Sempre più stati vogliono controllare i dati dei propri cittadini

Caricamento player

Negli ultimi anni, decine di governi hanno approvato o stanno approvando leggi e misure di gestione e controllo dei dati e dei contenuti online, con l'obiettivo di rafforzare la propria "sovranità digitale": l'idea, cioè, che i dati generati da una persona, un'azienda o un ente dovrebbero essere immagazzinati all'interno del loro paese d'origine, o almeno essere gestiti in conformità con gli standard di privacy e sicurezza stabiliti dal governo.

Le misure proposte per ottenere questo controllo sui dati, negli anni, sono state sia tecniche sia politiche e, come hanno scritto i giornalisti del *New York Times* David McCabe e Adam Satariano, potrebbero alterare in maniera consistente il modo in cui internet ha funzionato da quando si è diffuso a livello commerciale negli anni Novanta, ponendo limitazioni serie alla libera circolazione dei dati.

Soltanto tra il 2017 e il 2021, il numero di leggi, regolamenti e politiche governative che richiedono l'archiviazione delle informazioni digitali in un determinato Paese è più che raddoppiato, passando da 67 in 35 Paesi a 144 in 62 Paesi, secondo il centro studi Information Technology and Innovation Foundation (ITIF).

Ogni giorno, le persone che usano internet producono enormi quantità di informazioni. Pubblicare un post sui social, correre mentre si indossa uno smartwatch, parlare ad assistenti virtuali come Alexa, pagare con la carta di credito, fare una ricerca su Google: tutto genera dati, che

vengono poi venduti, scambiati, condivisi e analizzati da varie aziende che ricavano così un profitto, generalmente vendendo annunci pubblicitari. Nella maggior parte del mondo, negli ultimi trent'anni la libera circolazione dei dati è stata centrale per la crescita di aziende tecnologiche oggi onnipresenti come Amazon, Apple, Facebook o Google.

Se, inizialmente, la maggior parte dei dati veniva archiviata localmente, su computer privati o su server aziendali, oggi i servizi di "cloud computing" permettono a un italiano di archiviare le foto delle vacanze in un server nel Nevada, o a un'azienda francese di avere un sito web gestito da Amazon Web Services, i cui centri di elaborazione dati, o data center, sono sparpagliati in tutto il mondo, da Singapore all'Irlanda. Gli Stati Uniti sono il paese che ne ospita di più (oltre 2.600), seguiti da Regno Unito, Germania, Cina e Paesi Bassi.

La crescente diffidenza verso il modo in cui le aziende gestiscono i dati in loro possesso e le tensioni internazionali alimentate da rivelazioni come quelle di Edward Snowden – che nel 2013 rivelò come la National Security Agency statunitense spiasse le telecomunicazioni degli altri paesi attraverso i cavi e le reti che compongono internet – hanno portato diversi stati e attori istituzionali come l'Unione Europea a cercare soluzioni per limitare la propria dipendenza da un'architettura di internet realizzata e di fatto gestita dagli Stati Uniti: è per questo che negli ultimi anni si è cominciato a parlare sempre più di frequente di "sovranità digitale".

Oggi, alcuni governi limitano il trasferimento al di fuori dei propri confini di particolari tipi di dati, come quelli sanitari, bancari, finanziari o fiscali, ma anche quelli aziendali di società quotate in borsa o quelli relativi a contenuti generati dagli utenti sui social media. Altri stati limitano più vagamente il trasferimento di dati ritenuti "sensibili" o "legati alla sicurezza nazionale".

L’Unione Europea

A queste due possibilità si aggiungono i casi di leggi che rendono il trasferimento transnazionale di dati così complicato o costoso da rendere indirettamente obbligatorio per le aziende l’immagazzinamento locale dei dati: è il caso, secondo l’ITIF, del Regolamento generale sulla protezione dei dati (GDPR) introdotto nell’Unione Europea nel 2018, che ha fatto entrare in vigore molte nuove regole su come le aziende devono trattare i dati degli utenti. L’Unione sta lavorando anche ad altri progetti di legge, come quello sull’intelligenza artificiale, che aggiungerebbero ulteriori livelli di complessità per le aziende straniere.

Alcune di queste politiche, come il GDPR e le altre leggi in materia che vengono discusse in Europa, sono motivate principalmente da preoccupazioni per la privacy e la sicurezza dei dati dei cittadini, ma finiscono per avere ripercussioni anche sui rapporti economici e politici con paesi extraeuropei, anzitutto gli Stati Uniti.

Per esempio, una delle questioni più rilevanti nei rapporti tra Unione Europea e Stati Uniti in questo ambito ha riguardato gli accordi sul libero trasferimento dei dati dei cittadini europei verso gli Stati Uniti a fini commerciali, che sono stati annullati per ben due volte dalla Corte di giustizia europea (nel 2015 e nel 2020) perché non rispetterebbero gli standard europei di privacy. Questi accordi sono tuttavia essenziali per migliaia di aziende sia europee sia americane, che si sono trovate senza un quadro normativo chiaro sul trasferimento dei dati.

I regimi autoritari

In altri casi, in cui i governi che cercano di raggiungere la “sovranità digitale” sono meno affidabili per quanto riguarda il rispetto della libertà d’espressione e l’accettazione del dissenso politico, queste leggi sul controllo dei dati assumono connotazioni che preoccupano gli esperti di diritti umani.

È il caso della Cina, che fin dagli anni Novanta ha sviluppato un proprio internet separato quasi completamente da quello del resto del mondo, ma anche di stati come il Pakistan e il Vietnam, dove il rischio è che la localizzazione dei dati (cioè la presenza dei server con i dati dei cittadini sul territorio dello stato) non porti a una maggiore privacy, ma soltanto a un maggiore accesso alle informazioni sensibili da parte del governo.

"I governi autoritari, guidati da Cina e Russia, vedono l'accesso fisico ai data center come un fattore critico di sorveglianza e controllo politico. La localizzazione dei dati consente l'oppressione politica portando le informazioni sotto il controllo del governo e consentendo al governo di identificare e minacciare le persone, incidendo così sulla privacy, sulla protezione dei dati e sulla libertà di espressione", si legge nel rapporto dell'ITIF.

Le ricadute sulle aziende

A livello economico, queste leggi per la "sovranità digitale" complicano la vita delle aziende, che in questi anni hanno tratto grande beneficio dal libero flusso dei dati.

Benché affermino spesso che, se le società dovessero immaginare tutti i dati localmente, sarebbe molto complesso continuare a offrire gli stessi prodotti e servizi in tutto il mondo, le grosse aziende statunitensi leader del settore si sono finora adeguate alle richieste governative, cominciando a offrire servizi che consentono alle aziende di archiviare le informazioni all'interno di un determinato territorio.

Amazon Web Services ora consente ai clienti di controllare dove sono stati archiviati i dati in Europa; in Francia, Spagna e Germania, Google Cloud ha firmato accordi con fornitori di servizi tecnologici e di telecomunicazioni per far sì che siano aziende locali a gestire i dati prodotti sui servizi di Google.

La sicurezza

Una critica più interessante alla dottrina della "sovranità digitale" arriva dal mondo della sicurezza informatica, che da anni sottolinea come la privacy e la sicurezza dei dati dipendono più da come i dati vengono trasmessi e archiviati piuttosto che da dove si trovano fisicamente.

Come si legge anche nel rapporto dell'ITIF, "la sicurezza dei dati dipende principalmente dai controlli logici e fisici utilizzati per proteggerli, come la crittografia avanzata sui dispositivi e la sicurezza perimetrale per i data center. La nazionalità di chi possiede o controlla i server o il paese in cui si trovano questi dispositivi ha poco a che fare con la loro sicurezza".

"I politici sembrano non capire che la riservatezza dei dati non dipende generalmente dal paese in cui sono archiviate le informazioni, ma solo dalle misure utilizzate per archiviarle in modo sicuro. Un server sicuro in Malesia non è diverso da un server sicuro nel Regno Unito. La sicurezza dei dati dipende dai controlli tecnici, fisici e amministrativi implementati dal fornitore di servizi, che possono essere forti o deboli, indipendentemente da dove sono archiviati i dati", continua l'ITIF, secondo cui, anzi, "la localizzazione dei dati impedisce ai fornitori di servizi cloud di utilizzare le migliori pratiche di sicurezza informatica".

Read More