IL FOGLIO – 28 OTTOBRE 2024

Una diversa tutela dei dati

di Carlo Alberto Carnevale Maffè

Quando lo stato dimostra – e perfino ammette esplicitamente – di non saper proteggere i diritti di proprietà sui dati digitali dei cittadini, fallisce nella sua fondamentale missione istituzionale e va radicalmente riformato nelle sue funzioni. E' l'amara lezione che va tratta dalla vicenda portata alla luce dall'inchiesta di Milano e dalle accuse (ancora da dimostrare in Tribunale) sulla sistematica violazione di dati personali e sull'accesso illecito a banche dati governative, quali quelle dell'Inps, dell'Agenzia delle Entrate, e persino del ministero dell'Interno, sfruttando falle nella sicurezza e connivenze interne per prelevare informazioni riservate su migliaia di cittadini.

E tra quei cittadini sono inclusi personaggi di rilievo nel mondo della politica, dell'economia e delle istituzioni. Non interessa qui discutere delle pruderie o degli interessi che si celano dietro a tali violazioni, quanto della (in)capacità dello stato di dotarsi di infrastrutture adeguate a proteggere i dati dei cittadini, di cui detiene il monopolio di custodia e trattamento, e aprire un dibattito critico e propositivo su come mitigare in futuro i rischi di tale evidente violazione dei diritti di proprietà dei cittadini stessi.

Secondo gli investigatori dell'inchiesta di Milano, i presunti responsabili di queste violazioni rappresentano "un pericolo per la democrazia" in quanto, con la loro attività di dossieraggio, sono in grado di manipolare e ricattare individui e organizzazioni, compromettendo dinamiche istituzionali e pubbliche procedure. Questa chiave di lettura è tuttavia insoddisfacente: il primo pericolo per la democrazia sono le istituzioni che si dimostrano inadeguate a svolgere il proprio compito di tutela dei dati, e che quindi diventano facile target di predatori digitali, siano essi mossi da interessi privati o, peggio, da fini di aggressione geopolitica. Se il Leviatano statale pretende il monopolio della custodia dei dati, deve dimostrarsi in grado di farlo efficacemente, pena la radicale perdita di fiducia dei cittadini. nelle istituzioni, con gravissime conseguenze in termini sociali ed economici.

L'attuale quadro normativo è basato su una legislazione europea che, pur partendo da nobili e condivisibili intenti di tutela, ha finito per produrre un coacervo di regole burocratiche che tradiscono un'attitudine proibizionista e paternalista rispetto al rapporto tra cittadini e dati digitali personali, inducendo in essi passività e scarsa consapevolezza della necessità di essere parte attiva e diligente nella tutela e nella protezione. Non solo questo ha determinato un grave ritardo dello sviluppo di tecnologie e piattaforme competitive europee rispetto al contesto più liberale prevalente negli Stati Uniti, ma si sta rivelando sempre più inadeguato non solo a livello di sicurezza privata, ma anche per quanto riguarda la flessibilità e la capacità di rispondere tempestivamente alle minacce emergenti da

paesi autoritari. Invece di insistere su una visione monopolistica e burocratica della gestione dei dati personali, che mostra continui segni di inefficienza, è giunto il momento di considerare una nuova prospettiva: attribuire maggiore responsabilità ai cittadini, dando loro la libertà di scegliere quale operatore affidare la tutela dei propri dati personali.

L'introduzione di un quadro regolatorio basato sulla concorrenza tra fornitori di servizi di sicurezza digitale autorizzati potrebbe aprire la strada a una gestione più efficiente e innovativa dei dati personali, seguendo un modello simile a quello applicato originariamente nella definizione dell'architettura di Spid o, più genericamente, delle assicurazioni sanitarie private rispetto al monopolio pubblico della sanità. In questo contesto, i cittadini avrebbero la possibilità di selezionare operatori di cybersecurity qualificati e autorizzati a livello europeo, capaci di offrire servizi su misura e in linea con gli standard di mercato più elevati, colmando il vuoto lasciato da uno stato che, come dimostrano le inchieste come quella di Milano, ammette di essere costantemente in ritardo rispetto alla sofisticazione tecnologica degli hacker.

L'attuale modello di gestione dei dati personali, incentrato sul monopolio statale e sul controllo centralizzato, oltre a creare una vulnerabilità sistemica ("single point of failure") facilmente sfruttabile da parte dei criminali informatici, disincentiva anche la competizione e l'innovazione. Nella cultura burocratica e monopolistica delle istituzioni pubbliche, infatti, l'agilità e la reattività, caratteristiche essenziali per contrastare le minacce cyber, sono troppo spesso insufficienti. La mancata possibilità di scelta, inoltre, induce nei cittadini passività e carenza di consapevolezza sui rischi, riducendone la capacità di orientarsi verso servizi più efficaci, adattabili alle proprie esigenze e capaci di rispondere tempestivamente alle minacce emergenti.

Va quindi discussa un'architettura più avanzata e resiliente per la tutela dei dati, nella quale i cittadini devono avere la facoltà di selezionare tra vari operatori di sicurezza digitale autorizzati, ciascuno con differenti livelli di servizio e politiche di gestione del rischio. Gli operatori accreditati, sottoposti a rigorose verifiche di conformità e certificazione da parte di enti di regolamentazione europei, avrebbero l'incentivo a investire continuamente in nuove tecnologie di protezione e in metodologie di gestione dati avanzate, per attrarre e fidelizzare la clientela.

Un mercato concorrenziale di operatori di sicurezza digitale non solo stimolerebbe la crescita e l'innovazione, ma favorirebbe anche lo sviluppo di tecnologie e procedure sempre più avanzate per garantire la protezione dei dati personali. Gli operatori di cybersecurity, infatti, avrebbero un incentivo economico a migliorare costantemente le proprie offerte, per distinguersi dai competitor e guadagnare la fiducia dei cittadini. La trasparenza delle pratiche di gestione, inoltre, costituirebbe un ulteriore elemento di attrattiva per i cittadini, che potrebbero scegliere con maggiore consapevolezza, sulla base

di criteri di sicurezza e costi-benefici, quale operatore sia più adeguato a tutelare le proprie informazioni personali.

Per rendere operativa questa proposta, l'Unione europea dovrebbe creare un quadro regolatorio che stabilisca le linee guida per l'accreditamento degli operatori di cybersecurity per la gestione di dati personali di natura pubblica, contribuendo in tal modo a far nascere il tanto annunciato ma mai effettivamente realizzato mercato unico digitale. L'accreditamento sarebbe basato su criteri rigorosi di trasparenza, competenza tecnica, standard di sicurezza e rispetto della privacy, e includerebbe ispezioni periodiche e controlli di conformità. Potrebbero essere offerti servizi di assicurazione contro il furto di dati, pacchetti personalizzati di monitoraggio e consulenze mirate alla prevenzione delle violazioni, in modo che ciascun cittadino possa scegliere il livello di protezione più adatto alle proprie necessità.

Il nuovo modello di gestione proposto comporterebbe la fine dell'illusione dello stato onnipresente e unico custode dei dati personali. Un sistema monopolistico come quello attuale non è in tutta evidenza in grado di garantire la sicurezza dei cittadini in un'epoca di costante evoluzione tecnologica, in cui le minacce mutano rapidamente e richiedono risposte dinamiche e flessibili. Il passaggio a un mercato competitivo, supervisionato da regole e accreditamenti specifici, restituirebbe al cittadino il controllo sulla sicurezza dei propri dati, promuovendo una cultura di autonomia e responsabilità individuale.

Questa evoluzione normativa richiederebbe una campagna di sensibilizzazione e informazione, per educare i cittadini sui vantaggi della gestione autonoma dei propri dati e sulle opportunità offerte dal mercato della cybersecurity. In un sistema aperto e concorrenziale, ogni cittadino diventerebbe un attore attivo nel mercato della sicurezza digitale, libero di valutare e scegliere l'operatore che ritiene più efficiente e innovativo. Questo nuovo modello non solo contribuirebbe a creare un ambiente più sicuro, ma anche a stimolare l'innovazione, l'efficienza e l'adattabilità – caratteristiche che sono sempre più essenziali in un mondo digitale in rapida evoluzione. Non basta lanciare messaggi allarmistici sulla violazione dei dati personali e invocare maggiori controlli o perseguire il panpenalismo inventandosi nuovi reati informatici: consapevolezza, concorrenza e innovazione sanno essere molto più efficaci del burocratico paternalismo statale.