

Giorgia Biferali

***BIG DATA E VALUTAZIONE DEL
MERITO CREDITIZIO PER
L'ACCESSO AL *PEER TO PEER*
LENDING***

Estratto



Milano • Giuffrè Editore

GIORGIA BIFERALI

BIG DATA E VALUTAZIONE DEL MERITO CREDITIZIO PER L'ACCESSO AL PEER TO PEER LENDING

SOMMARIO: 1. Valore e limiti del consenso nella dimensione dei *Big data*. — 2. Sistemi di informazione creditizia e tutela della privacy. — 3. *Peer to peer lending* e tutela della privacy. — 4. Bitcoin *peer to peer lending* e tutela della privacy.

1. VALORE E LIMITI DEL CONSENSO NELLA DIMENSIONE DEI *BIG DATA*.

Negli ultimi anni la società è stata travolta da una vera e propria rivoluzione digitale fondata su rapporti tra miriadi di utenti ed un elevato numero di imprese che eseguono attività basate su informazioni. In tale dimensione si assiste, da una parte, all'attività degli utenti che consiste principalmente nella più o meno consapevole messa a disposizione di dati ai fornitori di servizi, dall'altra parte, all'attività dei fornitori di servizi che raccolgono dati tra gli utenti e successivamente svolgono attività di elaborazione, estrazione e sfruttamento degli stessi. L'interazione tra utenti e fornitori avviene tramite strumenti informatici in grado sia di attingere ad una molteplicità di fonti (quali ad esempio i motori di ricerca, i negozi virtuali, le e-mail, i *social network*, i servizi *cloud*), sia di aggregare una quantità elevata di dati. I dati raccolti, una volta analizzati, si prestano a fornire il quadro relativo ad un singolo utente, a grandi comunità o alla società globale.

Il risultato del processo di aggregazione a cui si fa riferimento sono i *Big data*, ossia *dataset* che per la loro estensione in volume, velocità e varietà consentono di estrarre informazioni aggiuntive¹. Tale disponibilità di dati segna il passaggio a una sempre

¹ Sul fenomeno dei *Big data*, Commissione Europea, *Digital Single Market - Big Data*, in www.ec.europa.eu, secondo la quale « *Big data* refers to large amounts of data produced very quickly by a high number of

diverse sources. Data can either be created by people or generated by machines, such as sensors gathering climate information, satellite imagery, digital pictures and videos, purchase transaction records, GPS

più pervasiva profilazione² dei singoli utenti che permette a fornitori di servizi, aziende private o Autorità pubbliche di risalire tramite la cronologia delle attività degli utenti alle loro preferenze, interazioni, stili di vita, al fine di proporre prodotti, di monitorare ampi gruppi sociali e di correlare fenomeni del più disparato genere con alta probabilità di conseguire risultati³. I progressi tecnologici e le capacità di analisi dei *Big data*, dell'intelligenza artificiale e dell'apprendimento automatico hanno reso più facile la creazione di profili e decisioni automatiche con il potenziale di incidere in modo significativo sui diritti e sulle libertà delle persone⁴.

Le informazioni in cui i *Big data* si sostanziano sono innumerevoli e di diversa natura e provengono da diverse fonti. In un immenso *database* confluiscono milioni di informazioni raccolte attraverso varie modalità da persone, computer, telecamere, e da ogni genere di strumento idoneo, che sono poi sottoposti a trattamenti automatizzati. L'uso dei *Big data*, oltre a fornire informazioni dettagliate sui soggetti cui si riferiscono (esse possono riguardare caratteristiche individuali, abitudini di comportamento, patologie ed ogni altra manifestazione della personalità di un individuo), permette, attraverso sofisticati sistemi informatici in grado di operare confronti, di accoppiare e di associare informazioni di diversa natura, di formulare con buona approssimazione ipotesi su scelte e comportamenti futuri (c.d. *Big data analytics*)⁵. Considerate queste potenzialità, occorre domandarsi

signals, etc. It covers many sectors, from healthcare to transport and energy». In dottrina, tra i molti, V. Mayer Schonberger, K. Cukier, *Big Data*, Milano, 2013, p. 15-16, secondo i quali «L'espressione Big Data designa delle cose che si possono fare solo su larga scala, per estrapolare nuove indicazioni o creare nuove forme di valore, con modalità che vengono a modificare i mercati, le organizzazioni, le relazioni tra cittadini e governi, e altro ancora»; H. V. Varian, *Big Data: New Tricks for Econometrics*, in *Journal of Economic Perspectives*, 28, 2014, p. 3 ss.; A. Giannaccari, *La storia dei Big Data, tra riflessioni teoriche e primi casi applicativi*, in *Merc. conc. Reg.*, 2017, p. 307 ss.

² Per profilazione si intende «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica» (art. 4 Reg. 2016/679). Sulla profilazione e sui pro-

blemi relativi al potere di autodeterminazione dell'interessato, cfr., R. De Meo, *Autodeterminazione e consenso nella profilazione dei dati personali*, in questa *Rivista*, 2013, p. 587 ss.

³ Parlano di sistema "dato-centrico" A. Mantelero, *The Future of Consumer Data Protection in the E.U. Rethinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics*, in *Computer Law & Security Rev.*, v. 30, n. 6, 2014, p. 643 ss.; O. Pollicino, *Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain*, in questa *Rivista*, 2014, p. 569 ss., in particolare p. 586-587.

⁴ Cfr. sul punto le osservazioni di G. Alpa, *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contr. impr.*, 2017, p. 723 ss.

⁵ WP29, *Guidelines on Automated individual decision — making and profiling for the purposes of regulation 2016/679*, WP251rev.01, 6 febbraio 2018, p. 5, «Advances in technology and the capabilities of big data analytics, artificial intelligence and

quali possano essere le implicazioni negative che derivano da un uso non corretto o non “governato” dei *Big data*.

L'art. 22, comma 1, del Regolamento 2016/679 (“Regolamento privacy”) stabilisce che « L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona ». Tale disposizione sembra rispecchiare la volontà del legislatore europeo di frenare l'utilizzo incontrollato dei *Big data analytics* o comunque di arginare i rischi di danno agli interessati; ma si tratta di un tentativo inidoneo a raggiungere lo scopo.

Il “dato” e le sue forme di elaborazione si pongono al centro di una nuova realtà economica ⁶, in cui il principio della capacità del soggetto di autodeterminarsi mediante il rilascio o il diniego del consenso rispetto alle scelte che riguardano il trattamento dei dati perde di valore ⁷.

Nella sua prima apparizione il diritto alla privacy evocava una concezione proprietaria e si presentava come diritto alla riservatezza e alla tutela della propria identità personale. In tale contesto, il consenso doveva essere consapevolmente prestato e non viziato da incapacità e determinava un atto di disposizione, a titolo gratuito od oneroso, che permetteva il trasferimento di un diritto di proprietà.

A partire dagli anni Ottanta, le esigenze di tutela mutavano. I soggetti per rivendicare parità di trattamento erano costretti a disvelarsi e, dunque, il diritto alla privacy si proiettava in una « dimensione sociale » ⁸ in cui il diritto alla riservatezza « cessa di essere un bene da tutelare integralmente. Al suo posto subentra il

machine learning have made it easier to create profiles and make automated decisions with the potential to significantly impact individuals' rights and freedoms. The widespread availability of personal data on the internet and from Internet of Things (IoT) devices, and the ability to find correlations and create links, can allow aspects of an individual's personality or behaviour, interests and habits to be determined, analysed and predicted [...] However, profiling and automated decision-making can pose significant risks for individuals' rights and freedoms which require appropriate safeguards. These processes can be opaque. Individuals might not know that they are being profiled or understand what is involved. Profiling can perpetuate existing stereotypes and social segregation. It can also lock a person into a specific category and restrict them to their suggested preferences ».

⁶ A. ROSS, *Il nostro futuro*, Milano, 2016.

⁷ A. MONTELERO, *Responsabilità e rischio nel Reg. UE 2016/679*, in NLCC, 2017, p. 144 ss.; G. STANZIONE, *Il Regolamento europeo sulla privacy: origini e ambito di applicazione*, in Eur. dir. priv., 2016, p. 1252; F. PIZZETTI, *La protezione dei dati personali e la sfida dell'intelligenza artificiale*, in Id., *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, p. 37 ss.

⁸ C. CAMARDI, *Mercato delle informazioni e privacy: riflessioni generali sulla L. N. 675/1996*, in Eur. Dir. priv., 1998, p. 1054, secondo la quale la suddetta dimensione era « connotata dalle dimensioni e dall'intensità delle contrattazioni di mercato, e dal modo in cui il mercato medesimo produce un autonomo bisogno di informazioni. Il diritto alla riservatezza, in questo specifico contesto, si riduce ad operare — per la

bisogno di far sapere di sé anche per reclamare diritti»⁹. Il consenso sembrava quindi atteggiarsi come contropartita volontaria per ottenere l'attuazione di diritti civili o sociali o altra utilità o vantaggio¹⁰.

I *Big data* segnano uno sviluppo ulteriore. Nella società della condivisione, in cui le informazioni personali sono destinate alla circolazione, la tutela della persona non è l'unico obiettivo da raggiungere, ma è parte di un insieme di interessi tesi allo sviluppo del mercato e dell'economia digitale¹¹. In tale contesto il consenso sembra divenire contropartita necessaria ad evitare un danno consistente nella esclusione da un contesto sociale o nell'impossibilità di ottenere l'accesso a servizi socialmente diffusi. Da qui l'impressione che il consenso abbia perso gradi di volontarietà e sia divenuto preconditione automatica dell'accesso richiesto, fino al punto di spegnere l'interesse dei richiedenti alla tutela della propria privacy, quasi che questa fosse stata implicitamente oggetto di rinuncia preventiva¹², salvo il riemergere di esigenze di protezione in caso di abusi conclamati. La "proprietà della privacy" si dissolve, salvo il limite aperto e frammentario del "divieto

forza del mercato — in quegli spazi nei quali il dato personale cessa di essere utile all'economia dell'affare, ma deve cedere di fronte all'obbligo di informare e al contestuale diritto di essere informati che sorge in capo a chi possiede comunque un ruolo nell'economia dell'affare (la controparte, il mediatore, l'agente, la banca ecc.)».

⁹ Id., *Mercato delle informazioni e privacy: riflessioni generali* sulla L. N. 675/1996, cit., p. 1059.

¹⁰ Sulla figura del consenso la dottrina, con riferimento alla legge n. 675 del 1996 e al Codice privacy, si è divisa tra coloro che hanno sostenuto una valenza negoziale del consenso stesso (tra gli altri, G. OPPO, *Sul consenso dell'interessato*, in *Trattamento dei dati e tutela della persona*, a cura di V. Cuffaro, V. Ricciuto, V. Zeno-Zencovich, Milano, 1998, p. 123 ss.) e coloro che ne hanno invece sostenuto la valenza "autorizzativa": cfr. D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in Riv. crit. dir. priv., 1998, p. 350 ss.; A. FICI, E. PELLECCIA, *Il consenso al trattamento*, in *Diritto alla riservatezza e circolazione dei dati personali*, a cura di R. Pardolesi, vol. I, Milano, 2003, p. 503; S. MAZZAMUTO, *Il principio del consenso e il problema della revoca*, in *Libera circolazione e protezione dei dati personali*, a cura di R. Panetta, I, Milano, 2006, p. 1026 e p. 1029-1030; F. PIRAINO, *La liceità e correttezza*, in *Libera circolazione e protezione dei dati personali*, cit., p. 813. Tale prospettiva è stata svilup-

pata, di recente, da A. IULIANI, *Note minime in tema di trattamento dei dati personali*, in Eur. dir. priv., 2018, p. 300. Sul consenso quale « autorizzazione in senso lato », con riferimento al Regolamento privacy, F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Milano, 2018, p. 123-124. Sulla funzione del consenso in base al modello di tutela prescelto, A. DI MAJO, *Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela*, in *Trattamento dei dati e tutela della persona*, cit., p. 230-231. Per una panoramica generale sul consenso, S. SICA, *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in Riv. dir. civ., 2001, II, p. 621 ss.

¹¹ Commissione Europea, *Building a European Data Economy*, Brussels, 10 gennaio 2017, COM (2017) 9 final. Sul punto cfr. F. Piraino, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civ. comm.*, 2017, p. 375 ss.

¹² Tuttavia, questa impressione si colloca sul piano naturalistico, mentre sul piano giuridico « il consenso, più che costituire una sorta di rinuncia dell'avente diritto alla propria privacy, esprime invece la condizione soggettiva per la reificazione dei dati personali, che per suo tramite entrano per così dire sul mercato in quanto beni suscettibili di autonoma considerazione economica » (V. CUFFARO, *A proposito del ruolo del consenso*, in *Trattamento dei dati e tutela della persona*, cit., p. 121).

di abuso”, che si concretizza in regole di correttezza nell’attività degli utilizzatori, definite tramite una procedimentalizzazione aperta agli adeguamenti resi necessari dalla natura modificabile di alcuni dati e diritti personali e dall’evoluzione tecnologica delle relative possibilità di trattamento e sfruttamento. Il consenso al trattamento dei dati diviene fase della formazione del contratto, preconditione e parte integrante del momento genetico dell’accordo inteso come elemento per l’esistenza del contratto¹³. Tale situazione sembra confermare la prospettiva secondo la quale l’accordo determina il trasferimento o l’autorizzazione o “licenza” all’uso di dati e informazioni intesi alla stregua di beni giuridici in senso lato o, comunque, possibili oggetti di scambio contrattuale¹⁴.

La propensione a favorire lo sviluppo dell’economia digitale è ben visibile nella nuova disciplina. Basti leggere il considerando 4 del Regolamento privacy, secondo il quale « la protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerata alla luce della sua funzione sociale e va temperata con altri diritti fondamentali, in ossequio al principio di proporzionalità »¹⁵. Oppure il considerando 47, in cui è previsto che i legittimi interessi di un titolare del trattamento possano costituire una base giuridica del trattamento e che possa « essere considerato legittimo interesse trattare dati personali per finalità di marketing diretto »¹⁶.

¹³ Sull’accordo come elemento necessario per l’esistenza del contratto (piuttosto che come requisito di validità dello stesso, ai sensi dell’art. 1325 c.c.), R. SCOGNAMIGLIO, *Contributo alla teoria del negozio giuridico*, II ed., Napoli, 1969, p. 123. Sulla rilevanza del consenso o “accordo” nel contratto, si rinvia, senza alcuna pretesa di esaustività e nell’ambito di una letteratura vastissima, alla disputa tra Irti, Oppo e Bianca (N. IRTI, *Scambi senza accordo*, in *Riv. trim. dir. proc. civ.*, 1998, p. 347 ss.; G. OPPO, *La disumanizzazione del contratto*, in *Riv. dir. civ.*, 1998, p. 525 ss.; C. M. BIANCA, *Diritto civile*, 3, *Il contratto*, Milano, 2000, p. 43; N. IRTI, *È vero, ma ... (Replica a Giorgio Oppo)*, in *Riv. dir. civ.*, 1999, p. 273 ss.; ID., *Lo scambio dei foulards (replica semiseria al prof. Bianca)*, in *Riv. trim. dir. proc. civ.*, 2000, p. 601 ss.). Sul tema anche F. GAZZONI, *Contratto reale e contratto fisico (ovverosia l’accordo contrattuale sui trampoli)*, in *Riv. dir. comm.*, 2002, I, p. 655 ss.; C. CAMARDI, *Contratto e rapporto nelle reti telematiche. Un nuovo modello di scambio*, in *Contr. impr.*, 2001, p. 557 ss.; F. BRAVO, *Contrattazione telematica e contrattazione cibernetica*, Milano, 2007, p. 376, nt. 27 e p. 450 ss.

¹⁴ Sul tema, V. ZENO-ZENCOVICH, voce *Cosa*, in *Dig disc. priv.*, sez. civ., IV, Torino, 1989, p. 453 ss.; P. PERLINGIERI, *L’informazione come bene giuridico*, in *Rass. dir. civ.*, 1990, p. 326 ss., in particolare p. 331-332; R. PARDOLESI, C. MOTTI, « *L’idea è mia!* »: *lusinghe e misfatti dell’economics of information*, in questa *Rivista*, 1990, p. 345 ss., in particolare p. 354-355; V. ZENO-ZENCOVICH, voce *Informazione* — *Profili civilistici*, in *Dig disc. priv.*, sez. civ., vol. IX, Torino 1993, p. 420; ID., *Sull’informazione come “bene” (e sul metodo del dibattito giuridico)*, in *Riv. crit. dir. priv.*, 1999, p. 485 ss.; G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ.*, 2018, p. 411 ss. In senso contrario, D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, cit., p. 347, per il quale l’informazione attiene « all’ambito giuridico della generale protezione della persona e della sua sfera personale in quanto tale ».

¹⁵ A. RICCI, *Sulla funzione sociale del diritto alla protezione dei dati personali*, in *Contr. Impr.*, 2017, p. 586 ss.

¹⁶ Tuttavia, l’art. 21 e il considerando 70 prevedono che qualora i dati personali

Il Regolamento privacy, sebbene modifichi profondamente le regole del trattamento dei dati personali, contenute nella direttiva 95/46/CE e nella legislazione interna in relazione ai modelli organizzativi e imprenditoriali e agli adempimenti in capo ai responsabili e titolari, non fa altrettanto riguardo al fondamento giuridico che legittima il trattamento ¹⁷.

Il consenso, anche se da presupposto necessario di legittimità del trattamento dei dati ¹⁸ è divenuto semplicemente uno dei possibili presupposti di liceità del trattamento dei dati (art. 6 Regolamento privacy), continua a ricoprire un ruolo di grande rilievo (v. i considerando 32, 40, 42, 43) ¹⁹. Esso è stato definito come « manifestazione del diritto all'autodeterminazione informativa » ²⁰ e agisce come mezzo per superare lo squilibrio informativo tra il titolare del trattamento e l'interessato ²¹.

Ai sensi dell'art. 4, comma 1, punto 11 del Regolamento privacy il consenso è « qualsiasi manifestazione di volontà libera, specifica e 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 oggetti di trattamento », il consenso deve dunque essere specifico ²². Tuttavia, nel mondo dei *Big data* la circolazione dei dati è complessa e segue regole tecniche di funziona-

siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano.

¹⁷ Sul punto, I.A. CAGGIANO, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo (GDPR) e analisi comportamentale. Iniziali spunti di riflessione*, in *Diritto Mercato e tecnologia*, 2017, p. 8, per la quale le scelte normative del legislatore europeo « rivelano un'impostazione volta a non impedire le prospettive tecnologiche di produzione sempre più massiva di dati, le sfere di utilizzo e le tecniche che consentono la moltiplicazione dei dati stessi, ma a disciplinare i trattamenti con meccanismi, ritenuti "virtuosi", finalizzati a minimizzare i rischi di perdita, dispersione, diffusione, nella dichiarata finalità di proteggere la sfera dei soggetti cui i dati si riferiscono ».

¹⁸ V. CARBONE, *Il consenso, anzi i consensi, nel trattamento informatico dei dati personali*, in *Danno e resp.*, 1998, 27.

¹⁹ Sul consenso nel nuovo regolamento, WP29, *Guidelines on Consent under Regulation 2016/679*, 10 aprile 2018, WP 259rev.01, le quali forniscono un'analisi approfondita della nozione di consenso nel regolamento 2016/679, alla luce dei cambiamenti avvenuti rispetto alla precedente di-

sciplina sulla protezione dei dati. Il consenso, se ottenuto nel rispetto del GDPR, rappresenta lo strumento che permette al titolare dei dati il controllo sull'elaborazione dei propri dati personali. Diversamente, il controllo dell'interessato diventa illusorio e il consenso costituirà una base non valida per l'elaborazione, rendendo illecita l'attività di elaborazione.

²⁰ Garante Privacy, Provv. 28 maggio 1997, in *Boll.* n. 1.

²¹ Sul punto, C. CAMARDI, *Mercato delle informazioni e privacy: riflessioni generali sulla L. N. 675/1996*, cit., p. 1061, per la quale le dinamiche della prestazione del consenso sono paragonabile a quella della adesione tipica dei contratti di massa uniformi stipulati tra consumatori e professionisti; S. RODOTÀ, *Protezione dei dati e circolazione delle informazioni*, in *Riv. crit. dir. priv.*, 1997, p. 600.

²² Sulla necessità che il consenso sia specifico, in luogo di molti, cfr. G. RESTA, *Autonomia privata e diritti della personalità*, Napoli, 2005, p. 286-287; G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ.*, 2018, p. 434. Sul punto anche S. THOBANI, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Eur. dir. priv.*, 2016, p. 513 ss.

mento difficilmente controllabili dal consenso del singolo e difficilmente compatibili con il requisito della determinatezza delle finalità di trattamento (considerando 39, 50, 61). L'oscurità e complessità del trattamento dei dati vanificano completamente il ruolo riconosciuto fino ad ora al consenso, che finisce per rappresentare un mero tributo alla retorica del personalismo ²³.

La vacuità del consenso si ritrova nel secondo comma dell'art. 22 del Regolamento privacy, in cui si prevede che il diritto dell'interessato di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato viene meno se vi è il consenso esplicito dell'interessato stesso ²⁴. Il processo decisionale automatizzato può coincidere con la profilazione ovvero risultare dalla profilazione. Nel caso in cui il processo decisionale sia esclusivamente automatizzato, l'assunzione di decisioni avviene mediante mezzi tecnologici senza alcun coinvolgimento umano (ad esempio quando è un algoritmo a decidere se concedere o meno un prestito, senza alcuna valutazione preventiva e significativa da parte di un essere umano). In questi casi la profilazione si basa solo su dati derivati o dedotti da altri dati e il consenso dell'interessato non è sufficiente a legittimare con certezza l'elaborazione. Tale legittimità richiede invero l'adozione di tecniche di effettiva informazione preventiva sulle specifiche modalità di trattamento che formano oggetto di autorizzazione ²⁵.

Nessun divieto è, inoltre, previsto rispetto alla prassi imprenditoriale di porre come onere indispensabile per l'accesso a determinati servizi un consenso avente direttamente o indirettamente ad oggetto dati o modalità di trattamento non strumentali alla prestazione dei servizi stessi.

In questa dimensione il requisito del consenso non è in grado di limitare i rischi di diffusione dei dati oltre un orizzonte ragionevolmente prevedibile e il consenso stesso diviene il pretesto per una silenziosa e sostanziale espropriazione interpretata dei diritti di utilizzo dei dati. Al riguardo tornano alla mente le parole di un'autorevole dottrina secondo cui nell'incontro tra tecnologia e personalità dei singoli « dire che talune informazioni possono essere assunte, schedate o fatte circolare solo perché l'interessato

²³ F. PIRAINO, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, cit., p. 384.

²⁴ Sul punto, WP29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 6 febbraio 2018, WP251rev.01; WP29, *Guidelines on Consent under Regulation 2016/679*, 10 aprile 2018, WP259rev.01, par. 4, p. 18.

²⁵ Sul punto, *European Data Protection Supervisor*, Opinion 7/2015, *Meeting*

the challenges of big data. A call for transparency, user control, data protection by design and accountability, 19 novembre 2015, p. 4 e p. 10 ss., per la quale: « When it comes to transparency, individuals must be given clear information on what data is processed, including data observed or inferred about them; better informed on how and for what purposes their information is used, including the logic used in algorithms to determine assumptions and predictions about them ».

ha dato il proprio consenso, significa essere ciechi o ipocriti, dal momento che la prestazione del consenso non è il risultato di una reale scelta tra alternative possibili e non può rappresentare, quindi, né uno strumento di difesa del singolo, né una forma di controllo su chi richiede o ottiene le informazioni » ²⁶.

2. SISTEMI DI INFORMAZIONE CREDITIZIA E TUTELA DELLA PRIVACY.

Tra i rischi che possono derivare da un uso non corretto dei *Big data* vi è quello di effetti pratici discriminatori rilevanti nella sfera giuridica di singoli soggetti, tra i quali la limitazione della facoltà di accesso al credito.

In tema di accesso al credito in generale, la circolazione delle informazioni rappresenta un elemento essenziale. Difatti, nei rapporti di natura creditizia la regola precontrattuale che impone al privato di comunicare tutti i dati necessari per valutare la convenienza dell'accordo viene sostituita da un sistema di rilevazione di dati esterno al soggetto interessato ad ottenere il finanziamento. Questo sistema si basa sulla rilevazione centralizzata dei rischi, ossia su « banche dati che raccolgono in modo centralizzato informazioni economiche inerenti alle caratteristiche delle posizioni debitorie degli affidati nei confronti del sistema creditizio e, più in generale, alla solvibilità dei soggetti prenditori di credito » ²⁷.

In Italia questo sistema di centralizzazione informativa dei rischi creditizi è realizzato dalla Centrale dei Rischi gestita da Banca d'Italia, che raccoglie le informazioni fornite da banche e società finanziarie sui crediti che esse concedono ai loro clienti ²⁸, e dai sistemi di rilevazione centralizzata dei rischi di natura privata che agiscono nel rispetto del Codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati

²⁶ S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973, p. 45.

²⁷ A. SCIARRONE ALIBRANDI, *Centrali dei rischi creditizi e normativa di privacy: informazione e controlli dell'interessato*, in *Riv. dir. civ.*, 2003, I, p. 423.

²⁸ Cfr. Decreto d'urgenza del Ministro dell'Economia e delle Finanze - Presidente del Comitato interministeriale per il Credito e il Risparmio (CICR) dell'11 luglio 2012 n. 663 e Circolare n. 139 del 11 febbraio 1991, aggiornata a giugno 2018. Il sistema informativo della Centrale Rischi si fonda sull'obbligo degli intermediari partecipanti di comunicare mensilmente alla Banca d'Italia i rapporti di credito in essere nei confronti di ciascun cliente, di importo pari o superiore a 30.000 euro e i crediti in sofferenza

di qualunque importo. In particolare, la banca dati della Centrale Rischi è strutturata su due principali flussi informativi: le comunicazioni di dati fatte dagli intermediari alla Banca d'Italia (c.d. segnalazioni) e le comunicazioni di dati che Banca d'Italia invia agli intermediari attraverso i flussi di ritorno ed il servizio di prima informazione. In dottrina, sulla Centrale dei rischi Banca d'Italia, tra i molti, F. CAPRIGLIONE, *Aspetti della problematica giuridica della Centrale dei rischi bancaria*, in *Bancaria*, 1974, p. 19 ss.; U. MORERA, *La centralizzazione dei rischi di credito: profili giuridici*, in AA.VV., *La nuova centrale dei rischi*, Roma, 1997, p. 19 ss.; G. SCOGNAMIGLIO, *Sulla segnalazione a sofferenza nella Centrale dei rischi della Banca d'Italia*, in *Banca borsa tit. cred.*, 1999, I, p. 303 ss.

in tema di crediti al consumo, affidabilità e puntualità nei pagamenti ²⁹.

Questi sistemi informativi offrono uno strumento utile per la valutazione del merito creditizio della clientela e per monitorare il rischio di sovraindebitamento. Inoltre, favoriscono l'accesso al credito e la riduzione dei relativi costi per la clientela meritevole. La raccolta di informazioni svolge, infatti, una funzione microeconomica ed è diretta a consentire ai singoli intermediari creditizi di migliorare la valutazione dei potenziali debitori.

La corretta valutazione del merito creditizio dei clienti da parte delle banche costituisce il presupposto per ottenere la c.d. referenza creditizia, ossia « la reputazione che il cliente ha presso le banche e gli intermediari finanziari e riflette la correttezza dei suoi comportamenti nell'ambito dei rapporti di finanziamento » ³⁰. I sistemi informativi contengono informazioni creditizie di tipo “negativo”, che riguardano rapporti di credito per i quali si sono verificati inadempimenti, e talora informazioni creditizie di tipo “positivo”, riferite ai regolari pagamenti delle rate o all'estinzione del debito, o anche informazioni creditizie di tipo “positivo e negativo”, che attengono a richieste o rapporti di credito a prescindere dalla sussistenza di inadempimenti registrati nel sistema al momento del loro verificarsi. Essi sono utilizzati dagli operatori del settore creditizio e finanziario al fine di condividere e scambiare informazioni su finanziamenti.

Da anni si avverte ormai il problema della tutela della riservatezza degli interessati nei confronti delle centrali rischi ³¹. Non sono stati pochi i casi di impossibilità o difficoltà di accesso al credito da parte degli utenti consumatori causati da un trattamento dei dati personali effettuato in modo improprio dalle centrali rischi private ³². Per il richiedente di un finanziamento essere considerato un “cattivo pagatore” può avere effetti negativi

²⁹ Il codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati è entrato in vigore il 1 gennaio 2005 ed è nato dall'accordo delle associazioni rappresentative del settore con la collaborazione delle associazioni dei consumatori al fine di condividere tra le diverse banche e gli intermediari finanziari i dati relativi all'esposizione debitoria della clientela in ordine ad operazioni di credito ai consumatori. Le regole in esso contenute sono il frutto dell'elaborazione compiuta dal Garante della privacy (v. *Dossier Centrali rischi*). Sul ruolo delle SIC, S. LOPREIATO, *Centrali dei rischi private, segnalazione erronea e responsabilità della banca*, in *Banca borsa tit. cred.*, 2007, II, p. 454 ss.

³⁰ Banca d'Italia, *Le informazioni sulle relazioni creditizie*, in www.bancaditalia.it.

³¹ Sul punto R. CAFARO, P. PAGLIARO, *L'accesso al credito. Banche dati, Centrali di rischio e privacy*, Milano, 2004.

³² Negli ultimi anni sono incrementate le controversie giudiziali riguardanti le segnalazioni presso le centrali rischi creditizie, in particolare quelle relative alla sussistenza dei presupposti per la dicitura “a sofferenza” presso la Centrale Rischi della Banca d'Italia. Sul punto, Cass., Sez. IV, 28 marzo 2018, n. 7594; Cass., 9 luglio 2014, n. 15609; Cass., 24 maggio 2010, n. 12626; Cass., 1 aprile 2009; Trib. Brindisi, 2 marzo 2011; Trib. Bari, 5 gennaio 2011. La questione delle indebite segnalazioni

sull'accesso al credito, sull'iniziativa privata e sulle proprie relazioni sociali e professionali ³³.

Sulla questione l'attenzione è rivolta principalmente ai presupposti e alle modalità con cui le informazioni relative ai rapporti di credito vengono raccolte e trasmesse alle centrali rischi e, di conseguenza, condivise all'interno del sistema bancario ³⁴.

La trasmissione dei dati che l'intermediario invia alla Centrale dei Rischi Banca d'Italia, è una comunicazione di dati personali ³⁵ da un soggetto privato ad un soggetto pubblico. I dati hanno carattere riservato e possono essere utilizzati solo per finalità legate all'assunzione e alla gestione del rischio di credito. La circolazione di tali informazioni sensibili trova giustificazione nella finalità pubblica e privata della segnalazione delle posizioni di rischio dei clienti, che assicura la conoscibilità delle notizie sulla solvibilità dei clienti, incentivando una migliore contrattazione sia per le banche sia per i clienti ³⁶.

presso le centrali rischi è trattata anche dall'Arbitro Bancario Finanziario. Tra le più recenti cfr., ABF, 9 gennaio 2018, n. 153; ABF, 7 marzo 2017, n. 2244; ABF, 2 maggio 2016, n. 4033; ABF, 24 giugno 2016, n. 5964; ABF, 17 dicembre 2015, n. 1160; ABF 31 gennaio 2014, n. 611; ABF, 30 luglio 2012, n. 2626; ABF, 13 aprile 2012, n. 1143.

³³ Cfr. Cass. 9 luglio 2014, n. 15609; Cass., 24 maggio 2010, n. 12626, in *Resp. civ.*, 2011, p. 272 ss., con nota di M. Gorgoni, *Misure di contenimento del rischio del credito e tutela della reputazione* e in *Danno resp.*, 2011, p. 285 ss., con nota di V. Trovato, *Illegittima segnalazione alla Centrale dei rischi e prova del danno alla reputazione economica*; Cass., 18 settembre 2009, n. 20120; Cass., 30 agosto 2007, n. 18316; Trib. Brindisi, 20 luglio 1999.

³⁴ Sui requisiti della segnalazione v. Collegio di coordinamento, ABF, 24 settembre 2012, n. 3089. Sul problema della segnalazione illegittima e della responsabilità degli intermediari nei confronti dei segnalati, A. DOLMETTA, *A proposito della responsabilità della banca nei confronti del cliente oggetto di segnalazione di notizie false alla Centrale dei rischi*, in *Banca borsa tit. cred.*, 1997, II, p. 358 ss.; U. MORERA, *La centralizzazione dei rischi di credito: profili giuridici*, cit., p. 469 ss.; G. SCOGNAMIGLIO, *Sulla segnalazione a sofferenza nella Centrale dei rischi della Banca d'Italia*, cit., p. 303 ss.; C. FRIGENI, *Segnalazioni presso le centrali rischi e tutela dell'interessato: profili evolutivi*, in *Banca borsa tit. cred.*, 2013, I, p. 365 ss.; F.S. MARTORANO, *Segnalazione in*

centrale rischi e violazione della privacy: gli strumenti di tutela interinale dopo il d.lgs. 150/2011, in *Banca borsa tit. cred.*, 2014, I, p. 218 ss.; F. MEZZANOTTE, *Centrali rischi private e "diritto di preavviso" della segnalazione*, in *Nuova giur. civ. comm.*, 2017, II, p. 303 ss.; S. LOPREIATO, *Centrale dei rischi private, segnalazione erronea e responsabilità della banca*, cit., p. 463 ss.

³⁵ I dati personali gestiti dalla Centrale Rischi Banca d'Italia sono sia di tipo obiettivo sia di tipo valutativo. I dati personali di tipo obiettivo riguardano le informazioni relative a fatti storici riguardanti l'interessato, mentre i dati di carattere valutativo concernono informazioni caratterizzate da elementi di giudizio o di valutazioni provenienti dalla banca che le trasmette. Diversamente, ai sensi dell'art. 3, comma 2, del Codice di deontologia e buona condotta, le centrali rischi private gestiscono solo dati personali di tipo obiettivo.

³⁶ Sul punto, F. CAPRIGLIONE, *Aspetti della problematica giuridica della Centrale dei rischi bancari*, cit., p. 22 e 26; F. VELLA, *Segnalazione di crediti in "sofferenza" alla Centrale dei rischi e responsabilità della banca*, in *Banca borsa tit. cred.*, 1997, II, p. 496; A. GABRIELLI, *La legittimità della segnalazione a sofferenza: una analisi giuridico-economica*, in *Banca Borsa tit. cred.*, 2007, II, p. 661-662; L. TREQUATTRINI, *Vigilanza informativa, in La nuova legge bancaria, Il T.U. delle leggi sulla intermediazione bancaria e creditizia e le disposizioni di attuazione. Commentario*, a cura di P. Ferro-Luzzi, G. Castaldi, II, Milano, 1996, p. 776; F. PASQUARIELLO, *Sulla segnalazione a soffe-*

Prima dell'entrata in vigore del Codice privacy ³⁷, il Garante si era espresso ritenendo che « La comunicazione dei dati personali relativi all'indebitamento della clientela effettuata dagli intermediari finanziari alla Centrale dei rischi della Banca d'Italia, in quanto dovuta per legge, non è sottoposta all'obbligo della preventiva acquisizione del consenso dei singoli interessati, cui è quindi preclusa la possibilità di ottenere la cancellazione dei dati in mancanza di un accertamento dell'illiceità, anche per altri profili, del trattamento » ³⁸. Il fondamento normativo dell'obbligo di effettuare le comunicazioni veniva individuato negli artt. 51 e 53 del TUB e nell'art. 27, comma 2, della legge n. 675 del 1996, per i quali ai fini della legittimità della comunicazione era sufficiente che la stessa risultasse comunque necessaria per lo svolgimento delle funzioni istituzionali, tra le quali le disposizioni del TUB prevedevano il controllo di stabilità e il contenimento dei rischi a cui il servizio di centralizzazione è strumentale ³⁹. Con l'entrata in vigore del Codice privacy, l'art. 18, comma 2, dispone che il trattamento di dati personali da parte di soggetti pubblici sia consentito solo per lo svolgimento delle funzioni istituzionali (dopo l'abrogazione dell'art. 18 da parte del d.lgs. 101/2018, si veda l'art. 2-ter, Codice privacy novellato). La tutela del rischio creditizio, cui il sistema informativo della Centrale Rischi è diretto, rientra nelle funzioni istituzionali della Banca d'Italia e, in particolare, nell'attività di vigilanza regolamentare disciplinata dall'art. 53 del TUB.

Per quanto riguarda i sistemi di rilevazione centralizzata dei rischi di natura privata il codice di deontologia e buona condotta non ha previsto finora alcuna disposizione sul consenso ⁴⁰.

Prima dell'introduzione del Codice privacy e con riferimento

renza alla centrale dei rischi, in *Banca borsa tit. cred.*, 2014, II, p. 240 ss.

³⁷ Il 4 settembre è stato pubblicato sulla Gazzetta Ufficiale il decreto legislativo n. 101 del 10 agosto 2018 recante "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)". Tale decreto novella e modifica il Codice della privacy.

³⁸ Garante privacy, 17 gennaio 2001, n. 40907. Diversamente G. ALPA, *Aspetti della disciplina sui dati personali riguardanti gli enti e l'attività economica*, in *Riv. trim. dir. proc. civ.*, 1998, p. 726-727, secondo il quale l'esonerazione dal consenso del cliente in questo caso non opera.

³⁹ Sul punto, P. GAGGERO, *Il trattamento dei dati personali nel settore bancario. Brevi note*, in *Contr. impr. Europa*, 1998, p. 308-309, per il quale l'esenzione dall'obbligo di acquisire il consenso dell'interessato trovava fonte nella configurabilità della centrale dei rischi come trattamento relativo a dati raccolti e detenuti in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria. In particolare, nella natura regolamentare della delibera CICR 29 marzo 1994 che regola il servizio di centralizzazione dei rischi.

⁴⁰ Per completezza di informazioni, si precisa che il codice deontologico all'art. 4, comma 7, prevede un obbligo di preavviso a carico dell'intermediario al verificarsi di ritardi nei pagamenti, al fine di avvisare l'interessato circa l'imminente registrazione dei dati in uno o più sistemi di informazioni creditizie. Inoltre, all'art. 5 è stabilito che al momento della raccolta dei dati personali

alla disciplina sulla privacy, poiché mancava un fondamento legale delle centrali rischi private, si riteneva necessario interpellare l'interessato ⁴¹. Tuttavia, il Garante non ha tenuto una linea costante sul punto, ritenendo in alcuni casi che l'utilizzazione e divulgazione a terzi dei dati relativi allo svolgimento di attività economiche potesse avvenire anche senza il consenso dell'interessato (ai sensi degli artt. 12, comma 1, lett. f), e 20, comma 1, lett. e), della legge n. 675/1996) ⁴². Con l'entrata in vigore del Codice privacy, invece, parte della dottrina ha ritenuto che il trattamento dei dati da parte delle centrali rischi private rientrasse nell'ipotesi di esenzione di cui all'art. 24, comma 1, lett. d), ormai abrogato ⁴³. Secondo questa interpretazione il concetto di « dati relativi allo svolgimento di attività economiche » avrebbe dovuto essere inteso in senso ampio ricomprendendo ogni informazione relativa alla consistenza patrimoniale e alla situazione economica di un debitore. Dopo l'abrogazione dell'art. 24 del Codice privacy, il trattamento di tale tipo di informazioni potrebbe essere ricompreso in determinati casi tra quelli necessari per l'esecuzione di un compito di interesse pubblico, ai sensi dell'art. 6, par. 1, lett. e) del Regolamento privacy.

Su questa linea, se si considerano le finalità a cui mira l'intero sistema delle informazioni creditizie private, ossia « la tutela del credito e il contenimento dei relativi rischi in modo da agevolare anche l'accesso al credito al consumo e ridurre il rischio di eccessivo indebitamento da parte degli interessati » ⁴⁴ (preambolo del codice deontologico), e l'impianto di protezione disciplinato dal codice deontologico, secondo il quale « il trattamento di dati personali effettuato nell'ambito di sistemi informativi di cui sono

relativi a richieste/rapporti di credito, l'intermediario è tenuto ad informare l'interessato del trattamento dei dati personali effettuato nell'ambito di un sistema di informazioni creditizie.

⁴¹ Garante privacy, 9 dicembre 1999, n. 1 e 10 gennaio 2002, n. 9.

⁴² Garante privacy, 25 febbraio 2000, n. 4. Sull'interpretazione del concetto "dati relativi allo svolgimento di attività economiche", C. CASTRONOVO, *Situazioni soggettive e tutela nella legge sul trattamento dei dati personali*, in *Eur. dir. priv.*, 1998, p. 663 ss.; V. RICCIUTO, *Il trattamento dei dati relativi allo svolgimento di attività economiche*, in *Eur. dir. priv.*, 1998, p. 685 ss., in particolare p. 707 ss.; F. CAFAGGI, *Qualche appunto su circolazione, appartenenza e riappropriazione nella disciplina dei dati personali*, in *Danno e resp.*, 1998, p. 613 ss., in particolare p. 618; V. ZENO-ZENCOVICH, *Commento agli artt. 20 e 21, in La tutela dei dati personali. Commentario alla l. 675/1996*, a cura di E. GIANNANTONIO, M. G. LOSANO, V. ZENO-ZENCOVICH, Padova, 1999, p. 269; E. PELLECCIA, *Il codice deon-*

tologico per le centrali-rischi private, in *Danno e resp.*, 2005, p. 255-256.

⁴³ A. SCIARRONE ALIBRANDI, *Trasmissione di dati alle centrali dei rischi: consenso e informazione dell'interessato*, in *Centrali dei rischi. Profili civilistici*, a cura di A. Sciarbone Alibrandi, Milano, 2005, p. 79 ss. e p. 82-83, secondo la quale la circolazione dei dati di natura economica è necessaria per il funzionamento del mercato che non può rischiare di essere ostacolato dalle remore del singolo. Diversamente, V. ZENO-ZENCOVICH, *Privacy e informazioni a contenuto economico nel d.lgs. n. 196/2003*, in *Studium iuris*, 2004, p. 452, secondo il quale i dati a contenuto economico si distinguono dai dati relativi allo svolgimento di attività economiche e rientrano nella disciplina generale che impone il consenso preventivo.

⁴⁴ Sul punto già M. PORZIO, *Il fondamento normativo del segreto bancario*, in *Banca borsa tit. cred.*, 1982, I, p. 1024-1025, per il quale la difesa del sistema creditizio costituiva un limite al segreto bancario e, dunque, giustificava le informazioni sulla clientela interbancarie.

titolari soggetti privati, utilizzati a fini di credito al consumo o comunque riguardanti l'affidabilità e la puntualità dei pagamenti, deve svolgersi nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone interessate, in particolare del diritto alla protezione dei dati personali, del diritto alla riservatezza e del diritto all'identità personale », il consenso preventivo al trattamento dei dati come presupposto di legittimità non risulta necessario ⁴⁵. Quest'ultimo potrebbe avere invece una funzione residuale e fungere da filtro in tutti i casi in cui il trattamento dei dati possa avvenire per finalità differenti, in virtù di quando stabilito dall'art. 2, comma 2, del codice deontologico, secondo il quale « Non può essere perseguito alcun altro scopo, specie se relativo a ricerche di mercato e promozione, pubblicità o vendita diretta di prodotti o servizi ».

In ogni caso, come già rilevato, il consenso non è sufficiente per tutelare l'interessato dai trattamenti dei dati illeciti e lesivi. Parte della dottrina sostiene che, in tema di trasmissione di dati dall'intermediario alle centrali rischi, il problema potrebbe essere superato tramite un'impostazione diversa, frutto di un « ribaltamento della prospettiva nella quale viene giuridicamente disciplinato il fenomeno » ⁴⁶, nel senso che l'attività di raccolta e trasmissione di informazioni alle banche dati da parte degli intermediari, ricadendo all'interno del rapporto banca-cliente, resti assoggettata ai principi che ne disciplinano lo svolgimento. L'intermediario procede alla raccolta e trasmissione dei dati sempre con riguardo alla propria clientela (o potenziale), sicché tale attività si innesta sulla relazione — essenzialmente negoziale — dalla quale è scaturito il rapporto di credito oggetto di segnalazione. Tale impostazione permetterebbe di considerare la segnalazione "errata" come fonte di responsabilità contrattuale per inadempimento del dovere di comportarsi secondo buona fede e correttezza.

3. PEER TO PEER LENDING E TUTELA DELLA PRIVACY.

Attraverso le tecnologie dell'informazione e delle telecomunicazioni le banche hanno aumentato la qualità e la quantità dei servizi offerti alla clientela e sono riuscite sia a sviluppare nuove tecniche di gestione dei rischi, sia a rendere più rapida e sicura la

⁴⁵ Cfr. A. SCIARRONE ALIBRANDI, *Trasmissione di dati alle centrali dei rischi: consenso e informazione dell'interessato*, cit., p. 78 ss.; L. BONZANINI, A. LEIDI, *Privacy e banche: il nuovo regime di trattamento dei dati personali* (d.lgs. 28 dicembre 2001, n. 467), in *Banca borsa tit. di cred.*, I, 2003, p. 498 e p. 514-515.

⁴⁶ C. FRIGENI, *Segnalazioni presso le centrali rischi creditizie e tutela dell'interessato: profili evolutivi*, cit., p. 371. Tale tesi è stata accolta anche dall'Arbitro Bancario Finanziario: ABF 5 settembre 2014, n. 5947.

gestione dei pagamenti. Le nuove tecnologie hanno, però, anche consentito ad alcune imprese, note come imprese *FinTech*, di offrire servizi (servizi di pagamento, di investimento, di consulenza e di finanziamento) che fino a pochi anni fa erano esclusivo appannaggio del sistema bancario ⁴⁷. Un esempio emblematico è quello delle piattaforme on-line che facilitano il cosiddetto prestito tra pari, o *peer-to-peer lending*.

Gli sviluppi delle imprese *Fintech* hanno finora sollevato questioni di vigilanza prudenziale, ma vi sono anche altri problemi, come la salvaguardia della privacy, della sicurezza IT e della tutela dei consumatori. Tali imprese si basano, infatti, su modelli di business di aggregazione di dati e utilizzano i dati dei clienti per ottenere una conoscenza approfondita dei clienti stessi attraverso la cronologia delle ricerche, i dati personali e le preferenze condivise sui *social media*, le abitudini di consumo e di spesa, e così via ⁴⁸.

Il successo delle imprese *Fintech*, soprattutto in chiave concorrenziale, è strettamente legato anche alla fiducia che i consumatori ripongono nelle modalità in cui i loro dati personali vengono trattati ⁴⁹. A seguito dell'emanazione del Regolamento privacy, tali imprese saranno obbligate a dotarsi di una serie di misure preventive per la protezione dei dati personali dei loro clienti.

Come è noto, il *peer to peer lending* consiste nel prestito tra privati attraverso l'utilizzo di internet. In particolare, gli utenti di internet, mediante una piattaforma web gestita e messa a disposizione da una determinata società specializzata (il gestore della piattaforma di *peer to peer lending*), prestano o richiedono in

⁴⁷ Per *FinTech* si intende « un'attività finanziaria resa possibile o offerta attraverso le nuove tecnologiche, che interessa l'intero settore finanziario in tutte le sue componenti, dal settore bancario a quello assicurativo, i fondi pensione, la consulenza in materia di investimenti, i servizi di pagamento e le infrastrutture di mercato » (Parlamento Europeo, *Tecnologia finanziaria: influenza della tecnologia sul futuro del settore finanziario*, 17 maggio 2017, 2016/2243 (INI)). Le imprese *FinTech* rappresentano un forte stimolo per l'industria bancaria in quanto sono in grado di alterare in modo rilevante la struttura e il funzionamento dell'industria finanziaria. L'attività svolta dalle imprese *FinTech* in un certo senso "costringerebbe" le banche a diminuire i costi dei canali distributivi tradizionali e a offrire servizi di elevata qualità alla clientela. Sul ruolo e il potenziale delle imprese *FinTech*, cfr. EBA, *Discussion paper on the EBA's approach to financial techno-*

logy (FinTech), 4 agosto 2017; Basel Committee on Banking Supervision, *Sound Practices. Implications of fintech developments for banks and bank supervisors*, Febbraio 2018, p. 22; Commissione europea, *Piano d'azione per le tecnologie finanziarie: per un settore finanziario europeo più competitivo e innovativo*, COM (2018) 109 final, 8 marzo 2018. In dottrina, AA.VV., *Fintech. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, a cura di M.T. Paracampo, Torino, 2017, *passim*.

⁴⁸ Molte imprese *Fintech*, in particolare quelle coinvolte in *Banktech* (offrono applicazioni e servizi bancari) e *Regtech* (offrono strumenti di regolazione e conformità), si basano sulla condivisione e sull'elaborazione di dati personali.

⁴⁹ Sul ruolo che svolge la fiducia nei mercati on line cfr., tra gli altri, G. SMORTO, *Reputazione fiducia e mercati*, in *Eur. dir. priv.*, 2016, p. 199 ss.

prestito somme di denaro ad altri privati cittadini (c.d. *social lending*) o imprese (c.d. *direct lending*) a costi contenuti ⁵⁰.

In tale attività si manifesta un conflitto tra obiettivi economici e obiettivi di protezione della privacy. Il *peer to peer lending* può essere, infatti, considerato come crocevia di questioni e scelte relative alla politica economica e alla regolamentazione della privacy. Il fenomeno, caratterizzato dalla semplicità di utilizzo, dalla velocità di erogazione dei prestiti e dalla capacità di valutare il merito creditizio della clientela, da una parte agevola l'accesso al credito ma, dall'altra, può mettere a rischio la privacy dei soggetti coinvolti, proprio per le modalità con cui avviene la valutazione del merito creditizio.

La valutazione del merito creditizio è uno dei servizi offerti dai gestori delle piattaforme e viene effettuata prendendo in considerazione un'ampia gamma di informazioni, che possono provenire anche da internet e dai *social media*. Difatti, se in passato la determinazione del *credit scoring* avveniva sulla base di informazioni raccolte dall'intermediario mediante la consultazione di dati contenuti nella Centrale dei rischi, oggi le nuove tecnologie consentono di utilizzare servizi di *credit-scoring* in *outsourcing* oppure di fare affidamento su *alternative sources of data and alternative credit-scoring methodologies* ⁵¹.

I gestori delle piattaforme di *peer to peer lending* assegnano un *rating* ad ogni utente richiedente e, di conseguenza, collocano l'operazione di prestito in un certo mercato a seconda della stima del sottostante livello di rischio. Il *rating* viene calcolato tenendo conto di diversi fattori, quali la storia creditizia, il reddito, la situazione familiare, l'area geografica, l'età, e via dicendo. Non sempre, però, gli utenti che si iscrivono a tali piattaforme hanno una storia creditizia. Spesso non risultano iscritti nelle banche dati dei sistemi di informazione del settore del credito. In tali casi, la valutazione del merito creditizio si basa esclusivamente sul c.d. *rating* di credito *social*, nel senso che il *rating* viene assegnato sulla base dei dati raccolti dai profili *social* del richiedente insieme ai dati relativi ai pagamenti "mobile" ⁵², allo stile di vita, alle relazioni, ai desideri e agli acquisti con carte di credito.

L'utilizzo di *alternative sources of data and alternative credit-scoring methodologies* è dovuto anche al fatto che l'Autorità

⁵⁰ Sul tema sia consentito rinviare a G. BIFERALLI, *Il social lending. Problemi di regolamentazione*, in *Riv. Trim. Dir. dell'Economia*, 2017, p. 443 ss., ove ulteriori riferimenti bibliografici.

⁵¹ BCE, *Guide to assessments of fintech credit institution license applications*, settembre 2017, 4.1, p. 9.

⁵² I "pagamenti mobile" sono paga-

menti effettuati mediante uno *smartphone*. La direttiva UE 2015/2366 (PSD2) ha stabilito nuove regole in tema di servizi di pagamento al fine di rendere possibile una più ampia diffusione sul mercato di nuovi mezzi di pagamento e garantire un elevato livello di protezione dei consumatori che si avvalgono di tali servizi di pagamento nel mercato europeo.

bancaria europea ha stabilito che l'attività dei gestori di piattaforme di *social lending* può ritenersi sufficientemente regolata qualora questi ultimi assumano la forma - e dunque si sottopongano alla disciplina - degli "Istituti di pagamento"⁵³. Difatti, gli Istituti di pagamento sono esclusi dal sistema informativo Centrale dei rischi e, dunque, per i gestori di tali piattaforme il ricorso ad informazioni alternative è necessario per valutare il merito creditizio⁵⁴. La scelta dell'Autorità Bancaria Europea di ritenere sufficiente che i gestori delle piattaforme di *social lending* si sottopongano al regime degli Istituti di pagamento si fonda sull'idea che quest'ultimi svolgano, mediante la piattaforma *web*, un servizio di intermediazione di pagamenti che consiste nel trasferimento di denaro tra soggetti privati che prestano o chiedono in prestito denaro. Tuttavia, l'attività svolta da tali operatori trascende la mera gestione di trasferimenti di denaro tra i clienti, ponendo dubbi sulla adeguatezza della disciplina degli Istituti di pagamento a tutelare gli interessi coinvolti⁵⁵.

In tali casi, si prospetta il rischio che taluni richiedenti vedano compromesse o diminuite le proprie *chances* di accesso al credito a condizioni vantaggiose a causa di "errori cognitivi computerizzati", presunzioni o pregiudizi derivanti da erronea programmazione o da "semplificazione algoritmica" e, più in generale, da valutazioni arbitrarie, discriminatorie o comunque "eterodosse", che con l'affidabilità finanziaria possono avere ben poco a che vedere⁵⁶.

Inoltre, ad ulteriore differenza di quanto avviene nel caso di richieste di finanziamento rivolte ad istituti bancari, in cui il richiedente è a conoscenza del fatto che l'ente finanziatore effettuerà un'istruttoria consultando le banche dati dei sistemi di informazione creditizia al fine di valutare le capacità di adempi-

⁵³ EBA, *Opinion of the European Banking Authority on lending-based crowdfunding*, 26 febbraio 2015.

⁵⁴ Cfr. A. SCIARRONE ALIBRANDI, F. MATTASSOGLIO, *Le centrali dei rischi: problemi e prospettive*, in *Dir. banca merc. fin.*, 2017, p. 778 ss.

⁵⁵ Sui problemi di regolamentazione del *peer to peer lending* si rinvia a G. BIFERALI, *Il social lending. Problemi di regolamentazione*, cit., p. 448 ss.

⁵⁶ L'elaborazione dei *Big Data* da parte di sistemi decisionali automatizzati, in particolare di sistemi opachi, c.d. *black box*, nei quali è esclusivamente la macchina a prendere decisioni che non sono conoscibili all'uomo, solleva dubbi riguardo ai profili di responsabilità nei casi di errore (v. la Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla

Commissione concernenti norme di diritto civile sulla robotica). Infatti la mancanza di trasparenza di questi sistemi incide sia sulla possibilità di risolvere gli errori presenti nei processi decisionali automatizzati sia sulla possibilità di garantire alla persona la conoscibilità dei processi decisionali che li riguardano (cfr. A. OTTOLIA, *Big Data e innovazione computazionale*, Torino, 2017, p. 7 ss. e p. 134 ss.). Il problema concerne l'individuazione del soggetto responsabile per l'errore da algoritmo, dal momento che nel fenomeno dell'intelligenza artificiale vi sono sia un creatore sia un produttore del bene (cfr. U. RUFFOLO, *Per i fondamenti di un diritto della robotica Self-Learning; dalla machinery produttiva all'auto driverless: verso una "responsabilità da algoritmo"?*, in *Intelligenza artificiale e responsabilità*, a cura di U. Ruffolo, Milano, 2017, p. 16 ss.

mento, il richiedente prestito nel *peer to peer lending* è il più delle volte sostanzialmente ignaro del fatto che il gestore lo inserirà in una determinata classe di rischio sulla base di informazioni di cui il richiedente stesso non ha contezza.

Per giustificare i metodi di valutazione del merito creditizio adottati per il *peer to peer lending* si potrebbe rilevare che, nell'ambito limitrofo del credito al consumo (oltre che in quello dell'attività di finanziamento in generale), il finanziatore è tenuto a valutare in modo approfondito tutte le informazioni necessarie a comprendere la capacità di rimborso del soggetto richiedente⁵⁷. Le informazioni possono essere ottenute da varie fonti, anche direttamente attraverso il consumatore, e dovrebbero essere opportunamente verificate dal creditore prima di concedere il credito.

In proposito una parte della dottrina⁵⁸ ritiene che il dovere di valutazione del merito creditizio possa essere considerato come un corollario dell'obbligo di astenersi dall'assunzione di decisioni arbitrarie e immotivate, finalizzato ad inibire al finanziatore di concedere credito ogni qualvolta emerga una scarsa capacità del consumatore di adempiere all'obbligo di restituzione della somma mutuata. Tale interpretazione permetterebbe di inquadrare l'obbligo di verifica della solvibilità del debitore quale espressione del più generale principio del dovere di sana e prudente gestione, che per vari tipi di intermediari è sancito dall'art. 5 del TUB e costituisce sempre di più una regola imprescindibile delle attività di finanziamento. In questa prospettiva la valutazione del merito creditizio effettuata dai gestori delle piattaforme di *social lending* mediante la consultazione di un'ampia gamma di informazioni,

⁵⁷ A seguito del d.lgs. 19 settembre 2012 n. 169, recante ulteriori modifiche ed integrazioni al d.lgs. 13 agosto 2010, n. 141, l'art. 124-bis, comma 1, TUB dispone che « Prima della conclusione del contratto di credito, il finanziatore valuta il merito creditizio del consumatore sulla base di informazioni adeguate, se del caso fornite dal consumatore stesso e, ove necessario, ottenute consultando una banca dati pertinente ».

⁵⁸ A. MIRONE, *L'evoluzione della disciplina sulla trasparenza bancaria in tempo di crisi: istruzioni di vigilanza, credito al consumo, commissioni di massimo scoperto*, in *Banca borsa tit. cred.*, 2010, 1, p. 592-593; M. GORGONI, *Spigolature su luci (poche) e ombre (molte) della nuova disciplina dei contratti di credito ai consumatori*, in *Resp. civ. prev.*, 2011, p. 765; M. DE POLI, *Gli obblighi gravanti sui « creditori » nella fase anteriore e posteriore alla stipulazione del contratto e le conseguenze*

della loro violazione, in *La nuova disciplina europea del credito al consumo*, a cura di G. De Cristofaro, Torino, 2009, p. 70; S. PELLEGRINO, *Le disposizioni attuative in materia di credito al consumo*, in *Obbl. contr.*, 2011, p. 298; G. BIFERALI, *Il credito ai consumatori*, in *Concorrenza, mercato e diritto dei consumatori*, diretto da G. Casano, A. Catricalà, R. Clarizia, Milano, 2018, p. 1857. Sul punto cfr. anche F. SARTORI, *Disciplina dell'impresa e statuto contrattuale: il criterio della « sana e prudente gestione »*, in *Banca borsa tit. cred.*, 2017, 1, 152; A. DOLMETTA, *Trasparenza dei prodotti bancari, Regole*, Bologna, 2013, p. 132 e p. 134, secondo il quale il dovere di cui all'art. 124-bis TUB deriva dalla clausola della sana e prudente gestione, intesa come « regola di incidenza negoziale, per la protezione del cliente (in genere), in punto di corretta concessione di credito ». In senso critico, cfr. L. MODICA, *Profili giuridici del sovraindebitamento*, Napoli, 2012, p. 239 ss.

che va oltre le banche dati dei sistemi di informazione creditizia, risulta perfettamente legittima. Ciò è vero a maggior ragione se si considera che in quel contesto la valutazione del merito creditizio è effettuata dai gestori direttamente a tutela di terzi investitori, ossia dei prestatori che accedono alla piattaforma. Sotto tale profilo, all'interesse dei richiedenti ad evitare pregiudizi o presunzioni negative sulla propria solvibilità che possono eventualmente derivare dall'utilizzo dei *Big data* si contrappone l'interesse dei prestatori, almeno nella misura in cui la domanda di credito si mantenga ad un livello sufficiente, ad una valutazione "ultra-prudenziale" del merito creditizio, per la quale qualsiasi "presunzione negativa" da *Big data* riguardo alla solvibilità di un richiedente dovrebbe sempre essere tenuta in considerazione.

Occorre inoltre tenere presente che, se i gestori delle piattaforme fossero costretti a circoscrivere le proprie indagini alla consultazione dei sistemi di informazione creditizia, il fenomeno del *peer to peer lending* riguarderebbe solo la parte di popolazione che è o è stata debitrice nei confronti di banche. Questo risultato limiterebbe un fenomeno che può svolgere un'indubbia funzione di utilità sociale.

In conseguenza di quanto si è rilevato, il problema relativo ai *Big data* nella valutazione del merito creditizio per il *peer to peer lending* impone di distinguere, anche riguardo ad eventuali responsabilità per danni, due diverse questioni: quella della legittimità delle modalità di utilizzo delle informazioni reperite da parte del gestore della piattaforma e quella della legittimità delle indagini e delle ricerche che esso ha svolto per reperirle.

La prima questione si incentra sull'esigenza di un utilizzo corretto, non pregiudizievole e non discriminatorio degli stessi e sull'esigenza di trasparenza riguardo alle modalità di tale utilizzazione. In altri termini, il gestore della piattaforma potrebbe essere chiamato a mettere i richiedenti a conoscenza, attraverso idonee forme di pubblicità e informazione precontrattuale, delle tecniche adottate per il reperimento dei dati e dei criteri secondo cui, e della misura nella quale, tali dati vengono considerati rilevanti per la valutazione del merito di credito⁵⁹. Almeno in una fase iniziale e ad ogni evoluzione delle modalità di formazione dei *Big data*, questo tipo di oneri informativi potrebbe richiedere ai gestori delle piattaforme o ad operatori specializzati da essi incaricati, per un verso, una sorta di opera di "reverse enginee-

⁵⁹ Cfr., nel diverso ambito della consulenza finanziaria automatizzata, R. LEENER, *La digitalizzazione della consulenza finanziaria: i robo advice e le regole mifid*, in Financial Community Hub, 6 giugno 2018, p. 4; sulle difficoltà di assoggettare l'algoritmo ad una forma di trasparenza, F. DI

PORTO, *La regolazione degli obblighi informativi. Le sfide delle scienze cognitive e dei big data*, Napoli, 2017, p. 162 ss., la quale, in particolare, mette in evidenza la scarsa capacità del consumatore di comprendere a pieno le implicazioni della sottoposizione dei propri dati a trattamenti automatizzati.

ring” rispetto ai *Big data* utilizzati, per individuare da quali dati e secondo quali criteri essi siano stati formati, e, per altro verso, l’elaborazione di modelli in grado di spiegare in modo relativamente semplice con quale metodo i dati ottenuti si combinano per dare luogo ad un determinato *rating* inerente al merito creditizio⁶⁰. Il “costo” che ne deriverebbe può essere tuttavia di gran lunga sopravanzato dai “benefici” che la trasparenza è in grado di determinare in termini di fiducia degli utenti e affidabilità dei servizi, anche sul piano della competizione tra i diversi gestori di piattaforme⁶¹.

La seconda questione sopra individuata, relativa alla legittimità delle indagini che il gestore della piattaforma svolge per la valutazione del merito creditizio dei richiedenti, dovrebbe invece essere impostata prendendo atto che l’eventuale violazione di norme a tutela della privacy è compiuta non dal soggetto (il gestore della piattaforma) che usa le informazioni disponibili grazie ad internet, bensì dal soggetto che permette che queste ultime siano reperibili da chiunque ne abbia interesse⁶². A questo riguardo vengono in considerazione le molte imprese che spesso non si accontentano di raccogliere dati personali dei clienti per svolgere in maniera adeguata i propri servizi, ma utilizzano tali dati anche come fonte ulteriore di ricavi tramite la rivendita degli stessi a vari livelli ad altre imprese di servizi⁶³.

Allo stato attuale tale fenomeno non sembra agevolmente e significativamente arginabile, anche perché legislatori e regolatori europei ed italiani temono che ciò pregiudicherebbe il mondo imprenditoriale. In una prospettiva *de iure condendo* si potrebbe considerare che dal 2009 negli Stati Uniti un importante istituto

⁶⁰ Tale esigenza incontra il limite costituito dall’opacità degli algoritmi e delle loro modalità di auto-apprendimento. Per alcune soluzioni alle difficoltà di analisi degli algoritmi incorporati in piattaforme software complesse, cfr. E. PROSPERETTI, *Algoritmi dei Big Data: temi regolamentari, responsabilità, concorrenza*, in *Informazione e big data tra innovazione e concorrenza*, a cura di V. Falce, G. Ghidini, G. Olivieri, Milano, 2018, p. 317.

⁶¹ Diversamente, O. BEN-SHAHAR, C. SCHNEIDER, *More than you wanted to know. The failure of mandated disclosure*, Princeton, 2014, p. 7 ss., per i quali gli obblighi di informazione raramente funzionano, nel senso che troppe informazioni o informazioni troppo complesse rischiano di confondere invece che aiutare il destinatario delle stesse. Tuttavia tale rilievo potrebbe essere superato dal fatto che l’adempimento agli obblighi di informazione si conforma alle

finalità di tali obblighi, che è quella di informare, e richiede dunque di fornire informazioni adeguate, ossia necessarie e sufficienti, ad evitare confusioni e consentire al cliente di pervenire ad un “giudizio informato e consapevole” per l’adozione delle proprie scelte di investimento. Ne deriva che le “troppe informazioni” o “informazioni troppo complesse” si porrebbero in contrasto con l’obbligo informativo.

⁶² Questo problema è molto sentito nel Regno Unito nell’ambito assicurativo, dove le imprese sono solite utilizzare i dati raccolti dai profili social per fissare i premi assicurativi su misura (Financial Conduct Authority (FCA), *Feedback Statement FS16/5, Call for Inputs on Big Data in retail general insurance*, settembre 2016, 7, p. 11 ss. e p. 27).

⁶³ Si pensi ad esempio alle società emittenti di carte di credito che vendono i dati grezzi relativi ai propri clienti attraverso intermediari specializzati come *Cardlytics*.

bancario utilizza un metodo che consente ai consumatori di monetizzare l'utilizzo dei propri dati⁶⁴. Segnatamente, le informazioni vengono raccolte in una banca dati chiamata "banca delle informazioni" e chi è interessato ad utilizzarle è tenuto a pagare una commissione direttamente all'interessato, che ha anche traccia del loro utilizzo. Questo meccanismo di "negoiazione" rappresenta un compromesso, seppure di marca monetaria o plutocratica, tra gli interessi degli utenti e quelli delle imprese in relazione al problema del trattamento dei dati e del rispetto della privacy⁶⁵.

Nel contesto dei *Big data analytics*, in cui l'originaria definizione della privacy come "*right to be let alone*"⁶⁶ è mutata in quella di privacy come diritto di controllare l'uso che altri fanno delle informazioni che ci riguardano o come « diritto di mantenere il controllo sulle proprie informazioni e di *determinare le modalità di costruzione della propria sfera privata* »⁶⁷, lo strumento della "negoiazione" potrebbe soddisfare l'esigenza di protezione dei dati personali degli interessati meglio di quanto accada mediante il semplice requisito del consenso⁶⁸.

Resta inteso che una tale apertura dovrebbe fare i conti con il fatto che nell'ordinamento italiano la circolazione dei dati personali è avvenuta sempre mediante il consenso, quale dispositivo che

⁶⁴ Cfr. i dati pubblicati su Osservatorio *Big Data analytics & business intelligence*, in www.osservatori.net.

⁶⁵ Sul punto cfr. la recente Risoluzione del Parlamento europeo, *Tecnologia finanziaria: influenza della tecnologia sul futuro del settore finanziario*, cit., par. 26, in cui si rileva l'utilità per i consumatori di stipulare contratti per la condivisione dei contenuti digitali in cambio di pagamento di una commissione e, pertanto, invita la Commissione a valutare la possibilità di approntare una strategia europea sulla condivisione dei dati allo scopo di dare ai consumatori il controllo dei loro dati. In dottrina G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ.*, 2018, p. 416-417; V. ZENO-ZENCOVICH, *Profili negoziali degli attributi della personalità*, in questa *Rivista*, 1993, p. 545 ss.; Id., *Il "consenso informato" e la autodeterminazione informativa nella prima decisione del Garante*, in *Corr. Giur.*, 8, 1997, p. 915 ss., in particolare p. 919-920; Id., *Una lettura comparatistica della L. 675/96 sul trattamento dei dati personali*, in *Trattamento dei dati e tutela della persona*, cit., p. 169.

⁶⁶ S. WARREN e L.D. BRANDEIS, *The Right to Privacy*, in *Harvard Law Review*, v. 5, n. 5, 1980, p. 193.

⁶⁷ S. RODOTÀ, *Tecnologia e diritti*, Bologna, 1995, p. 122.

⁶⁸ Affidare al contratto e alla sua disciplina il superamento del conflitto tra interessi delle imprese e protezione dei dati personali potrebbe permettere di valorizzare i *Big data* anche nel contesto bancario. Le banche conservano traccia di un'infinità di transazioni dei clienti, contratti di mutuo ipotecario e contratti credito al consumo, ma questa enorme mole di dati è in realtà statica e spesso utilizzata solo da alcune funzioni aziendali. I dati non sono aggiornati in tempo reale e sono di difficile gestione e integrazione, mentre con un approccio incentrato sui *Big data* si potrebbe fornire valore aggiunto alla raccolta e all'analisi degli stessi. Il sistema dei *Big data analytics* potrebbe infatti consentire di elaborare strategie per reagire alla concorrenza proveniente dai nuovi operatori non bancari come le imprese *Fintech*. Esso sembra inoltre in grado di anticipare le esigenze dei clienti e di ridurre i rischi di insolvenza. La grandissima quantità di dati che si "autoalimenta" con il flusso quotidiano di dati che provengono dai *social networks*, dai *tweet*, dalle e-mail, e così via, potrebbe in effetti costituire un grande potenziale per le banche.

permette l'accesso ad una determinata informazione personale, e che la disciplina sul trattamento dei dati personali non regola l'ipotesi di "negoiazione" di proprie informazioni personali a titolo gratuito o oneroso. Inoltre, i principi costituzionali vietano che l'autonomia privata sia esercitata in modo pregiudizievole per i "valori della persona" tra i quali la dignità umana ⁶⁹.

4. BITCOIN PEER TO PEER LENDING E TUTELA DELLA PRIVACY.

Vi è inoltre una questione a cui in questa sede si può soltanto accennare, ma che comunque merita di essere menzionata. I problemi di tutela della privacy connessi al "prestito tra pari" risultano esponenzialmente amplificati nel c.d. *bitcoin peer-to-peer lending*, ossia nel sistema di *peer-to-peer lending* che si serve dei bitcoin ⁷⁰, i quali costituiscono l'oggetto concesso in prestito. Tale sistema è già stato adottato da piattaforme specializzate, che forniscono diversi servizi accessori (tra i quali la valutazione del merito creditizio), ma, in virtù dell'utilizzazione dei bitcoin e della connessa "*blockchain technology*", è in grado, dal punto di vista tecnico, di consentire i trasferimenti di valuta tra prestatore e richiedente senza alcuna intermediazione.

I bitcoin rientrano nella nozione di valuta virtuale ⁷¹ e consistono in un oggetto crittografico a valore fisso, generato in maniera anonima da un dispositivo connesso alla rete ⁷², sul quale

⁶⁹ G. RESTA, *Autonomia privata e diritti della personalità*, Napoli, 2005, p. 276 ss., in particolare p. 280-281; P. RESCIGNO, *Presentazione a G. Resta, Autonomia privata e diritti della personalità*, cit., p. XIX.

⁷⁰ Sul funzionamento tecnico dei Bitcoin, S. NAKAMOTO, *Bitcoin: A peer to peer electronic cash system*, in www.bitcoin.org. Sui Bitcoin dal punto di vista giuridico cfr., in generale, BCE, *Virtual currency Schemes*, ottobre 2012; Id., *Virtual currency schemes — a further analysis*, febbraio 2015; ESMA, *Call for evidence. Investment using virtual currency or distributed ledger technology*, ESMA/2015/532, aprile 2015; Banca d'Italia, *Avvertenze sull'utilizzo delle cosiddette "valute virtuali"*, 30 gennaio 2015. Sulla natura giuridica dei Bitcoin cfr., G. LEMME, S. PELUSO, *Criptomoneta e distacco dalla moneta legale: il caso bitcoin*, in *Riv. dir. banc.*, 2016, p. 1 ss.; N. VARDI, "Crip-tovalute" e dintorni: alcune considerazioni sulla natura giuridica dei Bitcoin, in questa *Rivista*, 2015, p. 443 ss.; G. GASPARRI, *Timidi tentativi giuridici di messa a fuoco del bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?*, in questa *Rivista*, 2015, p. 415 ss.; R. BOCCHINI, *Lo sviluppo della moneta*

virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche, in *Dir. inf.*, 2017, p. 27 ss.; Tribunale di Verona, 24 gennaio 2017, con nota di M. Passaretta, *Bitcoin: Il leading case italiano*, in *Banca borsa tit cred.*, 2017, 2, p. 471 ss.; N. MANCINI, *Bitcoin: rischi e difficoltà normative*, in *Banca Impresa Società*, 2016, p. 111 ss.

⁷¹ Per valuta virtuale si intende « la rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente » (art. 1, comma 2, lett. qq) del d.lgs. 25 maggio 2017 n. 90, in attuazione della direttiva europea 2015/849 (c.d. Direttiva AML) relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo. Tale direttiva è stata peraltro modificata dalla direttiva 2018/843 (v. nota successiva).

⁷² Sul problema del regime di anonimato associato alle valute virtuali e ai rischi legati al riciclaggio di denaro e al finanzia-

opera un apposito *software* in grado di eseguire determinate transazioni. Le transazioni si realizzano mediante un sistema di crittografia a chiave pubblica che si serve della tecnologia informatica *peer to peer*.⁷³ La circolazione dei bitcoin avviene infatti tramite un *database* distribuito (c.d. “*blockchain*”)⁷⁴ che mantiene in modo continuo una lista crescente di registrazioni, le quali fanno riferimento a registrazioni precedenti contenute nella lista stessa.

I rischi per la privacy sono determinati dal fatto che tali registrazioni delle transazioni in *bitcoin* sono rilevabili pubblicamente, tracciabili e impresse in maniera permanente nella rete *bitcoin*, con la conseguenza che chiunque può prendere visione delle varie transazioni effettuate da un qualsiasi indirizzo *bitcoin* e del relativo bilancio⁷⁵. Gli indirizzi sono costruiti da sequenze casuali di numeri e lettere che non contengono informazioni riguardo all'identità dei titolari e sono creati a piacimento da ciascun partecipante alla rete senza particolari limiti: pertanto, nel trasferimento di bitcoin ciò che viene registrato e risulta pubblicamente è in teoria solo l'indirizzo da cui la transazione è effettuata. Tuttavia, l'identità dell'utente collegata ad un certo indirizzo diviene nota appena è rivelata nell'ambito di una delle operazioni compiute⁷⁶. Inoltre, i provider di servizi internet sono in grado di rintracciare l'indirizzo IP da cui è stato effettuato il trasferimento di valuta⁷⁷. La “democraticità” dello strumento comporta dunque anche un ampliamento dei problemi di protezione dei dati personali⁷⁸. Per evitare di fornire pubblicamente un quadro completo delle proprie attività di prestito o ricezione di fondi è possibile adoperare un indirizzo diverso per ogni nuova

mento del terrorismo v. la Direttiva europea 2018/843, 30 maggio 2018, che ha modificato la direttiva 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE.

⁷³ Questo sistema di crittografia permette a chiunque di scaricare su un computer il software, di collegarsi alla rete *Bitcoin* e, attivando l'opzione “genera bitcoin”, di partecipare al processo di creazione dei bitcoin. Sul punto v. R. RAZZANTE, *Bitcoin e monete digitali. Problematiche giuridiche*, in *Gnosis*, 2014, p. 110.

⁷⁴ Si tratta di un *database* che si trova sotto il controllo di un “*database management system*” in cui gli archivi di dati sono memorizzati, invece che su un solo elaboratore, su più elaboratori o nodi connessi tra loro.

⁷⁵ Cfr. P. CUCCURU, *Blockchain ed automazione contrattuale. Riflessioni sugli smart contract*, in *Nuova giur. civ. comm.*, 2017, II, p. 110. Sul punto v. anche S. CAPACCIOLI, *Criptovalute e bitcoin: un'analisi giuridica*, Milano, 2015, p. 44.

⁷⁶ Diversamente, M. MANCINI, *Valute virtuali e bitcoin, Analisi giuridica dell'economia*, 1, 2015, p. 120-121, secondo il quale il sistema garantisce l'anonimato degli utenti.

⁷⁷ Cfr. CUCCURU, *Blockchain ed automazione contrattuale. Riflessioni sugli smart contract cit.*, p. 110 nt. 16.

⁷⁸ L'intero sistema *Blockchain*, caratterizzato dalla decentralizzazione e dall'immutabilità delle informazioni inserite nella catena di blocchi, pone questioni di compatibilità con il Regolamento privacy, tra le quali, a titolo meramente esemplificativo, il rispetto del diritto all'oblio e l'individuazione del Responsabile della protezione dei dati (DPO).

transazione, ma non è detto che questa accortezza venga in concreto utilizzata.

Se gli stessi indirizzi sono impiegati per più transazioni, chiunque sia venuto a conoscenza dell'identità dei relativi utenti potrà riutilizzare le informazioni raccolte, anche inserendole in una strategia di *Big data analytics*. In questa situazione il requisito del consenso praticamente svanisce. Il controllo sull'osservanza delle norme sul trattamento dei dati personali si “disperde” e si complica, in quanto le informazioni sono diffuse nella rete *bitcoin*. Si pone così il rischio della creazione di una sorta di mercato nero e parallelo delle informazioni e dei *Big data*, fuori da ogni supervisione possibile in concreto. Ciò moltiplica i rischi di effetti espropriativi in sostanziale violazione della protezione dei dati personali.

Abstract

The article explores the issue of creditworthiness assessment in the context of peer to peer lending. It analyses the “consensus-based approach” to protect personal data in a Big data environment. Specifically, it highlights the inability of consent to be a suitable protection tool in automated data processing. Accordingly, it supports a “negotiation-based approach” to meet the need to protect the personal data of data subjects better than the mere requirement of consent does.