CORRIERE DEL TICINO

*L'OSSERVATORIO BANCARIO Paolo Bernasconi**

Se il segreto bancario ha la testa fra le nuvole

Il segreto bancario svizzero non è affatto scomparso. Anzi, il Parlamento svizzero gli ha generato qualche fratellino nelle nuove leggi finanziarie per gestori patrimoniali e trustee*. Concorre poi come alleata l'ondata in favore della protezione dei dati personali, scatenata dal Regolamento generale dell'UE (GDPR), così convincente che il Parlamento svizzero l'ha già recepito in gran parte nella Legge federale sulla protezione dei dati, di cui è già in corso una nuova revisione. Ma non mancano le minacce: il formidabile sviluppo dell'informatica si accompagna allo sviluppo della cibercriminalità, riguardo alla quale le banche rappresentano il bersaglio privilegiato, come comprovano recenti frequenti assalti che permettono ai ladri di identità di intascare milioni ad ogni colpo. Anche in Svizzera, polizia e magistratura sono ancora manifestamente impreparate. E per rincorrerli oltre frontiera, poi, non basta più la Convenzione sulla cibercriminalità del Consiglio d'Europa, ormai vecchia del 2001, che pure prevede interventi anche oltre gli antiquati scalini della cooperazione internazionale in materia penale (ratificata dalla Svizzera con un ritardo di ben dieci anni, poiché l'UDC la riteneva troppo invasiva, mentre gli USA corrono: hanno appena pubblicato un*

libro bianco sul loro Cloud Act*). Ma altri rischi incombono:* to cloud or not to cloud*? L'Associazione svizzera dei banchieri (ASB) ha appena deciso: tutte le banche svizzere si interessano vivamente al cosiddetto* cloud computing*, ma siccome esitavano a far migrare i dati bancari verso il* cloud*, l'ASB ha pubblicato una guida specifica contenente raccomandazioni di carattere legale. Benché la guida non sia obbligatoria e non rientri nemmeno negli standard minimi previsti dalla circolare della FINMA (2008/10), verrà applicata dalle numerose banche che si ripromettono una gestione più efficace e una riduzione dei costi. Interessante specialmente per banche medie e piccole, che potranno così fruire di questa democratizzazione dell'accesso alla tecnologia più costosa, generatrice di significative economie di scala. Scopo principale della guida: garantire il segreto bancario e la protezione dei dati personali dei clienti, i cosiddetti CID (*Clients Identifying Data*). Fino ad oggi le banche svizzere tenevano conto dei rischi per i dati personali, non appena fossero usciti dal controllo dei tribunali svizzeri. Pertanto non venivano comunicati all'estero ed era impossibile accedervi dall'estero. Secondo l'ASB, il mantenimento assoluto di questo principio renderebbe impossibile il ricorso al* cloud. *Pertanto, raccomanda una serie di misure tecniche, organizzative e contrattuali, in modo da limitare i rischi dovuti al fatto che i prestatori e i sotto-prestatori di servizi, possano accedere ai dati personali della clientela: anonimizzazione, pseudonomizzazione e criptazione. Inoltre viene raccomandato l'allestimento di rapporti di* audit *indipendenti, proprio riguardo all'esistenza e all'efficacia delle norme di sicurezza e di confidenzialità messe in atto da parte dei prestatori di servizi. Segue quindi una serie molto sofisticata di misure contrattuali che vengono imposte ai prestatori di servizi. Siamo tranquilli? È vero che oltre al luogo dei prestatori di servizi, questi devono informare ogni banca riguardo ai luoghi in cui si trovano i prestatori di* cloud computing*, chi utilizza e può utilizzare centri di dati e a partire da quali utilizzano il* cloud *(centri di utilizzazione). Siccome qualsiasi comunicazione dei dati dei clienti della banca effettuata nei confronti di terzi è punibile secondo l'art. 47 della Legge federale sulle banche, ci si chiede se sia necessaria una dichiarazione scritta, esplicita e sufficientemente orientata da parte del cliente, svincolando la banca dall'obbligo del segreto. Una prassi molto prudente e rigorosa viene rispettata da parte di avvocati che intendono impiegare o far capo alle prestazioni* cloud*. La guida dell'ASB è meno rigorosa, partendo dal presupposto che i dati personali non vengono messi a disposizione dei prestatori* cloud. *Ma rimane almeno necessario che il cliente sia orientato sul*

rischio che il prestatore e i suoi subappaltanti possano accedere ai suoi dati personali, per abuso oppure a seguito di negligenza. La trasmissione dei dati personali ai prestatori di servizi cloud *non sarebbe punibile nella misura in cui questi venissero considerati, invece che come terze persone, come ausiliari della banca. A questo riguardo la prassi per gli avvocati si mostra più prudente e non si vede perché tale prudenza non si debba applicare anche ai dati dei clienti delle banche. In ogni caso, le raccomandazioni della guida dovranno tenere conto della recente sentenza del Tribunale federale che ha assolto dall'accusa di violazione del segreto bancario quell'ormai noto dipendente del Gruppo Julius Baer, considerando che aveva lavorato all'estero e che non rientrava nella lista degli impiegati né degli ausiliari. La guida a giusta ragione raccomanda di scegliere comunque dei prestatori di servizi localizzati in paesi che diano garanzia sufficiente di rispetto della legislazione sulla protezione dei dati. Sembra prudente estendere questa verifica anche al livello del rispetto concreto delle regole generali dello stato di diritto e delle garanzie procedurali a favore dei diritti individuali. Per esempio il regime della Turchia o quello di alcuni Paesi dell'ex URSS si dimostrano talmente difformi dallo stato di diritto, da doverli considerare come paesi ad alto rischio. Pertanto, le banche dovrebbero escludere contratti con prestatori di servizi e loro subappaltanti che intrattengano qualsiasi relazione in Paesi sottoposti a questi regimi. Altra importante preoccupazione: secondo l'ASB il prestatore di servizi dovrà reagire di fronte ad una richiesta di informazioni da parte dell'autorità giudiziaria o di polizia nazionale, rinviando ai tribunali svizzeri. La guida rammenta, e non poteva essere altrimenti, che questo impegno contrattuale da parte di un prestatore vale soltanto se non contrasti con regole imperative del paese ospitante, il che equivale a riconoscere che questi impegni contrattuali sono deboli. Altrettanto vale per l'impegno contrattuale a carico dei prestatori di servizi di collaborare con la banca nel trattare le domande di informazioni provenienti dall'autorità del paese ospitante. Come si vede, una volta in più, il segreto bancario continuerà a sussistere nella misura in cui le banche saranno in grado di prevenire qualsiasi abuso. Intanto, dietro l'angolo, attende la definizione della responsabilità in caso di violazione del segreto bancario dovuta all'uso di intelligenza artificiale. Dobbiamo aspettare il Parlamento, oppure basterà l'autoregolamentazione?*

* professore e avvocato