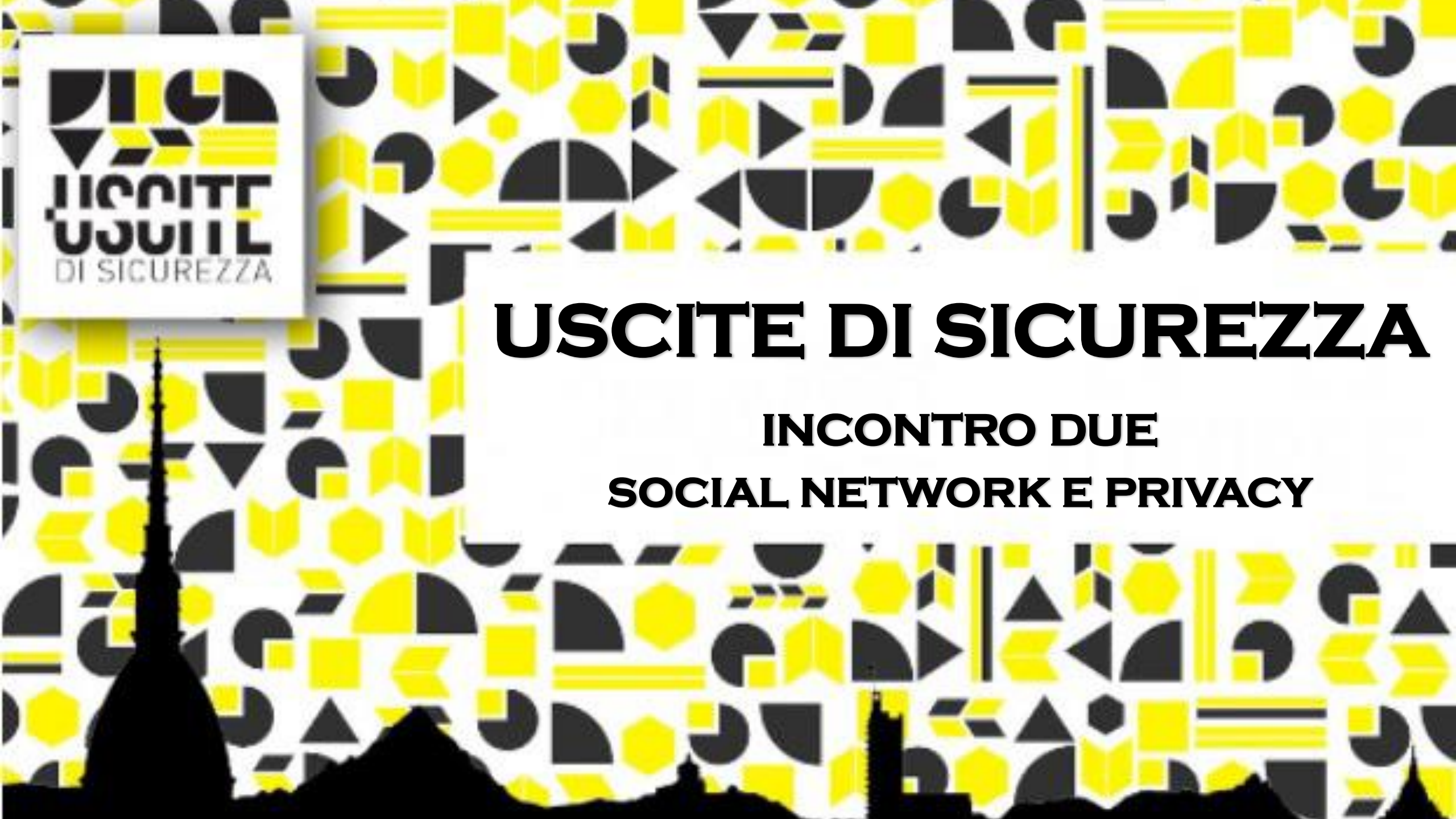
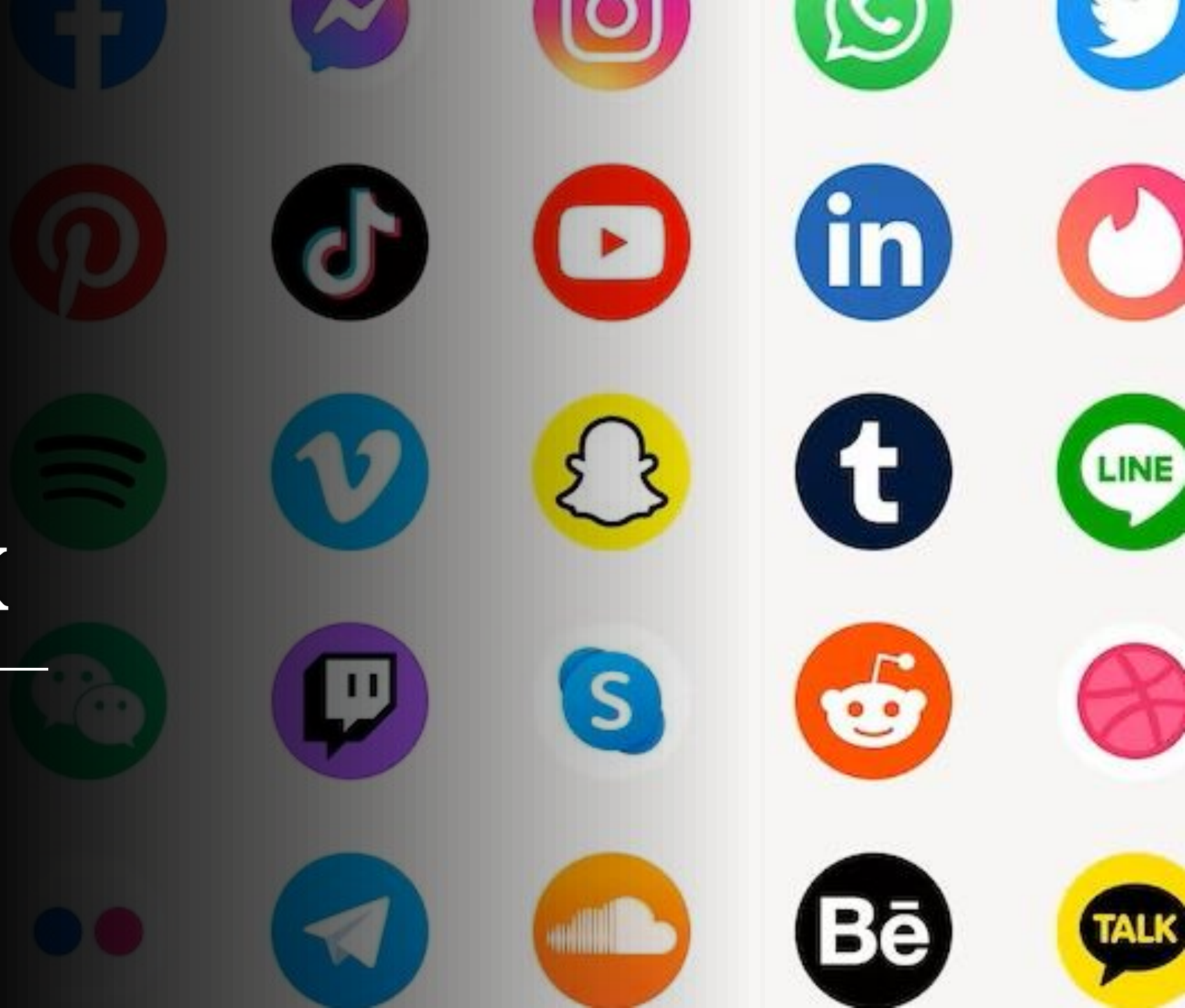


USCITE DI SICUREZZA

INCONTRO DUE

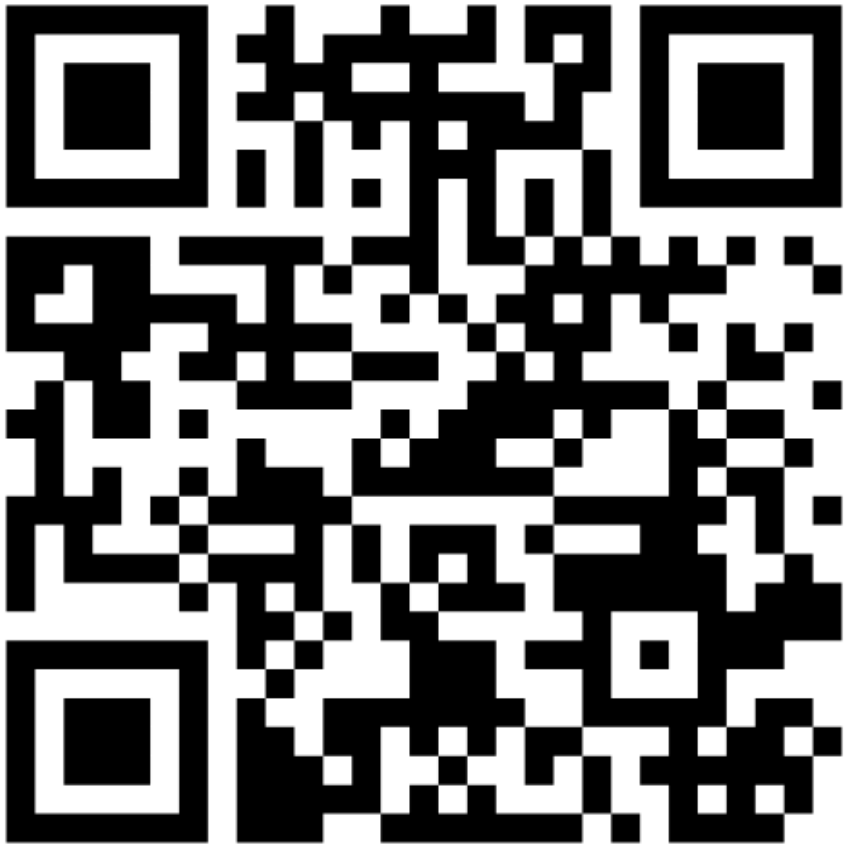
SOCIAL NETWORK E PRIVACY

SOCIAL NETWORK



SHARE, POST E BUONE MANIERE

INQUADRA IL QR CODE O VAI AL LINK:



https://www.menti.com/albk1qa6u75n

SOCIAL NETWORK

INQUADRA IL QR CODE O VAI AL LINK:

https://www.menti.com/aljc3jygdbwp

SOCIAL NETWORK
PRO E CONTRO

PRO

- Trovare persone attraverso nome o mail, riducendo la distanza geografica;
- Pubblicare e condividere contenuti;
- Diffondere le proprie opinioni molto rapidamente;
- Diffondere viralmente temi importanti, come una campagna di sensibilizzazione o la richiesta di aiuto;
- Aiutare e persone isolate a sentirsi meno sole.

CONTRO

- Trovare persone attraverso nome o mail, se non si hanno buone intenzioni;
- Pubblicare e condividere contenuti senza averne verificato la veridicità o se sono offensivi;
- Diffondere le proprie opinioni molto rapidamente, se queste comportano danni a terze persone;
- Diffondere viralmente temi importanti, come una campagna di sensibilizzazione o la richiesta di aiuto, se i contenuti non sono verificati rischiando di contribuire alla diffusione di truffe o bufale;
- Aiutare e persone isolate a sentirsi meno sole, se queste vengono circuite da malintenzionati.

Le medesime caratteristiche positive e utili possono essere lette anche in una prospettiva completamente diversa, creando spesso conseguenze dannose e addirittura pericolose per le persone.

IL WEB NON DIMENTICA

Tutto ciò che pubblicate o condividete online potrebbe rimanere per sempre, non essere più cancellabile e potrebbe influenzare la vostra **reputazione digitale,** la quale, a sua volta, avrà **conseguenze** nel mondo reale.

L'insieme di percezioni e opinioni condivise su un **soggetto**, come una persona, un'azienda o un prodotto, derivanti dalle **conversazioni** e **informazioni** pubblicate **sul web**, capaci di **influenzare l'utente** che naviga sui motori di ricerca e sui social media.

IL WEB NON DIMENTICA

Tutto ciò che pubblicate o condividete online potrebbe rimanere per sempre, non essere più cancellabile e potrebbe influenzare la vostra **reputazione digitale,** la quale, a sua volta, avrà **conseguenze** nel mondo reale.

Aziende e organizzazioni raccolgono e analizzano **dati su di voi** online per scopi di marketing o di profilazione.
Questi dati potrebbero essere utilizzati per **inviarvi pubblicità mirata** o per **prendere decisioni su di voi**, come il **rifiuto di una richiesta di prestito o di lavoro.**

Ad esempio, un **datore di lavoro** può cercare il vostro nome online prima di assumervi e, se trova **post o commenti inappropriati** o controversi, può decidere di **non assumervi**.

IL WEB NON DIMENTICA

Tutto ciò che pubblicate o condividete online potrebbe rimanere per sempre, non essere più cancellabile e potrebbe influenzare la vostra **reputazione digitale,** la quale, a sua volta, avrà **conseguenze** nel mondo reale.

Il fatto che le cose non vengano mai dimenticate online potrebbe comportare anche **rischi** per la vostra **privacy e sicurezza**.

Ad esempio, **se condividete** online **informazioni personali o sensibili**, come il vostro indirizzo di casa o il vostro numero di telefono, queste potrebbero essere **raccolte** da persone malintenzionate e **utilizzate per scopi illeciti**, come il **furto di identità**.

IL DIRITTO ALL'OBLIO

Come si è visto, in un'epoca in cui le informazioni possono rimanere online per sempre e avere conseguenze negative sulla vita di una persona, il **diritto all'oblio** è diventato particolarmente importante.

Concetto importante per la **tutela della privacy** e della **reputazione online.**

Un individuo ha il diritto di richiedere la **rimozione** di **informazioni personali** o sensibili che sono **obsolete**, **inaccurate**, **inappropriatamente pubblicate** o **non più rilevanti**.

Il **diritto all'oblio** è stato riconosciuto in Europa dalla **Corte di Giustizia dell'Unione Europea** nel **2014** e ha portato all'introduzione del **GDPR**, il Regolamento Generale sulla Protezione dei Dati, che garantisce alle persone il diritto di richiedere la rimozione di alcune tipologie di informazioni personali.

PER USARE I SOCIAL AL MEGLIO…

…E’ importante essere **consapevoli** di ciò che **condividete online** e di **adottare pratiche sicure** per **proteggere** la vostra **privacy** e la vostra **sicurezza online**.

Questo include:

- L'utilizzo di **password forti**;
- L'attivazione della **verifica in due passaggi** sui servizi online;
- L'utilizzo di **strumenti di crittografia;**
- La **limitazione** delle **informazioni personali** che condividete online.

PER USARE I SOCIAL AL MEGLIO…

- **Non** usarli per offendere e discriminare gli altri;
- **Non** condividere contenuti offensivi o che ledano la privacy altrui;
- **Non** pensare di conoscere una persona solo per aver visto il suo profilo;
- **Segnalare** immediatamente al social network o alla polizia postale eventuali furti di profilo o altri fenomeni illeciti;
- **Non pubblicare** dati personali di minori o di persone che non siano in grado di difendersi, se non strettamente necessario e comunque con l'autorizzazione dei genitori o delle persone responsabili;
- **Non** diffondere informazioni di cui non conosci la fonte;
- **Ciò che vale nella vita reale, deve valere anche online;**
- **Farsi le domande: «E' necessario che lo pubblichi?» e «Che conseguenze può avere la pubblicazione o la condivisione di tale post?».**

PRIVACY

BLINDATISSIMI?

INQUADRA IL QR CODE O VAI AL LINK:

https://www.menti.com/almihwqh4way

PRIVACY: DIRITTO E OBBLIGO

La **privacy** è un **diritto tutelato** dalla legge.
La dimensione privata di ciascuna persona
non può essere lesa, usata, pubblicata o **diffusa,**
senza l'autorizzazione di quest'ultima;
quando ciò avviene si parla di **violazione della privacy".**
Questo concetto può essere letto da **due prospettive diverse**:

Diritto di essere **difesi** e **tutelati**

Obbligo di rispettare la **privacy** degli altri

PRIVACY: DATI PERSONALI

La questione della **privacy** riguarda il **controllo dei dati personali** e la loro **protezione da possibili accessi non autorizzati**.

L'utilizzo di Internet e dei social media ha generato un ampio dibattito sulla **privacy degli utenti** e sulla **raccolta dei dati personali** da parte delle grandi aziende tecnologiche.

La nostra dimensione privata è, infatti, costituita da:

Dati personali: informazioni che identificano una persona e che forniscono dettagli sulle sue caratteristiche, le abitudini, le relazioni personali, la sua situazione economica, ecc…

Dati identificativi: permettono l'identificazione diretta

Dati sensibili: possono rivelare l'appartenenza etnica, le convinzioni religiose, le opinioni politiche e l'orientamento sessuale

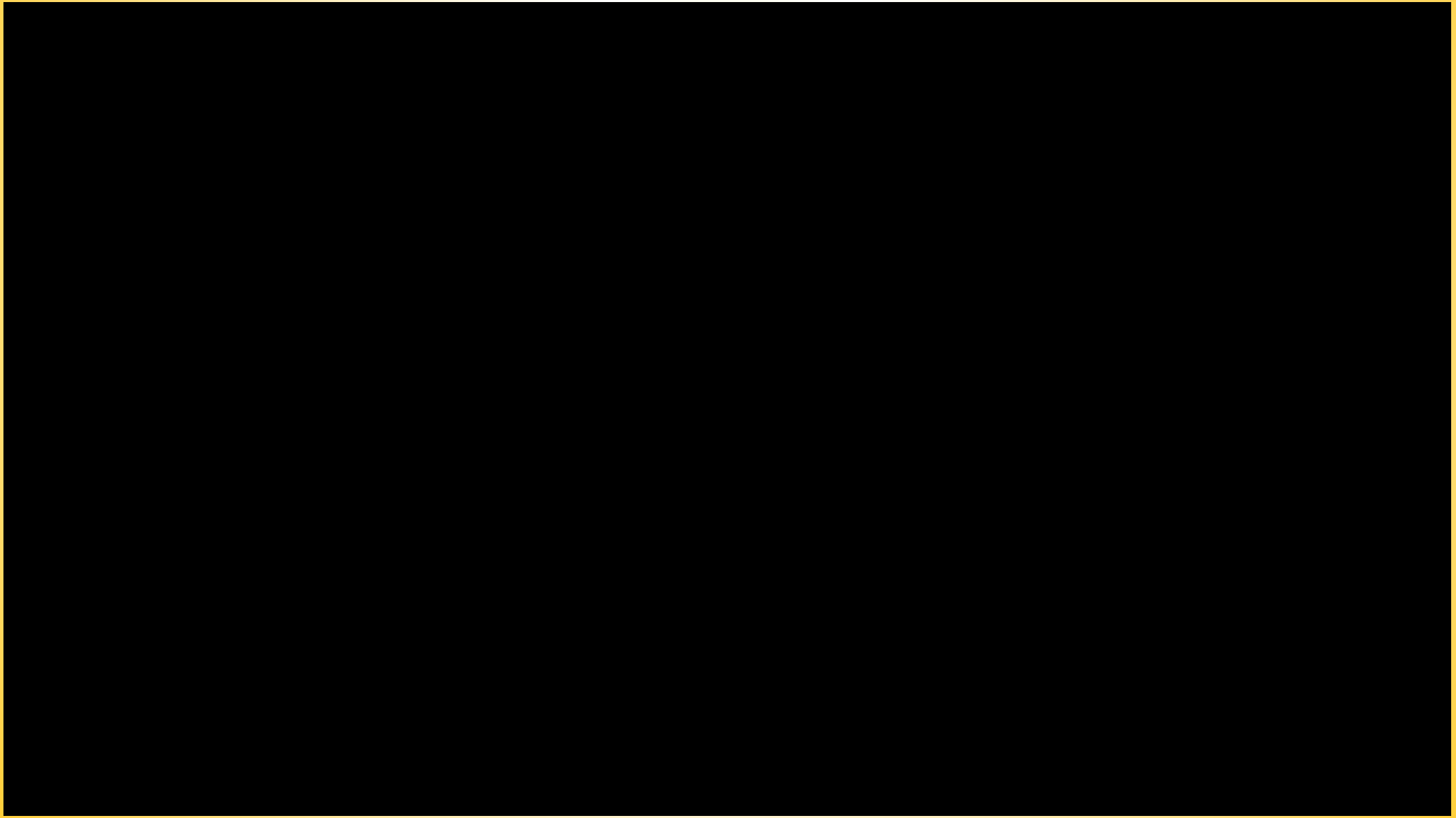
Dati giudiziari

PRIVACY:
TUTELA SUI SOCIAL

- **Evitare** di **pubblicare** i vostri **dati personali** su un profilo-utente;
- E’ meglio **non utilizzare** il vostro **vero nome** in un profilo;
- **Rispettate** la **privacy altrui**. Non pubblicate informazioni personali relative ad altri senza il loro consenso;
- Informatevi su **chi gestisce il servizio** e da quale Paese e se vi sono norme adeguate a tutela della privacy;
- **Limitate** al massimo **la disponibilità** di **informazioni;**
- Utilizzate **identificativi diversi** (login e password) da quelli che utilizzate su altri siti web;
- Mantenete il **controllo** sull'utilizzo dei **vostri dati personali da parte del fornitore del servizio**, ad esempio, rifiutate il consenso all'utilizzo dei dati per attività di marketing.

LA PAROLA ALL'ESPERTO

Vice Questore Assunta Esposito



10 BUONE PRASSI DI SICUREZZA INFORMATICA

1. Cambiare le password predefinite: molte periferiche di rete vengono fornite con password predefinite. Queste sono facilmente scopribili e devono essere cambiate.
2. Aggiornare regolarmente i dispositivi: gli aggiornamenti includono spesso *patch* di sicurezza importanti. Bisogna assicurarsi che tutti i dispositivi siano aggiornati alla versione più recente del *software*.
3. Utilizzare una rete Wi-Fi sicura: utilizzare la crittografia WPA2 per proteggere la rete Wi-Fi. Evitare di utilizzare la crittografia WEP, che è facilmente violabile.
4. Disattivare la connessione automatica alle reti Wi-Fi pubbliche: queste reti sono spesso non sicure e possono esporre i dati a rischio di accesso non autorizzato.
5. Utilizzare software antivirus: per proteggere i dispositivi domestici da *virus* e *malware*.
6. Utilizzare la crittografia: per proteggere i dati sensibili e assicurarsi che le informazioni personali siano sempre criptate quando si inviano o si ricevono.
7. Evitare di condividere informazioni personali online: come numeri di telefono, indirizzi e-mail, informazioni finanziarie o informazioni di login sui social media e sui siti web non affidabili.
8. Fare attenzione alle e-mail di *phishing*: queste cercano di ingannare l'utente a fornire informazioni personali o a cliccare su un link dannoso.
9. Utilizzare un firewall: per proteggere la rete domestica da accessi non autorizzati.
10. Configurare correttamente le impostazioni di *privacy* sui dispositivi: per limitare l'accesso a informazioni personali e sensibili.

USCITE DI SICUREZZA

Per i contenuti si ringrazia:

Fabio C.

Silvio C.

Promosso e finanziato da:

Città di Torino

Progetto realizzato da:

ismel

orso

MAGAZZINI Oz

UTILE PER IL SOCIALE