Convegno ABI – "Banche e Sicurezza 2020"

2 dicembre 2020

Protezione dati, tutela del credito e digitalizzazione alla prova dell'emergenza

Intervento di

Pasquale Stanzione

Presidente del Garante per la protezione dei dati personali

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Il settore bancario rappresenta, non da ora, un laboratorio assolutamente innovativo per la protezione dati. In tale contesto sono maturate, ad esempio, decisioni importanti sul bilanciamento tra controllo degli accessi e privacy, delineando limiti e condizioni per il ricorso alla biometria o alla videosorveglianza. Proprio in relazione al settore bancario sono stati affermati alcuni dei principi essenziali sulla responsabilità per omesso impedimento di frodi informatiche, così come criteri regolativi importanti rispetto ai trattamenti dei dati nei gruppi societari.

Dei principi affermati in tale contesto dovrà farsi tesoro anche oggi, a fronte di un'evoluzione tecnologica "disruptive" che rischia, se non governata, di negare molti dei progressi compiuti e che la pandemia ha accelerato con velocità esponenziale. Ben si dovrà valorizzare, dunque, l'esperienza maturata in questo campo in un momento, quale quello attuale, in cui la videosorveglianza ha ceduto il passo al riconoscimento facciale, il phishing è divenuto una pratica tanto endemica quanto sofisticata e il blockchain definisce rapporti multipolari e acefali, in un contesto di relazioni finanziarie tradizionalmente bilaterali.

Ed oggi, su questo terreno, percorso da fenomeni nuovi e ancora da normare, emersi in tutta la loro complessità in questa fase d'emergenza, si giocano sfide cruciali dal punto di vista economico, sociale, persino politico.

Da un lato, infatti, le nuove tecnologie hanno reso il ricorso alla profilazione del cliente sempre più ampio e invasivo, con implicazioni importanti sull'identità personale. Dall'altro lato, la convergenza tra fintech e disintermediazione bancaria e finanziaria ha reso assai più articolata e complessa la filiera lungo cui si snoda il trattamento dei dati personali dei clienti.

Ma proprio queste innovazioni hanno messo in evidenza come, alla tradizionale tensione tra ampliamento del potere informativo del soggetto finanziario e privacy individuale, si affianchino anche inattese sinergie tra sicurezza bancaria e protezione dati. Sinergie che sarà sempre più indispensabile promuovere, in un contesto in cui la perdita del monopolio dei rapporti finanziari da parte delle banche e la più estesa

applicazione, a queste attività, dell'intelligenza artificiale (dal roboadvisor alla delega all'algoritmo del credit scoring) esige un quadro organico di garanzie, per la sicurezza e la trasparenza dei rapporti creditizi.

La profilazione, in questo senso, rappresenta un banco di prova importante. Norme recenti ne hanno progressivamente esteso il campo di applicazione, a fini di tutela d'interessi tanto individuali quanto collettivi, non senza implicazioni di rilievo sulle garanzie individuali.

Significativa, in tal senso, la disciplina della *product governance,* che in applicazione del principio del miglior interesse del cliente (*suitability rule: direttiva Mifid II: 2014/65/UE*) ha favorito un'ampia profilazione del cliente finalizzata alla prestazione dei servizi di investimento. Tale disciplina promuove, infatti, la targettizzazione dei «prodotti» offerti alla clientela sulla base della specifica classe di propensione al rischio in cui l'algoritmo abbia collocato il soggetto. In questo caso la "clusterizzazione" della clientela è funzionale all'offerta, a ciascun cliente, di prodotti finanziari conformi alla sua condizione patrimoniale e alla propensione al rischio che gli sia attribuita. **Una profilazione funzionale ad un tempo al singolo e alla stessa sostenibilità del sistema finanziario nel suo complesso, dunque, ma dall'indubbia rilevanza** in ragione dell'invasività del monitoraggio cui il singolo e le sue scelte individuali sono sottoposti.

E se in tal caso la profilazione è imposta dalle norme di settore, in altre ipotesi essa è **connaturata alla stessa tecnica bancaria.** Per l' «istruttoria di fido», ad esempio, la banca è tenuta, secondo il TUB, a valutare la «situazione economica, patrimoniale o finanziaria» del soggetto finanziato e nel caso del credito al consumo, il merito creditizio è oggetto di un'indagine approfondita che contempla anche la consultazione delle specifiche banche dati. **Proprio l'invasività di tali forme di profilazione e il rischio di rappresentazioni non aggiornate della capacità patrimoniale del debitore,** è stata la ragione principale della sottoscrizione del codice deontologico (oggi codice di condotta) sul trattamento di dati personali nel contesto delle informazioni commerciali, tra i più innovativi del settore.

L'elemento su cui riflettere oggi attiene, però, alla progressiva estensione (e, per certi versi, ineludibilità) della profilazione, sempre più preordinata alla «**sana e prudente gestione**» dell'attività bancaria**.** Obiettivo, questo, centrale nel Tub al punto di configurare **un principio di ordine pubblico economico,** funzionale alla stessa **tutela, di rango costituzionale, del risparmio**, di cui va garantita la migliore allocazione, e degli interessi dei consumatori (art. 38 CDFUE). Solo attraverso l'erogazione di finanziamenti davvero sostenibili da parte del debitore, infatti, può impedirsi una situazione di collasso del sistema analoga a quella verificatasi nel caso dei mutui *subprime.*

E dal momento che la prognosi di rischio d'insolvenza è delegata, oggi, *q*uasi integralmente agli algoritmi, è necessario garantirne l'affidabilità, l'esattezza, la contestabilità, la trasparenza, per evitare bias o comunque false rappresentazioni, in eccesso o in difetto, della capienza del debitore. Ed è altrettanto necessario limitare lo "scoring" allo stretto indispensabile, non facendolo degenerare in una forma di controllo massivo e, oltretutto, predittivo. dalle potenzialità discriminatorie troppo spesso sottovalutate.

Sotto entrambi i profili, la disciplina di protezione dati offre strumenti preziosi per promuovere, ad un tempo, **l'affidabilità dello scoring e la tutela dell'identità personale**, in particolare attraverso la garanzia dell'esattezza dei dati utilizzati nella configurazione degli algoritmi, da cui dipende l' "intelligenza" delle loro scelte..

Rilevante, in tal senso, non solo l'obbligo di verifica (anche nell'ambito della valutazione d'impatto) della correttezza dei dati da analizzare, ma anche il diritto dell'interessato di contestare la decisione assunta dopo averne ricevuto la spiegazione della logica, ottenendo anche l'intervento umano sul processo da parte del titolare, per impedirne la totale e cieca devoluzione alla macchina.

Gli obblighi rafforzati di trasparenza sanciti in quest'ambito sono particolarmente rilevanti, proprio perché consentono di superare, almeno in parte, l'intrinseca **opacità algoritmica e l'asimmetria informativ**a che ne consegue, soprattutto ove il diritto alla spiegazione sia inteso come riferito anche a*lla decisione assunta*, dunque ex post, e non soltanto alla logica da utilizzarsi, *ex ante*.

Questo implica dunque l'impossibilità di ricorrere ad algoritmi black-box, dovendo invece preferire quelli "rule-based", ovvero suscettibili di una spiegazione realmente comprensibile anche ex post e, come tale, contestabile.

E, in termini più generali, i principi sanciti dalla disciplina di protezione dati su questo terreno – a partire dal diritto a non soggiacere a decisioni esclusivamente algoritmiche – impongono una generale responsabilizzazione dei titolari, indispensabile per ridurre il rischio di errori pregiudizievoli tanto dei diritti dell'interessato quanto della "sana e prudente gestione" dell'attività creditizia, nonché per contenere la tendenza alla devoluzione integrale all'algoritmo di valutazioni non interamente delegabili alla macchina.

L'inattesa sinergia di cui dicevamo all'inizio si manifesta così, su questo terreno, da un lato come **limite alla "deresponsabilizzazione algoritmica", dall'altro come selezione dei soli programmi in grado di assicurare condizioni essenziali di trasparenza e correzione degli** errori, spesso più gravi di quelli umani. Il tutto, a beneficio non soltanto dell'interessato ma della correttezza dell'attività finanziaria e bancaria in senso lato, oltre che della **complessiva sostenibilità del sistema.**

Ma le innovazioni apportate dal fintech, dall'open banking e in generale dalla disintermediazione funzionale nel settore (oggi assai più incisiva di come si manifestava all'origine, negli anni '80) dimostrano come le sinergie tra protezione dati e corretta attività finanziaria involgano anche un altro aspetto.

La normativa europea recente ha promosso un processo di **pluralizzazione soggettiva del settore,** legittimando l'emersione di nuovi organismi finanziari e figure intermediatrici aliene al tradizionale ambito bancario e che, se non sostituiscono tout court gli istituti di credito, comunque si affiancano loro rendendo più articolata la fisionomia del comparto: si pensi alla concessione di credito da parte delle imprese di assicurazione, ad alcune particolari tipologie di fondi di investimento come pure ai moduli alternativi di gestione collettiva del risparmio.

Ma le innovazioni maggiori si sono registrate nel settore dei servizi di pagamento, in cui l'esclusività del rapporto banca-cliente è stata scardinata non solo dall'emersione di soggetti quali gli istituti eroganti moneta elettronica e gli istituti di pagamento, ma soprattutto dalla "**rivoluzione" della direttiva Psd2 (2015/2366/UE),** in cui le innovazioni del Fintech sono state più profonde per l'assenza di riserve di attività. Tale disciplina, dal chiaro intento di liberalizzazione e promozione della concorrenza, ha imposto condivisione dei dati bancari del cliente (consenziente) tra i diversi attori dell'ecosistema bancario erodendo, in favore di una nebulosa di "terze parti", il tradizionale monopolio della banca sulla posizione soggettiva individuale

I conti correnti vengono, dunque, per la prima volta aperti anche a soggetti non bancari, al di fuori del quadro di obblighi cui questi ultimi soggiacciono, con le relative garanzie per i clienti.

Questo processo di **progressiva pluralizzazione soggettiva dei rapporti finanziari comporta, sotto il profilo della protezione dati, un grado di complessità nell'articolazione della filiera** del trattamento che esige garanzie supplementari per impedire che l'open banking degeneri in una licenza di abuso o in un'occasione di agevolazione delle frodi informatiche. La protezione dati è, in questo senso, un fattore di promozione della sicurezza informatica e di garanzia della corretta gestione delle informazioni bancarie e dei servizi di pagamento, in un contesto in cui **la legittima apertura dei rapporti di credito non deve degenerare in permeabilità dei flussi informativi,** con tutti i rischi (di frodi, cyber attacks, manovre speculative) che inevitabilmente ne conseguono.

E in tale contesto di destrutturazione del panorama soggettivo tradizionale del settore, la variabile tecnologica – che modifica profondamente relazioni e dinamiche di mercato – impone ulteriori cautele per la complessiva sostenibilità del sistema. Il digitale sviluppa, infatti, servizi nuovi e in forme nuove, mettendo in discussione l'ambito delle riserve di attività oggi esistenti: si pensi alla gestione automatizzata dei conti o alle cripto-valute gestite su registri blockchain, oggi definiti addirittura normativamente.

La tradizionale catena del valore si disarticola, così, con l'emersione di operatori che gestiscono (solo) specifici segmenti della filiera **disintermediandola**: si pensi alle piattaforme di *peer to peer (P2P) lending* e di *crowfunding* quali canali di raccolta del capitale alternativi a quello bancario o anche ai nuovi servizi di pagamento digitali.

Ma gli effetti che ne derivano non si limitano alla (pur rilevantissima) sfera privata, investendo aspetti di sistema e ridelineando l'allocazione del potere, con il rischio dell'emersione di nuovi oligopoli, più potenti di quelli tradizionali e, assai più di questi, votati all'espansione in settori diversi, politicamente sensibili.

Il **paradigma dell'*Open Banking*** favorisce, infatti, l'emersione di nuovi modelli di mercati a due versanti, basati su piattaforme bancarie *on line* che agiscono come intermediari tra i titolari di conti e le imprese FinTech, generando potenziale valore per entrambe le parti pur al netto di una mutazione genetica dell'attività bancaria e di un effetto paradossale, forse preterintenzionale.

La direttiva Psd2, nata per promuovere la concorrenza nei servizi di pagamento e l'innovazione delle imprese FinTech, ha finito per aprire le porte della finanza ai **big tech**, mutando così profondamente dinamiche competitive e la stessa articolazione del potere. In virtù delle possibilità offerte dalla direttiva, infatti, i GAFAM potranno gestire in proprio i pagamenti (anziché triangolarli con le banche), emettendo anche moneta elettronica, così da trattenere i clienti nel loro spazio virtuale in progressiva espansione e offrendo una pluralità di servizi quasi al pari di un'infrastruttura sociale o pubblica. Non si tratta di uno scenario troppo "futuribile" se si considera che Facebook, Amazon, Google hanno già ottenuto licenze, in vari Stati europei, per l'emissione di moneta elettronica e la prestazione di servizi di pagamento, secondo una tendenza che è difficile pensare venga arrestata, con implicazioni da non sottovalutare.

Soprattutto, non va sottostimato l'effetto della **concentrazione del potere** che in tal modo si determinerebbe in capo ai big tech, detentori di un patrimonio informativo così dettagliato ed esteso, su buona parte della popolazione mondiale, da sfidare ogni regola antitrust e, soprattutto, ogni esigenza di separazione tra gestione commerciale e delle reti sociali o delle risorse informative, valorizzata con lungimiranza anche dal Parlamento europeo.

Sotto questo profilo la disciplina di protezione dati- attraverso la rigorosa regolamentazione della filiera del trattamento, il principio di finalità che vieta l'utilizzo secondario di dati raccolti per fini diversi, gli obblighi di trasparenza volti a colmare

l'asimmetria informativa propria di relazioni così sbilanciate quali quelle tra singolo utente e big tech- offre sicuramente strumenti importanti per il governo di un settore sempre più disarticolato e a forte rischio di anomia.

Le garanzie imposte, dalla disciplina privacy, agli operatori, nel segno della trasparenza del trattamento, della loro responsabilizzazione rispetto al patrimonio informativo che gestiscono e degli obblighi di sicurezza cui adempiere per evitare cyberattacks e vulnerabilità dei sistemi si sono rivelate preziose in un contesto, quale quello emergenziale, di crescente dematerializzazione dei flussi finanziari e dei rapporti di credito. Basti pensare alla disciplina della responsabilità civile modellata su di un paradigma di colpa presunta, particolarmente favorevole alla persona offesa, che trasposto sul piano del rapporto tra banca e cliente consente di elevare gli standard di diligenza della prima, ad esempio rispetto al phishing realizzato sul sistema di home banking ai danni dei correntisti.

E si consideri anche come, proprio rispetto a un contratto di conto corrente, la Cassazione abbia recentemente applicato il principio di minimizzazione dei dati trattati quale norma imperativa la contrarietà alla quale determina nullità della relativa clausola contrattuale. La Corte ha dunque posto un limite – rinvenuto nella disciplina privacy- alla raccolta di dati personali eccedenti le necessità di gestione del rapporto bancario, conformando dunque l'autonomia privata sulla base di parametri eteroregolativi tali da impedire, anche, la concentrazione eccessiva del patrimonio informativo.

In questo senso, la protezione dati si dimostra anche **valida alleata tanto della disciplina consumeristica quanto di quella concorrenzial**e in senso proprio, ostacolando le condizioni per la concentrazione del potere, anzitutto (ma, appunto, non solo) informativo.

Al fondo vi è, però, **una grande questione democratica e politica** (nel senso più alto del termine), che involge anzitutto la capacità degli Stati di regolamentare, necessariamente su base non più soltanto nazionale, le sempre più incisive innovazioni indotte dalle nuove tecnologie e le relative implicazioni sulla dinamica e l'articolazione del potere e sulle corrispettive garanzie democratiche. *Hic Rhodus, hic salta.*