutelano altri e prevalenti diritti (tra questi, l'interesse pubblico alla celerità, trasparenza ed efficacia all'attività amministrativa); dall'altro, con le norme civilistiche in tema di negozi giuridici".

[15] Anche in tema di intelligenza artificiale, emerge la tensione tra protezione dei dati, da un lato, e condivisione e accesso ai dati, dall'altro. Nella Comunicazione (2018) 795, *Piano di coordinamento per l'IA*, e Allegato, *Piano coordinato per lo sviluppo e l'utilizzo dell'intelligenza artificiale «Made in Europe»*, 7 dicembre 2018, la Commissione europea sottolinea la necessità di realizzare uno "spazio dei dati europeo", affermando espressamente che "affinché l'IA possa svilupparsi ulteriormente è necessario un valido ecosistema dei dati basato sulla fiducia, sulla disponibilità dei dati e sull'infrastruttura" e che l'accesso ai dati "è un elemento fondamentale per un panorama di IA competitivo" (pp. 6-7). Il testo prosegue però specificando che l'Unione europea dovrebbe agevolare tale accesso ai dati "nel pieno rispetto delle norme sulla protezione dei dati personali". Analoghi concetti sono espressi anche nell'allegato alla menzionata comunicazione: "l'attuale diffusione dell'IA è alimentata dalla disponibilità di grandi *set* di dati, abbinata all'aumento della potenza di calcolo e della connettività. Mettere dati sicuri, solidi e di qualità a disposizione

Vero è che l'analisi di grandi moli di dati consente una più efficiente personalizzazione di prodotti e servizi e una stima più accurata dei profili di rischio relativi all'individuo [16]. Tuttavia, se da un lato clienti e consumatori possono trarre beneficio dall'offerta di servizi *tailor-made*, sconti, offerte speciali o pubblicità mirate, dall'altro lato potrebbero subire alcuni impatti negativi derivanti, ad esempio, da una profilazione imprecisa, da distorsioni nella creazione degli algoritmi fino a subire l'esclusione dall'accesso a determinati servizi se classificati (erroneamente) come soggetti inaffidabili [17].

Per assicurare un sistema non solo efficiente ma sicuro e garantista, è quindi essenziale curare la completezza e l'attendibilità dei dati e delle fonti utilizzate, la correttezza della loro elaborazione, un grado di trasparenza nei confronti dei consumatori dei processi decisionali fondati su algoritmi e sistemi automatizzati la cui logica, come noto, è spesso difficile da comprendere.

3. Le norme del Regolamento applicate a FinTech

L'attuale quadro normativo sembra sufficiente a comporre, o perlomeno ad attenuare, quella tensione sopra illustrata tra tutela dei dati e libera circolazione degli stessi, offrendo una cornice normativa adeguata a fronteggiare molti dei rischi emergenti.

Al momento il quadro è composito e annovera norme contenute in di-

---

di una vasta gamma di utenti a livello transfrontaliero è uno dei fondamenti della politica europea. L'apertura ai flussi di dati internazionali continuerà a essere garantita, nel pieno rispetto della normativa dell'UE per la protezione dei dati personali" (p. 14). Infine, sul punto, fondamentale è il richiamo alla Risoluzione del Parlamento europeo del 12 febbraio 2019 su una politica industriale europea globale in materia di robotica e intelligenza artificiale, ove è riconosciuto, da un lato, che lo sviluppo di prodotti e servizi basati sull'IA necessita del libero flusso di dati e dell'accessibilità ai dati all'interno dell'Unione europea e, dall'altro lato, che occorre garantire un elevato livello di sicurezza, protezione e riservatezza dei dati utilizzati per la comunicazione tra persone e *robot* e intelligenza artificiale, invitando "la Commissione a garantire che qualsiasi futuro quadro normativo dell'UE in materia di IA garantisca la riservatezza e la confidenzialità delle comunicazioni, la protezione dei dati personali, compresi i principi di legalità, equità e trasparenza, la protezione dei dati fin dalla progettazione e per impostazione predefinita, la limitazione delle finalità, la limitazione della conservazione, la precisione e la minimizzazione di dati, nel pieno rispetto del diritto dell'Unione in materia di protezione dei dati" (par. P, 125 e 128).

[16] Così anche l'allora Presidente del Garante per la protezione dei dati personali, Antonello Soro, nel corso di un'intervista rilasciata durante l'*Inaugurazione Corso di alta formazione ABI "Fintech e Diritto"*, il 10 maggio 2018 a Roma.

[17] Cfr. PALMERINI-AIELLO-CAPPELLI-MORGANTE-AMORE-DI VETTA-FIORINELLI-GALLI, *Il FinTech e l'economia dei dati. Considerazioni su alcuni profili civilistici e penalistici. Le soluzioni del diritto vigente ai rischi per la clientela e gli operatori*, in *Quaderni FinTech*, 2, dicembre 2018.

stinte discipline tra cui, oltre al citato Regolamento, la Direttiva (UE) 2015/2366 sui servizi di pagamento [18], la Direttiva (UE) 2015/849 in materia di antiriciclaggio [19] e la Direttiva (UE) 2016/1148 sulla *cybersecurity* [20].

In particolare, il Regolamento detta un complesso di regole uniformi di responsabilità, liceità, trasparenza e correttezza nel trattamento dei dati personali, applicabili a tutti coloro che fanno uso di tali informazioni e, dunque, anche agli attori coinvolti nel fenomeno FinTech.

3.1. Il principio di *accountability*

Il principio di *accountability* caratterizza ed informa la normativa europea sulla protezione dei dati personali, imponendo al titolare del trattamento di dati personali [21] di osservare le norme del Regolamento e di dare prova di tale osservanza [22].

Dunque, il principio di *accountability* comporta un cambio di paradigma e richiede l'adozione di un metodo radicalmente diverso rispetto a quanto previsto dalla previgente normativa dettata dalla Direttiva 95/46/CE. Il legi-

---

[18] Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio 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 (anche nota come "*Payment Services Directive 2*" o "PSD2").

[19] Direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio del 20 maggio 2015, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica il regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 2005/60/CE del Parlamento europeo e del Consiglio e la direttiva 2006/70/CE della Commissione.

[20] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (meglio nota come "Direttiva NIS"). Si noti che sono state recentemente proposte dalla Commissione europea l'abrogazione della Direttiva qui citata e la contestuale adozione di una nuova Direttiva, la c.d. "NIS2", volta a rafforzare il quadro normativo sulla *cybersecurity* in Europa estendendo l'ambito applicativo della NIS1 e rafforzandone l'apparato sanzionatorio. Il testo della proposta è disponibile al sito https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity – across-union, consultato il 3 maggio 2021.

[21] Giova richiamare la definizione dettata dall'art. 4, 1° comma, n. 7 del Regolamento, secondo cui titolare del trattamento di dati personali è "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali".

[22] Sul principio di *accountability*, cfr. ampiamente FINOCCHIARO, *L'*accountability *nel Regolamento europeo*, in BARBA-PAGLIANTINI (a cura di), *Delle persone. Vol. II*, in GABRIELLI (diretto da), in *Commentario del codice civile*, Milano, 2019, 513-523.

slatore europeo ha infatti adottato un approccio di tutela dei dati personali basato sulla gestione del rischio. Il Regolamento non prevede più soltanto prescrizioni dirette e precise alla cui mancata applicazione consegue una sanzione, ma invece un obiettivo da realizzare, secondo modalità che lo stesso titolare di trattamento deve di volta in volta determinare, le quali saranno oggetto di successiva valutazione da parte dell'autorità di controllo e del giudice.

Si passa dunque da un approccio normativo che dettava indicazioni assai precise ad uno basato sui principi e volto a responsabilizzare il titolare del trattamento di dati personali.

In forza del principio di *accountability*, anche i protagonisti dello scenario Fintech, in quanto trattino dati personali, dovranno essere in grado di giustificare il trattamento di dati personali nel suo complesso, dalla scelta dei dati personali trattati e dei soggetti a cui comunicare gli stessi fino all'adozione delle misure ritenute idonee alla loro tutela, dimostrando il rispetto dei principi fondamentali del trattamento e quindi che i dati siano adeguati, pertinenti, aggiornati e conservati limitatamente al tempo necessario al perseguimento delle finalità del trattamento.

3.2. Il principio di trasparenza

In virtù del principio di trasparenza, "dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché la misura in cui i dati personali sono o saranno trattati. 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" [23].

Il principio di trasparenza non è del tutto nuovo nella disciplina dei dati personali [24], ma assume una rilevanza ancora più significativa nel contesto odierno dove le analisi automatizzate di dati personali, l'accresciuto impiego

[23] V. considerando n. 39 del Regolamento.

[24] Già la Direttiva 95/46/CE, al considerando n. 63, sottolineava che le autorità di controllo dovessero "contribuire alla trasparenza dei trattamenti effettuati nello Stato membro". Inoltre, pur in assenza di ulteriori riferimenti espressi, il principio di trasparenza era contemplato nel principio di correttezza, esplicitamente sancito dalla menzionata Direttiva: così RICCI, *I diritti dell'interessato*, in FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019, 392-472.

di algoritmi e l'adozione di decisioni senza l'intervento umano rendono più complesso evincere le modalità con cui sono trattati i dati personali, i soggetti che possono venirne a conoscenza e le altre caratteristiche del trattamento.

Questo principio rappresenta quindi, da un lato, un obbligo in capo al titolare del trattamento di dati personali che deve fornire adeguate informazioni sul trattamento effettuato. Dall'altro, costituisce per l'interessato uno strumento di controllo che gli consente di conoscere i rischi connessi al trattamento, nonché un parametro di valutazione circa la gestione dei dati personali che possa guidarlo in una scelta più consapevole di servizi e prodotti.

Esempi di applicazione del principio appena descritto si possono rinvenire nello stesso Regolamento. Ad esempio, l'art. 13, 2° comma, lett. f) del Regolamento prevede espressamente che l'interessato debba essere edotto de "l'esistenza di un processo decisionale automatizzato e, almeno in tali casi, (debba ricevere) informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato".

Si tratta di una disposizione senz'altro applicabile alle moderne tecnologie basate sull'utilizzo di algoritmi che permettono di esaminare interessi e aspetti personali degli individui al fine di categorizzarli e crearne, appunto, dei profili[25]. In questi casi, il titolare del trattamento di dati personali dovrà non solo fornire una spiegazione intellegibile del meccanismo sottostante al processo decisionale che ha portato alla definizione del profilo, ma anche mettere "in atto misure tecniche e organizzative adeguate al fine di garantire che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale"[26].

---

[25] Basti pensare alle tecniche di profilazione in uso presso gli istituti bancari volti a valutare il merito creditizio del cliente (c.d. *rating*) e il grado di rischio connesso in caso di concessione di investimenti. Se i processi decisionali automatizzati possono risultare utili in termini di incremento di efficienza e personalizzazione dei servizi, è vero anche che l'esito di questi processi può sfociare nell'errata categorizzazione dell'individuo limitandone le scelte, alimentando stereotipi, impedendo l'accesso a servizi o prodotti e, in taluni casi più gravi, causando forme ingiustificate di discriminazione. Sull'argomento, cfr. *Linee guida in materia di processi decisionali automatizzati e profilazione*, adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017, versione emendata e adottata il 6 febbraio 2018.

[26] V. considerando n. 70 del Regolamento.

Tutte le disposizioni connesse al principio di trasparenza sopra descritto sono riconducibili all'obiettivo del legislatore di porre rimedio all'asimmetria informativa tra interessato e titolare del trattamento che di fatto risulta più accentuata nell'ambito di prodotti o servizi che, basandosi sull'analisi automatizzata di dati, non contemplano l'intervento dell'interessato o del consumatore che spesso finisce così per subire l'esito di tali processi.

3.3. Il diritto alla portabilità dei dati personali

Infine, in aggiunta ad alcuni diritti dell'interessato già riconosciuti dalla previgente disciplina, il Regolamento ha introdotto il diritto alla portabilità dei dati personali[27].

Si tratta di un diritto nato proprio per rispondere alle esigenze di interoperabilità e di concorrenza dell'economia e del mercato contemporanei. Attraverso tale diritto, infatti, il legislatore persegue un duplice obiettivo: da un lato, agevola l'alternanza di servizi e prodotti, assicurando la migrazione tra operatori distinti e, dall'altro lato, riduce il rischio della creazione di monopoli fondati sull'acquisizione e sulla disponibilità di dati e informazioni.

Il diritto alla portabilità dei dati consente, dunque, agli interessati di ricevere, "in un formato strutturato, di uso comune e leggibile da dispositivo automatico", i dati personali forniti a un titolare del trattamento e di trasmetterli a un diverso titolare senza impedimenti. Affinché tale diritto possa essere legittimamente esercitato, occorre però che i dati personali siano trattati con mezzi automatizzati e siano stati forniti con il consenso dell'interessato oppure per l'esecuzione di un contratto di cui l'interessato è parte.

4. Le criticità nell'attuazione concreta del Regolamento nel settore FinTech

Sebbene il Regolamento offra un quadro normativo utile alla disciplina delle nuove tecnologie dal punto di vista della protezione dei dati persona-

---

[27] V. art. 20 del Regolamento. A proposito del diritto alla portabilità dei dati personali, cfr. RICCI, *cit*.; PIRAINO, *I "diritti dell'interessato" nel Regolamento Generale sulla protezione dei dati personali*, in *Giur. it.*, 12, 2019, 2789-2799; BORGHI, *Portabilità dei dati e regolazione dei mercati digitali*, in *Mercato concorrenza regole*, 2, 2018, 223-245; WEBER, *Data portability and Big data analytics. New competition policy challanges*, in *Concorrenza e mercato*, 1, 2016, 59-72.

li, è pur vero che in alcuni casi potrebbe risultare complesso applicare pedissequamente le norme sopra descritte.

Il principio di trasparenza, ad esempio, impone di fornire all'interessato una serie di informazioni sul trattamento di dati personali, tra cui le finalità perseguite attraverso il trattamento. Tuttavia, quando il trattamento di dati personali viene effettuato mediante l'impiego di certe tecnologie, come ad esempio quelle basate su tecniche di *machine learning*, la finalità del trattamento potrebbe non essere chiara fin dal principio, bensì potrebbe andarsi definendo con il trattamento stesso. Non essendo nota sin dall'inizio, dunque, la finalità non potrebbe essere comunicata all'interessato. Ciò comporta, altresì, che l'eventuale consenso al trattamento di dati personali potrebbe non essere ritenuto valido se espresso in relazione ad un trattamento le cui finalità non sono chiare o note.

Analogamente, l'obbligo di fornire informazioni sulla logica di funzionamento di processi automatizzati, tra cui la profilazione, sembra applicarsi solo alle decisioni interamente automatizzate. Tale specificazione costituisce un forte limite all'applicabilità della norma la cui effettività risulta di fatto ridotta – se non annullata – a fronte di un, seppur minimo, intervento umano.

Ancora, l'efficacia del principio di *accountability* potrebbe risultare inficiata quando nel trattamento di dati personali sono coinvolti molteplici attori i cui ruoli e le cui responsabilità non sono chiaramente definiti, come può accadere ad esempio proprio nel settore FinTech dove si avvicendano svariati *player*, dai fornitori di servizi agli sviluppatori dei programmi fino ai gestori dei *digital marketplace*, con l'effetto di creare così una lunga catena su cui si snoda la responsabilità.

Come è noto, poi, la qualità dei dati è essenziale nel contesto di tecnologie che si alimentano di dati personali. Da dati qualitativamente non corretti, non possono che scaturire elaborazioni non corrette, secondo il noto principio "garbage in, garbage out". Secondo il principio di qualità dei dati, infatti, i dati devono essere "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati; esatti e, se necessario, aggiornati", dovendo essere "adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati", nonché "conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati".

Il parametro della qualità dei dati assurge, oltre che a requisito di protezione dei dati personali, ad elemento essenziale affinché l'elaborazione automatizzata e il risultato basati sui dati siano corretti. È chiaro come l'osservanza di tale principio sia particolarmente onerosa quando siano coin-

volte innumerevoli informazioni che richiedano cadauna un controllo specifico di qualità.

Queste criticità sono ben note alla Commissione europea che le illustra sistematicamente nel *report* "30 Recommendations on Regulation, Innovation and Finance", pubblicato dall'*Expert Group on Regulatory Obstacles to Financial Innovation (ROFIEG)*, incaricato di identificare gli ostacoli normativi allo sviluppo del FinTech e di elaborare raccomandazioni per affrontare questi problemi. In particolare, la *Recommendation No. 25* si occupa dell'interazione tra la normativa sulla protezione dei dati personali e le nuove tecnologie basate sui dati. Riconoscendo l'importanza strategica per le imprese di utilizzare dati e informazioni, il Gruppo avverte circa le incertezze attuative del Regolamento rispetto alle nuove tecnologie.

Ad esempio, il Gruppo rileva la complessità di coniugare il principio di minimizzazione dei dati personali nell'ambito di tecnologie che si fondano proprio sull'utilizzo di grandi moli di dati. In questo ambito, la minimizzazione dei dati, e dunque la cancellazione o l'anonimizzazione di tutti i dati non (più) necessari allo scopo specifico per il quale sono stati raccolti, rischiano di rappresentare un limite a qualsiasi utilizzo dei dati personali non previamente determinato restringendo di fatto le potenzialità dell'analisi di grandi quantità di dati.

Le difficoltà ora accennate nell'applicazione delle norme del Regolamento non devono però indurre a ripensare alla validità delle medesime rispetto al contesto delle tecnologie finanziarie, per il cui sviluppo il Regolamento rimane un riferimento centrale.

5. Conclusioni

Il fenomeno FinTech è, al tempo stesso, risultato e propulsore della rivoluzione digitale fondata sull'utilizzo dei dati. Si tratta di un processo strategico e rilevante che si inserisce nel più ampio obiettivo di rendere l'Unione europea competitiva dal punto di vista economico e di consolidarne la posizione nel panorama del mercato internazionale.

Lo sviluppo di tale settore non può tuttavia ignorare la cultura e la politica europee fondate sui diritti fondamentali dell'uomo e, tra essi, sul diritto alla protezione dei dati personali. Il sistema dei valori europei deve dunque essere salvaguardato all'insegna del bilanciamento tra esigenze del mercato, della concorrenza e dell'innovazione e la tutela dei diritti fondamentali.