Privacy e Sicurezza

La tutela della libertà individuale nell'era digitale

🇮🇹 **ITALIANO – Italo Svevo e la libertà interiore: Zeno Cosini nell'era della sorveglianza**

Il romanzo *La coscienza di Zeno* di Italo Svevo è un capolavoro della letteratura introspettiva e anticipa, con sorprendente attualità, molti temi dell'era digitale.

Zeno Cosini è un uomo tormentato dalla propria coscienza, incapace di agire con coerenza. Scrive un diario sotto indicazione del suo psicanalista, credendo che l'autoanalisi lo porterà alla guarigione. Ma in realtà, **non trova risposte**, solo nuove domande. Vive una vita osservata, giudicata, non dagli altri ma da se stesso, in una spirale di **auto-sorveglianza mentale**.

Questo senso di osservazione costante, che Svevo descrive sul piano interiore e psicologico, è perfettamente parallelo alla **sorveglianza esterna** di oggi.

Oggi, non è solo la coscienza a giudicarci, ma un sistema invisibile fatto di algoritmi, dati e piattaforme digitali. Ogni post pubblicato, ogni like, ogni ricerca diventa **tracciabile**. Come Zeno, anche noi ci raccontiamo bugie: pensiamo di essere liberi, ma siamo **condizionati da modelli digitali che ci profilano**.

Il diario di Zeno era privato, intimo. Oggi i nostri diari sono pubblici, condivisi con milioni di persone – o peggio, con aziende e governi. La nostra **libertà interiore è compromessa** non da una malattia, ma da un sistema di controllo sistemico, algoritmico, digitale.

Svevo ci invita a riflettere: **quanto di ciò che facciamo è davvero nostro, e quanto è già stato calcolato da qualcun altro?**

📜 **STORIA – Dalla sorveglianza totalitaria alla sorveglianza invisibile**

Nel Novecento, i regimi totalitari hanno fatto della **sorveglianza una strategia di potere**.

In Germania nazista, la Gestapo raccoglieva informazioni su dissidenti e oppositori politici. In Unione Sovietica, il KGB controllava ogni aspetto della vita dei cittadini. In Germania Est, la **Stasi** aveva un numero impressionante di informatori: quasi 1 su 3 tra la popolazione adulta. Ogni parola, ogni gesto, ogni relazione era potenzialmente **una minaccia alla sicurezza dello Stato**.

L'effetto psicologico era devastante: **la paura del controllo generava autocensura**, conformismo, perdita di fiducia perfino nei propri familiari. Questo sistema non si basava solo sulla forza, ma su una forma perversa di **controllo sociale e mentale**.

Oggi la sorveglianza è cambiata. Non è più visibile, ma è ovunque. Ogni volta che usiamo uno smartphone, un social network o facciamo una ricerca su Google, **lasciamo tracce digitali**. Le grandi aziende raccolgono questi dati, li aggregano, li vendono. Non c'è bisogno di un poliziotto: è l'algoritmo a sapere chi siamo.

Ma c'è un paradosso: mentre nei regimi totalitari la sorveglianza era imposta con la forza, **oggi la accettiamo volontariamente**, in cambio di servizi, comodità, connessione. Ed è proprio questo che la rende ancora più pericolosa: **non ci accorgiamo nemmeno di essere controllati**.

🇬🇧 **INGLESE – Cryptography

Cryptography is the study and practice of hiding information so that only those having a special knowledge can read and process it.

It means scrambling a plaintext into cipher text through a process called encryption and then back again through decryption.

Encryption is the process of transforming information using an algorithm or cipher to make it unreadable to anyone except those possessing a special knowledge (called *key*). The result is encrypted data.

Decryption is the opposite process and takes place when the key is used to convert the data back into its original form.

There are two types of cryptography according to the type of key:

- **Asymmetrical Cryptography** is a system using a pair of related keys. Any person can encrypt a message using the public key, but only the holder of the private key can decrypt the message;
- **Symmetrical Cryptography** is a system that uses the same key for encryption and decryption. The keys may be identical or just slightly different.

Digital signatures are an example of public key cryptography. In fact, a message signed with the sender's private key can be verified by anyone who has access to the sender's public key.

Modern cryptography has four objectives:

1. **Confidentiality**: the information cannot be understood by people for whom it was not intended;
2. **Integrity**: the information cannot be altered;
3. **Non-repudiation**: the creator or sender of the information cannot deny at a later stage his/her intentions in the creation or transmission of the information;
4. **Authentication**: the sender and the receiver can confirm each other's identity.

🌐 **SISTEMI E RETI – VPN, Proxy, Firewall: strumenti di tutela (e controllo)**

Nella sicurezza delle reti, strumenti come **VPN**, **Proxy** e **Firewall** sono fondamentali per gestire **privacy e accesso**.

- Una **VPN** (Virtual Private Network) crea un tunnel criptato tra l'utente e il server, **nascondendo l'indirizzo IP** e proteggendo i dati da occhi esterni. È molto usata per **evitare censure**, proteggere identità e **navigare in modo anonimo**.
- Un **Proxy** agisce da intermediario tra client e server, e può essere usato sia per proteggere la navigazione sia per **filtrare contenuti**, diventando uno strumento di controllo (es. in scuole o paesi autoritari).
- Un **Firewall** protegge la rete da accessi non autorizzati, ma può anche **limitare la libertà** se usato per censurare.

Questi strumenti sono ambivalenti: **possono difendere la libertà o limitarla**. Dipende da **chi li usa e con quale scopo**.

Un utente consapevole può usarli per tutelarsi. Ma uno Stato può usarli per **sorvegliare e filtrare**, come abbiamo visto nel "Great Firewall" cinese.

💾 **INFORMATICA – GRANT e REVOKE: chi decide cosa puoi fare?**

Nel mondo dei database, i comandi **GRANT** e **REVOKE** servono per **assegnare o revocare permessi** a utenti e ruoli. Questi meccanismi di accesso sono fondamentali per la sicurezza: impediscono che chiunque possa modificare, leggere o cancellare dati.

Ma possono essere letti anche in modo più ampio: **chi controlla i permessi ha il potere**. In un sistema informatico, questo è l'amministratore. Ma nel mondo reale? Chi decide quali informazioni puoi leggere? Quali diritti hai su ciò che produci online?

Oggi molte piattaforme non permettono nemmeno di **cancellare completamente i propri dati**. L'utente non ha un vero controllo: può usare il sistema, ma non modificarlo.

Questo squilibrio è il cuore del problema della **libertà digitale**: se non possiamo decidere cosa fare dei nostri dati, non siamo davvero liberi.

TPSIT – Privacy e sicurezza nei progetti software

Nel processo di **ingegneria del software**, uno dei momenti più delicati è la **definizione dei requisiti non funzionali**, tra cui rientrano **privacy, sicurezza e integrità**.

Un software ben progettato deve:

- garantire **l'accesso solo agli utenti autorizzati**,
- **cifrare i dati sensibili**,
- rispettare **la normativa GDPR**,

- e applicare il **principio del minimo privilegio**, secondo cui ogni utente ha accesso solo a ciò che strettamente gli serve.

Ma spesso, per motivi commerciali, si scelgono **scorciatoie pericolose**: tracciamento invasivo, raccolta eccessiva di dati, assenza di cifratura. In questo modo, il software diventa **uno strumento di sorveglianza**.

Il programmatore ha quindi una **responsabilità etica**, non solo tecnica. Progettare sistemi sicuri significa **difendere la libertà individuale** degli utenti. Non farlo può trasformare un servizio utile in **un'arma di controllo invisibile**.

📊 GESTIONE – Sicurezza aziendale, GDPR e libertà individuale

Nel contesto aziendale, **la sicurezza delle informazioni** è oggi uno degli aspetti più delicati. Le imprese raccolgono enormi quantità di **dati personali**: dai CV dei dipendenti, alle mail, agli accessi badge, fino ai dati sanitari.

Se questi dati venissero rubati o usati male, si metterebbe a rischio **non solo l'organizzazione, ma anche la dignità e la libertà** delle persone coinvolte.

Per questo l'Unione Europea ha introdotto il **Regolamento Generale sulla Protezione dei Dati (GDPR)**, in vigore dal 2018.

Le aziende devono:

- ottenere **consenso esplicito** per il trattamento dei dati,
- garantire il **diritto all'oblio**,
- nominare un **Data Protection Officer**,
- e soprattutto, **evitare trattamenti eccessivi o non giustificati**.

Ma la realtà è che spesso le aziende installano software che **monitorano ogni azione del lavoratore**, analizzano le sue performance in modo automatizzato, e **archiviano dati sensibili** anche senza motivo.

Qui nasce il problema etico: **dove finisce la tutela dell'azienda e dove inizia la violazione della persona?**

La libertà individuale non è un ostacolo alla sicurezza, è **la sua condizione essenziale**. Solo rispettando la privacy si può costruire una cultura aziendale sana, sostenibile e giusta.