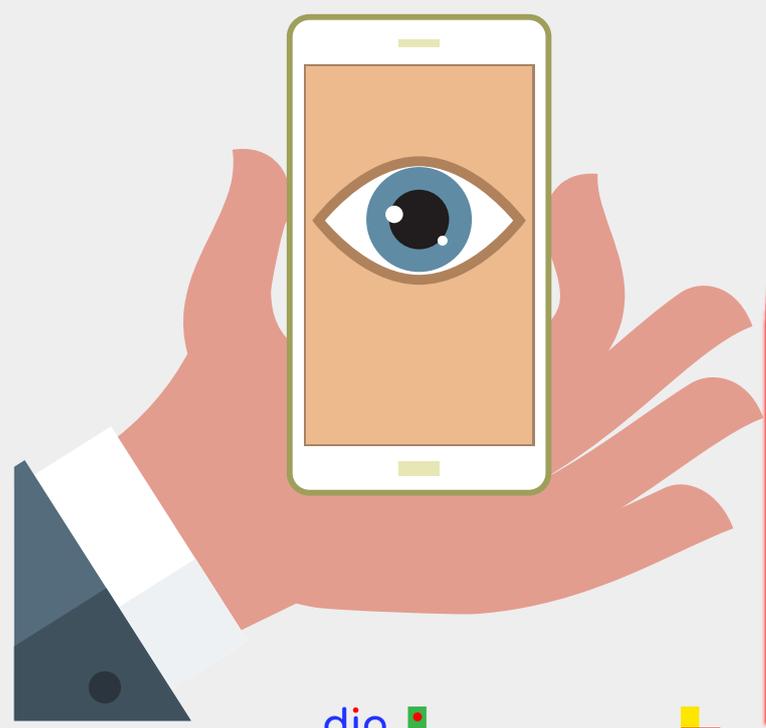




5 consigli per garantire la tua privacy (e quella dei tuoi figli) online

La privacy è un tema caldo da qualche anno a questa parte, anche perché la definizione è cambiata rispetto a qualche lustro fa. Pensaci: quanta gente vedresti scendere in strada inferocita se oggi ci fosse un servizio come la vecchia guida del telefono, quell'enorme tomo che tutti gli anni ricevevano gli abbonati a SIP che includeva nome, cognome, indirizzo e numero di telefono di tutti i residenti, città per città?

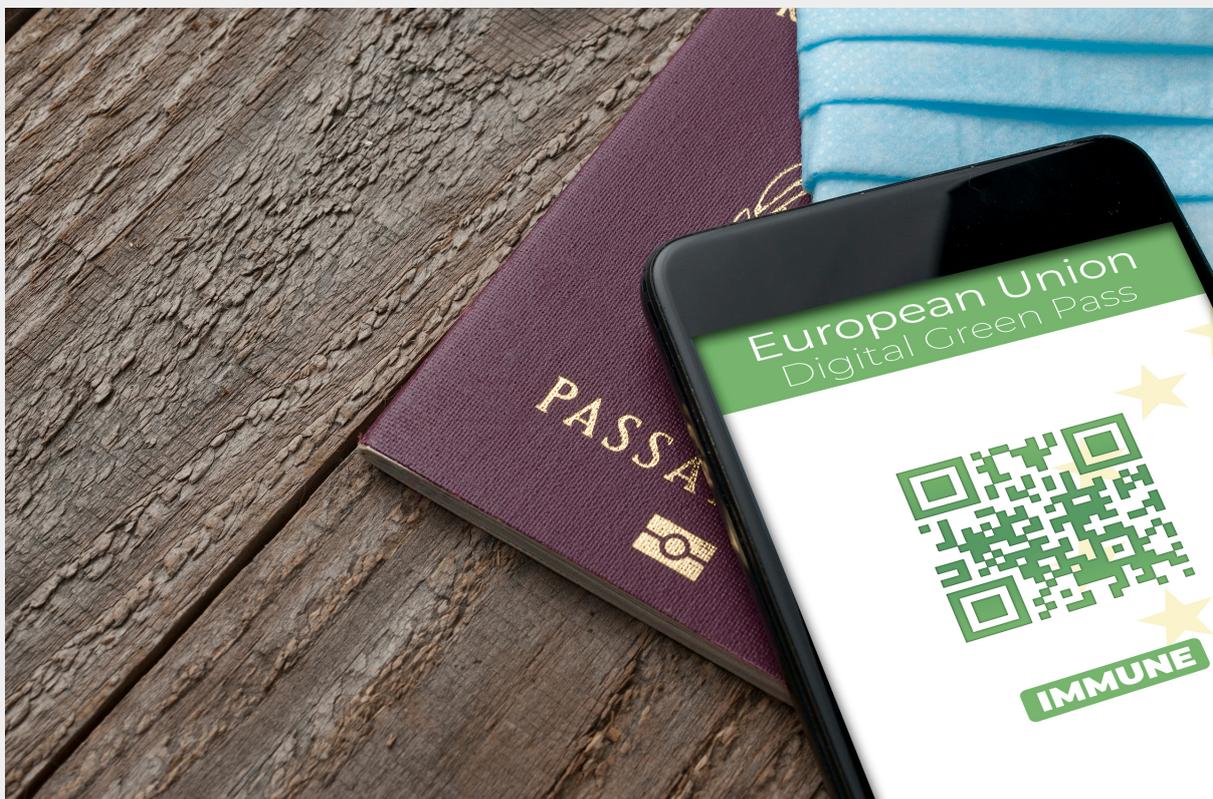


Quello che negli anni 80/90 era la norma oggi sarebbe non solo inaccettabile dal punto di vista etico, ma sarebbe anche sanzionato dalla legge. La cosa che fa sorridere, è che non è da escludere che molte delle persone che si opporrebbero a una tale violazione dei propri dati personali (sì, un numero di telefono, soprattutto se associato a un indirizzo, è un dato personale) abbiano inserito il proprio numero di cellulare in bella vista su Facebook o altri social network. Probabilmente, senza accorgersene.



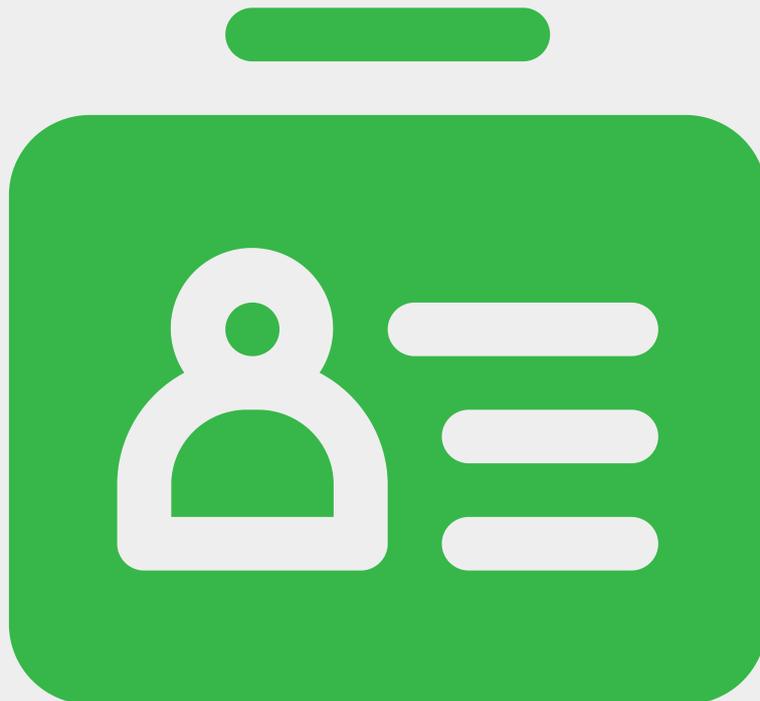
Sia chiaro, è comprensibile. Nell'arco di decenni il concetto di privacy, di dati per modo in cui sono gestiti e trattati è cambiato in maniera radicale e non è semplice comprendere la portata di questa rivoluzione innescata dal digitale. Tanto da poter cadere in facili inganni.

Ti faccio un esempio concreto su un tema molto in voga in questo periodo: il green pass. Per alcuni, esibirlo per entrare al ristorante, al museo o per andare a sciare, è una violazione della privacy. Del resto, stai esponendo a un terzo un dato personale, no? La realtà è che no, non lo stai facendo. Non più di quando lasci un documento per noleggiare un pedalò o lo mostri per prendere una birra in un locale, se sei abbastanza giovane da poter sembrare minorenne.

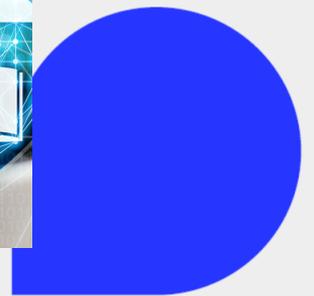




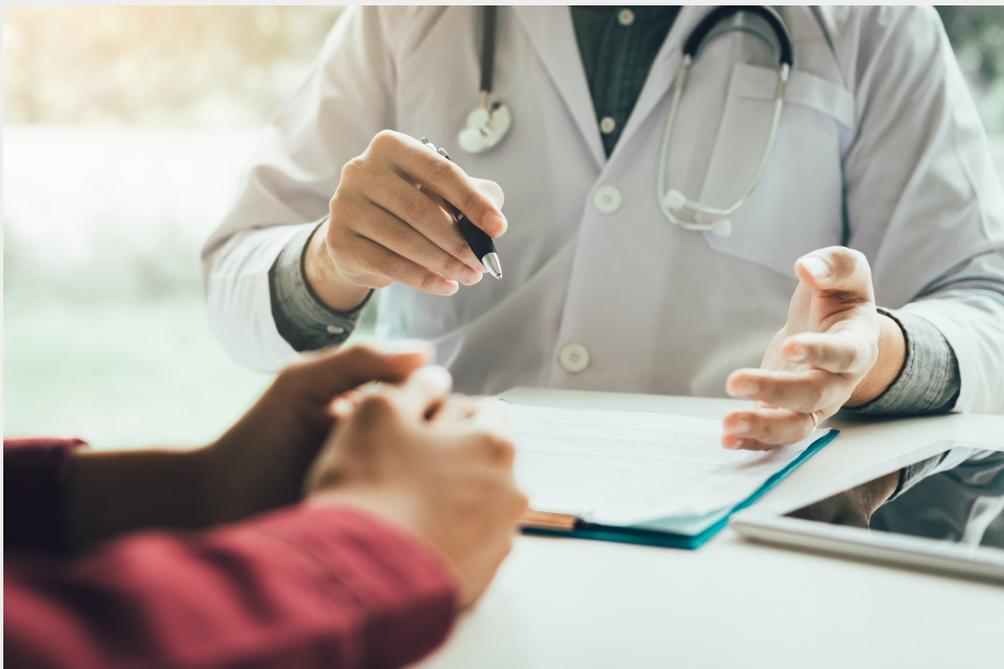
Quando stai mostrando il green pass o il documento al barista, non gli stai “cedendo” un dato: stai solo certificando un’informazione. Che sei vaccinato/hai un tampone positivo nel caso del green pass, o che sei maggiorenne al pub. Il dato non viene registrato né salvato da nessuna parte. Non viene tecnicamente “trattato”. È il motivo per cui se torni 10 volte nello stesso locale in un mese, ti chiederanno (o dovrebbero chiederti) ogni volta di esibire il passaporto vaccinale: questo certificato dice solo sei autorizzato a entrare.



Che lo sia in quanto vaccinato, perché hai fatto il tampone o immune in quando hai già contratto il Covid, non esplicito. Allo stesso modo, chi tiene la tua patente mentre te la spassi sul pedalò, non sta registrando il tuo passaporto su un archivio: lo sta tenendo come garanzia, e quel dato tornerà in tuo possesso non appena riconsegnerai l'imbarcazione. Questo preambolo per farti capire che il problema della privacy non è nel mostrare un dato una singola volta a una persona, autorizzata a farlo in quello specifico frangente.



Il problema è poi come questa persona gestirà quei dati, se li archivia. Quando il dottore ti dà alcuni giorni di malattia, permettendoti di assentarti dal lavoro, il tuo datore di lavoro non sa il motivo. Può trattarsi di una gamba rotta, così come di esami particolari che potrebbero rivelare le tue condizioni di salute. Questi dati sono sensibili, e non a caso li tratta solo il servizio sanitario. L'unico che può insomma far conoscere al tuo datore di lavoro la tua condizione di salute sei tu. E non sei obbligato a farlo, naturalmente.



A meno di attacchi informatici, i tuoi dati sono tendenzialmente al sicuro. Il più grande rischio, però, sei tu. Non è colpa tua, sia chiaro: senza accorgertene, ogni giorno metti a disposizione un sacco di informazioni apparentemente innocue che potrebbero dire un sacco di cose di te o della tua famiglia. E sono due i tipici “errori” fatti dalle persone, di ogni età: il primo è non comprendere a pieno il funzionamento delle opzioni di privacy dei social network.



È quello che accade quando sei convinto di parlare a un gruppo ristretto di persone – amici, famiglia, colleghi – ma in realtà non ti stai rendendo conto che quanto dici è pubblico. Il secondo è quello di trascurare i metadati, quelle informazioni nascoste nei file.



Nel caso di una foto, per esempio, sono l'apertura del diaframma e il tempo di esposizione. Ma anche l'ora e il giorno dello scatto, la posizione GPS, la macchina con cui è stata scattata, e molto altro. Sotto questo profilo, un po' i social ti aiutano, eliminando la maggior parte di queste informazioni. Non è lo stesso se la foto la alleggi a una mail, o la carichi sul tuo blog.



Come evitare questi errori? Ti darò cinque suggerimenti per proteggere meglio la tua privacy e quella della tua famiglia, in particolare quella dei tuoi figli.