GIORNATA TIPO

Una mia giornata tipo è caratterizzata da numerose situazioni in cui interagisco con i dati.

Utilizzo i social come IG e FB quotidianamente e condivido varie informazioni, come il mio nome, cognome, data di nascita, indirizzo e-mail e, eventualmente, account collegati. Quando pubblico una storia, condivido dati di geolocalizzazione e indico la mia posizione. Inoltre, quando cerco persone, locali o cose di interesse su Instagram, sto fornendo dati relativi ai miei gusti personali e interessi. Questo consente di personalizzare la mia esperienza utente e per scopi di pubblicità mirata.

Utilizzo Google Maps, condividendo dati come la geolocalizzazione, i dati relativi al mio account Google e i luoghi che visito frequentemente. Quando condivido foto o recensioni dei luoghi che visito tramite il mio profilo, sto fornendo ulteriori dati. Google Maps mi permette di avere informazioni sul traffico, i tempi di percorrenza e i dati relativi ai mezzi pubblici, oltre a informazioni su locali, negozi e luoghi di interesse.

Utilizzo un orologio digitale collegato al telefono tramite app o Bluetooth. Condivido dati personali come la mia frequenza cardiaca, i passi percorsi, la qualità del sonno e, in alcuni casi, anche informazioni mediche come la pressione sanguigna. I dati che utilizzo sono visualizzati in modo grafico sull'app. Penso che i dati relativi alla salute siano dati sensibili che rientrano nelle categorie dei dati protetti dalla privacy.

Quando utilizzo app di messaggistica come WhatsApp e Telegram, condivido messaggi di testo, foto, video, registrazioni vocali, link, documenti e la mia foto del profilo. Inoltre, condivido informazioni come il mio numero di telefono, le informazioni sul dispositivo e i dati relativi all'utilizzo dell'app. Le chat possono contenere numerosi dati, tra cui informazioni personali, conversazioni private, foto e video. Alcuni di questi dati possono essere sensibili a seconda del contesto. Posso essere selettiva su cosa condividere attraverso le chat e utilizzare funzionalità come la crittografia end-to-end per proteggere la privacy delle mie conversazioni.

Quando utilizzo app bancarie per gestire le mie finanze, effettuare transazioni, pagare bollette e tenere traccia delle spese, condivido dati finanziari come il saldo del mio conto, gli estratti conto, le transazioni, i dettagli della carta di credito e le informazioni di contatto. La mia banca raccoglie questi dati per gestire il mio conto, prevenire frodi e fornire assistenza clienti. Tutte queste informazioni finanziarie sono estremamente sensibili e possono essere utilizzate per accedere ai miei fondi e ai miei dettagli personali.

Quando utilizzo un motore di ricerca come Google e visito siti web, condivido informazioni come i dati di ricerca, l'indirizzo IP, i cookie, le pagine visitate e i dati inseriti nei moduli dei siti web (ad esempio, quando compilo un modulo di registrazione). Uso i motori di ricerca per trovare informazioni e servizi online. Questi raccolgono dati per migliorare i risultati delle ricerche e per scopi di pubblicità mirata. I siti web raccolgono dati per personalizzare l'esperienza dell'utente, analizzare il traffico e fornire contenuti mirati. Le ricerche possono rivelare gli interessi personali, e i dati inseriti nei siti web possono includere informazioni personali come il nome, l'indirizzo e-mail e il numero di telefono. Posso utilizzare opzioni di navigazione in incognito o motori di ricerca che rispettano la privacy per ridurre la quantità di dati condivisi.

La condivisione di dati è costante nella vita quotidiana, e penso che sia il contesto a definire se i dati siano più o meno sensibili. Ovviamente ci sono dati come quelli derivati dall'uso di app bancarie che sono molto sensibili. Accettare il trattamento dei dati è diventato così automatico che lo facciamo abitualmente. Di solito, accetto le informative sulla privacy che vengono richieste. È difficile pensare di non condividere dati sensibili, ma le app forniscono anche la possibilità di impostare alcune opzioni, come non attivare la geolocalizzazione o limitarla solo quando utilizzo l'app, non dare l'accesso alla rubrica, alla fotocamera o al microfono.