LUISS

La Pubblica amministrazione e la sfida delle piattaforme digitali

di Paolo Spagnoletti
Professore di Digital Business and Workplace Technology, Luiss

Policy Brief n. 03/2021

Cosa accomuna un sito web d'incontri, una biglietteria online e un sistema pubblico di incentivi messo in campo con gli sforzi della Pubblica amministrazione di uno Stato sovrano? Apparentemente poco se si trascura il fatto che, per poter funzionare, tutti e tre i sistemi necessitano di infrastrutture affidabili per la gestione di dati e il coinvolgimento degli utenti. Esaminando meglio queste realtà, collocandole in un ecosistema economico e sociale sempre più spesso popolato da piattaforme digitali, e mettendo a fuoco i rispettivi punti di rottura, in questo Policy Brief scopriremo che per evitare un futuro distopico non troppo remoto occorrerà bilanciare benefici e rischi del digitale soprattutto nelle aree di confine tra pubblico e privato, lì dove la minaccia cyber si insinua e spesso sfugge ai tradizionali meccanismi di controllo. Una nuova sfida anche per la Pubblica amministrazione italiana.

15 luglio 2015. *AshleyMadison.com*, sito web di incontri per persone sposate, annuncia di aver subito un attacco informatico senza precedenti. Un gruppo di hacker, che si fa chiamare "The Impact Team", chiede all'azienda canadese di cancellare l'intero sito web. Di fronte al rifiuto che gli viene opposto, gli hacker pubblicano online i dati degli utenti registrati al sito: nomi, indirizzi, e-mail, numeri di telefono, gusti e preferenze sessuali di circa 35 milioni di persone sparse in 50 Paesi nel mondo. L'affidabilità del sito e dell'azienda che lo controlla è fortemente compromessa. Non solo. Le cronache dell'epoca parlano di decine di casi di ricatto: cybercriminali che chiedono migliaia di dollari per non rivelare informazioni sugli utenti più facoltosi. Almeno due, inoltre, i suicidi accertati come conseguenza della pubblicazione online dei dati sensibili. Senza contare i casi di divorzio. Infine alcune persone, residenti in Paesi in cui l'adulterio è un reato punibile con la pena di morte – un migliaio le utenze hackerate in Arabia Saudita –, sono spinte a chiedere asilo politico all'estero.

23 giugno 2018. *Ticketmaster*, società americana specializzata nella vendita e nella distribuzione di biglietti per grandi eventi, comunica a tutti gli utenti di aver individuato una falla nel proprio sistema di *customer service*. Un problema che riguarda meno del 5% dei clienti del gruppo, precisano subito da *Ticketmaster*. Si tratta di una magra consolazione, però, per gli 11 milioni e mezzo di clienti coinvolti tra i 230 milioni complessivi del colosso. Trafugati – tra le altre cose – nomi, indirizzi fisici e-mail, dati delle carte di credito. Nelle ore successive, solo l'istituto di credito inglese Barclays Bank registra 60.000 pagamenti irregolari, fatti a nome di correntisti ignari di tutto. Migliaia, nelle settimane successive, le carte di credito da sostituire. *Ticketmaster* si è difesa scaricando ogni responsabilità su un software di Chatbot, progettato per simulare una conversazione con uno dei nuovi numerosissimi clienti, creato da una società esterna, *Ibenta*, e presto rimosso.

Sono soltanto due episodi, tra centinaia avvenuti negli ultimi anni, in cui attori malevoli hanno messo in luce certe criticità dell'"economia delle piattaforme". Si tratta di due casi riferibili al mondo privato dell'economia, tuttavia contengono lezioni potenzialmente utili per il settore pubblico, compresa la Pubblica amministrazione italiana. Infatti **la cosiddetta *platformization* (o *piattaformizzazione*) dell'economia e della società contemporanea è cominciata e si è diffusa innanzitutto nel mondo privato, ma il fenomeno coinvolge sempre più spesso la PA**. Anche nel pubblico, quindi, se da una parte crescono quantità e qualità dei servizi offerti grazie alle piattaforme, dall'altra si palesano enormi rischi di nuova generazione. La PA italiana ne è sufficientemente consapevole?

Cos'è la "piattaformizzazione" dell'economia globale

Cosa si intende, prima di tutto, per "platformization" o "piattaformizzazione" dell'economia e della società? Per citare un saggio scritto dagli influenti studiosi Panos Constantinides, Ola Henfridsson e Geoffrey G. Parker, "quelle che definiamo 'piattaforme

digitali' sono un insieme di risorse digitali – inclusi servizi e contenuti – che rendono possibili interazioni tra produttori e consumatori esterni, interazioni che creano valore. Riteniamo simili piattaforme diverse dalle piattaforme di prodotto, come quelle presenti nel settore *automotive*. La piattaforma digitale di per sé non detiene necessariamente *asset* fisici nella forma di infrastrutture fisiche, né genera valore attraverso la vendita di prodotti. Nei modelli tipo Airbnb la piattaforma ha poco in comune con i vecchi modelli di catena del valore lineare per lo sviluppo di prodotto. Piuttosto essa è riconducibile a un modello di funzionamento che enfatizza interazioni fondamentali tra partecipanti alla piattaforma, inclusi consumatori, produttori e attori terzi. In altri casi, come per MacOS, iOS, watchOS e tvOS di Apple, le piattaforme digitali consentono la creazione di un potente ecosistema d'innovazione. Nei due esempi citati, le piattaforme mostrano di avere regole costitutive e di governance che cercano di bilanciare il controllo della piattaforma e i necessari incentivi per i partecipanti alla piattaforma ad impegnarsi sulla piattaforma e a generare valore l'uno per l'altro".

Piattaforme digitali e PA, il caso (virtuoso) di SPID e Cashback

La presenza di piattaforme digitali nella nostra economia è sempre più pervasiva. Anche perché, solo per rimanere ai casi da cui siamo partiti, alle piattaforme digitali sono associate per esempio "esternalità positive di rete", cioè la possibilità – come nel caso di *AshleyMadison.com* – di vedere aumentare il valore di un servizio offerto all'aumentare del numero di utenti coinvolti. Oppure perché, come dimostra l'esperienza di *Ticketmaster*, le potenzialità dell'e-commerce vengono ampliate dalla creazione di vere e proprie community online. Dinamiche di questo tipo sono sfruttate sempre più spesso anche nel settore pubblico. Si pensi per esempio allo SPID, Sistema Pubblico d'Identità Digitale, di cui si è tornati a parlare nelle ultime settimane sulla scorta di nuove iniziative come il Cashback. Attraverso lo SPID, "puoi accedere ai servizi online della pubblica amministrazione e dei privati aderenti, con una coppia di credenziali (username e password) personali". In base al progetto iniziale, ancora lungi dall'essere pienamente realizzato, con lo SPID si dovrebbe creare uno scenario caratterizzato da pochi "gestori di identità abilitanti" (per esempio Poste o Tim) e da molti *service provider* – sia pubblici sia privati – che consentono agli utenti di accedere ai loro servizi ricorrendo allo stesso SPID. I service provider privati, potendo ridurre i costi legati a una identificazione certa e univoca dei loro clienti, e potendo offrire così a questi ultimi un accesso più rapido e conveniente ai servizi, sarebbero di conseguenza disposti a pagare una "fee" ai gestori di identità. Fino al gennaio di un anno fa, a più di tre anni dal lancio dell'iniziativa, erano solo 5 milioni le identità SPID erogate nel nostro Paese; in 12 mesi, complici la pandemia e alcune popolari iniziative come il Cashback, le identità assegnate hanno superato quota 16 milioni. Ecco dunque una massa critica che potrebbe finalmente dare vita a "esternalità di rete" positive tipiche di una piattaforma digitale, in questo caso imperniata su una struttura pubblica. I potenziali e numerosi vantaggi sono solo in parte immaginabili. Un primo vantaggio indiscusso è determinato dal fatto che il Governo ha deciso di ricorrere per la prima volta

a una App per smartphone per attuare una politica di incentivi all'uso dei pagamenti elettronici, influenzando il comportamento dei cittadini-consumatori. L'App fa leva sulle logiche del digitale per rendere il ricorso al Cashback accessibile senza troppe complicazioni a milioni di residenti nel Paese e comunica direttamente con i sistemi degli operatori convenzionati per il calcolo di bonus e incentivi. La scelta di affidarsi a una soluzione interamente digitale ha evitato il ricorso alla ennesima "Carta nazionale di servizi", con annessi costi e tempi di adozione sicuramente non trascurabili. Infine questo metodo offre la possibilità, in futuro, di integrare o aggiungere servizi "in corsa" alla stessa App, magari attraverso pochissimi clic.

Piattaforme digitali e PA, i nuovi potenziali rischi da considerare

Continuando a riflettere su SPID e Cashback, va detto che ai potenziali e numerosi vantaggi della piattaforma digitale, però, sono associati anche potenziali e numerosi rischi di nuova generazione. L'esempio di AshleyMadison.com fa riflettere su possibili implicazioni per la privacy. Si pensi solo a cosa potrebbe accadere nel caso siano intercettati illegalmente e poi diffusi su internet i dati di reddito e i comportamenti di consumo di milioni di Italiani: possiamo davvero escludere cause, divorzi, suicidi e altre conseguenze dirompenti per le vite di tanti di noi? Mentre il caso di *Ticketmaster* ci ricorda come le piattaforme digitali, specie nel momento in cui hanno successo, diventano strutturalmente più esposte ad attacchi esterni, tra cui tentativi di hackeraggio finalizzati alla frode. Vediamo perché. *Ticketmaster* ha visto crescere a dismisura il numero dei suoi utenti in poco tempo; non avendo *in house* le capacità tecnologiche e le risorse umane necessarie per gestire una crescita così impetuosa, l'azienda si è affidata a un soggetto esterno – il gruppo *Ibenta* – che ha prodotto e fornito accesso al software di Chatbot "incriminato". Tra i punti di forza della rivoluzione digitale e del modello delle piattaforme, infatti, c'è proprio la possibilità di "agganciare" specifiche capacità tecnologiche di attori terzi, consentendo in pochissimo tempo di metterle al servizio di una piattaforma esistente che ne avesse bisogno. Quando però si aggiungono "moduli" esterni a una piattaforma esistente, ecco che si creano aree di confine tra piattaforma e moduli che possono essere caratterizzate da regole diverse e standard di sicurezza meno stringenti. Nel caso dell'hackeraggio ai danni di *Ticketmaster*, infatti, il gruppo *Ibenta* ha subito respinto al mittente le accuse, imputando a *Ticketmaster* di aver inserito alcune righe di codice all'insaputa del fornitore del software di Chatbot e di aver inficiato così la sicurezza di tutto il sistema. In definitiva, nel caso in esame, a non aver funzionato è stata proprio l'interfaccia tra piattaforma e modulo aggiuntivo. Si tratta di un fenomeno sempre più frequente nell'economia delle piattaforme digitali. A maggior ragione nel settore pubblico, in cui più spesso potrebbe sorgere la necessità di "agganciare" applicazioni esterne, è da mettere in conto una potenziale vulnerabilità delle interfacce. Il sistema può mostrare dunque falle che non sono dovute alla capacità del fornitore, né alla scarsa solidità del sistema legacy esistente, ma a fragilità che si manifestano proprio nel punto di contatto tra cosiddetto *heavyweight IT* e *lightweight IT*. Di fronte alla crescita tumultuosa

dell'iniziativa del Cashback, o all'ipotesi di estensione del servizio tramite ulteriori futuri "moduli", possiamo davvero escludere scenari simili a quelli visti nei casi AshleyMadison.com e *Tickermaster*? Impossibile.
Nel nuovo mondo delle piattaforme digitali c'è un altro fattore ancora da considerare: la crescita esponenziale di utenti e transazioni che avvengono su una piattaforma di successo non può che attirare la criminalità organizzata, oppure attori malevoli sponsorizzati magari da governi stranieri interessati a carpire informazioni o a colpire credibilità e incisività di un'azienda di un altro Paese.

Quali competenze e strategie per la PA ai tempi dell'economia delle piattaforme?

In definitiva, da una parte la complessità crescente dei sistemi, dall'altra la presenza di attori malevoli sempre più agguerriti, permettono di dire con certezza che prima o poi un incidente alle piattaforme digitali gestite della PA avverrà, esattamente come accade per centinaia di gestori privati di piattaforme. Come limitare l'impatto di attacchi del genere? In questa sede, ci limitiamo per il momento ad alcune indicazioni generali e di metodo. Nella Pubblica amministrazione italiana, non manca una tradizione di sviluppatori informatici di alto livello. Si può anzi essere piuttosto fiduciosi del fatto che nelle principali branche della nostra PA ci siano le professionalità e le competenze necessarie per una progettazione di piattaforme digitali improntate al principio cardine della security by design. Tuttavia, come emerso dai casi esaminati finora, l'artefatto digitale contemporaneo assomiglia sempre meno a un "monolite". Il suo successo, piuttosto, dipende dalla capacità di funzionare in simbiosi con altri artefatti digitali. Assieme alle possibilità di successo, però, crescono i rischi. Più un sistema è dinamico e distribuito, più i percorsi potenzialmente critici aumentano. Detto in altre parole: considerata la fragilità delle "interfacce" tra piattaforme e "moduli" esterni forniti da soggetti terzi, occorreranno meccanismi di governance e controllo alternativi rispetto a quelli classici. Il concetto (un po' abusato) di "resilienza" va aggiornato al tempo delle piattaforme digitali. Nel perimetro della PA si dovrà investire di più sulla capacità di proteggere infrastrutture e dati allo stesso tempo, andando anche al di là degli steccati delle singole amministrazioni se l'obiettivo è tutelare una intera piattaforma. Inoltre, alle capacità tecniche vanno affiancate capacità organizzative di risposta rapida, sempre trasversali alle singole amministrazioni. Una risposta rapida consiste naturalmente nella tempestiva individuazione dell'incidente e nella soluzione del danno subito. Essa comporta anche la capacità di comunicare efficacemente quanto accaduto, per rassicurare gli utenti, per tutelare allo stesso tempo il buon nome e dunque l'attrattività di società partecipate strategiche che fossero state vittime di attacchi, insomma per non aggravare con un danno d'immagine l'agibilità futura delle piattaforme della PA.

LUISS

Per approfondire, leggi anche:

Paolo Spagnoletti, Andrea Resca, Gwanhoo Lee, "**A Design Theory for Digital Platforms Supporting Online Communities: A Multiple Case Study**", Journal of Information Technology, 2015: https://journals.sagepub.com/doi/abs/10.1057/jit.2014.37

"**Così le autostrade dell'informazione digitale rivoluzionano le nostre vite. Intervista a Panos Constantinides**", Luiss Open, 2017: https://open.luiss.it/2017/11/13/cosi-le-autostrade-dellinformazione-digitale-rivoluzionano-le-nostre-vite-intervista-a-panos-constantinides