ABI - Inaugurazione Corso di alta formazione

Fintech e Diritto

L'intervento Antonello Soro - Presidente dell'Autorità Garante per la protezione dei dati personali

Il fenomeno Fin Tech fa parte dei profondi mutamenti economici e sociali, negli stili di vita, nelle preferenze e nei comportamenti delle persone, delle imprese e delle organizzazioni determinato dalla rivoluzione digitale.

Una rivoluzione a lungo sottostimata dai diversi decisori politici del pianeta e affidata per un lungo periodo all'esclusivo governo dei gestori delle piattaforme, fondato su un uso intensivo dei dati, una velocità inarrestabile nella circolazione delle informazioni insieme alla straordinaria capacità di ricerca, elaborazione e stoccaggio delle stesse.

E paradossalmente si è sviluppata un'economia fondata sui dati in un regime di scarsa attenzione alla protezione dei dati.

Tra le tecnologie più "caratterizzanti" il fenomeno Fin Tech assumono particolare ruolo i Big Data, le applicazioni dell'intelligenza artificiale, il machine learning nonché le tecnologie basate sulla Blockchain.

L'impiego delle tecnologie consente di realizzare nuove modalità operative per lo svolgimento delle tradizionali attività (dai servizi di pagamento a quelli d'investimento e a quelli in ambito assicurativo), di disegnare nuovi servizi, oppure di sviluppare attività tecnologiche innovative, strumentali all'erogazione degli stessi

Altro fattore non meno importante che favorisce lo sviluppo globale del FinTech, è il cambiamento nella domanda di servizi finanziari, creditizi e assicurativi da parte delle nuove generazioni, determinata non solo da bisogni ed esigenze concrete, ma anche dalla maggiore "propensione" tecnologica, dalla semplicità ed accessibilità dei servizi e dalla fiducia riposta nelle grandi imprese del digitale.

Alle tradizionali attività e servizi in ambito finanziario, creditizio e assicurativo, riconducibili ad un unico intermediario vigilato, operante su mercati regolamentati, si

affiancano, così, nuovi mercati telematici che diventano campi di sperimentazione e competizione per nuovi operatori specializzati, i quali sono, per definizione, in grado di superare i confini nazionali e di operare a livello globale, per l'offerta di beni e servizi alla clientela in contesti geografici in cui non sono stabiliti.

Nuove imprese e fra queste anche i Big Tech sono i protagonisti di questa trasformazione.

In particolare, questi ultimi, grazie alla disponibilità della gigantesca potenza di calcolo e al patrimonio informativo accumulato, possono contare su un considerevole vantaggio competitivo, rispetto agli intermediari tradizionali, diventandone i concorrenti più aggressivi e temibili. Perché sono i più forti detentori del potere di profilazione.

La profilazione rappresenta uno dei cardini principali su cui ruota l'economia digitale e naturalmente costituisce una risorsa strategica essenziale per lo svolgimento delle attività del settore FinTech.

Per un verso le tecniche di Big Data Analytics possono facilitare una maggiore personalizzazione dei prodotti e dei servizi, favorendo una stima più accurata dei profili di rischio e delle esigenze dei consumatori.

Dall'altro lato, tuttavia, le medesime tecniche possono avere effetti negativi sulla disponibilità e la convenienza economica degli stessi prodotti e servizi, in particolare, per alcuni consumatori con profili di rischio più elevati o per i quali sono disponibili solo poche informazioni a causa della loro limitata attività online.

Inoltre, le previsioni basate sui Big Data possono essere errate, a causa di imprecisioni o preconcetti nella generazione degli algoritmi.

L'analisi di grandi quantità di dati fa emergere nuove correlazioni tra variabili diverse, ma la correlazione non sempre significa causalità, così la profilazione può portare a decisioni erronee con impatti negativi sui singoli individui.

In questo scenario, ulteriori distorsioni potrebbero derivare dal fatto che consumatori e risparmiatori sarebbero incentivati a migliorare artificialmente il proprio rating/scoring attraverso il ricorso a società che gestiscono la reputazione online o manomettendo i dati generati su di essi.

La dirompente trasformazione , originata dal FinTech, può portare con sé, non solo nuove opportunità per le imprese e possibili benefici per la clientela, ma anche nuove e preoccupanti incognite, in particolare, anche sotto il profilo della protezione dei dati personali di consumatori e risparmiatori.

Particolarmente significativi, in tal senso, sono i meccanismi di funzionamento delle piattaforme telematiche di servizi, i cosidetti marketplace: canali di intermediazione diretta tra risparmiatori e imprese, debitori e creditori, l'assicuratori e assicurati, in cui gli operatori FinTech effettuano attività di ranking/scoring del profilo di rischio, del grado di solvibilità o dell'adeguatezza delle controparti contrattuali, orientando le scelte di investimento, o quelle assicurative della clientela, senza tuttavia assumersi alcun rischio in proprio.

Questo solleva legittimi interrogativi collegati alla completezza e all'attendibilità dei dati e delle fonti utilizzate, alla correttezza della loro elaborazione, al grado di trasparenza nei confronti dei consumatori.

Peraltro, i rischi di comportamenti sleali o fraudolenti nei confronti della clientela aumentano con l'accresciuto impiego degli algoritmi e l'ulteriore sviluppo delle tecniche di intelligenza artificiale, poiché rendono il processo decisionale più opaco e sempre più difficile per consumatori e risparmiatori intuire la logica sottostante all'offerta di servizi o prodotti a loro dedicati.

Senza dimenticare che i rischi di frode rilevano anche in relazione a comportamenti scorretti o fraudolenti, eventualmente tenuti dalla clientela o da terzi, a danno degli stessi fornitori di servizi FinTech ad esempio autenticandosi con false identità o appropriandosi indebitamente delle informazioni fornite dalla clientela.

Altri profili meritevoli di attenzione, con riferimento all'intensità della digitalizzazione delle attività finanziarie, creditizie e assicurative sono quelli relativi alla cyber

sicurezza e, in generale, ai rischi informatici, specie in termini di compromissione della continuità operativa dell'impresa e della tutela dei dati relativi alla clientela.

Le peculiarità operative delle FinTech, basate su "sistemi aperti" rendono, infatti, tali società particolarmente vulnerabili a questi rischi, soprattutto nel momento in cui i dati personali degli utenti sono suscettibili di essere trasferiti presso terzi fornitori di servizi, inclusi quelli di cloud computing.

Ulteriori criticità possono emergere in relazione al grado di robustezza delle procedure digitali per l'autenticazione dei clienti, nonché di quelle finalizzate all'adeguata verifica della clientela, anche a fini di antiriciclaggio.

In tale quadro, va tuttavia sottolineato che il contesto sempre più "interconnesso" dei mercati, all'interno dei quali agiscono gli operatori del FinTech, in larga parte in assenza di specifica regolamentazione, non esenta tali soggetti dal rispetto della disciplina sulla protezione dei dati personali.

E questo, a prescindere dal supporto utilizzato dall'impresa, dalla scelta del territorio di insediamento e dal suo operare o meno in settori regolamentati.

La piena applicabilità, ormai imminente, del Regolamento europeo sulla protezione dei dati personali rafforzerà ulteriormente le garanzie a protezione dei consumatori europei, attraverso un complesso di regole uniformi di liceità, trasparenza e correttezza nel trattamento dei dati della clientela, applicabili a tutti i fornitori di servizi che fanno uso di tali informazioni, indipendentemente dal fatto che si tratti di istituzioni finanziarie o entità non regolamentate.

Il nuovo quadro giuridico estende il proprio ambito di applicazione anche ai soggetti stabiliti al di fuori dell'Unione europea, qualora essi offrano beni o servizi agli individui che si trovano nell'Unione o ne controllino il comportamento.

Viene così assicurato ai consumatori e ai risparmiatori europei un livello di tutela omogeneo, che potrà costituire un modello - fondato sul primato della persona - verso il quale anche gli altri ordinamenti potranno via via convergere.

Sintomatico, al riguardo, il disegno di legge che disciplina la raccolta dei dati da parte delle Big Tech, che il Senato americano si appresta a discutere, sotto la spinta del Caso Cambridge Analitica.

Sotto il profilo della tutela dei dati personali della clientela, la normativa europea è perciò già configurata in modo che la competizione tra gli operatori del Fin Tech e gli intermediari tradizionali possa svolgersi su basi paritarie, poiché nasce dall'ambizione di fornire risposte adeguate ed efficaci al continuo evolversi della tecnologia, sulla base del principio di neutralità tecnologica, promuovendo, al contempo, la responsabilizzazione dei "gestori" dei dati, mediante un approccio di prevenzione dei rischio.

Pertanto, come hanno sottolineato anche le Autorità europee di vigilanza del settore bancario, finanziario e assicurativo, nel rapporto finale sui Big Data del marzo scorso, non occorre ripensare alla disciplina che regola la raccolta, la gestione e l'elaborazione di dati personali.

Il nuovo quadro giuridico europeo sul trattamento dei dati e quello in materia di cybersecurity e identificazione elettronica – forniscono, infatti, una cornice normativa adeguata a fronteggiare molti dei rischi emergenti.

Penso agli strumenti a disposizione dei consumatori, preordinati a incrementare la trasparenza e la correttezza del trattamento, nonché a consentire di comprendere e controllare meglio l'utilizzo dei loro dati.

Innanzitutto, in forza del principio dell'accountability, anche gli operatori FinTech dovranno essere in grado di giustificare l'uso di determinate categorie di informazioni ed assicurare che queste siano adeguate e non eccedenti le finalità del loro impiego, nonché accurate e aggiornate nel tempo.

Dovranno poi garantire che i dati più delicati dei clienti siano utilizzati con il loro consenso esplicito (o in base ad altri stringenti presupposti) e solo per scopi limitati.

Inoltre, i consumatori hanno diritto di essere informati, in anticipo, in modo chiaro e facilmente accessibile, di tutti i possibili usi dei loro dati, specie se questi sono destinati a essere utilizzati in processi decisionali automatizzati come la profilazione.

In particolare, in questo caso, dovrà essere fornita agli interessati una spiegazione intellegibile della logica sottostante al processo decisionale che ha portato allo sviluppo del loro "profilo" e alle conseguenze di tale processo.

Gli utenti dei servizi FinTech potranno esercitare in ogni momento il diritto di accesso ai dati che li riguardano, compresi i propri "profili", al fine di verificare l'esattezza e la liceità del trattamento, di richiedere modifiche o addirittura opporsi al trattamento in determinate circostanze.

E nel caso di profilazione che produca effetti significativi sulla loro persona, i consumatori potranno chiedere l'intervento umano nel processo decisionale, contestandone l'esito.

Il regolamento richiederà quindi una maggiore trasparenza anche da parte delle piattaforme on line e una crescente attenzione alla qualità dei dati e alla correttezza del loro uso.

Ciò permetterà ai clienti delle piattaforme di comprendere meglio i vari rischi connessi al trattamento, ai fini di una più consapevole valutazione dei servizi offerti, al di là della loro convenienza economica.

Tra i diritti dei consumatori, un posto di rilievo, nel contesto FinTech, va, inoltre accordato a quello alla portabilità dei dati.

Tale diritto, com'è noto, permette agli interessati di ricevere, in un formato interoperabile, i dati personali forniti a un titolare del trattamento e di trasmetterli a un diverso titolare senza impedimenti.

Anche questa prerogativa contribuirà ad accrescere il controllo dei consumatori sui dati che li riguardano e, nello stesso tempo, favorirà la concorrenza fra i fornitori di servizi FinTech.

In tema di sicurezza, la nuova disciplina europea sulla protezione dei dati, tutta improntata a un modello di tutela in chiave proattiva, fondata sulla minimizzazione del rischio e sulla complessiva responsabilizzazione dei titolari, potrà inoltre favorire l'adozione da parte degli operatori FinTech di una serie di misure e processi organizzativi interni, volti a mitigare i pericoli di distruzione o perdita dei dati, di accesso non autorizzato o comunque di trattamenti illeciti o non conformi alle regole.

A ciò contribuirà il ricorso agli strumenti di tutela preventiva, previsti dal Regolamento europeo, quali la valutazione d'impatto privacy, le regole di privacy by design e by default, nonché il principio di minimizzazione, tramite l'adozione, ove necessario, di misure di anonimizzazione e pseudoanonimizzazione.

Un discorso a parte merita la direttiva europea sui servizi di pagamento (c.d. PSD2),

Innanzitutto va detto che essa, rispetto alla normativa previgente, tenta di introdurre un certo numero di specifiche garanzie per la protezione e la sicurezza delle informazioni riferite ai clienti.

Inoltre, resta ferma la piena applicabilità delle regole sul trattamento dei dati personali a tutti i prestatori di servizi di pagamento - siano essi banche, istituti di pagamento o nuovi operatori del mercato .

In particolare, la direttiva richiede a tali soggetti di individuare preliminarmente gli specifici scopi del trattamento, la pertinente base giuridica, i requisiti di sicurezza, nonché di assicurare il rigoroso rispetto dei principi di necessità, limitazione delle finalità e proporzionalità nella conservazione dei dati e, ancora, di adottare tecniche di privacy by design e by default

Cionondimeno, vi sono alcuni aspetti sottesi a questa disciplina che suscitano preoccupazione sotto il profilo della protezione dati.

Com'è noto, la direttiva apre il mercato dei pagamenti elettronici a nuovi operatori (non bancari) ampliando il novero dei soggetti coinvolti nella loro erogazione a c.d. terze parti che - se autorizzate dal cliente- si inseriscono nel rapporto tra questi e la propria banca, potendo accedere ai dati relativi ai conti correnti del primo.

Ciò fa sorgere seri interrogativi circa la verificabilità di legittimità dell'accesso da parte di tali soggetti e della non eccedenza dei dati acceduti, tenuto conto che tra l'istituto di credito e le terze parti non è obbligatoria la stipula di contratti mediante i quali poter regolare i rispettivi rapporti, ivi incluse le responsabilità di ciascun operatore in ordine all'utilizzo dei dati della clientela.

In questo quadro andrebbero ridefinite, implementandone la verificabilità, le modalità di accesso ai conti correnti bancari dei clienti da parte delle terze parti, con lo scopo di

rilevare operazioni illegittime, nonché individuate le basi giuridiche di volta in volta più adeguate per il trattamento dei dati degli utenti da parte degli operatori coinvolti.

A suo tempo abbiamo evidenziato tali perplessità al Governo: le stesse sono adesso all'attenzione del Gruppo Art. 29 che riunisce le autorità nazionali di protezione dei dati, perché in questa materia è necessario un approccio condiviso a livello almeno europeo.

Ma vi sono altri elementi che possono 'giocare a favore' di un quadro di maggiori garanzie.

Innanzitutto, in tema cybersecurity, la direttiva NIS sulla sicurezza delle reti e dei sistemi informativi ha introdotto specifici obblighi per gli operatori dei servizi essenziali (compresi gli enti creditizi e le infrastrutture del mercato finanziario).

Obblighi che si estendono anche ai principali fornitori di servizi digitali, al di fuori del settore finanziario, quali quelli di cloud computing e i mercati digitali.

Non va poi dimenticato il fattore reputazionale : che può rappresentare un importante incentivo a che i fornitori di servizi FinTech si dotino di regole interne volte a garantire una gestione lecita, corretta e trasparente dei dati e di procedure adeguate di valutazione dei rischi connessi al loro trattamento.

Proprio in questi giorni, le vicende del caso Facebook/Cambridge Analitica, che l'Autorità sta seguendo con grande attenzione, mostrano quanto sia centrale per le Tech companies dimostrare di operare nel rispetto delle regole e di meritare la fiducia della loro clientela.

In caso di uso improprio dei dati personali degli utenti, di violazione delle regole di correttezza e trasparenza, oppure di incidenti di sicurezza, oltre alle elevate sanzioni economiche ora previste dal Regolamento sulla protezione dei dati(fino al 4% del fatturato annuo globale), la sanzione forse maggiore a cui sarebbero esposti (anche i fornitori di servizi Fin Tech) è l'erosione della fiducia nei loro confronti o l'abbandono dei marketplace da parte dei clienti.

In questo scenario, ferma restando la necessità di definire, in modo unanime e condiviso, l'ambito soggettivo e le caratteristiche del fenomeno "Fintech",

significativo sarà il ruolo del Garante che, a norma del nuovo Regolamento, potrà favorire l'istituzione di meccanismi di certificazione e sigilli, nonché marchi di protezione dei dati, insieme ad adeguati organismi di certificazione, al fine di consentire ai clienti di valutare rapidamente il livello di tutela offerto dai prodotti, servizi e piattaforme FinTech.

Allo stesso tempo, insieme alle altre Autorità di controllo, incoraggeremo l'elaborazione di codici di condotta finalizzati a facilitare la corretta applicazione delle regole sulla privacy in questo settore.

In particolare, guardando all'esperienza nazionale, in tema di codici deontologici, quelli nei settori dei sistemi di informazione creditizia e delle informazioni commerciali hanno mostrato nel tempo di essere strumenti concreti di equo bilanciamento tra le esigenze, da un lato, della tutela del credito, della stabilità del sistema finanziario e delle relazioni commerciali e, dall'altro, della dignità e dei diritti della clientela e degli altri individui coinvolti.

Indispensabile è infine la collaborazione tra autorità di regolazione e di controllo, competenti sulle diverse tematiche.

In questo quadro, il Garante ha scelto di partecipare insieme ad altre Autorità al comitato di coordinamento istituito presso il Ministero dell'economia, che rappresenta un importante spazio di condivisione, confronto e di proposta sulle tematiche afferenti al FinTech .

Tematiche nelle quali sempre più si evidenzia come la protezione dati costituisca uno strumento prezioso, per coniugare innovazione e diritti, mercato e libertà.

14562