Perché dovrei preoccuparmi della self-sovereign identity, se sono un’azienda o un cittadino?

Author : Efrem Zugnaz

Date : 24 Giugno 2020

Cominciamo dal principio: la *self-sovereign identity* è un principio, prima che una tecnologia. Un principio basato sul concetto di **identità digitale**.
L’identità digitale, che dovrebbe essere parte della cultura comune nel mondo odierno, ci rappresenta in tutti i possibili contesti pubblici, privati e ricreativi.

Recentemente si vedono molti articoli tecnologici legati alla *“self-sovereign identity”* ma purtroppo sfugge ai più, che traducono troppo frettolosamente gli articoli anglo-americani, il concetto filosofico che sta alla base.

Il ragionamento tecnologico dietro al tema *mainstream* è di solito la Blockchain, ma già nel 2017, molte organizzazioni e associazioni[1] ne parlavano come estensione e attuazione del principio sotteso al dover controllare molteplici identità digitali.

Già più di dieci anni prima, Kaliya Hamlin e altri autori si ponevano il problema della **multi-identità su Internet**. Ma perché solo oggi la gestione delle multi-identità online è così difficile da affrontare?

La risposta è: perché continuiamo a ragionare come nel mondo fisico.

Qui nascono i **primi problemi**, *come posso gestire la multi identità se non l’ho compresa? Come posso dire subito che la Blockchain è la soluzione senza analizzare il contesto?*

Partiamo già dall’assunto che non vogliamo semplificare il problema, ma gestirlo *as-is*, con la migliore tecnologia disponibile sul mercato. La verità è che abbiamo fatto molti progressi sui sistemi di identità online, ma abbiamo peggiorato la complessità e specialmente **peggiorato la percezione degli utenti**.

Le persone in generale, le aziende, le scuole, le istituzioni, trattano l’identità digitale come un account.

La prima considerazione è che tradizionalmente viene confusa l'identità digitale con l'account, che possiamo considerare invece un semplice schema utente / password per accedere - tipicamente - a un servizio.

Oggi il paradigma è un po' più complesso perché si aggiungono, allo schema dell'account, i dati degli utenti.
Dati che cambiano la loro dimensione e funzione nel tempo; e questo non è poco.

Costruire l'identità digitale, per la maggior parte delle aziende, si è tradotto nel creare gli account con vecchie concezioni su nuovi servizi, tra tutti il telelavoro e la telescuola post emergenza. Dispositivi mobili e nuovi servizi dei social media ci hanno fornito sistemi di identità molto più sofisticati, flessibili, che non sempre proteggono la privacy e non sempre sono compresi dall'utente. Eppure siamo ancora molto lontani da un sistema di identità per Internet, che funziona ancora in una modalità diversa e non deve essere confuso con la logica della Blockchain.

Internet è stato progettato per consentire a qualsiasi macchina di inviare messaggi a qualsiasi altra macchina senza il permesso dell'autorità amministrativa.
E questo non lo dobbiamo dimenticare.

Se genero dati che non controllo, e qualcuno comincia a comunicarli, in base alla programmazione ricevuta, allora debbo pormi domande non solo tecnologiche ma culturali.

La *self-sovereign identity* gestisce un sistema di identità simile a Internet ma dovrebbe consentire a qualsiasi persona di organizzare e gestire le relazioni di identità reclamando, cancellando e gestendo i dati **senza necessità di autorizzazione** da parte di qualcun altro. Capiamo fin da subito che se i dati sono posseduti dalle aziende o dai privati le cose cambiano. Non comprendere le clausole o i dati coinvolti da parte dell'utente appare un problema evidente.

Andiamo per gradi. Prima degli utenti è importante che istituzioni e aziende capiscano il concetto, perché i *Major Brand* lo hanno capito benissimo. Internet è stato costruito senza un modo standard ed esplicito per identificare persone o organizzazioni, quindi i siti web hanno semplicemente iniziato a offrire i propri account locali con nomi utente e password, e questa è stata la soluzione predominante. Le aziende hanno fatto lo stesso. Internet, la scuola, le aziende, le società sportive, si sono espansi enormemente e le persone hanno iniziato a usare sempre più servizi integrati ogni giorno. Questo approccio basato su silos, in cui gli utenti devono mantenere le identità per ogni sito con cui interagiscono, è diventato insostenibile. Non è solo un disastro di usabilità per gli individui, ma crea anche **una moltitudine di *honeypot* di dati** per gli hacker, la cui violazione compromette la fiducia in tutti. La cultura sarà la chiave.

Le aziende hanno cercato di collegare diversi silos di identità in vari modi e li hanno federati con utenti inconsapevoli (o quasi) della gestione dei propri dati e soprattutto dei termini e condizioni di utilizzo degli account (es. Facebook).

Questa **mancanza di cultura** ha prodotto effetti collaterali involontari, concentrando il controllo

su un numero limitato di fornitori, aumentando la perdita di dati e soprattutto la condivisione involontaria.

Ovviamente andrebbero sviluppate anche tutte le tematiche sulla privacy ma la considerazione certa è che, ad oggi, l'utente non ha la percezione del vero controllo.

Allo stesso tempo si aggiunga l'inefficienza economica delle organizzazioni e delle istituzioni che devono raccogliere, archiviare e proteggere i dati personali nei propri silos, andando avanti così sarà possibile raggiungere un punto di non ritorno, pensando per esempio al **diritto all'oblio** o al collasso delle risorse tecnologiche.

Senza porre condizioni minime di **sostenibilità digitale** delle soluzioni proposte non si coglie il vero senso della sovranità dei dati da parte dell'utente. La politica, le aziende e le istituzioni come anche la scuola non devono abdicare alle proprie responsabilità delegando questioni strategiche ad un'armata di tecnici o commerciali con la soluzione tecnologica salvifica, ma collaborare con essi per trovare il giusto equilibrio.

Lo sforzo per comprenderci è imprescindibile, compreso quello di capire intimamente la Blockchain, non proclamandola come una sorta di panacea tecnologica. Altrimenti il risultato sarà che il dibattito, partendo da domande sbagliate, finirà con il produrre risposte sbagliate. Comprendere l'intimo legame che intercorre tra dati dell'utente, privacy e tecnologia è diventato urgente, irrinunciabile.

Diverso sarebbe stato chiedersi come evitare la diffusione incontrollata dei dati, agevolando comunque il telelavoro senza delegare la responsabilità all'utente, ma piuttosto coinvolgendolo.

Non è socialmente sostenibile una compressione dei diritti fondamentali dell'individuo che arrivi a concepire un sistema atto a restituire all'utente la sovranità dei propri dati, senza una seria differenza ontologica tra enti tecnologici ed Essere, senza determinare l'«oblio» dell'Essere. Essere i nostri dati è il punto focale, non scegliere una tecnologia.
Come ci ricorda Heidegger**[2]**:

> *«L'essenza più profonda della tecnica non è nulla di tecnico».*

Se ci si fosse fatti la domanda corretta, sarebbe emerso già da tempo che **la soluzione per tutelare la l'identità dell'utenti e i loro relativi dati esiste, ma non può basarsi solamente sulla centralizzazione dei dati**.
La Blockchain aiuta ma il concetto di *self sovereign identity* non è da confondersi con la tecnologia stessa, e **la tecnologia non è la soluzione ai problemi etici**.

Il concetto che le informazioni del cittadino sono e restano nelle mani del cittadino è chiaro. Per le aziende ed i dati dei dipendenti il problema è evidentemente più complesso. Account privati (es. Google e WhatsApp) usati nelle aziende complicano, in maniera esponenziale, il problema.

Quindi, se ad un problema complesso aggiungo l'eterogeneità degli account, ottengo un

grande pasticcio se gli utenti non fanno la loro parte. Ecco perché tutti dovrebbero interessarsi al concetto di *self sovereign identity.*

Le tecnologie esistono già. Ma per usarle bene è necessario porsi la domanda giusta.

La creazione di identità dei 7.599.259[3] studenti, di diversi milioni di lavoratori, associazioni sportive, enti di formazione che hanno creato identità digitali con account Google, Microsoft, Zoom, Cisco etc. durante l'emergenza sanitaria dovranno essere gestite o cancellate nei prossimi anni.

La mente è uno strumento prezioso ma è, per sua natura, "separatista"; analizziamo il particolare e non teniamo presente il tutto.

Questo è il centro del problema: siamo a un punto molto interessanrte della storia ed è necessario trovare nuove vie per aprirsi a un pensiero di più ampio respiro. La rivoluzione digitale è una cosa meravigliosa anche perché ci pone delle domande difficili, inaspettate. Le aziende tecnologiche ci aiutano ma dobbiamo prendere coscienza del tutto, senza dimenticarci anche della **sicurezza informatica**.

Capito cosa dobbiamo diventare, poi sarà più facile farlo con la tecnologia giusta.
Queste suggestioni servono per focalizzare un punto di analisi e alimentare il relativo dibattito. Le risorse delle aziende vanno indirizzate a proteggere le identità digitali degli utenti, guardando più in là. Cosa succederebbe se le identità digitali venissero gestite da uno Stato straniero o da un'azienda concorrente? Coinvolgere l'utente è la chiave, con la cultura. C'è bisogno della collaborazione di tutti.

> Non esiste democrazia senza un *demos* e **un *demos* non esiste senza un'aggregazione di senso**, che deve essere chiaro, comune e condiviso; e in questo caso si tratta di un *demos* di identità digitali.

In conclusione, con i dati *self-sovereign*, i vostri dati digitali saranno, in linea teorica, di vostra proprietà e controllati da voi. Le piattaforme non controlleranno i vostri dati, ma dovrete imparare a leggere i contratti. Le aziende dovranno capire i concetti degli oggetti descrittori DID (DDO) e quello delle chiavi pubbliche e private, nonché del funzionamento del registro condiviso. La condivisione degli identificatori digitali sarà possibile attraverso l'infrastruttura a chiave pubblica e l'archiviazione attraverso il *ledger* distribuito. Ma le aziende saranno pronte ad integrarlo nei propri sistemi di autenticazione? Da DPO dico anche che la cancellazione dei dati sarà a carico del titolare se l'utente capisse di avere un diritto. Più semplice sarebbe avere **un approccio *privacy-oriented*** - *by design* e *by default* - risolvendo la tematica chiedendosi di chi sia la titolarità sui dati. Porsi queste domande dovrà diventare una prassi, una pratica quotidiana che l'utente e le aziende dovranno apprendere. E per questo servirà Cultura.

Note

[1] https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf

[2] M. Heidegger, *La questione della tecnica*, trad. it. in Saggi e discorsi, Mursia, 1976

[3] https://bit.ly/2nLNHgI

Articolo a cura di **Efrem Zugnaz**