

- Luiss Open - <https://open.luiss.it> -

Nella pubblica amministrazione è a rischio la privacy degli utenti. La perdita di controllo sui dati è un pericolo reale

Rischi e benefici delle piattaforme digitali

Cosa accomuna un sito d'incontri, una biglietteria online e un sistema pubblico di incentivi? Apparentemente poco se si trascura il fatto che per poter funzionare i tre sistemi necessitano di infrastrutture affidabili per la gestione di dati e il coinvolgimento degli utenti. Guardando però più a fondo queste realtà e mettendo a fuoco i rispettivi punti di rottura 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** in cui la minaccia cyber si insinua e che spesso sfuggono ai tradizionali meccanismi di controllo. Negli ultimi anni abbiamo assistito a centinaia di centinaia di data breach, in cui attori malevoli hanno messo in luce le criticità dell' "economia delle piattaforme". **I data breach interessano spesso il mondo privato dell'economia**, tuttavia contengono lezioni potenzialmente utili per il settore pubblico, compresa la Pubblica amministrazione italiana. Anche nel pubblico, quindi, se da una parte crescono la quantità e la qualità dei servizi offerti grazie alle piattaforme, dall'altra si palesano pure enormi rischi di nuova generazione. La PA italiana ne è sufficientemente consapevole?

Perdita di controllo sui dati e rischio di violazioni

Per rispondere a questa domanda prendiamo in esame i casi di due data breach che hanno coinvolto un sito di incontri e un servizio online per la vendita di biglietti per eventi mettendo in evidenza le condizioni esterne e organizzative in cui gli incidenti si sono manifestati, nonché gli effetti da essi causati. Nel primo caso, un gruppo di **hacker pubblica online i dati degli utenti registrati** al sito di incontri dedicato a persone sposate: nomi, indirizzi, e-mail, numeri di telefono, gusti e preferenze sessuali di circa 35 milioni di persone sparse in 50 Paesi nel mondo. Le cronache 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, sono spinte a chiedere asilo politico all'estero. Nel secondo caso, sono stati trafugati i dati di 11 milioni di clienti, **inclusi i dati delle carte di credito** con conseguenti danni economici e di immagine per l'azienda e per una società esterna, fornitrice di servizi software, specializzato in soluzioni Chatbot basate su intelligenza artificiale. Il primo caso mette in luce gli effetti drammatici che la perdita di controllo sui dati e la conseguente violazione della privacy degli utenti può avere in regimi non democratici o in presenza di attori con **finalità estorsive**. Il secondo caso aiuta invece a capire che il controllo di una piattaforma risponde a logiche diverse rispetto a quelle della normale protezione di asset fisici nei processi aziendali. Entrambi i casi mostrano inoltre che nel nuovo mondo delle piattaforme digitali c'è un altro fattore 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.

Security by design

Per rispondere alla nostra domanda di partenza e comprendere il nesso con i servizi della PA, proponiamo un approfondimento sul concetto di piattaforma digitale, sempre più popolare anche nelle iniziative dalla PA che intende sfruttarne i vantaggi in termini di quantità di utenti e possibilità di influenzarne i comportamenti. L'esperienza di SPID e Cashback fornisce un esempio di queste dinamiche virtuose ma ci spinge anche a riflettere sul tema del rischio cyber e degli strumenti organizzativi e tecnologici di cui occorre dotarsi per prepararsi a rispondere. 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, i nuovi servizi digitali sono erogati da piattaforme che assomigliano sempre meno a "monoliti" da recitare. Il loro successo, piuttosto, dipende dalla capacità di funzionare in simbiosi con altri servizi 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.

Proteggere le infrastrutture

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.

Il presente articolo si basa sul policy brief 3/2021 con lo stesso titolo, School of government, Luiss.

Article printed from Luiss Open: <https://open.luiss.it>

URL to article: <https://open.luiss.it/2021/02/05/nella-pubblica-amministrazione-e-a-rischio-la-privacy-degli-utenti-la-perdita-di-controllo-sui-dati-e-un-pericolo-reale/>

Copyright © 2020 Luiss Open. All rights reserved.