GUIDA COMODA IN SITUAZIONI SCOMODE

MANIFESTAZIONE DIGITALE

PERCHÉ UNA GUIDA?

Hai un telefono?
Hai un computer?
Hai una faccia?
Allora questa guida fa per te…!
La tecnologia di serie distopiche come Black Mirrors non è più solo fantascienza: il tuo telefono è ormai tecnologicamente in grado di raccogliere informazioni su di te e su cosa fai, ma anche su chi ti sta accanto.
Il microfono del computer sente quello che dici e archivia i tuoi gusti e preferenze, pronti per essere venduti alle multinazionali o utilizzati per ragioni di sicurezza.
Il telefono riconosce il tuo volto e raccoglie le tue impronte digitali. Tutti questi dati potrebbero essere utilizzati dalle forze dell'ordine nelle loro attività d'indagine, senza alcuna autorizzazione e controllo.

La guida fa per te se tieni a difendere la tua privacy e la tua libertà di manifestare liberamente.

CHI SIAMO

StraLi

StraLi è un'associazione ETS – ODV (Ente del Terzo Settore - Organizzazione di Volontariato) apartitica, aconfessionale, a struttura democratica e senza scopo di lucro che, ispirandosi a finalità civiche, solidaristiche e di utilità sociale, svolge la propria attività nel settore della tutela dei diritti e delle libertà fondamentali attraverso gli strumenti propri della strategic litigation.

Hermes

Il Centro Hermes per la Trasparenza e i Diritti umani Digitali è un'organizzazione italiana per i diritti umani digitali composta da esperti ed esperte di tecnologie, informatica e giornalismo. L'associazione ricerca, promuove e sviluppa consapevolezza e attenzione ai temi della privacy, anonimato, libertà di parola online e, più in generale, alla protezione dei diritti e delle libertà personali in un mondo connesso.

STRALI FOR STRATEGIC LITIGATION

HERMES CENTRO STUDI PER LA TRASPARENZA E I DIRITTI UMANI IN RETE

ISTRUZIONI PER L'USO

Usa questa guida così:

- La guida è strutturata in ordine crescente di situazioni di rischio e di difficoltà;
- Per ogni livello troverai una descrizione della situazione di partenza ed una serie di raccomandazioni;
- Il livello 0 è il livello di base e contiene le norme di "igiene digitale";
- I livelli successivi integrano quelli precedenti.

Avvertenza: l'utilizzo della guida non sostituisce MAI la consulenza di un legale di fiducia.

LIVELLO 0
NORME DI
IGIENE DIGITALE

COME DIFENDERSI DA ATTACCHI ESTERNI E COME CAPIRE SE IL TUO TELEFONO E' STATO INFETTATO

Entry level, rookie, beginner... o semplicemente le norme comportamentali base per evitare che il tuo dispositivo sia infettato o attaccato dall'esterno. Ecco alcune norme di igiene digitale base!

Innanzitutto, ricordati sempre di fare il backup del dispositivo.
In caso di problemi di qualsiasi tipo, saresti in grado di recuperare i tuoi file!

Aggiorna sempre il sistema operativo.
Questo non solo ti fornisce maggiore protezione contro nuovi attacchi, ma potrebbe anche neutralizzare malware già presenti sul tuo sistema.

Proteggi l'accesso ai tuoi account (anche e soprattutto sui social media).
Usa una password complessa (utilizza più di dieci caratteri tra cui anche caratteri speciali e numeri), evita di usare parole comuni o la tua data di nascita. Non usare la stessa password per più siti, applicazioni o servizi. Se ri-utilizzi la stessa password o se ne usi una "debole" esponi i tuoi dati a gravi rischi!

Se possibile, utilizza sempre l'autenticazione a due fattori. Qui puoi trovare una guida su come attivare l'autenticazione a due fattori per diversi servizi e app.

In generale, ricordati di tenere sempre il telefono bloccato mentre non lo usi e mantieni un codice di accesso—per ottenere la massima protezione usa un PIN con almeno 8 cifre.

E' sicuro conservare le mie password su una app?
Le password migliori sono quelle lunghe, complesse, e quindi tendenzialmente più difficili da ricordare. Ci sono alcune applicazioni specifiche che ti permettono di conservare tutte le tue password in un posto sicuro, protette con una master password che solo tu conosci. I dati sono cifrati e senza la master password è impossibile leggere il contenuto. Queste applicazioni si chiamano password manager e ne esistono di diversi tipi: alcune sono incluse ad esempio nei browser che utilizziamo, come il servizio offerto da Google Chrome; o nei dispositivi, come il Portachiavi su iOS; altre invece (come KeePass) permettono di salvare sul proprio computer (o smartphone) le password. Esistono anche password manager a pagamento che permettono di condividere le password con più account e dispositivi, come 1Password.
Bisogna tenere a mente, però, che non esiste la soluzione

perfetta per i bisogni di ogni persona. In alcuni casi, ad esempio, potrebbe essere molto più sicuro avere un quaderno con tutte le password scritte e conservato in casa in un luogo sicuro, piuttosto che salvare le password sul nostro computer con il rischio che ci venga rubato o che noi, sbadatamente, lo perdiamo da qualche parte.

LIVELLO 1 CONSAPEVOLEZZA DIGITALE

COME PARTECIPARE AD UNA MANIFESTAZIONE IN MODO SICURO

Ok, livello successivo, consapevolezza digitale: vuoi partecipare ad una manifestazione pubblica e non vuoi avere problemi.

Andare alla manifestazione
Sicuramente l'utilizzo di un mezzo pubblico, rispetto ad una macchina (sia essa di proprietà o noleggiata), ti permette di evitare che venga registrata la presenza di un veicolo a te collegato nelle vicinanze della manifestazione (anche se tale evenienza è remota, non è da escludersi!).
Al contempo, però, l'uso di un mezzo pubblico ti porta ad essere maggiormente esposto alle telecamere che ormai coprono capillarmente la città o sono installate sui mezzi di trasporto.

Lascia il telefono a casa!
Il massimo della sicurezza sarebbe non avere nessun dispositivo digitale con sé: non si corre il rischio di lasciare tracce digitali della propria presenza a una manifestazione o che il proprio dispositivo venga sequestrato e tutti i dati copiati dalle forze dell'ordine. Chiaramente, portarsi dietro uno smartphone ha anche benefici, è per questo che bisogna sapere come prepararsi prima!

Considera l'acquisto di un "burner phone"
Il burner phone è un telefono muletto da usare temporaneamente che ha pochissime funzionalità e un basso prezzo. Puoi acquistarlo in un negozio di elettronica. Attenzione: avrai comunque bisogno di comprare una sim da inserire nel telefono (a differenza di come avviene negli USA).

Metti il telefono in modalità aereo!
I nostri smartphone comunicano con le celle telefoniche per aggiornare in background le app, e anche per mantenerci raggiungibili nella rete nel caso qualcuno ci voglia chiamare. Questo però fa sì che sia possibile individuare la nostra posizione (c.d. geolocalizzazione o triangolazione del segnale GSM o con le celle): gli smartphone, infatti, parlano costantemente e lasciano tracce su di noi. Mettendo lo smartphone in modalità aereo possiamo proteggerci e ridurre le informazioni sulla nostra posizione.

Full-disk encryption
Quando esci di casa ti ricordi sempre di chiudere a chiave la porta? La full disk encryption (FDE) funziona allo stesso modo, ma è più potente: fai sì che nessuno possa accedere alle informazioni che hai sul dispositivo, senza conoscere la password da te impostata. Nei dispositivi di ultima generazione la FDE è spesso attivata in

automatico quando si impostano un pin o password di sblocco.

- iOS: se hai già impostato un codice di sblocco, il tuo iPhone è già protetto in automatico. Altrimenti trovi qui le istruzioni su come fare.
- Android: anche i dispositivi Android più recenti sono di solito già cifrati, se vuoi essere sicuro e verificare puoi andare su Impostazioni > Sicurezza (o Sicurezza e posizione) > e a quel punto impostare un PIN o un passcode di sblocco seguendo la guida di Google in base alla versione del sistema operativo del dispositivo.

Accesso biometrico allo smartphone (viso/impronta digitale)

La tecnologia è spesso molto comoda e utile, ci semplifica delle azioni. Tutti siamo affascinati dalla rapidità di sblocco dello smartphone con il volto o l'impronta digitale. Funzionano così bene che però qualcuno potrebbe prenderci il cellulare di mano e metterlo davanti alla nostra faccia contro il nostro volere. A quel punto il cellulare è sbloccato e quella persona potrebbe fare ciò che vuole: vedere le foto che abbiamo scattato, leggere i nomi delle persone con cui abbiamo organizzato la partecipazione alla manifestazione o persino peggio. Prima di una manifestazione dobbiamo quindi disattivare questa funzione e usare il caro vecchio PIN o password di sblocco. Per farlo:

- clicca qui per le istruzioni per disattivare FaceID e qui per quelle per disattivare Touch ID su iOS;
- per disattivare SmartLock di Google su Android
  - Impostazioni > Sicurezza e posizione (o Sicurezza) > Smart Lock > Viso attendibile > Rimuovi riconoscimento viso > Avanti. Si aprirà una schermata col tuo viso, attendi il riconoscimento e poi premi Fine. Clicca poi sul Rimuovi viso attendibile e Rimuovi.
- per disattivare Face Unlock su Android

• Impostazioni > Biometria e Sicurezza > Riconoscimento viso > Inserire Pin > Spegnere Face Unlock

Utilizzo di app di messaggistica sicure

Quando parliamo con le nostre persone care vogliamo assolutamente avere la certezza di essere noi e loro, e non orecchie e occhi indiscreti che trasformano le nostre conversazioni in qualcosa di pubblico. La tecnologia end-to-end permette solo a noi e alle persone alle quali scriviamo di leggere i messaggi e foto inviati - un po' come la differenza tra mandare una cartolina e una lettera chiusa con un sigillo di ceralacca. L'unica differenza è che, con la crittografia end-to-end, anziché la ceralacca, stiamo mandando una lettera chiusa in una cassaforte le cui chiavi sono in mano solo a te e alla persona con cui stai comunicando.

Alcune delle app che offrono questa garanzia sono:

- *Signal*: per utilizzare Signal bisogna fornire il proprio numero di telefono e si è subito pronti ad utilizzare l'app. Ogni conversazione, tra due persone o in un gruppo, è cifrata con la tecnologia end-to-end. Nell'app si possono anche impostare i messaggi a scomparsa: dopo un tempo prestabilito vengono cancellati e non saranno più presenti nella chat. Qui c'è una spiegazione fornita direttamente da Signal. Per attivare questa funzionalità bisogna andare nelle impostazioni della chat e selezionare "Messaggi a scomparsa" e scegliere la durata.
- *Wire*: è una piattaforma di messaggistica che cifra le conversazioni con una tecnologia end-to-end e permette di creare un account senza dover fornire il proprio numero di cellulare: basta semplicemente fornire un'email. Si può creare un account direttamente online. E anche Wire offre la possibilità di usare i messaggi a scomparsa: per usarli fai click sull'icona e scegli la durata.
- *Telegram*: per creare un account su Telegram devi fornire il

tuo numero di cellulare, ma in un secondo momento puoi decidere di non renderlo visibile alle altre persone andando su Impostazioni > Privacy e sicurezza > Numero di telefono. Le persone che hanno già il tuo numero di telefono in rubrica riusciranno comunque a vederlo. Malgrado sia percepita come un'app sicura, Telegram non offre la cifratura end-to-end di default per ogni chat. Bisogna infatti avviare una Chat Segreta selezionando "Nuova chat segreta" nel profilo della persona che si vuole contattare. Nelle chat segrete si possono anche abilitare i messaggi che si autodistruggono facendo click sull'icona dell'orologio e selezionando il timer per l'autodistruzione. Le chat segrete non esistono per le conversazioni di gruppo e per i canali: è bene, quindi, fare attenzione e capire l'uso che se ne vuole fare.

Motori di ricerca sicuri

Prima di andare a una manifestazione probabilmente avrai cercato informazioni online: questo lascia una traccia della tua attività. Se hai visitato la pagina XX o il gruppo FB, o cercato informazioni su come organizzare una manifestazione, questo potrebbe renderti un potenziale sospettato agli occhi delle forze dell'ordine. Evita di cliccare "Interessato/a" o "Partecipa" sull'evento.

Ci sono diversi browser e motori di ricerca che si possono utilizzare per evitare di lasciare una traccia, e in molti casi è bene usare la modalità incognito. Ad esempio, se hai un sistema Android puoi scaricare l'app di Tor o di Vivaldi. Per sistemi sia Android che iOS esiste l'app di Brave oppure il motore di ricerca online DuckDuckGo.

Non farti pedinare dal tuo stesso smartphone!

I sistemi operativi dei nostri smartphone possono monitorare la nostra posizione e gli spostamenti che facciamo, ricostruendo così una traccia indelebile dei luoghi che visitiamo—e, indirettamente,

anche delle persone che incontriamo.
Per essere certi che nessuna delle app installate stia raccogliendo dati sulla tua posizione, preservando così una traccia dei tuoi spostamenti su cui le forze dell'ordine potrebbero mettere le mani, considera la possibilità di interrompere tutti i servizi di localizzazione:

- iOS: trovi qui le istruzioni;
- Android: Impostazioni > Geolocalizzazione o Localizzazione > Accesso alla mia posizione off
- Localizzazione di Google: qui le istruzioni.

Inoltre, elimina la cronologia delle posizioni/il salvataggio delle posizioni:

- iOS: Impostazioni > Privacy > Servizi di Localizzazione > Servizi di Sistema > Luoghi Frequenti > Cancella Cronologia
- Android: Impostazioni > Google > Account Google > Dati & personalizzazione > Cronologia delle posizioni > Spegni;
- Cancellare la cronologia delle posizioni dal tuo account Google: qui le istruzioni.

Nascondi le tue notifiche!
Probabilmente non ti è mai capitato di pensarci ma dalle tue notifiche, anche a smartphone bloccato, si possono raccogliere moltissime informazioni: ad esempio leggere il nome di chi ti sta scrivendo e il contenuto dei messaggi. Limita le informazioni che si possono leggere dalle tue notifiche così:

- iOS: Impostazioni > Notifiche > "Mostra anteprime" e poi seleziona un'opzione: "Quando sbloccato" o Mai.
- Android:
    - Impostazioni > App e Notifiche > Notifiche > Non visualizzare del tutto le notifiche
    - Impostazioni > Notifiche > Apparirà l'elenco completo delle app. Cliccare "Blocca tutto" oppure togli la spunta

da “Mostra notifiche”

- Impostazioni > Sicurezza & Localizzazione > Preferenze blocco schermo > Blocco schermo > Non mostrare le notifiche

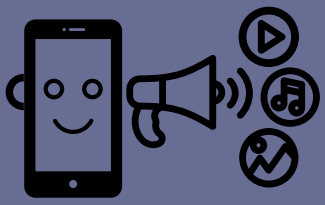
Se le istruzioni sopra non ti sono state utili, prova a bloccare le notifiche dell’app tramite le impostazioni dell’app stessa.

Spegni sempre il tuo dispositivo in caso di rischio di perquisizione o di arresto.
Questo lo renderà molto più difficile da analizzare (in particolare i sistemi operativi iOS). Ricordati che non hai nessun obbligo giuridico di fornire il codice di accesso del tuo dispositivo alle autorità.

Abbigliamento e segni di riconoscimento.
Le forze dell’ordine possono effettuare l’analisi dei social network alla ricerca di indizi (foto in cui appari con una particolare maglietta, o in cui si vede un tuo tatuaggio), sfruttare sistemi di riconoscimento facciale, e persino strumenti di riconoscimento vocale per i video online. Indossa vestiti simili a quelli di altri partecipanti, evita fantasie particolarmente stravaganti, copri eventuali tatuaggi, cicatrici o altri segni unici che sono presenti in parti esposte della tua pelle. Se puoi, portati un cambio di vestiti da indossare a fine manifestazione e cercare di prestare attenzione ai video di altri partecipanti in cui potresti essere ripreso. Se hai i capelli rosa, mettiti un cappello!

LIVELLO 2
LEVEL UP!

COME DOCUMENTARE E DIFFONDERE LE IMMAGINI DI UNA MANIFESTAZIONE



Ultimo livello di difficoltà: sei un* attivist* e vuoi partecipare ad una manifestazione, documentarla e, se del caso, utilizzarne le immagini o i video. Non hai paura della tecnologia o comunque vuoi imparare ad addomesticarla. Bene! I seguenti consigli ti aiuteranno a usare i tuoi dispositivi per documentare, informare e difendere, senza incorrere (o far incorrere) in troppi rischi.

Se vuoi effettuare delle riprese, ricordati di farlo senza sbloccare il tuo smartphone (se il dispositivo te lo permette). Presta sempre attenzione agli altri partecipanti alla protesta, e cerca di non riprenderli (soprattutto in viso) durante degli scontri o in eventuali comportamenti o azioni illecite.

Fare un passaparola in sicurezza (e senza internet).
In alcune situazioni, per colpa della rete congestionata a causa della presenza di molte persone, i servizi internet potrebbero non funzionare—o si potrebbe decidere intenzionalmente di disattivare

il proprio traffico dati. In questi casi, se la distanza tra le persone che devono comunicare non è enorme, si possono usare app come Bridgefy, che sfruttano la comunicazione via bluetooth tra dispositivi vicini. La comunicazione avviene tra dispositivi che si trovano in un raggio massimo di 100 m di distanza. Se più dispositivi hanno l'app installata, possono creare un tunnel per comunicare permettendo di inviare messaggi a distanze maggiori anche senza la connessione internet.

Se vuoi pubblicare le riprese che hai fatto alla manifestazione.
Documentare tutto ciò che avviene durante una manifestazione può essere un'azione fondamentale. Permette di raccogliere prove che possono essere usate in un secondo momento e, se pubblicate in diretta, possono offrire la possibilità di monitorare subito ciò che sta avvenendo, esponendo così eventuali violenze da parte delle autorità. Ricorda però che, se posti questi contenuti sui tuoi profili personali sui social network, chiunque faccia parte della tua rete di contatti potrà vederli e condividerli. Incluso, ad esempio, il tuo datore di lavoro o altre persone a cui non vorresti farlo sapere. In questi casi, dovresti valutare la possibilità di creare un nuovo profilo ad hoc e condividere da lì le foto e i video. In questo modo, potresti anche scollegare tutti i tuoi altri profili social dal tuo smartphone e avere così un dispositivo sostanzialmente pulito.
Non dimenticare poi che alcuni dettagli inclusi nelle foto e nei video potrebbero comunque rivelare la tua identità: ad esempio, il nome di una via o qualcuno che ti chiama per nome mentre stai registrando. Presta sempre particolare attenzione al tipo di informazioni che finiscono nelle tue riprese, soprattutto se stai facendo delle dirette.

Proteggi l'identità delle tue compagne e compagni.
Se scatti foto o registri video durante la manifestazione potrebbe

capitare che nelle inquadrature siano inclusi anche volti di altri partecipanti o segni distintivi: questi permetterebbero di svelare la loro identità ed esporli a ulteriori rischi. Per rimuovere i volti e i segni distintivi si possono usare strumenti come Image scrubber (funziona anche senza connessione internet), lo strumento incluso in Signal che permette di modificare direttamente le foto, oppure app dedicate per smartphone come Anonymous Camera (disponibile solo per iOS.)

VIENI FERMATO DALLA POLIZIA

CONOSCI I TUOI DIRITTI

Posso registrare e, successivamente, diffondere video che ritraggono soggetti appartenenti alle forze dell'ordine nel momento in cui sono impegnati in operazioni di controllo?
I funzionari pubblici e i pubblici ufficiali, compresi i rappresentanti delle forze di polizia impegnati in operazioni di controllo o presenti in manifestazioni o avvenimenti pubblici, possono essere *fotografati* e *filmati*, purché ciò non sia espressamente vietato dall´Autorità pubblica o l'attività eseguita dai pubblici ufficiali sia coperta da segreto istruttorio. Si tratta infatti di un'attività della Pubblica Amministrazione che è soggetta al principio di trasparenza. Non esiste, quindi, un divieto generale di effettuare una ripresa video o fotografica delle operazioni delle forze dell'ordine.

Regole diverse riguardando però la *diffusione* di tali fotografie e filmati. Alle foto e ai video delle forze dell'ordine si applicano le norme in materia di privacy: valgono, cioè, i limiti imposti alla

diffusione dei dati personali di un normale cittadino.
Le immagini relative agli agenti delle forze dell'ordine rientrano, infatti, nella definizione normativa di "dato personale" di cui all'art. 4, par. 1, n. 1) GDPR, in quanto atti ad individuare ed identificare una persona fisica. Di conseguenza, tanto l'acquisizione quanto la diffusione dei dati personali in esame costituiscono un "trattamento" che necessita di una base giuridica che legittimi l'operazione.

L'illecito trattamento di dati personali ai sensi dell'art. 167 del novellato D.lgs. 196/2003 costituisce una fattispecie di reato, e sotto il profilo civilistico invece, potrà essere ritenuta lesiva del diritto alla riservatezza e, pertanto, dare adito a pretese di risarcimento di danni.

Dunque, non è possibile riprendere il volto dei poliziotti o altri tratti che siano idonei a identificarli, se poi si divulga la ripresa (senza oscurare i tratti identificativi), salvo il caso in cui la ripresa sia fatta in presenza di particolari circostanze, come ad esempio il filmato girato per motivi di cronaca.

La divulgazione del video delle forze dell'ordine è protetta dal diritto di cronaca quando essa serve a diffondere una notizia o un'informazione di interesse generale, senza ledere il decoro e la dignità degli interessati (es. commissione di un illecito) oppure per tutelare un proprio diritto (nel caso si subisca un sopruso).

Le forze dell'ordine possono obbligarmi a consegnare filmati/ immagini?
In base all'art. 6, lett. c) del GDPR le forze dell'ordine possono chiedere al titolare di esportare le immagini dalle memorie e consegnarle, al fine di utilizzarle in un procedimento. Il titolare non

può opporsi alla richiesta della polizia giudiziaria, la quale, ai sensi dell'art. 354 cpp, potrà procedere al sequestro o intimare al titolare di conservare le immagini fino a nuova disposizione dell'Autorità.

Possono obbligarmi a consegnare il codice di sblocco del mio telefonino o a sbloccarlo con i miei dati biometrici?
Se vieni fermato dalle forze dell'ordine per un controllo ordinario, queste non potranno obbligarti a consegnargli il tuo cellulare.

Tuttavia, se si è verificato un reato, le forze dell'ordine potrebbero procedere al sequestro del tuo telefono (in situazioni di urgenza anche senza un "mandato" di un magistrato), specie se ritengono che contenga dati utili per l'accertamento di reati (e a prescindere dal fatto che tu sia indagato).

Se seguirai i consigli contenuti in questa guida, al momento della consegna il tuo cellulare dovrebbe essere spento o quantomeno bloccato (...meglio spento!).

Cosa succede se l'autorità ti richiede di fornire un codice di sblocco?

In Italia non c'è alcuna norma che preveda l'obbligo di consegnare password e/o codici di accesso. Come regola generale, se sei indagato o imputato del reato, non hai alcun obbligo di consegnare il codice. Esiste, infatti, un principio secondo il quale nessuno può essere costretto a collaborare alla propria accusa.

La questione è più complessa qualora tu non sia indagato o imputato. In linea teorica, il principio del diritto a non collaborare alla propria accusa potrebbe comunque trovare applicazione:

se all'interno del tuo dispositivo fossero idealmente presenti dati che ti sottoporrebbero ad un procedimento penale, ben potresti rifiutarti di aprirlo. Potresti anche dichiararti disponibile a consegnare specifici dati ma non a sbloccare integralmente il tuo dispositivo. D'altra parte, esso contiene molti dati personali che non sono d'interesse dell'autorità inquirente e che sono coperti dal diritto alla riservatezza. È infine discutibile che ti possa essere contestato il reato previsto dall'art. 371 bis del codice penale, che punisce "chiunque, nel corso di un procedimento penale, richiesto dal pubblico ministero (...) di fornire informazioni ai fini delle indagini, rende dichiarazioni false ovvero tace, in tutto o in parte, ciò che sa intorno ai fatti sui quali viene sentito". Difatti, rifiutare la consegna di un codice di sblocco non sembra significare tacere ciò che si sa su dei fatti.

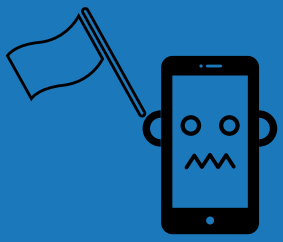
Insomma, nel dubbio, il nostro consiglio è di non consegnare il codice e di contattare il tuo avvocato di fiducia. Analogo consiglio è applicabile anche qualora tu decida di fornire un codice di sblocco, in modo da minimizzare il rischio di far estrapolare dati che possono compromettere la tua posizione.

Ricorda che la polizia non può mai usare la forza per sbloccare un dispositivo con i tuoi dati biometrici, ad esempio costringendoti fisicamente a mettere le tue impronte per lo sblocco. Ricorda anche, però, che qualcuno potrebbe prenderti il dispositivo di mano e metterlo davanti alla tua faccia contro il tuo volere, quindi è meglio disabilitare la funzione di accesso biometrico allo stesso (vedi indicazioni del livello 1 della guida).

Posso coprire il volto per proteggermi dalle riprese?
No.
Per motivi di ordine pubblico e sicurezza c'è un generale obbligo

di permettere l'identificazione da parte delle forze dell'ordine e di fornire le proprie generalità a queste ultime. Vige, quindi, un divieto generale di comparire mascherato in un luogo pubblico (art. 85 Testo Unico delle Leggi di Pubblica Sicurezza o TULPS): devi essere sempre riconoscibile.
In più: non si può partecipare a manifestazioni in luogo pubblico a volto coperto, con caschi protettivi, o con qualunque altro mezzo atto a rendere difficoltoso il riconoscimento della persona, in luogo pubblico o aperto al pubblico, senza giustificato motivo.
Fino a quando continueranno a sussistere necessità di salute pubblica, tuttavia, è permesso l'utilizzo di mascherine.

I TUOI DIRITTI SONO STATI VIOLATI? CONTATTACI!



Se hai bisogno di altre informazioni o ritieni che i tuoi diritti siano stati violati, puoi mandarci una mail a info@strali.org. Puoi creare un account email anonimo e gratuito per contattarci utilizzando Protonmail o Tutanota. Se preferisci, nella mail puoi anche darci un contatto di Telegram o di un altro servizio che non rivela la tua identità.

Realizzato in collaborazione con -ini architetti

Contatti
info@strali.org
C.so Re Umberto 5 bis, 10121 Torino

StraLiAssociazione

strali_forstrategiclitigation

StraLi for strategic litigation