Pubblicazione Trimestrale
ISSN: 2279-9737

Rivista di Diritto Bancario

dottrina
e giurisprudenza
commentata

Aprile/Giugno
2019

rivista.dirittobancario.it

Rivista di Diritto Bancario
dottrina e giurisprudenza commentata

2019 | 2020

Rivista di Diritto Bancario | dottrina e giurisprudenza commentata

NORME PER LA VALUTAZIONE E LA PUBBLICAZIONE

La Rivista di Diritto Bancario seleziona i contributi oggetto di pubblicazione sulla base delle norme seguenti.

I contributi proposti alla Rivista per la pubblicazione vengono assegnati dal sistema informatico a due valutatori, sorteggiati all'interno di un elenco di ordinari, associati e ricercatori in materie giuridiche, estratti da una lista periodicamente soggetta a rinnovamento.

I contributi sono anonimizzati prima dell'invio ai valutatori. Le schede di valutazione sono inviate agli autori previa anonimizzazione.

Qualora uno o entrambi i valutatori esprimano un parere favorevole alla pubblicazione subordinato all'introduzione di modifiche aggiunte e correzioni, la direzione esecutiva verifica che l'autore abbia apportato le modifiche richieste.

Qualora entrambi i valutatori esprimano parere negativo alla pubblicazione, il contributo viene rifiutato. Qualora solo uno dei valutatori esprima parere negativo alla pubblicazione, il contributo è sottoposto al Comitato Esecutivo, il quale assume la decisione finale in ordine alla pubblicazione previo parere di un componente della Direzione scelto ratione materiae.

2019 | 2020

Rivista di Diritto Bancario
dottrina e giurisprudenza commentata

SEDE DELLA REDAZIONE

Università degli Studi di Trento, Facoltà di Giurisprudenza, via Verdi 53,
(38122) Trento – tel. 0461 283836

2019 | 2020

BRUNELLA RUSSO

Tecnologie digitali e tutela dei dati personali: quali possibili impatti sulla PSD2?

SOMMARIO[*]: 1. La rilevanza giuridica del "dato personale". Dal Codice Privacy al Regolamento europeo GDPR – 2. Big Data e privacy: quali rischi per la tutela e la riservatezza dei dati trattati? – 3. *Segue*. Le nuove frontiere della tutela della *privacy*: il *cloud computing*. – 4. La *blockchain* alla sfida del *Data Protection*. – 5. Privacy e PSD2: necessità di un intervento legislativo di coordinamento.

1. *La rilevanza giuridica del "dato personale". Dal Codice* Privacy *al Regolamento europeo* GDPR

In un'epoca di transazioni mediate sempre più frequentemente ci si affida alle tecniche di digitalizzazione, cui vanno delegate la scelta di beni, di servizi e l'insieme di informazioni richieste, tanto che il concetto di *dato personale* ha finito via via con lo spingersi oltre le previsioni originarie, divenendo a tutti gli effetti un bene di scambio e pertanto difficile da monitorare a causa dell'impossibilità di esercitare un pieno controllo da parte del singolo individuo[1].

[*] Il presente scritto farà parte del volume che accoglierà gli Atti del Convegno in ricordo del Prof. Giuseppe Restuccia dal titolo "*I servizi di pagamento nell'era della digitalizzazione: innovazione tecnologica, esigenze della clientela e regolazione*", svoltosi a Taormina il 15 e 16 febbraio 2018.

[1] La *Foundation for Accountability Information* distingue quattro tipologie di dati personali: *Provided Data*, forniti consapevolmente e volontariamente dagli individui (ad esempio la compilazione di un modulo on line); *Observed Data*, raccolti automaticamente (ad esempio dati raccolti tramite cookie o sistemi di videosorveglianza collegati al riconoscimento facciale); *Derived Data*, prodotti da altri dati in modo relativamente semplice e diretto (ad esempio calcolando la redditività del cliente dal numero di visite a un negozio e agli oggetti acquistati); *Inferred Data*, prodotti utilizzando un metodo analitico complesso per trovare le correlazioni tra i set di dati e utilizzarli per categorizzare o profilare le persone (ad esempio calcolare i punteggi di credito o predire lo stato di salute futuro di un soggetto). Si basano sulle probabilità e possono dunque essere meno "certi" dei dati derivati.

Sono tutti dati personali e tutti devono essere trattati conformemente alla

Questo cambio di paradigma, inteso come cambio di regole e prospettive, nonché di adeguamento del nostro modo di percepire e interpretare la realtà attuale, ha determinato un processo di *spersonalizzazione* del dato stesso[2] imputabile principalmente alla natura di alcune informazioni (o pezzi di informazioni) aggregate e apparentemente anonime che, seppur "spogliate" di alcuni elementi identificativi, sono a disposizione di soggetti pubblici e privati e possono essere comunque ritenute di carattere personale.

Diversamente argomentando si può dire che la quantità di informazioni creata e gestita dai titolari del trattamento consente di poter "sfruttare" i dati per scoprire tendenze, migliorare i risultati aziendali (attraverso la gestione del rischio), ridurre tempi e costi del ciclo e creare contemporaneamente un funzionamento sostenibile e un vantaggio competitivo.

Ciò nonostante, l'utilizzo e la gestione delle informazioni, processate da sistemi informatici, sfuggono spesso ad ogni forma di controllo comportando effetti di alterazione nel modo di produrre e scambiare beni: la diretta conseguenza è quella di profilare in modo granulare miliardi di persone in tempo reale e di prevedere i loro comportamenti, massificandone l'indirizzo non senza preludere a possibili discriminazioni in chiave di marginalizzazione di condotte minoritarie, sul piano dei beni e dei consumi, con la conseguenza di spingere a privilegiare modelli predominanti di business, capaci di fidelizzare sempre maggiore clientela.

Ne consegue che se, da un lato, è impossibile frenare lo sviluppo tecnologico e il flusso delle informazioni, dall'altro, diventa indispensabile che le persone siano a conoscenza di chi è in possesso dei loro dati e dell'utilizzo (spesso generalizzato) che ne viene fatto.

Nel solco di siffatte questioni si colloca il Regolamento europeo

---

normativa.

[2] Mette conto ricordare che il "dato personale" rappresenta, ai sensi dell'art.4 del Codice *Privacy,* quell'informazione riferibile a "individui *identificati* o *identificabili*".

Cfr., Regolamento, art.4, co.1, «[…] *si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*».

sulla protezione dei dati[3] costituendo a livello internazionale l'unico tessuto normativo rispetto ad altri partner strategici dell'Ue, come ad esempio gli Stati Uniti, i quali non si sono conformati pienamente agli obblighi sulla *privacy* preferendo invece un approccio indiretto attraverso la costituzione di accordi *ad hoc*[4]. C'è da dire, per vero, che oltreoceano la definizione di violazione dei dati è una concezione giuridica percepita nei fatti come più attenuata e limitata all'"*accesso o acquisizione non autorizzati*" di una serie ristretta di elementi sensibili[5], senza alcuna riconducibilità del rischio di danno ai "diritti e alle libertà" delle persone; un concetto questo per lo più inesistente nelle leggi americane sulla violazione dei dati.

Parimenti inesistente risulta essere, del resto, il diritto di cancellare dai siti web informazioni vecchie suscettibili di diventare lesive della persona se esposte per periodi eccessivamente lunghi (cd. "diritto all'oblio") avvertito dalla maggior parte dei giuristi statunitensi quale limite alla libertà di espressione, spianando così la strada ai più grandi colossi americani operanti nel settore dei servizi in rete (quali, per citarne alcuni, NSA, Facebook, Google, Microsoft ed Apple) non solo nell'accesso a tutte le comunicazioni elettroniche ma anche nella raccolta ed elaborazione di una moltitudine di informazioni sulla quasi totalità della popolazione esistente al mondo[6].

[3] Il 27 aprile 2016 è entrato in vigore il cd. GDPR (Regolamento Ue 2016/679 del Parlamento europeo e del Consiglio europeo). La sua vigenza – a far data dal 25 maggio 2018 – ha abrogato la precedente Direttiva 95/46/Ce del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Il Regolamento è parte del "Pacchetto Protezione Dati" che è stato presentato dalla Commissione Europea nel gennaio 2012.

[4] Quanto alla posizione degli USA nei confronti del *Data Protection*, sarebbe opportuno che i governi statali americani che commercializzano per l'Europa prendano nota delle azioni richieste dal GDPR. Ad esempio, le agenzie di viaggi e turismo americane che sponsorizzano viaggi per gli europei dovrebbero prepararsi a recepire il GDPR nell'utilizzo dei dati raccolti.

[5] Il GDPR parla più ampiamente di una "*violazione della sicurezza che porta alla distruzione accidentale o illecita, perdita, alterazione, divulgazione non autorizzata o accesso ai dati personali*."

Inoltre a livello europeo si definisce "dati personali" qualsiasi dato che può essere associato direttamente o indirettamente a un individuo vivente (un ambito molto ampio che ora include, ad esempio, gli indirizzi IP).

[6] Per una compiuta analisi sul tema anche con riguardo all'inchiesta condotta sulla

Nel vecchio continente, il problema del rapporto tra diritto all'informazione e tutela della sfera privata, intesa nell'accezione più ristretta di *privacy* e riservatezza è, di contro, sempre stato percepito come importante già dalla Convenzione Europea dei Diritti dell'Uomo (CEDU) del 1950, laddove il diritto alla riservatezza per sé e per la propria famiglia costituiva una prerogativa fondamentale dell'uomo, successivamente ribadita e rafforzata agli inizi degli anni Settanta del Novecento a seguito delle prime grandi banche dati elettroniche, che imposero l'esigenza di norme a tutela della *privacy* e riservatezza dell'individuo nell'ambito della raccolta, elaborazione e diffusione elettronica dei dati personali. Cosicché al diritto alla *privacy* e riservatezza si è andato ad aggiungersi un principio del tutto nuovo riguardante il trattamento dei dati personali[7].

Dunque la spinta a considerare "riservatezza" e "protezione" quali diritti fondamentali, specificamente espressi e costituzionalmente previsti, ha portato il legislatore europeo – a distanza di più di vent'anni dalla sua entrata in vigore – a superare la pregressa normazione (Direttiva 1995/45/Ce) mediante l'emanazione di un nuovo Regolamento (679/2016/Ce)[8]. Quest'ultimo invero riflette integralmente (*ex* artt.5 e 6) i principi previsti dal combinato disposto degli artt. 6 e 7 della Direttiva del 1995, aggiungendo l'ulteriore presupposto dell'*integrità* e della *riservatezza* ed estendendo le condizioni di *liceità* del trattamento dei dati personali[9].

costruzione di un gigantesco *data centre* dell'NSA nel deserto dello Utah per l'immagazzinamento e l'analisi di dati degli utenti ricavati da Internet, si veda D. LYON, *Surveillance, Snowden, and Big Data: Capacities, consequences, critique*, in *Big Data and Society*, 2014.

[7] Seguono la Convenzione di Strasburgo del 1981, adottata in ambito CEDU, in cui si ricostruiva il diritto alla riservatezza ed il diritto alla protezione dei dati personali come un unico diritto fondamentale (la riservatezza) e condizione essenziale di libertà (la protezione dei dati personali). Successivamente si segnalano la Direttiva 95/46/Ce e la Carta europea dei diritti fondamentali (Carta di Nizza).

[8] Si rinvia a U. PAGALLO, *Il diritto nell'età dell'informazione. Il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti*, Giappichelli, 2014, 225 e ss., per una compiuta disamina sulle differenze fra *privacy* informazionale e protezione dei dati personali.

[9] Fra questi principi, quello della "minimizzazione" nel prevedere che i dati personali siano «*adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*»; segue il principio della "limitazione della finalità", per il quale «*i dati personali sono* [...] *raccolti per finalità determinate, esplicite e*

Non vi è dubbio allora che il DGPR diventa misura di attuazione di un equilibrio tra sviluppo tecnologico e dignità umana, consentendo per tale via all'Europa di consolidare il suo ruolo di leader mondiale nell'individuazione di regole moderne per la gestione delle informazioni detenute dai grandi *player* del mondo del *Big Data*, dell'intelligenza artificiale e della robotica[10].

Resta tuttavia una certa disomogeneità normativa di fondo – sulla quale vale la pena soffermarsi – che può (o potrebbe) dare origine a inevitabili contrasti tra il *Data Protection* e le leggi nazionali scritte spesso con non sufficiente attenzione.

Una preliminare questione attiene la sfera d'incidenza della norma in oggetto rispetto alla vecchia regolamentazione del Codice *Privacy*[11].

---

legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità», e quello di "liceità del trattamento", stabilito dall'art.6 par. I del Regolamento. Con specifico riferimento alla *liceità* l'articolo in oggetto ne stabilisce la validità quando «*a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; b) il trattamento è necessario all'esecuzione di un con- tratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore*».

[10] Passi in avanti, in tal senso, sono stati compiuti globalmente e ormai 121 Paesi nel mondo si sono dotati di una normativa sulla protezione dei dati. Oggi il concetto di dato personale si è spinto oltre le previsioni originarie, divenendo a tutti gli effetti un bene di scambio. I dati sono da considerare la merce del presente e del futuro al punto tale che la Commissione europea, in una recente iniziativa normativa sul cd. *digital content*, ha proposto di estendere le garanzie dei consumatori anche agli utenti e agli abbonati di un servizio a cui, anziché il pagamento di una somma in denaro, venga richiesta la cessione dei propri dati, consacrando così il principio che si tratti a tutti gli effetti di una moneta. Questa ipotesi è stata duramente criticata al Garante europeo della protezione dei dati. Allo stesso tempo, la visione dei dati personali quale semplice merce e oggetto di scambio è ormai limitata ed è oggi evidente come essi abbiano finito per acquisire a tutti gli effetti il connotato di potere.

[11] Cfr., D. Lgs. 196/2003 rubricante «*Codice in materia di protezione dei dati personali*».

Con specifico riferimento alla protezione dei diritti della personalità (immagine, identità personale, *privacy*, oblio) il GDPR, pur mantenendo fermi i presupposti della passata legislazione in materia, si colloca su una scala più ampia di valori e pone l'individuo al centro della *policy* individuando un limite alla negoziabilità di questi diritti nel campo dell'informazione. In tal senso, appare indicativo soprattutto il fenomeno dei *Big Data*, nei termini in cui si specificherà, inteso quale concentrazione di informazioni nelle mani di pochi gestori in grado di disporre di algoritmi software e apparecchiature hardware che gestiscono e trattengono una quantità di informazioni illimitate per scopi di diversa natura.

Questo dà la percezione di come le piattaforme digitali siano destinate ad acquisire sempre più il ruolo di filtro della realtà tra ciò che avviene e cosa potrà accadere, prendendo decisioni con effetti importanti sul modo di vivere ed organizzare le relazioni tra i soggetti, non solo sul piano individuale ma soprattutto sociale e collettivo.

2. Big Data *e* privacy*: quali rischi per la tutela e la riservatezza dei dati trattati?*

L'ampiezza di siffatta prospettiva pone dunque un ulteriore interrogativo circa la reale possibilità di proteggere i dati personali, cui discende la necessità di individuare quali di questi in particolare debbano essere tutelati.

E' noto come gli algoritmi (ma anche i software e i potenti processori), applicati nell'analisi dei *Big Data,* permettono di controllare in modo *autonomo* e *automatizzato*[12] banche dati di grandi dimensioni[13]. Non è un caso dunque come proprio quel particolare

[12] Sulle qualità computazionali automatiche e sul livello di autonomia, cfr., M. VAN OTTERLO, *A Machine Learning View on Profiling*, in *Privacy, Due Process and the Computational Turn-Philosophers of Law Meet Philosophers of Technology*, a cura di M. HILDEBRANDT, K. DE VRIES, London, 2013 per il quale «*machine learning is a branch of AI that seeks to develop computer systems that improve their performance automatically with experience*»); B.D. MITTELSTADT ET AL., *The ethics of algorithms: Mapping the debate*, in *Big Data & Society*, 2016, 3 ss.; J.M. BALKIN, *The Three Laws of Robotics in the Age of Big Data*, in 78 *Ohio State Law Journal*, 2017 allorquando afferma «*Collection and processing of data produces ever more data, which in turn, is used by algorithms to improve themselves*».

[13] La "qualità" del dato rilevato comporta spesso taluni costi per i consumatori in

segmento di mercato caratterizzato da transazioni di natura finanziaria più di altri abbia saputo cogliere le opportunità offerte dalla tecnologia informatica[14] e che, allo stesso tempo, ne sia stato maggiormente influenzato.

La possibilità di raccogliere, organizzare ed analizzare grandi insiemi di dati – forniti in modo più o meno diretto e consapevole dal consumatore nell'utilizzo dei diversi canali digitali – con l'obiettivo di facilitare e velocizzare le decisioni strategiche nella gestione del business ha spinto sempre più le banche verso processi di *Big Data analytics*, incrociando e valorizzando dati interni strutturati provenienti dalle transazioni delle carte di pagamento, dagli investimenti finanziari e immobiliari, dall'elenco fidi e affidamenti. Non di meno, l'utilizzo congiunto delle informazioni finanziarie ricavabili dalle altre banche dati (si pensi alla Centrale dei Rischi o al Crif) unite a quelle ricavabili dai *Big Data* hanno certamente favorito un miglior controllo del rischio e il relativo *pricing* ma anche la *compliance*[15] e la capacità di previsione di rimborso, rendendo possibile un servizio personalizzato e centrato sulle reali esigenze del cliente. Questo vale indubbiamente anche per la gestione dei risparmi laddove la raccolta dei dati sulle transazioni di pagamento e la propensione al rischio di un cliente può mettere l'intermediario nelle condizioni di proporre prodotti capaci di rispondere meglio alle esigenze d'investimento.

Inoltre, lo sviluppo dei software e delle infrastrutture informatiche per l'operatività on line ha consentito di elaborare in ambito finanziario sistemi di negoziazione talmente avanzati da essere in grado di

termini di esternalità negative (cd. "*spill-overs*") nei confronti di terzi dal momento che «*la loro curva di indifferenza (o di utilità) è affetta da comportamenti di altri individui, al di fuori dai consueti meccanismi dello scambio di mercato*». In tal senso, il "costo sociale" diventa più o meno elevato per il consumatore a seconda che l'utilizzo di algoritmi provochi danni alla reputazione di alcune categorie tracciandone profili identitari distorti con possibile preclusione dell'accesso a determinati servizi.

[14] Si pensi alle negoziazioni elettroniche di strumenti finanziari, operatività eseguita per il tramite di sistemi e procedure informatiche che, nella prassi, ha preso il nome di "*trading on line*". Sul tema si rinvia alla compiuta analisi di G. BENEDETTO, F. MIGLIOLI, *Trading on-line. Guida operativa all'investimento in rete*, Milano, 2000.

[15] Il controllo sistematico dei dati relativi alle transazioni, unito all'azione di algoritmi atti a individuare comportamenti sospetti nelle operazioni di pagamento, nel prelevamento di contanti o nella negoziazione di titoli, consentono in via prospettica di integrare i processi di *compliance* degli istituti di credito evitando, con il tempo, il riciclaggio di denaro e altri atti illeciti.

realizzare la completa automazione di tutte le fasi dell'attività di *trading*, a partire dalla definizione dei parametri del singolo ordine fino all'esecuzione dello stesso in una *trading venue*. Non secondario il ruolo della regolazione e soprattutto delle Direttive MiFID che attraverso l'obbligo di esecuzione degli ordini dei clienti alle "migliori condizioni praticabili" (cd. *best execution*), da un lato, e tendenza alla frammentazione dei mercati dovuta alla presenza di numerose piattaforme di scambio, dall'altro, hanno creato i presupposti per la diffusione degli algoritmi di negoziazione tra gli intermediari del settore chiamati a garantire costantemente ai propri clienti l'accesso al miglior prezzo di contrattazione presente su ciascun mercato di riferimento.

In questo contesto, ad esempio, il *trading* algoritmico – ponendosi quale attività differente dal tradizionale servizio di esecuzione di ordini per conto dei clienti – costituisce una modalità di negoziazione basata sull'utilizzo di programmi informatici (in genere molto complessi) capaci di raccogliere ed elaborare le informazioni e i dati di mercato in tempo reale[16] e avviare in automatico gli ordini dell'utente (di vendita o di acquisto di strumenti finanziari) sulle diverse piattaforme di negoziazione in cui l'intermediario è abilitato ad operare.

Qui il problema si focalizza sulle correlazioni effettuate dagli algoritmi nei processi decisionali automatizzati che richiamano – con un approccio più funzionale e proattivo – il principio di *accountability,* vale a dire di "responsabilizzazione" dei soggetti preposti al trattamento dei dati in base al quale si richiede di dimostrare la conformità del proprio operato (e delle proprie scelte) agli obblighi imposti dal GDPR quali, in particolare, i requisiti di *liceità*, *equità* e *trasparenza*[17].

In senso più generale, l'acquisizione dei dati sensibili non ha risposto solo ad una logica di mera raccolta ma ha riguardato l'utilizzo degli stessi quale fonte ulteriore di ricavi tramite la rivendita (a vari livelli)

[16] Quando viene svolto a velocità molto elevata prende il nome di trading ad alta frequenza o *high-frequency trading* (HFT).

[17] Attraverso tale principio, appunto, il GDPR indica lo scopo da raggiungere: la garanzia della tutela e protezione effettiva dei dati personali, rimettendo alla loro responsabilità l'individuazione delle misure adeguate da adottare nell'ambito di un vero programma di protezione dei dati (*privacy by design*). Resta fermo l'obbligo di "essere in grado di dimostrare" agli stessi interessati al dato – di fatto una sorta di obbligo di rendicontazione – che le misure adottate siano idonee a garantire il rispetto del Regolamento.

ad altre aziende di servizi[18]; cosa che ha posto, in maniera concreta, una serie di problematiche in tema di garanzie a protezione dei dati personali, mettendo in evidenza così il complicato rapporto tra *Big Data* e *privacy* dal punto di vista giuridico.

Nel solco di siffatte argomentazioni si aprono ulteriori scenari circa le modalità tecnologiche con cui il dato è acquisito[19]: esse infatti risultano di particolare importanza in quanto influenzano in modo determinante il ruolo e il valore delle informazioni raccolte.

Con Internet delle Cose (*Internet of Things*) – considerata l'avanguardia dell'innovazione della Rete – e, come si dirà successivamente, con il *Cloud* ingenti quantità di dati[20] vengono rilevati mediante sensori, capaci di trasformare le rilevazioni effettuate in entità digitali in tempo reale, riferibili a coordinate spazio-temporali ben precise. Il meccanismo è molto semplice: collegare oggetti del mondo reale per scambiare i dati raccolti da questi e perseguire un obiettivo comune[21].

Dunque non è difficile comprendere come, anche in questo caso,

[18] Un esempio può essere dato da alcune delle maggiori banche retail e società emittenti di carte di credito per esempio vendono i dati grezzi relativi ai propri clienti attraverso intermediari specializzati come Cardylitcs. O ancora da colossi come American Express, la quale commercializza studi di marketing basati sui propri dati clienti tramite una sua società specializzata, American Express Business Insights.

[19] I metodi di estrazione dei dati variano a seconda che la produzione del dato avvenga in Rete, in un ambiente *IoT*, ovvero off line, in quest'ultimo caso si pensi ai sondaggi e ai "programmi fedeltà" (*loyalty programs*) dei supermercati. Al riguardo, cfr., FEDERAL TRADE COMMISSION, *Big Data. A Tool for Inclusion or Exclusion? Understanding the Issues*, 2016, 4.

[20] Si tratta di dati geografici, ambientali, o generati da una *smart car*, da uno *smartphone* o ancora mediante tecnologie *wearable* del tipo *smartwatch*.

[21] Si rimanda all'analisi approfondita di Article 29 Data Protection Working Party, *Opinion 8/2014 on the on Recent Developments on the Internet of Things*, 2014; P. HOWARD, *Pax Technica. How the Internet of Things May Set Us Free or Lock Us Up*, New Haven, 2015. Ancora sul tema, cfr., M. PAEZ, M. LA MARCA, *The Internet Of Things: Emerging Legal Issues For Businesses*, in 43 *Northern Kentucky Law Review*, 2016, 31, i quali parlando in termini di superamento della vecchia concezione di Internet così affermano «*In sum, the IoT marks a paradigmatic departure from the Internet technology of previous decades: instead of simply facilitating human interaction through machine-to-machine communications, the IoT allows devices to measure and interact with the physical environment, gather information from that environment, and transmit that information to other devices, people, or environments*»).

risulti abbastanza complessa la gestione sicura del dato personale affidato[22].

In quest'ottica i termini della precedente domanda si invertono ed allora occorre capire se si può collezionare una grande mole di dati garantendo nel contempo il rispetto della *privacy*.

Sulla scorta di quanto già accennato, la detenzione di un enorme patrimonio informativo da parte dei *Big Data* pone inevitabili problemi di tutela e riservatezza dei dati trattati; tuttavia la questione non sta tanto nell'adozione di differenti modalità di applicazione di siffatti principi – giustificata dalle peculiari caratteristiche dei *Big Data* – quanto nella concomitante assenza sia di trasparenza che di effettivo anonimato. Invero, la "quantità" risulta essere predominante rispetto alla loro "qualità", inducendo gli attori di questa "catena del valore" dei dati personali (chi li genera, chi li raccoglie, chi li tratta e chi prende decisioni a seguito di questi trattamenti) verso il loro ri-uso piuttosto che verso la verifica della loro affidabilità.

E' prassi come, una volta inseriti nei sistemi, i dati contenuti negli strumenti di storage dei *Big Data* vengano "persi di vista", comportando inevitabilmente un elevato rischio per l'interessato, in quanto il titolare del trattamento potrebbe utilizzarli per finalità non perseguibili rispetto alle informative e ai consensi raccolti[23].

Inoltre, anche informazioni apparentemente "anonimizzate" possono presentare delle problematiche, posto che attraverso la fusione di diverse banche dati, si può facilmente riuscire a "re-identificare" un

[22] Per le fonti normative in materia, vedasi "*Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU"* - Article 29 Data Protection Working Party, 2014; Resolution Big Data of the 36th International Conference of Data Protection and Privacy Commissioners of 2014; Working Paper on Big Data and Privacy Privacy principles under pressure in the age of Big Data analytics - International Working Group on Data Protection in Telecommunications, 2014; GDPS, Opinion 7/2015 - Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability, 2015.

[23] Il tema delle informative e dei relativi moduli di raccolta di consenso è cruciale in quanto la numerosità delle fonti informative fa sì che le persone interessate abbiano grandi difficoltà nel comprendere come i dati vengano integrati tra loro e trattati. È necessaria dunque una manifestazione espressa, prima del trattamento, da parte degli interessati del consenso all'utilizzo dei propri dati per fini di analisi o di profilazione. Cfr., Garante per la protezione dei dati personali, *Linee guida in materia di trattamento di dati per profilazione on line*, 19 marzo 2015.

interessato (un dato considerato *anonimo* infatti, può essere successivamente attribuito a una determinata persona) anche veicolando informazioni apparentemente anonime.

Ci si chiede allora quale tipo di protezione dei dati personali è veramente possibile.

Un approccio regolamentare potrebbe ricavarsi proprio dal "diritto di portabilità" contenuto all'art.20 del recente GDPR[24], la cui estensibilità è giustificata dal fatto che la nozione di «*dati che riguardano l'interessato*» – e che sono da questi forniti a un titolare per effettuare trattamenti automatizzati sulla base del "consenso" o del "contratto" – potrebbe ricomprendere anche le valutazioni, frutto delle analisi realizzate dal titolare sui dati grezzi, mediante tecniche di *Big Data analytics*.

Per la verità la questione non è del tutto pacifica in quanto non è chiaro se il concetto di dati "forniti"[25] direttamente dall'interessato – e

[24] Cfr., art.20 del GDPR per il quale «*l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti*». In questo senso, il 68° *Considerando* del GDPR promuove lo sviluppo di formati "interoperabili" da parte dei titolari così da consentire la portabilità dei dati, configurando per gli interessati la possibilità non soltanto di ottenere e riutilizzare i dati forniti a un titolare, bensì anche di trasmettere questi dati a un diverso fornitore di servizi. I dati inoltre devono essere forniti «*senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa*». La conservazione, su supporto personale o su cloud privato, consente all'interessato di poter facilmente spostare un contratto di servizi senza dover fornire nuovamente tutti i suoi dati ma semplicemente, chiedendo al vecchio gestore di trasportarli ad un diverso fornitore di servizi. In tal modo le persone possono migrare da un fornitore di servizi ad un altro, impedendo così il formarsi di fenomeni di *lock-in* (blocco all'interno di un servizio).

[25] Il diritto alla portabilità riguarda i dati "forniti" dall'interessato, pertanto è limitato ai soli dati personali (non si applica ai dati anonimi, ma ai dati pseudonimi essendo questi ultimi chiaramente collegati ai dati personali). Secondo l'interpretazione del Gruppo Articolo 29, l'espressione "forniti" dev'essere inteso in senso ampio, per cui il diritto non si limita ai soli dati personali comunicati dall'interessato al titolare del trattamento (ad esempio indirizzo mail), ma si estende anche ai dati personali generati (*observed*) dalle attività dell'interessato (dati di localizzazione, etc.) Non sono compresi, invece, i dati generati dal titolare sulla base dell'analisi dei dati forniti o raccolti dall'interessato (*inferred and derived data*, come ad esempio il "*credit score"*), né ovviamente i dati ottenuti da terze parti.

a questo riferibili – sia circoscritto o circoscrivibile solo a quelli *generati* nell'ambito del rapporto col titolare, o piuttosto "allargato" a quei dati che il titolare ricava usando sistemi di *Data analysis* attraverso cui è possibile catalogarne comportamenti ed attitudini, con evidenti benefici per l'azienda come l'aumento delle vendite, miglior soddisfazione del cliente, maggiore efficienza e, più in generale, aumento della competitività.

Si ripropone in termini concreti il quesito posto all'inizio: quali dati proteggere?

Benché l'orientamento sia proteso a considerare i dati "creati" dal titolare (cd. *Inferred Data*) non oggetto del "diritto di portabilità" per il fatto stesso di non essere forniti direttamente dall'interessato – anche se ipoteticamente a lui riferiti o riferibili – una siffatta circostanza potrebbe dar luogo a qualche difficoltà applicativa nei casi in cui risulti difficile individuarne la provenienza, aprendo a scenari abbastanza ampi connessi ai trattamenti dei dati ricavabili dai *Big Data* e basati sulla *Data analysis.* A tacer del fatto che il titolare del trattamento potrebbe utilizzare i dati raccolti per finalità non perseguibili rispetto alle informative e ai consensi ottenuti riproponendo il discusso tema delle informative e dei relativi moduli di raccolta di consenso[26].

L'argomento, visto in termini più generali, può riguardare, come si accennava prima, un dato considerato «anonimo» poi successivamente attribuito a una determinata persona – attraverso la fusione di diverse banche dati o la generazione di nuove informazioni e spesso di nuovi dati personali – mediante l'utilizzo di algoritmi applicati nell'analisi dei *Big Data.*

Questa avvertita esigenza di tutela del dato, tra l'altro, ha trovato spazio anche nell'ambito delle disposizioni di vigilanza delle autorità europee, le quali hanno richiesto alle imprese di sviluppare *best practices* sull'uso dei Big Data[27] ai fini di una maggiore sicurezza delle informazioni mentre sono archiviate e in transito.

[26] L'adeguatezza ai nuovi principi normativi non consente, in particolare, una descrizione troppo vaga e generica delle finalità del trattamento, determinando pertanto la *nullità* del consenso. Inoltre, la numerosità delle fonti informative fa sì che le persone interessate abbiano grandi difficoltà nel comprendere come i dati vengono integrati tra loro e trattati.

[27] Trattasi di principi generali, come quello della promozione di un trattamento dei consumatori equo**,** trasparente e non discriminatorio.

L'approccio legislativo del GDPR, entrato in vigore lo scorso maggio, cambia sostanzialmente gli scenari: l'utilizzo dei Big Data, secondo quanto stabilito nel nuovo Codice, deve sempre bilanciare gli interessi del titolare/responsabile con quelli degli interessati,28 garantendo, nella raccolta dei dati di grandi dimensioni, prioritariamente il rispetto della privacy.

Per questo è fatto obbligo ai responsabili del trattamento di mettere in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza coerente con il grado di rischio, supportate da procedure valutative circa la loro efficienza ed efficacia al fine di garantire la concreta tutela dei dati trattati (privacy by design e by default).

3. *(Segue). Le nuove frontiere della tutela della* privacy*: il cloud computing*

Stesse riflessioni devono essere fatte in merito ai nuovi modelli di servizio offerto alla clientela, sempre più spesso esternalizzati (cd. *outsourcing*), basati sul ricorso al *cloud computing*[29], la piattaforma in grado di archiviare dati trasferendoli tramite Internet, o un'altra rete, a un sistema di archiviazione esterno gestito da una terza parte nella cui "nuvola" sono conservati i dati. Questi, infatti, non risiedono fisicamente nell'ambiente informatico del fruitore bensì nel server del

[28] Secondo quanto imposto dalla MiFID2 gli algoritmi devono essere presentati alle autorità, di modo che possano essere giudicati idonei ed eventualmente autorizzati. Grazie a questa norma è possibile eventualmente bloccare l'algoritmo in maniera tempestiva.

[29] I maggiori *cloud providers* in Europa hanno aderito al CISPE (*Cloud Infrastructures Services Provider in Europe*) adottando il 26 settembre 2016 un Codice di condotta ed un modello di *compliance* che consente ai clienti di accertare la conformità del proprio venditore d'infrastruttura agli standard di protezione dei dati. Il Codice anticipa in parte l'applicazione dei dettami previsti dal nuovo Regolamento europeo 679/2016 (GDPR) e, infatti, il fornitore di servizi *cloud* dovrà trattare i dati dei clienti in base alle istruzioni da questi impartite. Il *Code of Conduct* vieta poi ai *cloud provider* di effettuare il cd. "*data mining*", ovvero quel processo che permette di estrarre, da grandi quantità di dati, tutta una serie di informazioni "nascoste" per poi poterle utilizzare ai fini di marketing o pubblicità. Le informazioni non possono assolutamente essere vendute a terzi né utilizzate per altri scopi personali. Sul punto, A. MANTELERO, *Processi di Outsourcing Informatico e Cloud Computing*, in *Dir. informaz. Informatica*, 2010, I, 675 e ss.

provider che oltre a fornire servizi di storage dei dati, permette in aggiunta la fruizione di applicativi software cui si può accedere direttamente on line oppure la configurazione di ambiti di sviluppo e programmazione.

La contrattazione *cloud* è standardizzata[30], per cui la scelta dell'utente attiene al servizio che più risponde alle proprie esigenze[31], senza la possibilità di cambiarne nessun aspetto (né durante gli stadi iniziali, né durante l'esecuzione del contratto). Questa che si definisce tecnicamente una situazione di "*take-it-or-leave*"[32] comporta che l'utilizzatore, pur non essendo a conoscenza degli aspetti peculiari della fornitura del servizio, provveda comunque a sottoscrivere il contratto: è il caso, ad esempio, dell'erogazione di un servizio *cloud* cui corrisponde una catena di *sub-provider* della quale l'utente quasi sempre ne ignora l'esistenza[33].

L'evidente sproporzione contrattuale e le asimmetrie informative e

[30] Anche i servizi offerti sono standardizzati e di solito si basano su servizi gestiti da *sub-provider*, tenendo conto dei relativi sub-contratti. Molto comune nel *cloud* è il fenomeno del *sub-processing*. Per un approfondimento cfr., K. HON, C. MILLARD, *Cloud Technologies and Services*, in C. MILLARD, *Cloud Computing Law*, 2013, Oxford, 3; AA.VV., *Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services*, disponibile all'indirizzo *ssrn.com/abstract=1662374*, 1 settembre 2010, 15. Sui contratti di *cloud computing* si veda A.R. POPOLI, *Il contratto di cloud computing: natura giuridica e clausole limitative di responsabilità*, in giustiziacivile.com; G. FAGGIOLI, A. ITALIANO, *I contratti di cloud computing*, Franco Angeli, 2017.

[31] Sinteticamente i modelli di fruizione del *cloud* si distinguono *public*, *community* e *private cloud*, a seconda che il servizio sia messo a disposizione di una pluralità indistinta o omogenea di fruitori, ovvero di singoli soggetti. Sono presenti sul mercato, altresì, modelli misti, o ibridi, che presentano profili di commistione tra i differenti modelli.

[32] Si rinvia sull'argomento a A. CUNNINGHAM, C. REED, *Caveat Consumer? Consumer Protection and Cloud Computing Part 2. The Application of* ex ante *and* ed post *Consumer Protection Law in Cloud*, disponibile all'indirizzo *papers.ssrn.com/sol3/papers.cfm?abstract.id=2212051*, 40-41.

[33] È la natura dell'offerta dei servizi *cloud* a contribuire alla stessa integrazione tra *cloud providers;* quest'ultimo tuttavia, in qualità di responsabile del trattamento, non potrebbe nominare un altro soggetto, a sua volta responsabile del trattamento, senza un'autorizzazione scritta del titolare, ovvero il cliente *cloud*. Un esempio di sub-trattamento di dati, da parte di ulteriori soggetti sub-responsabili del trattamento, è dato dal servizio di storage Dropbox: Dropbbox fornisce SaaS, ma per offrire questo servizio, Dropbox fa affidamento ai server che Amazon gli fornisce come IaaS.

conoscitive riguardante il fruitore richiederebbe, ai fini di un riequilibrio tra le parti, che gli incaricati del trattamento informassero il cliente sulla gestione dell'offerta on demand, descrivendone nel dettaglio la tipologia concessa in sub-appalto, le caratteristiche dei sub-contraenti attuali o potenziali e le garanzie offerte da queste entità al fornitore di servizi di *cloud computing*.

Tuttavia, in quasi tutti i contratti emerge la presenza di una serie di clausole tendenti a limitare la responsabilità del fornitore di siffatto servizio, sia in termini di garanzia nella fornitura sia di esclusione di responsabilità e/o di limiti di risarcibilità per danni da esso causati al fruitore[34]. Esse solitamente si accompagnano nei contratti all'indicazione secondo cui il servizio di *cloud computing* è fornito *"as is*", in altre parole "così com'è", "com'è disponibile", cosa che lo rende, di fatto, privo di alcuna garanzia espressa e implicita, quanto alla qualità e affidabilità del servizio, nonché alla sua sicurezza[35].

Un altro tema che ricorre spesso quando si valutano i rapporti esistenti tra *cloud computing* e GDPR è l'individuazione dei ruoli delle parti. Nella peculiarità del quadro normativo, anche il fornitore di servizi presenta delle caratteristiche proprie, risultando sostanzialmente una figura ibrida con un grado di autonomia incompatibile con il ruolo di esecutore delle istruzioni impartite dal titolare del trattamento[36], che gli consente di svolgere solo una mera attività di custodia delle banche

[34] Si tratta, principalmente di responsabilità per la perdita o la compromissione di dati ospitati nel *cloud service*, ovvero l'oggetto stesso della prestazione fornita. Solo allorquando si verifichino situazioni di inadempimento vi sarebbe una presa di conoscenza da parte del fruitore delle clausole contrattuali, ivi comprese quelle riguardanti l'esclusione di garanzia del servizio offerto, quelle limitative di responsabilità e risarcitorie.

[35] Cfr., F. COLLINA, *Aspetti di sicurezza nel* Cloud Computing, disponibile all'indirizzo *amslaurea.unibo.it/4653/1/ collina_francesca_tesi.pdf*, 38; E. PROSPERETTI, *Gli obblighi di assicurare la custodia e la sicurezza dei dati in un sistema cloud*, in *Trattato di diritto dell'Internet*, di G. Cassano - G. Scorza - G. Vaciago (a cura) Padova, 2012.

[36] La struttura del servizio *cloud* sembra porsi dunque al di là delle definizioni dei poteri e delle responsabilità dei soggetti coinvolti disciplinate dal Codice *Privacy*, laddove il titolare del trattamento dei dati personali è il soggetto cui viene riservato ogni potere decisionale con riguardo alle finalità ed alle modalità del trattamento dei dati; mentre il responsabile rappresenta il soggetto al quale vengono delegate dal titolare stesso alcune particolari operazioni di trattamento, sulla base di specifiche istruzioni.

dati delle società clienti. Questa sfera di autonomia particolarmente ampia – indispensabile per la gestione della "nuvola" – pone in rilievo la necessità di un intervento normativo volto a ridistribuire i pesi di responsabilità tra i diversi player, attraverso l'introduzione di una speciale figura di responsabile, in grado di offrire ai clienti particolari garanzie in termini di affidabilità e di assumersi in prima persona specifici obblighi.

Strettamente connesso al profilo della responsabilità si pone l'analisi degli indiscussi vantaggi – sintetizzabili nella diminuzione dei costi, investimenti iniziali bassi e vincoli di servizio assunti dall'*outsourcer*[37] – ai quali si contrappongono una serie di rischi dovuti all'inevitabile diminuzione di controllo sui dati per quanto riguarda la *business continuity* e in ambito di *Data Protection*[38].

E' di immediata comprensione come la tutela della *privacy* diventi in questo caso delicatissima e di grande importanza per due ordini di motivi, entrambi riconducibili a evidenti lacune di regolamentazione (da affrontare sulla base di parametri contrattuali ben definiti) che tuttavia non appaiono facilmente superabili se rapportati all'ampiezza dei servizi *cloud* e dei modelli di fruizione, i quali rendono estremamente complesso racchiudere tale tecnologia all'interno di una definizione giuridica stringente[39].

[37] I vantaggi risiedono nella possibilità di usufruire delle risorse di cui l'utente necessita in un qualsiasi momento (a patto di avere una connessione Internet funzionante), gratuitamente o a costi estremamente ridotti, senza che queste debbano risiedere nei sistemi informatici dello stesso non essendo necessaria, in molti casi, la previa installazione di software o l'acquisto di particolari infrastrutture hardware. Le soluzioni *cloud* rappresentano una risorsa sfruttabile soprattutto per le piccole e medie imprese. Queste si affidano ad un servizio che presenta standard elevati in termini di efficienza e sicurezza, consentendo un vantaggio competitivo grazie ai costi ridotti e alle caratteristiche di scalabilità dello stesso. Sui profili economici del servizio cfr., AA.VV., *Above the clouds: A Berkley View of Cloud Computing*, in https://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf

[38] Per maggiori approfondimenti in merito Cfr., A. CARDETTA, *IT outsourcing: il cloud computing tra sicurezza e privacy*, disponibile all'indirizzo *https://www.ictsecuritymagazine.com/articoli/it-outsourcing-cloud-computing-sicurezza-privacy/*

[39] Una prima definizione, per quanto ampia, viene data dal National Institute of Standard and Technology secondo cui *«il cloud computing è un ambiente di esecuzione elastico che consente l'accesso via rete e su richiesta ad un insieme condiviso di risorse di calcolo configurabili (ad esempio reti, server, dispositivi di*

La prima ragione va posta in termini di rischio di non adeguata tutela del dato trattato dal momento che il *cloud* è offerto sovente, come si diceva poc'anzi, attraverso l'adozione di servizi "esternalizzati", collocati oltre i confini europei, in Paesi dove mancano livelli adeguati di protezione anche sotto il profilo contrattuale. In questo caso per rendere il trasferimento lecito è necessario che il committente (titolare del trattamento) e l'*outsourcer* (responsabile dello stesso) adottino le misure previste dalla normativa in materia di *privacy* (consenso interessato, *model clauses*, *binding corporate rules*). Inoltre, il committente dovrà acquisire idonee garanzie in merito alle modalità di elaborazione e di conservazione dei dati caricati in *cloud*[40].

Succede spesso che in molti di questi Paesi le leggi sulla sicurezza dei dati sono inapplicabili anche se l'urgenza, in ambito europeo, di affrontare le questioni relative a dati sembra trovare nel GDPR la strada per appianare le differenze legali oltre i confini comunitari creando un ambiente sicuro in cui le organizzazioni private e pubbliche possano utilizzare, acquistare e vendere servizi *cloud*.

La questione dunque attiene sia alla protezione, archiviazione e conservazione del dato sulle memorie dei computer che a quello in transito su reti informatiche più o meno sicure, tenuto conto del fatto che non sempre le aziende valutano attentamente come governare i rischi relativi alla protezione in caso trasferimento fuori dallo Spazio Economico Europeo.

Questo fa ben comprendere come per il fruitore non sia affatto ininfluente il luogo ove risiedono i propri dati personali in quanto la normativa in materia di protezione stabilisce cautele ed obblighi particolarmente penetranti, unitamente alla previsione di sanzioni amministrative e penali nel caso in cui il "trasferimento" – sul quale proprio di recente si è espresso il nuovo Codice *Privacy* a proposito di

memorizzazione, applicazioni e servizi) sotto forma di servizi a vari livelli di granularità. Tali servizi possono essere rapidamente richiesti, forniti e rilasciati con minimo sforzo gestionale da parte dell'utente e minima interazione con il fornitore».

[40] Negli Stati Uniti, i dati possono essere lecitamente trasferiti soltanto verso società che si siano rese conformi al *Privacy Shield*, un accordo stipulato fra la Commissione Europea ed il Governo degli Stati Uniti, nel quale si indicano una serie di requisiti necessari a certificare il rispetto di un adeguato livello di protezione dei dati. Soltanto le imprese statunitensi che rispettino questi requisiti potranno dirsi conformi al *Privacy Shield* e consentire il trasferimento dei dati dall'Europa agli Stati Uniti.

lex domicilii[41] – avvenga oltre l'ambito comunitario. Invero, il semplice spostamento della sede della società e dei *data center* potrebbe consentire al *provider* di sottrarsi ai vincoli previsti in materia di protezione anche laddove i propri servizi fossero diretti principalmente a tale mercato.

Pertanto il fornitore del servizio dovrà procedere ad una mappatura dei luoghi, cioè della rete di data center, in cui i dati della società potrebbero essere ospitati42, al fine di assicurarsi che il loro trasferimento da Paese a Paese avvenga sempre nel rispetto di quelle garanzie minime, in termini di misure di sicurezza, previste dalle disposizioni europee.

A fortiori, la trasparenza della piattaforma del fornitore43 – sia riferibile al momento della instaurazione della relazione contrattuale (con riguardo alla mappa dei data center e alla policy privacy) sia in costanza di rapporto (mediante l'offerta di adeguate garanzie patrimoniali per il caso di eventuali accessi abusivi, sottrazione o perdita di dati) – è estremamente rilevante anche per una ulteriore ragione.

Considerato l'ampio ricorso all'outsourcing e all'hosting dei sistemi, tendenti sempre di più verso la "delocalizzazione" dei dati conservati, risulta di notevole importanza l'operato dell'autorità giudiziaria del Paese ospitante la quale, sul presupposto della sussistenza di leggi interne, potrà dare esecuzione ad ordini di esibizione, di accesso o di sequestro, consentendo all'autorità italiana di superare i limiti di un'azione diretta sui data center se non attraverso complicate rogatorie

[41] Il GDPR introduce la nuova regola basata sul principio di *territorialità* del dato, per cui il trattamento, nell'ambito dell'offerta di beni e servizi, di dati personali di residenti nell'Unione dovrà essere sempre effettuato secondo gli obblighi e le cautele previste dalla normativa europea a prescindere dal fatto che il titolare o il responsabile abbiamo sede al di fuori dell'Unione. La nuova regola determina un significativo cambiamento in relazione soprattutto all'ipotesi cui il *cloud service provider* stabilito al di fuori dell'EU assuma il ruolo di titolare nel trattamento.

[42] Ciò richiede altresì un'accorta individuazione dell'operatore al quale i propri dati saranno affidati, anche attraverso una valutazione della solidità finanziaria e del grado di trasparenza e di sicurezza garantito dalle *policy* aziendali del partner prescelto.

[43] Per una valutazione delle problematiche sottese si rinvia all'interessante articolo disponibile su www.ilsole24ore.com/ art/tecnologie/2011-01-05/protezione-dati-personali-tempo-133601.shtml?uuid=AYbqmNxC

internazionali.

Tornando al delicato problema di legittimità del trasferimento di dati personali all'estero, il quadro normativo ad oggi risultante dal Regolamento, lascia sostanzialmente immutato quanto già tracciato dall'ormai abrogata direttiva 95/46/Ce, prevedendo quale aspetto di rilievo una disciplina di maggiore dettaglio in relazione all'emanazione di decisioni di adeguatezza.

Quanto al concetto di "trasferimento", sebbene non definito dal GDPR, esso trova riscontro in vari punti della disciplina a cominciare dall'art.44 e ss., contenenti le regole cardine per il trasferimento di dati personali in Paesi terzi, nonché in relazione a specifici adempimenti come il registro dei trattamenti, *ex* art.30; i contenuti dell'informativa, *ex* art.13 e la valutazione di impatto, art.35 del *Data Protection*.

In particolare, l'art.44 fissa il principio generale secondo cui un trasferimento di dati personali oggetto di un trattamento – oppure destinati ad esserlo dopo il trasferimento verso un Paese terzo o un'organizzazione internazionale[44] – possa aver luogo, fatte salve altre disposizioni del GDPR, soltanto se l'operatività del titolare e del responsabile sia aderente a determinati meccanismi[45] volti a garantire un principio cardine: quando i dati personali dei cittadini europei vengono trasferiti all'estero, la protezione si sposta con i dati[46].

Il secondo motivo riguardante la tutela della *privacy* è dato dall'interesse crescente delle banche per la tecnologia *cloud* che prelude ad una sua adozione sempre più generalizzata[47].

---

[44] Vanno altresì ricompresi i trasferimenti successivi da un Paese terzo o un'organizzazione internazionale verso un altro Paese terzo o un'altra organizzazione internazionale.

[45] In quest'ottica si rinvia alle condizioni di cui al capo V del GDPR redatte sulla base di regole fissate su criteri di adeguatezza ed adeguate garanzie; nonché su norme vincolanti d'impresa (*Binding Corporate Rules* o "BCR").

[46] Cfr., Digital Single Market: Commission strengthens trust and gives a boost to the data economy, European Commission, January 2017; Digital Single Market: Communication on Exchanging and Protecting Personal Data, January 2017.

[47] Tra gli studi più recenti si cita A. BROWN, *Six reasons why cloud computing will transform the way banks serve clients – and the five hurdles to overcome*, in *Banking Technology on line*, 28 luglio 2014, disponibile all'indirizzo http://www.bankingtech.com/236322/six-reasons-why-cloud-computing-will-transform-the-way-banks-serve-clients-and-the-five-hurdles-to-overcome/; P. CROSMAN, *Banks Pushed Toward Cloud Computing by Cost Pressures*, in *Americanbanker.com*, 10 marzo 2014. Ed ancora per le sperimentazioni bancarie

Il *cloud* infatti offre alle banche la capacità di rispondere rapidamente alle mutevoli esigenze del mercato, della clientela e delle tecnologiche, consentendo ad esse di sviluppare sistemi idonei a fornire informazioni puntuali sui clienti e prendere decisioni migliori a loro nome (i servizi potrebbero diventare così più personalizzati).

Anche qui la sicurezza dei dati viene posta in primo piano. Poiché le grandi banche forniscono servizi *cloud* da diversi *provider* ciò comporta, per un verso, la gestione congiunta di più sistemi di sicurezza e, per l'altro, – dal momento che l'*interoperabilità* è d'obbligo in ambiente *cloud* – la necessità di garantire che tutte le parti della propria attività possano comunicare tra loro e, ove opportuno, con i clienti.

E' superfluo dire che la sicurezza dei dati passa da una verifica preliminare dell'"affidabilità" del *cloud provider*, il quale insieme al requisito della "serietà" devono essere declinati non solo in termini di capacità di comprovato rispetto dei livelli di servizio garantiti e degli impegni contrattuali, ma anche in termini di esperienza e presenza sul mercato[48].

Secondo quanto stabilito dal Regolamento il *cloud service provider* dovrà sviluppare, in modo coordinato con il titolare del servizio, e garantire nel tempo tutte le misure di sicurezza tecniche e organizzative adeguate a mantenere al sicuro i dati di cui è in possesso[49].

4. *La blockchain alla sfida del Data Protection*

La preoccupazione crescente da parte degli utenti circa la perdita di controllo sui propri dati e informazioni personali che viaggiano su Internet pone un'ultima questione, questa volta sul fronte dei servizi di

verso siffatta tecnologia, *Is cloud computing almost too good to be true for banks?*, rinvenibile alla pagina www.flinders.edu.au/its/essentials/its-security/cloud-security-guidance/cloud-security-guidance_home.cfm; T. GROENFELDT, *Some Banks Are Heading To The Cloud - More Are Planning To*, in *Forbes on- line*, 26 giugno 2014.

[48] Un elemento per misurare la capacità di rispettare effettivamente termini e condizioni può essere il riferimento a rapporti di *audit* sviluppati da terzi soggetti indipendenti e alla presenza di certificazioni. Elementi ulteriori che rafforzano l'affidabilità economica possono essere costituiti da adeguate polizze assicurative del fornitore *cloud*.

[49] Tali misure di sicurezza devono essere applicate a tutti i sistemi che siano sotto il controllo del *cloud provider* (*data centre, network, server* nonché tutti gli *host software*).

pagamento laddove la diffusione non solo delle criptovalute ma anche di altri strumenti di pagamento innovativi ha richiesto – a motivo anche dell'espandersi degli attacchi della nuova criminalità informatica – una ferrea regolamentazione giuridica ed organizzativa riservata agli intermediari e traducibile sostanzialmente in specifici obblighi di precauzione[50] e misure di sicurezza intraprese ai fini della conservazione e del trattamento dei dati personali.

Occorre rammentare, ma si dirà meglio dopo, come il duplice obiettivo della PSD2 è stato quello di aumentare la concorrenza, il "*fair play*" e l'innovazione nel settore dei pagamenti, ma anche di dare un impulso significativo alla garanzia di adeguate misure di salvaguardia della clientela[51].

Orbene, il *Regulatory Technical Standard* (RTS) adottato dalla Commissione europea nel novembre 2017 è stato progettato proprio allo scopo di definire le norme tecniche di regolamentazione: il documento infatti delinea i protocolli che devono essere implementati per proteggere la sicurezza e la riservatezza delle informazioni dei clienti e per garantire comunicazioni sicure e aperte durante tutto il processo di pagamento e, non meno importante, per monitorare il trattamento di rilevanti quantità e tipi di dati personali, cosa che comunque non esime ma anzi impone al regolatore una rilettura delle RTS[52] alla luce delle prescrizioni della nuova *Data Protection.*

[50] Primo fra tutti l'obbligo di garantire l'inaccessibilità dei dispositivi di pagamento a soggetti non autorizzati (ossia diversi dal loro legittimo titolare), ai sensi dell'art. 8, co. 1, lett. *a)* del D. Lgs. 11/2010.

[51] Un obiettivo importante è stato quello di garantire una forte autenticazione del cliente. Gli standard tecnici di regolamentazione (RTS) specificano vari elementi per garantire l'autenticazione del cliente forte come richiesto in PSD2. La comunicazione sicura tra banche, istituzioni finanziarie, fornitori di servizi di informazioni di pagamento e di conto (AISP e PISPS) è forse il requisito più importante per PSD2 che è coperto da RTS che definisce in dettaglio gli elementi necessari per una forte autenticazione del cliente. Gli standard impongono alle istituzioni finanziarie di definire KPI (*Key Performance Indicators*) trasparenti e obiettivi di livello di servizio per la loro interfaccia di pagamento.

[52] Il *Regulatory Technical Standard* (RTS) prevede alcuni principi fondamentali, tra cui il monitoraggio e la profilazione del comportamento degli utenti dei servizi di pagamenti allo scopo di mitigare i rischi di frodi ed in generale di uso illecito dei servizi. In base al livello di rischio ipotizzato, l'ammontare e la ricorrenza della transazione, il canale utilizzato, si dovrà ricorrere a sistemi di *Strong Customer Autentication* (SCA), con accertamento dell'identità attraverso due o più strumenti di

Il confronto invero si rende necessario tenuto conto dell'ampia casistica approntata dal GDPR in merito alla definizione di dati personali, lasciando desumere come molti di questi – utilizzati ai fini delle RTS – sono considerati appunto "*dati personali*" (incluso l'indirizzo IP associato al mezzo con il quale un utente interagisce con un servizio di pagamento)[53] così come quasi tutti i trattamenti previsti dalle RTS comportano le necessità di conformarsi a specifiche prescrizioni del Regolamento per non incorrere nelle consistenti sanzioni amministrative (fino a 20 milioni di euro o 4% del fatturato se superiore).

Il binomio criptovalute-blockchain – tecnologia alla base delle transazioni finanziarie ma che nel giro di un decennio si estenderà rapidamente a tutta una serie di altre attività e servizi – apre un ulteriore scenario nella valutazione della capacità di adattamento alle regole sulla protezione dei dati personali introdotte dal recente Regolamento[54].

Anche qui è d'obbligo la domanda: le blockchain trattano dati personali e se sì quali in particolare.

---

autenticazione. Inoltre è previsto che siano adottate misure volte a garantire la riservatezza e l'integrità delle credenziali degli utenti; infine che le comunicazioni tra banche, TPP, ordinanti e beneficiari, siano basate su standard aperti, comuni e sicuri. Per quanto riguarda i *Third Party Players* (AISP, PISP e CISP), questi avranno accesso alle sole informazioni utili all'erogazione dei propri servizi, sulla base di un mandato per uno specifico conto o di una richiesta individuale. Dovranno identificarsi per interagire con le banche e potranno scambiare dati solo tramite soluzioni sicure e comunicazioni cifrate. In questo senso i *trust services* avranno un ruolo importante entro i nuovi scenari creati dalla PSD2.

[53] Si rinvia al noto caso Breyer sul quale si è espressa la Corte di Giustizia dell'Unione Europea con sentenza del 19 ottobre 2016, causa C-582/14, con nota di A. BERTI SUMAN, *Indirizzi IP dinamici e cybersicurezza: la conservazione dei "dati personali" degli utenti da parte dell'*Internet Provider *nel caso Breyer*, in *Orientamenti della Corte di Giustizia dell'Unione Europea in materia di responsabilità civile*, a cura di Alpa G., Conte G., Torino, 2018, 119 e ss.

[54] A riguardo si richiama il report **"***Blockchain Innovation Europe***"** del 21 agosto 2018 redatto dall'European Union Blockchain Observatory and Forum che sottolinea come la tecnologia blockchain sia in realtà ancora immatura e che probabilmente, evolvendo, sarà più semplice conciliarla con quanto previsto dal Regolamento. Sono in elaborazione, infatti, nuove tecniche finalizzate ad una maggiore protezione dei dati personali che eliminano la possibilità di risalire al singolo. Questo dovrebbe persuadere il legislatore a far operare tutte le eccezioni previste dal GDPR in modo da evitare che un'interpretazione troppo restrittiva possa comportare un freno all'innovazione.

Iniziamo col dire che la blockchain contrasta con la *Data Protection* su due aspetti che, a ben guardare, rappresentano gli elementi fondanti della tecnologia in oggetto: la *pubblicità* dei dati (quelli inseriti nelle blockchain sono pubblici e accessibili da chiunque partecipi alla catena) e la loro durata temporale (essi infatti sono conservati illimitatamente a tutela dell'intero registro distribuito), elementi insieme che consentono di creare un archivio "decentralizzato" ed immutabile[55].

I dubbi sollevati circa l'applicabilità delle disposizioni contenute nel Regolamento *privacy* riguardano principalmente il fatto che esso nasce con il fine di disciplinare i cosiddetti *data silos* ovvero i casi di trattamento "centralizzato" di dati personali; mentre la tecnologia blockchain si basa fondamentalmente sulla "decentralizzazione" e distribuzione delle operazioni di computo su un network.

Benché l'analisi di tale tecnica giustificherebbe un approfondimento decisamente più ampio di questo, è necessario tuttavia sottolineare la difficoltà di conciliare profili più squisitamente privatistici del *Data Protection* con un sistema di blocchi all'interno del quale confluiscono enormi quantità di dati e informazioni, non più cancellabili né modificabili[56], cosa che sin da subito appare del tutto confliggere con quanto stabilito all'art.17 del Regolamento secondo cui l'interessato ha diritto ad ottenere la cancellazione dei propri dati personali quando la finalità per cui sono stati raccolti è venuta meno; in altre parole, quando

[55] Partendo proprio dalla caratteristica dell'"immutabilità" tipica della blockchain che può ritenersi non rispettato il cd. "*diritto all'oblio*" riconosciuto nel GDPR a tutti gli interessati in quanto manca del tutto sia il diritto alla cancellazione dei dati, da parte del titolare del trattamento, sia l'obbligo di questi – qualora abbia comunicato i dati a terzi – di cancellarli ed informare gli altri titolari della richiesta dell'interessato di eliminare qualsiasi link, copia o riproduzione dei suoi dati personali.

[56] La tecnologia blockchain utilizza una serie di dati che rientrerebbero nella definizione data dall'art.4 del Regolamento UE n.679/2016. Possono essere inseriti, anche se rappresentano un utilizzo anomalo della blockchain, documenti contenenti dati personali ed è, inoltre, possibile che siano registrate informazioni cifrate. Il file contenente i dati personali rimane *off chain*, mentre l'informazione cifrata viene registrata sulla blockchain (rendendo tracciabile la transazione). Le blockchain agiscono tramite l'utilizzo di chiavi asimmetriche da parte degli utenti: chi partecipa al network non conosce la chiave privata degli altri interlocutori, ma solamente la chiave pubblica che attraverso il *Public Key Hash* definisce gli identificativi dei destinatari delle transazioni. Nel primo caso sicuramente si rientra nella fattispecie del trattamento dati personali come delineato dal GDPR. Negli altri due casi la questione è più complessa.

è stato revocato il consenso che ne autorizza il trattamento e in una serie di altri casi (cd. "diritto all'oblio" o *right to be forgotten*)[57].

Guardando da un'altra angolazione – ed in linea di principio – attraverso la blockchain un utente è sempre in grado di controllare i propri dati personali, anzi, è l'unico a sapere a quali informazioni corrisponde la propria chiave pubblica, secondo un principio di "disaccoppiamento" dei dati dall'entità individuale per essere attribuito ad uno pseudonimo[58]. Questo consente di tracciare lungo tutta la catena distribuita dove e come sono usate le informazioni oggetto di una transazione: ogni dato inserito in una blockchain è necessario per mantenere la "catena" di transazioni relative alla medesima "informazione digitale", caratterizzando nello specifico siffatta tecnologia rispetto alle altre.

Inoltre, le ricadute delle disposizioni normative della V Direttiva antiriclaggio[59], hanno estenso gli obblighi di riconoscimento anche in capo ai soggetti che offrono servizi di *wallet provider* cosicché la chiave pubblica – attraverso la quale vengono sottoscritte le transazioni sulla blockchain – costituisce sempre più un dato personale in quanto associata o associabile ad una persona fisica determinata.

Ora, vista dalla prospettiva della protezione dei dati personali degli utenti, tale tecnologia adotta sicuramente un approccio *privacy by design* secondo quanto stabilito dall'art.25 del Regolamento – mediante il quale si riducono al minimo l'elaborazione e la confidenzialità dei dati fin dalla progettazione del sistema di trattamento – puntando sui suoi aspetti di maggiore forza, ovvero le tecniche della crittografia e, come già accennato, della pseudonimizzazione[60], elemento di grande

[57] Vale la pena menzionare anche il cd. "diritto di rettifica", previsto dall'art.16 del GDPR. L'interessato ha diritto a pretendere dal titolare la correzione dei propri dati, quando essi non sono veritieri o aggiornati.

[58] Solitamente la chiave è cifrata di modo che dalla singola transazione non è possibile risalire a colui che è titolare di detta chiave, ma l'eventuale riutilizzo di quest'ultima in altre transazioni (anche in congiunzione con altre chiavi pubbliche) consentirebbe di "linkarla" ad un utente specifico potendo quindi risalire alla sua identità. Oltretutto, l'eventuale disponibilità di log di accesso con conservazione di indirizzi IP renderebbe facilmente individuabile il titolare della chiave pubblica della transazione.

[59] Cfr., Direttiva (UE) 2018/843.

[60] Se ne ha contezza nell'ambito dello stesso art.32 del Regolamento *Data Protection*, il quale prevedere tali misure come adeguate a garantire la sicurezza del

novità rispetto al precedente Codice *Privacy*.

In particolare quest'ultima tecnica consiste nel disaccoppiare i dati dall'identità individuale attraverso uno schema del tutto simile a quello contenuto nella funzione di hash utilizzata dalla blockchain[61], rendendo di fatto applicabile il GDPR[62]: l'hashing infatti è una tecnica di pseudonimizzazione (e non di anonimizzazione) idonea a registrare dati personali riferiti ad individui (anche solo in potenza) identificabili.

Quanto alla tecnica della crittografia (firme digitali, crittografia dei dati, marcatura temporale) invece essa consente che un dato crittografato, all'interno della blockchain, sia leggibile soltanto da chi possiede la chiave per decifrarlo, rappresentando, in questo senso, una misura di sicurezza adeguata a minimizzare il rischio.

---

trattamento dai dati personali. Mentre l'art.4, co.1, n.5 definisce la tecnica di pseudonimizzazione come «*il trattamento di dati personali in modo tale che (...) non possano più essere attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile*». Si veda anche, Raccomandazione n.3/97, *Anonymity on Internet* (WP6), dell'*Article 29 Working Party*, e Parere n. 5/2014, *Anonymisation Techniques* (WP216). L'introduzione del concetto di *pseudonimizzazione* rappresenta una significativa opportunità per le imprese in quanto consente di definire nuove strategie e modelli di business basati sull'analisi/correlazione della grande mole di dati disponibili in azienda (cd. *Big Data Analysis*), limitando il rischio per la *privacy* degli interessati.

[61] E' noto che la funzione di hash è irreversibile, nel senso che non è possibile risalire dalla stringa di caratteri generati tramite la funzione al contenuto del documento cui la stessa è stata applicata, ma al contempo consente di verificare se un determinato contenuto digitale sia identico a quello alla quale è stata applicata originariamente la funzione. Pertanto, in questo senso, anche l'hash è un dato personale. Cfr., Working Party 29, nella propria *Opinion* n.5/2014 del 10/4/2014 ha chiarito che l'hashing, così come altre tecnologie, rientra tra le tecniche di pseudonimizzazione (e non di anonimizzazione), in quanto risulterebbero comunque collegabili i dati contenuti nell'hash a dati personali esterni allo stesso e, soprattutto, facilmente ricostruibili attraverso un attacco "brute force". La soluzione a tale ultimo problema potrebbe essere risolto cifrando i dati prima di attestarli sulla blockchain e poi applicando sui dati cifrati la relativa funzione di hash. In questo modo il dato diverrebbe inintelligibile e sarebbe messo al sicuro anche contro attacchi "brute force", garantendo così l'accesso al dato stesso solo al soggetto titolare della componente privata della chiave di cifratura.

[62] A questa conclusione perviene anche la Risoluzione del Parlamento UE P8_TA-PROV(2018)0373.

Tuttavia, non può trascurarsi il fatto che, sebbene indecifrabile, il dato personale criptato continua ad esistere, lasciando aperto la questione sulla sua potenziale decifrabilità una volta distrutta la chiave privata. È stato dimostrato infatti che, mediante l'aggregazione dei dati di diverso genere, pur "de-identificati" (tra cui i meta-dati dei messaggi crittografati), si può facilmente "re-identificare" la persona in questione[63].

Indubbiamente il testo del Regolamento europeo sui dati personali costituisce un approccio verso una nuova consapevolezza del valore dei dati nella moderna società tecnologica, in un'ottica di trasparenza e di *accountability* dei soggetti preposti al trattamento[64]. Ma in una blockchain, chi svolge questo ruolo?

L'applicabilità del Regolamento alla tecnologia blockchain passa attraverso la valutazione del numero degli attori che all'interno della rete possono prendere o meno decisioni. Così nel caso della blockchain *permissioned* (o chiusa) si viene a configurare una contitolarità del trattamento in modo da identificare i ruoli e le responsabilità nel rispetto del GDPR: questa è l'ipotesi sostanzialmente del soggetto (persona fisica o ente) che partecipa ad un consorzio che gestisce una blockchain chiusa (o il caso di un consorzio che offre determinati servizi ai suoi utenti finali registrando i dati sulla blockchain chiusa).

L'individuazione di ruoli è più complessa nei casi di blockchain *permissionless* (ad esempio, Bitcoin o Ehereum) caratterizzate dal fatto di essere "*decentralizzate*" e aperte: essa infatti opera in senso orizzontalmente, non richiedendo la necessità di un organismo di controllo.

Inoltre, dal momento che non può definirsi un software ma un

[63] Cfr., L. HARDESTY, *How hard is it to 'de-anonymize' cellphone data?*, in *MIT News*, 27 marzo 2013 disponibile all'indirizzo http://news.mit.edu/2013/how-hard-it-de-anonymize-cellphone-data; DE MONTJOYE ET AL., *Unique in the Crowd: The privacy bounds of human mobility*, in 3 *Scientific Reports*, 2013, a proposito di uno studio condotto dall'MIT e dell'Università Cattolica di Lovanio (Belgio) che procedendo ad un'analisi dei dati sull'utilizzo del cellulare di un milione e mezzo di persone residenti in un piccolo borgo europeo (acquisiti nell'arco di tempo di 15 mesi) è emerso che erano sufficienti per l'identificazione precisa del 95% di loro.

[64] L'art.4 del Regolamento europeo definisce il responsabile del trattamento come «*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, da solo o insieme ad altri, determina le finalità e i mezzi del trattamento*». È inoltre legalmente responsabile del trattamento dei dati.

protocollo, questa circostanza rimarca ancor di più il mancato carattere di responsabilità dei soggetti nel trattamento dei dati.

Gli stessi miners (che portano potenza computazionale), gli sviluppatori e gli utenti non possono essere identificati come responsabili del trattamento, in quanto, i primi, si limitano a svolgere un mero ruolo tecnico, mentre di solito gli sviluppatori agiscono sotto pseudonimo e sono muniti di licenza libera. Anche la stessa soluzione di considerare ciascun nodo della blockchain come titolare non è sembrata idonea ad individuare il soggetto preposto al trattamento.

Il rischio è dunque quello di compromettere anche la possibilità di introdurre la figura del *Data Protection Officer* (DPO) – come del resto impone lo stesso GDPR – deputata ad assistere chi controlla o gestisce i dati al fine di verificare l'osservanza del Regolamento.

A queste considerazioni si aggiungono altresì le problematiche di applicazione dei principi individuati dal GDPR, quali la *liceità* del trattamento secondo un'opportuna base giuridica, gli obblighi in materia di sicurezza, la disciplina del trasferimento dei dati all'estero (essendo la natura di questi network quella di assumere dimensioni internazionali), nonché le questioni relativa al diritto di ottenere la rettifica o la cancellazione dei dati inesatti che, come si è detto, mal si concilia con il carattere tecnico di potenziale immutabilità dei dati all'interno delle blockchain, con le già evidenziate conseguenze sul diritto all'oblio.

5. *Privacy e PSD2: necessità di un intervento legislativo di coordinamento*

Il Regolamento generale in oggetto e la Direttiva 2015/2366 sono certamente la prova di come il legislatore abbia cercato di contemperare l'utilizzo esteso della tecnologia, da parte degli intermediari, e il bisogno di accedere – sempre più velocemente e più facilmente – ai servizi digitali da parte dei consumatori, per trarne benefici e garanzie in termini di tutela[65].

[65] In questo binomio di servizi e necessità, tra l'intermediario e il consumatore si colloca inoltre la vigilanza prudenziale di Banca d'Italia attraverso la Circolare n. 285/2013, che esalta il sistema informativo bancario (inclusivo delle risorse tecnologiche – hardware, software, dati, documenti elettronici, reti telematiche – e delle risorse umane dedicate alla loro amministrazione) come uno strumento di

Tuttavia nel perseguire il suo obiettivo uniformatore, finalizzato ad una disciplina europea in materia dei dati personali, il regolatore sembra però non aver fatto i conti con sé stesso, dal momento che la *Data Protection* presenta alcuni punti di attrito con la costruzione giuridica della nuova direttiva *Payment Service Directive.*

Principio cardine su cui poggia la PSD2[66] (recepita con Legge del 12 agosto 2016 n.170) è l'attivazione di un unico standard europeo al fine di favorire lo sviluppo delle transazioni di pagamento digitali: la finalità è quella di implementare un mercato unico integrato – la *Digital Economy* in tutta l'area Ue – dove vigono regole uniformi in un'ottica di rafforzamento della sicurezza del sistema sia mediante un elevato livello di concorrenza tra soggetti che di trasparenza nei confronti dei consumatori.

L'affermarsi del digitale ha certamente imposto la nascita di nuove figure, o per meglio dire di nuovi intermediari, sul mercato; la direttiva dunque introduce per tutti i soggetti che utilizzano ad esempio un conto corrente on line, la possibilità di compiere operazioni di pagamento o di accedere a rendicontazione bancaria attraverso i *Third Party Provider* i quali, previa autorizzazione, potranno eseguire operazioni sui conti correnti dei clienti finali, ponendosi appunto come nuovi interlocutori tra le banche e i loro correntisti[67].

La domanda che andrebbe formulata in questo caso è quale sarà l'impatto diretto della *Data Protection* sui *Third Party Provider,* sulle App o sulle categorie di App di tali *provider* che sulla profilazione degli

primaria importanza per il conseguimento degli obiettivi strategici e operativi degli intermediari, in considerazione della criticità dei processi aziendali che dipendono da esso.

[66] Cfr., 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.

[67] Brevemente per inquadrarli i TPP vengono suddivisi in *Account Information Services Providers* (AISP) che si collegano a conti correnti bancari al fine di recuperare informazioni (ad esempio gli utenti potranno usare gli AISP per avere un corretta visione di insieme della propria situazione finanziaria) e in *Payment Initiation Service Provider* (PISP), i quali invece permettono di effettuare una transazione di pagamento dal proprio conto verso un altro soggetto mediante un software che, di fatto, si comporta come un ponte tra i due account bypassando l'utilizzo della carta di credito.

utenti stanno cercando di costruire il proprio vantaggio competitivo.

Ora dal momento che la direttiva PSD2 non sembra aver fatto nessuna menzione al Regolamento generale in materia di protezione – e ciò lo si deduce dal tenore letterale dell'art. 94 – è corretto ritenere, rispondendo al quesito di cui sopra, come una siffatta regolamentazione esuli dal campo di applicazione della direttiva sui sistemi di pagamento. Cosa per la verità alquanto singolare, se posta in questi termini, tenuto conto del fatto che il servizio reso dai *Third Party Provider* presuppone la comunicazione, da parte della banca, di tutta una serie di dati personali dei clienti finali con quel che comporta in termini di *compliance* al Regolamento Europeo.

Stesse perplessità sorgono in relazione al diritto alla portabilità dei dati dal titolare originario ad un nuovo titolare (si pensi, ad esempio, il trasferimento di un *account* personale da una piattaforma on line ad un'altra) e conseguentemente al diritto alla *interoperabilità* previsti dall'art.20 della GDPR.

Ci si chiede allora quale comportamento dovrà tenere la banca qualora la richiesta dei dati del cliente in suo possesso provenga da una terza parte che non è in grado ipoteticamente di garantire le misure necessarie per la tutela della *privacy*.

Ancora una volta sembra non evidenziarsi alcuna correlazione con il principio di responsabilità del titolare dei dati (cd. *accountability*) e di sicurezza – in termini di protezione dell'interessato – che invece costituisce il tratto caratterizzante il quadro giuridico europeo istituito dal Regolamento. A fare le spese delle antinomie tra GDPR, da un lato, e Direttiva PSD2, dall'altro, sembrano soprattutto le banche europee, le quali secondo quanto previsto da quest'ultima normativa, dovranno soddisfare le richieste effettuate tramite appunto un *provider* di terze parti autorizzato a condividere i dati dei propri clienti[68] di cui esse sono responsabili.

Resta da capire se la banca, alla luce delle disposizioni contenute nella PSD2, potrà sottrarsi a tale obbligo allorquando non sia sicura dell'affidabilità di un determinato TPP, venendosi così a configurare la singolare situazione in cui l'ente creditizio per ottemperare a quanto

[68] Ovviamente la questione si pone nel caso in cui potrebbe essere attribuito ad un *Third Party Provider* un'eventuale perdita di dati o allorquando sia esso stesso vittima di un attacco informatico.

richiesto dal GDPR in materia di trattamento dei dati personali si esporrebbe alla comminazione delle sanzioni previste dalla PSD2, con l'unico vantaggio (forse) di pene meno onerose.

Sarebbe dunque auspicabile – come da più parti sostenuto – che il legislatore intervenisse in tempi brevi a eliminare gli attuali problemi di coordinamento normativo considerate le inevitabili ricadute.

In un'ottica di più ampio respiro occorre ricordare come la tutela dei dati personali non è più un tema esclusivamente legale ma diventa un argomento che riguarda l'organizzazione, la gestione dei processi produttivi e distributivi, la struttura degli strumenti informatici messi a disposizione degli utenti, in una parola, le tecnologie sempre più imperanti.

Questo si ritiene debba essere la sfera d'azione entro cui dovrà muoversi nei prossimi mesi il Regolamento *Data Protection* il quale, pur nella necessità di un assestamento e adeguamento nei vari ordinamenti europei, sembra costituire un efficace freno ad un processo tecnologico che, in un'era di galoppante *digitalizzazione,* potrebbe finire con il prendere il sopravvento e determinare le decisioni degli individui invece di limitarsi ad accompagnarle e sostenerle, come sarebbe più giusto attendersi.