Audizione Commissione parlamentare di vigilanza sull'anagrafe tributaria
Indagine conoscitiva "Digitalizzazione e interoperabilità delle banche dati fiscali"
Audito: Fabrizio d'Amore

Roma, 10 novembre 2021

Egregi onorevoli, rispettati colleghi,
porgo loro i miei saluti. Desidero ringraziare la Commissione per questa opportunità.

Sono docente in Sapienza dall'inizio degli anni '90 e mi sono sempre occupato di informatica teorica ed algoritmica. Da circa dieci anni mi occupo anche di sicurezza e privacy.
È dai tempi delle famose "leggi Bassanini" che sento parlare di digitalizzazione, semplificazione e firma digitale; tuttavia, quello a cui ho potuto assistere non era esattamente in linea con le tematiche menzionate. Tutto diveniva continuamente più complesso, burocratico, nella cultura del sospetto, e la penetrazione della firma digitale piuttosto scarsa.
Gli accademici che studiano la cybersecurity sono spesso impegnati sul fronte della ricerca, che si posiziona su temi estremamente specialistici. La digitalizzazione, nonché l'associata sicurezza, sono invece temi già noti da almeno un ventennio, che per un motivo o l'altro sono stati applicati/sviluppati maldestramente: è mia opinione che esistano potenzialità ancora smisurate legate a una digitalizzazione applicata correttamente e un insieme di operatori non impreparato ad essa. In altre parole, vedo un importante efficientamento della P.A., di cui si è potuto intravedere piccoli esempi a causa della presenza della pandemia, ovvero di un'importante motivazione; quasi forse che l'efficientamento della P.A. non lo fosse. E che tutto avvenga all'insegna della sicurezza permette di assicurare velocità, ridurre errori e costi.
Da ciò derivano due temi fondamentali, egualmente validi nel mondo pubblico e privato:

a) la dirigenza deve governare l'informatica e definire politiche di governance in maniera corretta ed oculata, legate alle finalità per cui i processi sono destinati;
b) gli operatori debbono usare consapevolmente gli strumenti informatici, nel rispetto delle politiche assegnate.

In generale appare irrinunciabile non gestire la sicurezza e la privacy attraverso un approccio strutturato e corretto. È nota l'esistenza di due famiglie di attacchi informatici: quelli "a pioggia" (per il solo fatto di essere raggiungibili da Internet) e quelli mirati (in cui il bersaglio è unico e precisamente individuato).
Semplificando, ci si difende abbastanza bene dai primi, con una corretta igiene della sicurezza (che richiede, quindi, formazione), mentre i secondi sono efficaci e micidiali. Io credo che potrebbe esserci una svolta in termini di efficientamento anche solo preparandosi ai primi, mentre è assai impegnativo difendersi dai secondi, e si può decidere di farlo solo in casi molto importanti, se non critici.
Non sono favorevole a regole stringenti e severe sull'uso delle password: a mio avviso, oltre a favorire comportamenti insicuri, si osserva un danno economico associato al tempo necessario a ritrovare una password, o rigenerarla (tale danno andrebbe sommato per tutti i casi che si verificano in un periodo); danno superiore ai benefici ottenuti dall'incremento di sicurezza delle password nello stesso periodo. Il tema può essere sviluppato nell'ambito dell'igiene della sicurezza.
Sono favorevole alla sicurezza e alla privacy "by design", piuttosto che "by patching" per ragioni di flessibilità, scalabilità e applicabilità, senza perdere di vista i vantaggi economici.

Per le stesse ragioni tali obiettivi dovrebbero essere raggiunti attraverso un approccio il più possibile aperto: non è un caso, ad esempio, che il più usato metodo di cifratura dell'informazione – ancora sicuro – sia stato proposto dall'americano NIST (il National Institute of Standards and Technologies propose l'Advanced Encryption Standard come metodo standard di cifratura dell'informazione – AES – nel 2001, https://www.nist.gov/publications/advanced-encryption-standard-aes) in modalità open-source, per cui una comunità mondiale di dimensioni ragguardevoli l'ha studiata (e testata) per oltre un ventennio, potendo ottenere la consapevolezza che la sicurezza del metodo deriva dalla sola segretezza della chiave. Ciò in opposizione alla "security-by-obscurity", assai più onerosa, vista la platea ridotta di tester e il fatto che ci si trovi a dover modificare continuamente parametri e chiavi.
Tale argomento non è irrilevante e trova immediatamente applicazione nell'odierna discussione relativa al cloud per la P.A. Una proposta emersa da soggetti autorevoli ha menzionato l'uso di un metodo di cifratura nazionale, ma si può replicare con due osservazioni:

1) Per raggiungere il livello di sicurezza pari a quello che oggi si può avere già disponibile, ed open-source, occorrono anni, se non decenni
2) Lo standard oggi disponibile, trascurando vari altri esempi di qualità, è l'AES, proposto dal NIST, che è stato testato ed attaccato da venti anni ed è noto per la sua robustezza.[1]

Ciò posto, appare irragionevole la proposta di un metodo di cifratura nazionale, per i suoi tempi e per le risorse necessarie (pur disponendo di ottimi crittografi sul territorio nazionale). Appare molto più promettente lo studio/analisi di come applicare i requisiti della sicurezza delle informazioni (i requisiti CIA, oltre a non-ripudio, autenticazione e accounting) ai dati trattati: quali categorie di informazione ne sono interessate e come farlo? È un quesito a cui si risponde dando un giusto riscontro al punto a) di cui sopra, relativo alla governance della sicurezza. Sottovalutare ciò conduce a disastri annunciati.
Ed una volta identificati alcuni dati da cifrare, quali soluzioni pratiche occorre adottare? Questa è una questione tecnica, per cui non è sufficiente scegliere un buon metodo, ma bisogna domandarsi se la cifratura vada fatta a livello di file system, di DBMS o a livello utente. Inoltre, appare cruciale la politica di gestione della chiave, unica informazione che necessita di essere mantenuta segreta.
Piuttosto che discutere di quali cloud (italiani, europei, extra-europei) convenga utilizzare, occorrerebbe individuare servizi cloud, di adeguato livello certificato, in cui la gestione delle chiavi di cifratura venga lasciata all'utente, così che l'intervento di una Stato straniero che cerchi di violare i dati risulti vano e la gestione delle normali operazioni di ricerca testo vengano fatte attraverso la crittografia omomorfica.[2]
L'unica ragione per cui appare preferibile l'uso di un cloud nazionale/europeo è il requisito di *disponibilità* dei dati (il terzo dei requisiti CIA): questo onde prevenire la possibilità che uno stato straniero possa bloccare l'accesso ai dati, rendendoli inarrivabili.
L'altra questione, vedi punto b), è legata alla disomogeneità e alla scarsezza della cultura di base informatica, che includa una alfabetizzazione sulla sicurezza, limiti che occorre superare in maniera netta e totale, facendo dimenticare il passato, a costo di dover affrontare possibili crisi sindacali. La formazione, differente da quella necessaria per il punto a), appare l'unico strumento viabile, non affidandola "a casaccio" ma a persone che, più depositarie di competenza tecnica,

[1] Ciò è noto alla comunità accademica mondiale, mentre l'ipotesi che qualcuno sia in possesso di un metodo pratico per violarne la cifratura, senza essere in possesso della chiave, appare inverosimile oltre che mantenuta assolutamente segreta negli ultimi venti anni. Ed anche ammettendo che tale soggetto esista, solo entità con le capacità di uno Stato potrebbero permettersi tali apparati.
[2] V., ad esempio, https://it.wikipedia.org/wiki/Crittografia_omomorfica

siano didatticamente esperte e valide, perché gli argomenti in questione sono disciplinarmente di base, piuttosto che avanzati.

Grazie a tutti.