

L'intesa sui dati per le due sponde dell'Atlantico

di Rosario Cerra* e Francesco Crespi**

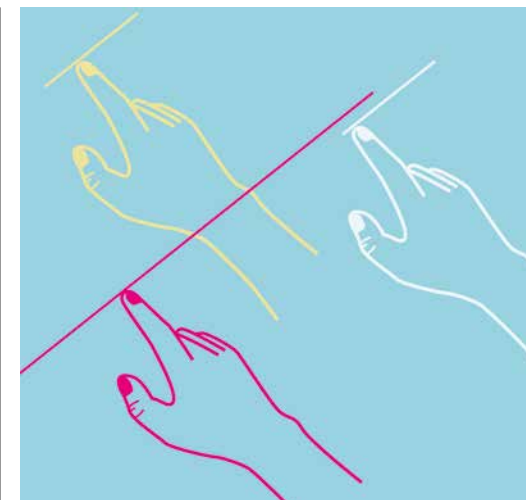
Il nuovo accordo transatlantico per lo scambio dei dati, una volta adottato, renderà possibile alle entità europee trasferire dati personali verso gli Stati Uniti, senza dover mettere in atto ulteriori garanzie per la loro protezione. Nell'attuale contesto geopolitico, costruire un contesto di regole certe e un clima di reciproca fiducia tra le due sponde dell'Atlantico rispetto alla condivisione dei dati potrà contribuire in maniera decisiva a scambiare conoscenze scientifiche e tecnologiche e a rafforzare le rispettive capacità di sviluppare innovazioni

In seguito alle dichiarazioni dei presidenti Biden e von der Leyen nel marzo 2022, il processo verso un nuovo accordo transatlantico per lo scambio dei dati è andato avanti. Auspicabilmente la Commissione concluderà l'iter per approvare la decisione di adeguatezza prima della prossima pausa estiva. Una volta adottata questa decisione, sarà possibile alle entità europee trasferire dati personali verso gli Stati Uniti senza dover mettere in atto ulteriori garanzie per la loro protezione. Si tratta di un passaggio importante. Non solo perché con questo accordo si supera un vuoto normativo che riduce l'enorme potenziale dei dati in termini di innovazione e creazione di valore economico, ma anche perché così si prova a riequilibrare i rapporti tra Unione europea e Stati Uniti in questo campo. Sul piatto c'è una regolazione completamente nuova, che sottintende un passo significativo dell'amministrazione americana nei confronti dell'Unione europea verso un contesto certo e sicuro per i flussi transatlantici dei dati. In particolare, l'accesso ai dati europei da parte

delle agenzie di Intelligence statunitensi per proteggere la sicurezza nazionale sarà limitato a quanto necessario e proporzionato. Inoltre si costituirà un sistema per dirimere le controversie, riconosciuto da entrambe le parti, che dovrebbe consentire l'effettivo esercizio dei diritti dei cittadini europei relativi alla tutela dei dati. Oltre alle importanti ricadute economiche, questo accordo rappresenta un tassello importante nell'ambito della strategia europea sulla sovranità digitale. Un tema su cui l'Europa è arrivata in ritardo e su cui ha peccato di eccessiva passività, come dimostrato non solo dalla necessità di rinegoziare i rapporti transfrontalieri sui flussi di dati ma, soprattutto, dalle limitate capacità tecnologiche e produttive sviluppate nel campo delle piattaforme e, più in generale, dell'economia digitale. Dovrebbe essere ormai chiaro che la tecnologia digitale è una quinta dimensione strategica, oltre alla terra, al mare, all'aria e allo spazio, attraverso la quale si veicolano e concretizzano le espressioni della sovranità nazionale o sovranazionale nel caso dell'Unione. E d'altra parte il digitale non è una dimensione strategica come le altre poiché non è un dominio separato, in quanto attraversa, nel profondo, tutti gli altri. Ecco perché le capacità sviluppate in questo ambito permettono di consolidare la propria sovranità nelle altre dimensioni strategiche. Dopo aver partecipato alla prima ondata della rivoluzione digitale praticamente da spettatrice, o al massimo da arbitro – guidando lo sviluppo degli aspetti regolatori – nella sfida tra Stati Uniti e Cina, l'Europa deve cercare di trarre il massimo vantaggio dalle grandi opportunità offerte dall'utilizzo della nuova ondata di dati provenienti dal

–“La tecnologia digitale è la quinta dimensione strategica, oltre alla terra, al mare, all'aria e allo spazio, attraverso la quale si concretizzano le espressioni della sovranità nazionale o sovranazionale. Ma non è una dimensione strategica come le altre poiché non può essere vista come un dominio separato, in quanto attraversa tutti gli altri” –

mondo industriale e dalle applicazioni Iot (*Internet of things*). Sono settori in cui l'Europa e anche l'Italia, come seconda manifattura del continente, svolgono ancora un ruolo significativo. In questo contesto la condivisione dei dati non personali sarà fondamentale per il successo dell'economia europea nei prossimi anni, con un contributo fornito dai dati pari almeno a un trilione di euro entro il 2030 secondo le stime della Commissione. Su questo il Data act dell'Ue è l'elemento finale, e probabilmente il più importante, di un ambizioso programma legislativo sulla trasformazione digitale dell'Europa. È un pacchetto che dovrà stabilire le regole di base per l'accesso ai dati, la loro condivisione, l'interoperabilità e le responsabilità delle piattaforme *online*. E come con il precedente regolamento generale sulla protezione dei dati (Gdpr), è ragionevole aspettarsi che queste norme europee avranno un impatto globale. Sarà dunque importante imparare le lezioni derivanti dalle precedenti esperienze. Rispetto alle considerazioni fin qui effettuate ne segnaliamo in particolare due. In primo luogo, consultare in modo tempestivo gli Stati Uniti potrebbe contribuire a evitare conflitti transatlantici simili a quelli registrati per anni sui trasferimenti di dati personali e che, solo ora, sembrano avviarsi alla conclusione. Nell'attuale contesto geopolitico, costruire un contesto di regole certe e un clima di reciproca fiducia tra le due sponde dell'Atlantico rispetto alla condivisione dei dati migliorerà lo scambio di conoscenze scientifiche e tecnologiche e rafforzerà le rispettive capacità di sviluppare innovazioni. In secondo luogo, considerato che il Data act agisce sui fondamenti dei modelli di *business*



basati sui dati delle imprese europee, occorre evitare pericolosi salti nel buio perché, come l'esperienza ci insegna, intervenire dopo per riparare i danni è molto difficile. Se, infatti, da un lato bisogna evitare che l'attuale o prospettica eccessiva concentrazione dei dati limiti la crescita di un ecosistema di imprese europee, bisogna anche evitare che l'obbligo di scambio dei dati impatti negativamente sui vantaggi tecnologici e produttivi che queste imprese hanno o stanno sviluppando, oltre che sugli aspetti legati alla *cyber-security*. In altre parole, la protezione del segreto commerciale necessita di un'attenta riflessione su quale sia il meccanismo più efficace per garantire la protezione di un *know how* che va condiviso solo quando e quanto necessario.

*Fondatore e presidente del Centro economia digitale
**Direttore ricerche Ced e professore di Economia dell'innovazione presso l'Università degli Studi Roma Tre