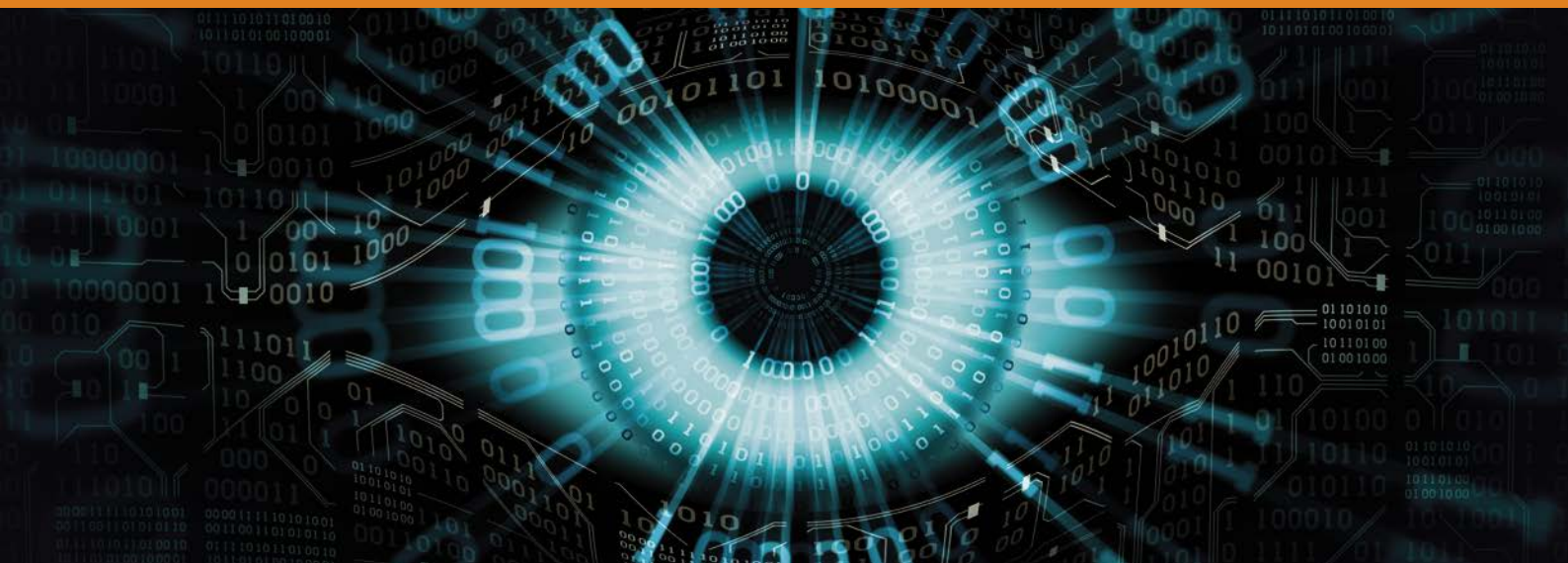
# INFO PSC

LA RIVISTA DELLA PREVENZIONE SVIZZERA DELLA CRIMINALITÀ

2 | 2021

## Tema
## Sorveglianza



## Gentili lettrici, stimati lettori,


PSC

Per molti di noi la parola "sorveglianza" evoca probabilmente in primo luogo il "Grande Fratello", ossia il nemico della sfera privata, un potenziale strumento di oppressione dei potenti. Oppure anche l'omonimo reality show, in cui i partecipanti rinunciano volontariamente alla loro sfera privata per divertire il pubblico. Questi sono già due degli aspetti importanti trattati in questo numero di INFO PSC. In un'intervista, Erik Schönenberger (direttore della "Società Digitale") mette in guardia contro l'uso delle tecniche di sorveglianza da parte dello Stato senza che sussistano le basi legali (statali) in materia. E in un'altra intervista, Jürg Halter, scrittore politicamente attivo, mette in evidenza lo strano squilibrio esistente tra il fatto che molte persone da un lato rivelano costantemente e volontariamente i propri dati privati, per esempio sui canali dei media sociali e, dall'altro, non vogliono consentire la loro tracciabilità in questo periodo di pandemia, perché temono un uso improprio dei loro dati. Per quanto riguarda la questione di chi può filmare chi e quando, l'avvocato Martin Steiger spiega nel suo contributo perché sarebbe opportuno rafforzare e perfezionare la legislazione in materia, in un'epoca in cui si ha la sensazione che tutti stiano sempre filmando tutti.

La sorveglianza sotto forma di "cyber patrolling" come strumento di lotta alla criminalità sta diventando una pratica sempre più importante, come illustrato nell'articolo di Tamara Schmid, analista di NEDIK. Alain Hofer (Vice segretario generale della CDDGP) e Janine Repetti-Dittes (Associazione Electronic Monitoring) spiegano invece come la "sorveglianza elettronica" (più comunemente chiamata "braccialetto elettronico") potrebbe essere usata in futuro anche per contrastare la violenza domestica e lo stalking. Inoltre, Nadja Capus, professoressa all'Università di Neuchâtel, descrive le difficoltà tecniche e giuridiche a cui sono confrontati i mediatori linguistici durante la sorveglianza in tempo reale delle comunicazioni fra criminali. La Professoressa Capus sta facendo delle ricerche su questo tema di nicchia altamente interessante allo scopo di sviluppare e stabilire delle norme per la pratica della mediazione linguistica. E infine, l'articolo di Sandra Bodmer e Amanda Boekholt ci illustra come si possono utilizzare o meno i droni dal profilo legale.

Da quanto appena descritto, si capisce subito che la sorveglianza ha così tanti volti che possiamo presentarne solo una piccola selezione in questo numero di INFO PSC. Non bisogna neppure dimenticare che una sorveglianza efficace può impedire non solo reati penali, ma anche incidenti stradali e disastri ambientali per esempio, e che questo strumento è indispensabile per controllare lo spazio aereo e salvare vite ogni giorno, soprattutto nel campo della medicina! L'importante è che si basi sempre su un fondamento giuridico solido, che sia democraticamente convalidata e che ci siano effettivamente dei controlli sull'uso dei dati raccolti.

E ora vi auguro una buona lettura!

**Fabian Ilg**
Direttore della PSC e capo progetto per la criminalità informatica


## IMPRESSUM

**Editore e fonte di informazioni**
Prevenzione Svizzera della Criminalità
Casa dei Cantoni
Speichergasse 6
3001 Berna

e-mail: info@skppsc.ch
tel. 031 511 00 09

**L'INFO PSC 2 | 2021** è disponibile come file PDF nel sito: www.skppsc.ch/skpinfo.
**L'INFO PSC 2 | 2021** esce anche in tedesco e francese.

| | |
|---|---|
| **Responsabile** | Chantal Billaud, Vicedirettrice PSC |
| **Redazione, interviste** | Volker Wienecke, Berna |
| **Versione francese** | ADC, Vevey |
| **Versione italiana** | Annie Schirrmeister, Massagno |
| **Grafica** | Weber & Partner, Berna |
| **Stampa** | Länggass Druck AG, Berna |
| **Tiratura** | i: 250 \| f: 300 \| t: 1350 |
| **Data di pubblicazione** | dell'edizione 2 \| 2021: luglio 2021 |

# «La Svizzera è uno Stato ficcanaso, signor Schönenberger?»

In questa intervista, Erik Schönenberger, specialista della sicurezza informatica, parla dell'utilizzo in Svizzera di vari strumenti di sorveglianza – come la conservazione dei dati, l'esplorazione di segnali via cavo e il riconoscimento facciale – e si interroga sulla liceità di queste pratiche. Erik Schönenberger è direttore della *Società Digitale,* di cui è anche uno dei membri fondatori.

***La Svizzera è uno Stato ficcanaso, signor Schönenberger?***
Sì, si potrebbe dire così. Perché da noi si introducono e si sviluppano sempre più programmi di sorveglianza di massa, come la conservazione dei dati o l'esplorazione di segnali via cavo.

***Come funziona la conservazione dei dati?***
La conservazione dei dati permette di tracciare chi ha chiamato chi, quando è avvenuta la chiamata e quanto è durata, chi si è collegato a Internet, quando lo ha fatto e per quanto tempo, chi ha inviato un'e-mail o un SMS a chi e quando. Se si utilizza un telefono cellulare, si memorizzano anche le informazioni sulla posizione del telefono (geolocalizzazione). Tutte queste informazioni devono essere conservate per sei mesi e fornite, su richiesta, alle autorità di perseguimento penale o ai servizi segreti.

I *provider* sono quindi tenuti a conservare per sei mesi il protocollo di comportamento dei loro clienti in materia di comunicazione. Originariamente, questa prassi veniva usata per registrare le comunicazioni tra persone allo scopo di individuare reti di contatti dettagliate. Nel frattempo, però, per ogni comunicazione fatta con uno smartphone viene già creato un record di dati,

m.a.d.

*Erik Schönenberger, specialista della sicurezza informatica e direttore della* Società Digitale

persino quando un'app controlla in background se è arrivato un nuovo messaggio.

È già possibile accedere ai dati non appena sussiste il sospetto di un crimine o delitto. Inoltre, i dati conservati sono utilizzati anche per le cosiddette ricerche per zona di copertura dell'antenna, cioè per indagini incrociate in caso di sospetto di reato contro "ignoti". L'obiettivo è di scoprire chi si trovava in un certo luogo in un determinato momento e chi potrebbe aver commesso un reato. Questo può obbligare a dover provare la propria innocenza se il proprio telefono cellulare era collegato a una delle celle telefoniche sotto inchiesta in quel momento. Esiste un caso noto in cui il fornitore di telefonia mobile ha fornito oltre 150 000 dati di connessione.

A tutt'oggi, però, non esiste ancora una base giuridica sufficiente per effettuare le ricerche per zona di copertura dell'antenna. La sorveglianza di una persona può essere ordinata solo se sussiste un sospetto di reato concreto nei suoi confronti. Spesso, si giustifica la conservazione dei dati adducendo che le autorità inquirenti devono poter lottare "ad armi pari" contro i criminali che commettono reati in Internet. Tuttavia, questa misura di sorveglianza non riguarda specificatamente i reati in Internet. Si creano quindi ulteriori strumenti investigativi, sfruttando impropriamente i nostri smartphone come spie di localizzazione.

***E come funziona la conservazione dei dati in Internet?***
La conservazione dei dati applica anche un obbligo d'identificazione. Inoltre, gli indirizzi IP assegnati devono essere conservati per sei mesi. Questi indirizzi sono necessari per la comunicazione in Internet e sono assegnati ad una connessione come per esempio ad un modem ADSL o un cavo TV. Dato che non vi sono indirizzi IP a sufficienza, solitamente questi sono condivisi con le reti pubbliche WLAN e le reti di telefonia mobile. Questa tecnologia si chiama *Network Address Translation* (NAT), ovvero la traduzione degli indirizzi di rete. I *provider* devono anche conservare queste tabelle di traduzione per sei mesi. Conseguenza: anche da noi il volume dei dati sta esplodendo, raggiungendo un miliardo di operazioni di traduzione NAT per rete mobile al giorno!

Ciò che originariamente era stato pensato per permettere l'identificazione,

123RF/Kheng Ho Toh

*«Il reclamo contro la conservazione dei dati è pendente a Strasburgo, con buone possibilità di successo.»*

serve ora a sorvegliare il nostro modo di usare Internet, poiché il Servizio di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (SCPT) esige la conservazione non solo del processo di traduzione in sé, ma anche degli indirizzi di destinazione. Con questi dati è ora possibile tracciare tutti i server web visitati e i servizi internet utilizzati da una persona, o identificare tutti gli utenti di un servizio o di un server.

***Ma questi dati non dovrebbero servire per elucidare i crimini?***

Purtroppo esistono solo pochi studi che analizzano la necessità di conservare i dati per combattere la criminalità. In una perizia commissionata dall'Ufficio federale di giustizia tedesco all'Istituto Max Planck, quest'ultimo giunge alla conclusione che la conservazione dei dati praticata in Svizzera non si è tradotta in un aumento sistematico del tasso di elucidazione dei crimini. Orbene, è illegale restringere i diritti fondamentali se l'utilità della misura non è o non può essere provata!

Come possiamo constatare, la conservazione dei dati riguarda tutti, senza eccezione. Rappresenta una grave e sproporzionata violazione della protezione della sfera privata garantita dalla Costituzione e mette anche in pericolo il segreto professionale di avvocati, medici o redattori. Finora, tutte le corti costituzionali in Europa e la Corte di giustizia europea che hanno dovuto giudicare leggi sulla conservazione dei dati, le hanno annullate senza eccezione.

Per quanto riguarda la Svizzera, la *Società Digitale* ha intentato un procedimento giudiziario strategico alla Corte europea per i diritti dell'uomo. Il reclamo contro la conservazione dei dati è pendente a Strasburgo, con buone possibilità di successo.

***Lasciamo l'ambito del perseguimento penale. E che ne è della sorveglianza praticata dal Servizio delle attività informative?***

L'attuazione della nuova legge federale sulle attività informative e l'introduzione dell'esplorazione dei segnali via cavo hanno favorito una nuova sorveglianza di massa. L'esplorazione dei segnali via cavo trae le sue origini dall'esplorazione radio, che all'inizio era una sorveglianza puramente militare di operazioni condotte all'estero. Questa esplorazione radio militare è poi stata subdolamente estesa alla sorveglianza satellitare. All'epoca si trattava di sorvegliare le comunicazioni all'estero, ma si era poi già iniziato a controllare anche quelle civili.

Dato che oggi si trasmettono sempre più comunicazioni in fibra ottica, l'esplorazione dei segnali via cavo compie un terzo passo in avanti. A differenza dei satelliti stranieri, tuttavia, i cavi stranieri non possono essere sottoposti a sorveglianza. Per questo motivo, si sfruttano le linee transfrontaliere in fibra ottica. Ogni comunicazione transfrontaliera coinvolge però anche una persona in Svizzera, poiché non ci sono praticamente linee che attraversano unicamente il nostro Paese.

In pratica, la situazione si presenta così: le comunicazioni che passano attraverso linee transfrontaliere sono vagliate dal Centro operazioni elettroniche (COE) dell'esercito in base a parole chiave di ricerca predefinite. La legge consente l'uso dei segnali captati se il mittente e/o il destinatario si trovano all'estero. Si tratta degli indirizzi IP.


123RF/pixinoo

*«Il riconoscimento facciale è sempre più spesso utilizzato negli aeroporti e nelle stazioni ferroviarie.»*

Nel caso delle linee transfrontaliere, succede praticamente sempre che un indirizzo IP si trovi in Svizzera e uno altro all'estero. In altre parole, siamo tutti costantemente sorvegliati e le nostre comunicazioni vengono passate al setaccio. Questa sorveglianza, il cui obiettivo era di individuare operazioni all'estero, ora serve ovviamente anche a reperire le minacce nel nostro Paese.

***E che ne è della sorveglianza mirata, per esempio quella che permette l'uso di trojan statali?***

L'impiego di trojan statali (GovWare) è consentito alle autorità di perseguimento penale e ai servizi segreti. Mentre le autorità di perseguimento penale sono autorizzate ad accedere ai dati delle comunicazioni, i servizi segreti hanno persino il diritto di effettuare una ricerca online e di usare una telecamera e un microfono. Questo rappresenta un'intrusione – almeno potenziale – nella sfera privata delle persone coinvolte, perché noi memorizziamo una quantità incredibile di informazioni altamente personali sui nostri smartphone, notebook e PC. Questi dati forniscono informazioni per esempio sulla nostra salute, sulle nostre opinioni politiche e sulle nostre preferenze sessuali. Ma su questi dispositivi sono spesso memorizzati anche segreti aziendali o la corrispondenza con il proprio avvocato. È come se qualcuno s'introducesse segretamente nella vostra abitazione per piazzare dei microfoni spia.

Un tale modo di procedere dovrebbe essere autorizzato solo come *ultima ratio,* nel caso di una minaccia concreta e immediata di esposizione al pericolo della vita, dell'integrità personale, della libertà o della sicurezza nazionale. Tuttavia, l'elenco ristretto dei reati comprende già quasi un centinaio di infrazioni, compreso il furto semplice!

## Società Digitale

La *Società Digitale* è un'associazione per la protezione dei cittadini e dei consumatori nell'era digitale senza scopo di lucro che gode di un ampio sostegno. In quanto organizzazione della società civile, essa s'impegna dal 2011 a favore di una società sostenibile, democratica e libera. Il suo obiettivo è difendere i diritti fondamentali in un mondo digitale interconnesso.

www.digitale-gesellschaft.ch
(Sito solo in francese e tedesco.)

***Secondo lei, qual è il problema principale legato all'uso di GovWare?***

Oltre alla grave intrusione nella sfera privata digitale, si pone effettivamente il problema dell'infezione del sistema, in quanto questi GovWare sfruttano sempre una falla di sicurezza. Di solito, ci si procura queste falle direttamente o indirettamente sul mercato nero che è così sostenuto da fondi statali. Inoltre, circostanza aggravante, la falla di sicurezza non viene eliminata e tutti noi rimaniamo quindi vulnerabili.

***Un esempio?***

Nel 2017, il malware WannaCry si è diffuso attraverso una falla di sicurezza che era già stata utilizzata e tenuta segreta dalla NSA per diversi anni prima di essere poi sfruttata da altri criminali. Diverse centinaia di migliaia di computer in 150 paesi sono stati colpiti e messi fuori uso. Tra questi c'erano i dispositivi di ospedali in Inghilterra e

Scozia, ma anche di gruppi come Nissan, Renault e Deutsche Bahn. Dev'essere nell'interesse dello Stato garantire la propria e la nostra sicurezza, segnalando le falle di sicurezza ai produttori affinché le eliminino. Queste falle non devono certo essere tenute segrete!

***Quale sarebbe la sua conclusione? Come vede il futuro della sorveglianza in Svizzera?***

La sorveglianza è sempre effettuata in base a criteri di fattibilità tecnica. Non esistono praticamente studi sulla sua utilità. Manca inoltre una mappatura globale delle misure di sorveglianza che tenga conto del loro impatto sulla democrazia e sulla società.

A peggiorare le cose, c'è il fatto che la Svizzera non ha una corte costituzionale competente ad esaminare la proporzionalità delle leggi. Ciò significa che il nostro reclamo del 2014 contro la conservazione dei dati inoltrato a Strasburgo non sarà trattato prima del prossimo anno. Il nostro secondo reclamo del 2017 contro l'esplorazione di segnali via cavo è appena stato rinviato dal Tribunale federale al Tribunale amministrativo federale per una valutazione contenutistica.

La via legale è incredibilmente lenta, mentre la tecnologia e le misure di sorveglianza continuano a svilupparsi rapidissimamente. Lo vediamo, per esempio, con il riconoscimento facciale. Questa misura è sempre più spesso utilizzata negli aeroporti e nelle stazioni ferroviarie. Ci sono già enormi banche dati di visi, come ClearView AI. La combinazione di telecamere di sorveglianza in rete con l'apprendimento automatico potrebbe effettivamente portare a una situazione distopica dove regna l'intrusione istituzionalizzata.

Chiediamo quindi – tra l'altro insieme ad altre 60 organizzazioni di difesa dei diritti fondamentali di tutta l'Europa – un divieto della sorveglianza biometrica di massa negli spazi pubblici!

*Signor Schönenberger, la ringrazio molto per questa istruttiva conversazione.*

# La sorveglianza con droni nel rispetto della sfera privata

Dall'inizio della cosiddetta rivoluzione digitale a partire dalla seconda metà del secolo scorso, le innovazioni tecnologiche si susseguono ad un ritmo incalzante. L'invenzione del drone ne è un perfetto esempio. Con i suoi innumerevoli modelli, questo veicolo aereo senza pilota può essere utilizzato in molti modi, per esempio in agricoltura, per ispezionare infrastrutture, ma anche dalla polizia per sorvegliare grandi eventi e da piloti privati per hobby. Questi apparecchi offrono certo dei vantaggi, ma sono anche una fonte di problemi.

La cosiddetta "Industria 4.0", il cui obiettivo è una totale digitalizzazione della produzione industriale, immette costantemente nuove tecnologie sul mercato. Queste si caratterizzato per la loro "iperautomazione" e "iperconnettività", ossia una maggiore automazione dei processi e della connessione degli oggetti con il loro ambiente. I droni ne sono un perfetto esempio. Il loro uso pone tuttavia una problematica che preoccupa sempre più anche i cittadini: la protezione della loro sfera privata. Un esempio eclatante di questa problematica è stato osservato in Francia, dove la polizia ha fatto uso di droni per controllare l'osservanza delle misure anti COVID-19 imposte. Questo articolo si propone ora di esaminare gli aspetti legali del conflitto d'interesse che oppone il rispetto della sfera privata all'uso dei droni.

## L'origine del drone

Il drone – così chiamato perché per via del suo ronzio – è stato originariamente sviluppato a scopi militari. Solo in un secondo tempo questa tecnologia è stata utilizzata anche per le applicazioni civili. Anche se ora questi apparecchi sono diffusi un po' ovunque, a tutt'oggi il termine "drone" non ha ancora una definizione legale. I droni appartengono alla categoria dei veicoli aerei senza pilota che possono essere telecomandati o volare autonomamente. Sono anche chiamati UAV/UAS o RPAS: l'acronimo UAV significa *unmanned aircraft vehicle,* ossia veicolo aereo senza pilota; l'acronimo UAS significa *unmanned aircraft*


## Autrici


m.a.d.

**Amanda Boekholt** è specialista della comunicazione e responsabile della gestione degli stakeholder nella Sezione Innovazione e digitalizzazione dell'Ufficio federale dell'aviazione civile (UFAC).


m.a.d.

**Sandra Bodmer** è giurista e lavora nell'Unità Innovazione e digitalizzazione dell'Ufficio federale dell'aviazione civile (UFAC). È responsabile dell'implementazione del regolamento UE sui droni da parte della Svizzera.

Adobe Stock/Iuliia Sokolovska

*«Dopo tutto, non si sa chi sia il pilota e quale sia il suo scopo mentre fa volare il suo drone sopra il giardino di un privato.»*

*system,* ossia sistema di aeromobile senza equipaggio; l'acronimo RPAS significa *remotely piloted aircraft system,* ossia sistema di aeromobile pilotato da remoto, ma si riferisce limitatamente ai veicoli aerei senza pilota telecomandati.

## La sfera privata

Grazie ai progressi tecnologici, le dimensioni dei droni si sono ridotte sempre più. Inoltre, questi apparecchi sono liberamente in vendita nei negozi e possono anche essere acquistati da privati a prezzi sempre più contenuti. Questo aspetto, unitamente alle innumerevoli possibilità d'impiego, sono all'origine del boom dell'industria dei droni a livello mondiale. Nel 2018, approssimativamente 80 aziende attive nella produzione di droni impiegavano circa 2500 persone in Svizzera. Come capita sempre con l'avvento di una nuova tecnologia, non tutti ne sono entusiasti. Soprattutto l'uso dei droni in ambito privato suscita incertezze e paure, che alimentano spesso un atteggiamento di rigetto. L'Ufficio federale dell'aviazione civile (UFAC) deve trattare regolarmente richieste di cittadini preoccupati che si sentono osservati o importunati da droni nel loro ambiente. Dopo tutto, non si sa chi sia il pilota e quale sia il suo scopo mentre fa volare il suo drone sopra il giardino di un privato. Il drone scatta delle foto? Se è così, cosa si fa di queste foto? Ma si è poi è autorizzati a farlo?

## Interesse degno di protezione (art. 667 CC)

Se un drone sorvola una proprietà privata, occorre tener conto del fatto che i diritti del proprietario del fondo si estendono non solo al suolo, ma anche allo spazio sopra il fondo. Gli interessi dei proprietari devono essere determinati caso per caso. Anche se il Tribunale federale non si è ancora pronunciato sull'altezza massima di sorvolo dei fondi, nella dottrina c'è chi in parte considera che sussista già un interesse degno di protezione quando un drone sorvola un fondo ad un'altezza molto bassa (10–40 metri). Prima di affrontare la questione della violazione della sfera privata, presentiamo qui di seguito una panoramica degli aspetti della sfera privata.

## Protezione della personalità

La Costituzione federale svizzera (Cost.) disciplina la protezione della personalità e dei dati in diversi articoli di legge. Il diritto alla libertà personale, in particolare all'integrità fisica e mentale, così come il diritto alla libertà di movimento sono contemplati nell'art. 10, cpv. 2, Cost. Inoltre, l'articolo 13 Cost.

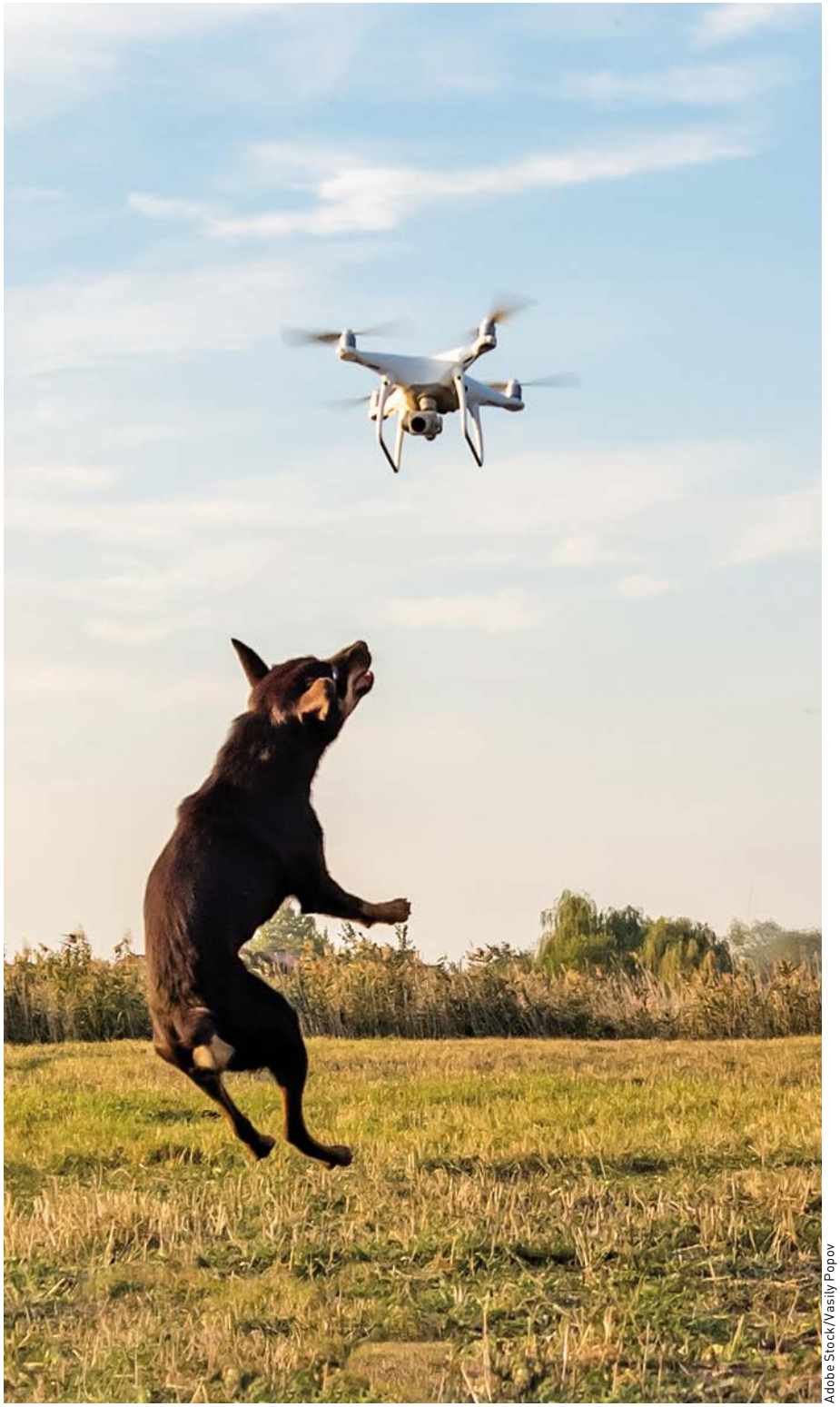
regola il diritto di ogni persona alla protezione della sua sfera privata in generale e il diritto alla protezione da un impiego abusivo dei suoi dati personali in particolare.

Nei suoi articoli 28 e ss., il Codice civile svizzero (CC) concretizza gli articoli 10 e 13 della Costituzione federale. L'art. 28 CC tratta la protezione della personalità nel suo insieme, senza elencare i singoli beni della personalità. Affinché sussista una violazione del diritto della personalità ai sensi dell'art. 28 CC, il pregiudizio deve avere oggettivamente una certa intensità. Secondo l'art. 28, cpv. 2 CC, la violazione del diritto della personalità è illecita quando non è giustificata dal consenso della persona lesa, da un interesse preponderante pubblico o privato, oppure dalla legge. Di conseguenza, fare foto senza il consenso della persona interessata può già costituire di per sé una violazione dell'art. 28 CC, a condizione che ciò non avvenga nel pubblico interesse. Sussiste certamente una violazione della personalità quando, sulle immagini di una telecamera di sorveglianza, il viso di una persona è riconoscibile anche da terzi.

Nella sua decisione del 18 aprile 2018, il Tribunale cantonale di Lucerna ha analizzato approfonditamente la questione della protezione della personalità nel caso delle immagini riprese con i droni: le riprese aeree delle proprietà lungo le sponde del lago nei pressi di Horw allo scopo di sorvegliare i lavori in corso sono state considerate illecite per mancanza di basi legali. Malgrado l'annuncio dei lavori, i residenti – dopo un mese – avevano la sensazione di essere sorvegliati. Secondo il tribunale, questa situazione costituiva una grave limitazione del diritto a disporre liberamente delle informazioni che li riguardavano e quindi una violazione del diritto alla protezione della sfera privata, conformemente all'articolo 13 Cost. Per questo motivo, le immagini riprese con droni hanno dovuto essere cancellate per mancanza di basi legali.

## Protezione dei dati

Infine, occorre anche menzionare la legge sulla protezione dei dati (LPD), il cui scopo è di proteggere la personalità di quelle persone oggetto di un trattamento dei dati. La LPD si occupa quindi di una delle questioni centrali "dell'Industria 4.0". Questa legge è applicabile



Adobe Stock/Vasily Popov

*«C'è anche chi sostiene che, data l'attuale tendenza a pubblicare immagini sui media sociali, un'azione rapida sia del tutto giustificabile e che, in singoli casi, potrebbe quindi anche giustificare il sequestro o l'abbattimento del drone.»*

quando si trattano i dati personali ai sensi dell'art. 3, lett. a, LPD. Tuttavia, se le immagini riprese con il drone sono destinate esclusivamente ad uso personale, le disposizioni della legge sulla protezione dei dati non sono applicabili come disposto dall'art. 2, cpv. 2, lett. a, LPD. Questo punto di vista non è tuttavia condiviso da tutta la dottrina. Infatti, anche se i dati sono esclusivamente destinati ad uso personale e la LPD non è applicabile *de jure*, questo non elimina la possibilità di una violazione della sfera privata e la sensazione di essere spiati. Per quanto riguarda la protezione dei dati e l'uso dei droni, l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) ha pubblicato una scheda informativa sulla videosorveglianza con droni nella sfera privata che elenca i vari punti da osservare quando si utilizzano questi apparecchi[1]. L'IFPDT considera che le immagini riprese con i droni siano autorizzate solo se sussiste un motivo giustificato adeguato (o il consenso della persona interessata, un interesse privato o pubblico preponderante o per legge).

m.a.d.

*«Il servizio d'identificazione remota della rete permette di identificare il pilota di un drone quando fa volare il suo apparecchio grazie al suo numero di registrazione, analogamente al sistema di immatricolazione delle automobili.»*

## Misure contro le ingerenze nella sfera privata

I proprietari e i possessori di un bene hanno a loro disposizione diverse possibilità legali per difendersi da queste ingerenze.

**Azione negatoria** (art. 641, cpv. 2, CC)
Per respingere un'indebita ingerenza, il proprietario di un fondo può ricorrere all'azione negatoria per intentare un'azione contro il perturbatore. Tale indebita ingerenza può sussistere se, durante il sorvolo di un drone, i confini verticali o orizzontali – determinati dall'interesse del proprietario del fondo degno di protezione – sono stati violati contro la volontà dell'avente diritto.

**Rapporti di vicinato** (art. 679 ss. CC)
L'azione di rapporti di vicinato si basa su eccessi pregiudizievoli provenienti da un fondo vicino. Se il vicino possiede un drone e usa regolarmente il suo bene per farlo decollare e atterrare, questo può costituire una violazione dei diritti d'uso che spettano al fondo.

**Protezione del possesso**
(art. 926 e art. 928 CC)
Analogamente al proprietario, anche il possessore di una cosa (per esempio, l'inquilino di una casa) può aver ricorso ad alcuni rimedi giuridici. Se è turbato nel suo possesso da un atto di illecita violenza, il possessore ha il diritto di difendersi con la forza contro l'altrui illecita violenza. La sua azione deve tuttavia essere proporzionata alla turbativa. Secondo la dottrina prevalente, l'abbattimento del drone è l'ultima risorsa da utilizzare per difendersi da una turbativa (il cosiddetto diritto di autodifesa conformemente all'art. 926 CC). C'è anche chi sostiene che, data l'attuale tendenza a pubblicare immagini sui media sociali, un'azione rapida sia del tutto giustificabile e che, in singoli casi, potrebbe quindi anche giustificare il sequestro o l'abbattimento del drone. Tuttavia, questo vale solo durante l'ingerenza. Se il possessore non esercita il diritto di autodifesa, può far valere le sue pretese sporgendo denuncia.

**Codice penale** (art. 179$^{quarter}$ CP)
Anche il diritto penale offre una protezione dalle ingerenze causate dai droni. Si può invocare la violazione della sfera segreta o privata mediante apparecchi di presa d'immagine quando le riprese sono effettuate in un'area che è protetta in un modo o nell'altro dagli sguardi altrui.

A causa della loro lunga durata, però, i procedimenti civili e penali permettono raramente di contrastare con tempestività le ingerenze dirette dei droni. Sono invece molto più adatti per difendersi dall'uso pianificato e ripetuto di droni e quando la persona all'origine della turbativa ("il perturbatore") è nota.

## Misure tecniche

Tutti i casi di violazione della protezione della personalità e dei dati hanno un punto in comune: l'identità del pilota è raramente nota e questo complica notevolmente l'applicazione della legge. Infatti, non è facile ritrovare il pilota per

1 IFPDT, Videosorveglianza con droni nella sfera privata (www.edoeb.admin.ch → Protezione dei dati → Tecnologie → Videosorveglianza → Droni)

ingiungergli di cancellare le riprese fatte. Fortunatamente, i progressi tecnici e l'adeguamento della regolamentazione in materia stanno ponendo le basi per eliminare anche questo problema e facilitare il perseguimento penale.

Da un lato, con l'entrata in vigore delle nuove disposizioni europee sui droni – la cui attuazione in Svizzera è stata posticipata – i piloti di droni devono registrarsi in un registro nazionale se il loro apparecchio ha un peso al decollo superiore ai 250 g o se è dotato di un sensore in grado di rilevare dati personali. Dall'altro, quando entrerà in vigore il "regolamento U-Space", si introdurrà anche il cosiddetto servizio d'identificazione remota della rete *(network remote identification,* abbreviata "Net-RID"). Questo servizio permette di identificare il pilota di un drone quando fa volare il suo apparecchio grazie al suo numero di registrazione, analogamente al sistema di immatricolazione delle automobili. Questa soluzione serve prima di tutto a migliorare la visibilità e l'integrazione di tutti coloro che sono presenti nello spazio aereo. Dal canto suo, la Svizzera sta introducendo e testando l'identificazione a distanza su base volontaria nell'ambito del partenariato "Swiss U-Space Implementation" (SUSI).

## Considerazioni finali

I vari rimedi giuridici qui descritti e soprattutto le nuove misure tecniche dovrebbero – speriamo – produrre due effetti: da un lato, rafforzare la consapevolezza dei piloti di droni affinché rispettino le regole e, dall'altro, prevenire o punire le violazioni della sfera privata di tutte le persone. Questo dovrebbe anche aumentare l'accettazione di questi nuovi apparecchi volanti da parte della popolazione. L'obiettivo che si vuole raggiungere è il seguente: occorre evitare che la problematica della protezione dei dati e la paura di violazioni della sfera privata complichino o addirittura impediscano del tutto lo sviluppo e l'uso di nuove tecnologie molto promettenti per tutta la società.

# Via libera al "cyber patrolling" contro la criminalità in rete!

Per lottare contro la criminalità digitale, la Svizzera si è dotata di una rete di supporto digitale alle indagini sulla criminalità informatica (NEDIK). I corpi di polizia, che fanno parte della rete NEDIK, si dedicano fra l'altro anche al "cyber patrolling" o pattugliamento informatico. Quest'attività comprende l'osservazione, la registrazione e la conduzione di indagini preliminari sulle attività criminali commesse in Internet e nella Darknet, in applicazione alla legge sulla polizia.

Nell'era della digitalizzazione, non possiamo esimerci dal fare una considerazione: non ci sono praticamente limiti alle attività online. Internet soddisfa qualsiasi desiderio, non importa quanto stravagante. Che si tratti di armi, di contraffazioni di articoli di marca, di una nuova identità, di stupefacenti o ancora di materiale fotografico e video vietato, se si sa dove e come cercare, si riesce quasi sempre a trovare quello che si vuole. Confrontate a questa sfida, anche le forze di polizia svizzere devono affrontarla. Occorre operare una chiara distinzione tra i reati che vengono segnalati da quelli che si devono ricercare attivamente. È risaputo che i cittadini denunciano unicamente gli atti criminali di cui sono stati vittime in prima persona. Ma nel caso della criminalità inerente gli stupefacenti, per esempio, le cose stanno diversamente. In questo caso, la stessa polizia o più generalmente le autorità di perseguimento penale si avvalgono del "cyber patrolling" per cercare in modo mirato reati in Internet. Il "cyber patrolling" in sé non è una novità, perché è semplicemente un trasferimento delle attività di pattugliamento sul terreno nel cyberspazio. Obiettivo: dare ai cybercriminali la sensazione che non possono navigare e agire impunemente in Internet, perché questo non è uno spazio senza legge.

Attualmente, le forze di polizia svizzere stanno rafforzando i loro reparti di cybercriminalità e istruiscono il loro personale con corsi di formazione di base e continua, per dotarsi degli strumenti necessari a combattere la criminalità informatica in modo ancora più efficace. I reparti si compongono di volta in volta di specialisti sperimentati: inquirenti, investigatori, informatici e personale scientifico senza formazione di polizia. Insieme danno la caccia a spacciatori di droga, truffatori e pedofili attivi in Internet. In quest'ambito, anche l'approccio proattivo delle *cyberpattuglie* svolge un ruolo importante, perché permette di individuare e poi di impedire le attività illegali o la loro preparazione. Anche gli investigatori delle forze di polizia svizzere ricevono regolarmente informazioni concrete su attività illegali commesse in Internet, sulle quali poi indagano sistematicamente.

**Autrice**

**Tamara Schmid**
Analista NEDIK
Polizia cantonale zurighese

m.a.d.


123RF | Montage: Weber & Partner

*«La stessa polizia o più generalmente le autorità di perseguimento penale si avvalgono del 'cyber patrolling' per cercare in modo mirato reati in Internet.»*

## Caso di studio

All'inizio di un'indagine per traffico di droga in Internet, si controllano gli specifici mercati online per vedere se si possono rilevare attività criminali in relazione con la Svizzera. In questo caso, le *cyberpattuglie* non si focalizzano su una persona in particolare, ma indagano piuttosto su un fenomeno specifico.

1. I team di specialisti passano al setaccio i mercati online noti, compresi i profili dei trafficanti, poi analizzano le specifiche attività di vendita.
2. Selezionano quindi alcuni trafficanti basandosi su criteri predefiniti e valutano i possibili passi investigativi da intraprendere nei loro confronti.
3. Dall'analisi effettuata, si possono già ottenere i primi indizi sulla possibile identità dei trafficanti.
4. Se i sospetti sono fondati, si avvia un'indagine contro gli spacciatori.

Le prime due tappe mostrano qual è effettivamente il lavoro di "cyber patrolling". La 3ª tappa descrive le indagini preliminari effettuate. Una volta superate queste tre tappe, si avvia l'indagine (4ª tappa) che ha una buona probabilità di riuscita.

## Coordinamento

Uno dei compiti centrali della rete NEDIK è di coordinare la collaborazione in materia di lotta alla criminalità informatica a livello nazionale e internazionale. I cittadini, così come le forze di polizia straniere quali Interpol ed Europol, forniscono regolarmente informazioni su attività illegali. In Svizzera, le segnalazioni provenienti dall'estero sono dapprima comunicate a "fedpol", l'Ufficio federale di polizia, che le trasmette poi ai corpi di polizia cantonali. Senza un'intensa cooperazione tra i cantoni, tra questi ultimi e la Confederazione e tra quest'ultima e l'estero, le indagini saranno difficilmente coronate da successo. Per combattere efficacemente la criminalità digitale, la rete NEDIK utilizza strumenti d'analisi specifici e gestisce una banca dati di conoscenze centralizzata che permette di condividere in modo ottimale i risultati delle indagini con gli altri corpi di polizia.

Il coordinamento è di centrale importanza. Come in altri paesi, anche in Svizzera sussiste il rischio di condurre indagini o attività di "cyber patrolling" parallele senza consultarsi. Un servizio di coordinamento ben funzionante riduce il rischio che diverse forze di polizia indaghino sullo stesso caso e aiuta a sfruttare in modo più sensato queste risorse altrove.

## Lotta alla pedocriminalità

In quanto membro della rete NEDIK, la Polizia cantonale bernese ha assunto il 1° gennaio 2021 il coordinamento del monitoraggio peer-to-peer e, in singoli casi, delle misure preventive mascherate supplementari adottate nello spazio digitale. La criminalità informatica in generale, e la pedocriminalità in

particolare, non conoscono frontiere. In quest'ambito è quindi essenziale avere un'intensa cooperazione tra i singoli cantoni, la Confederazione e anche con gli altri stati. "fedpol" elabora e smista per i cantoni le attività sospette segnalate da autorità straniere partner, come per esempio le segnalazioni delle autorità statunitensi sulla pedocriminalità, le cosiddette segnalazioni NCMEC*. Non appena un sospetto è fondato, il ministero pubblico competente a livello cantonale può avviare un procedimento. Nell'ambito della prevenzione, ogni cantone, di concerto con la rete NEDIK, continua ad essere responsabile di condurre le proprie inchieste mascherate per combattere la pedocriminalità e di mobilitare le risorse di polizia corrispondenti. Gli investigatori che svolgono inchieste preventive mascherate nel settore del pedocriminalità devono conoscere bene i modi operandi e le intenzioni di questi criminali. Questi ultimi, solitamente attivi a livello internazionale, sono veri e propri esperti nel loro campo. Gli specialisti del "cyber patrolling" devono quindi essere in grado di adattarsi al profilo dei criminali, competenza indispensabile per svolgere un lavoro di prevenzione non solo nel settore della pedocriminalità, ma anche per individuare altri delitti commessi in Internet.

## Prevenire la criminalità grazie al "cyber patrolling"

Le forze di polizia svizzere sono presenti in Internet non solo in modo mascherato, ma anche a viso scoperto. Su varie piattaforme, i corpi di polizia forniscono alla popolazione consigli per evitare di diventare vittime dei cybercriminali. Svolgono quindi un lavoro di prevenzione, rispondendo anche a domande specifiche poste dalla popolazione e raccogliendo segnalazioni e informazioni sulla criminalità in Internet. Pattugliare nel cyberspazio permette pure di svolgere un lavoro di polizia trasparente e preventivo proprio negli ambienti in cui navigano gli internauti, e di consigliare questi ultimi su come usare Internet in tutta sicurezza.

Con il suo sito cybercrimepolice.ch, la Polizia cantonale zurighese assicura il monitoraggio dei pericoli attuali in tempo reale. Questo sito fa dei suoi utenti i migliori pattugliatori informatici, perché offre loro la possibilità di segnalare in modo semplice e rapido nuove forme di criminalità, con l'intento di sensibilizzare e mettere in guardia altri internauti.

## Cooperazioni

Si è già potuto ripetutamente stabilire quanto siano importanti le indagini preventive e il "cyber patrolling", perché questo approccio ha già permesso di chiudere molti casi. Nel campo della cybercriminalità è fondamentale combinare misure repressive e preventive per varie ragioni. Il compito centrale della rete NEDIK è di promuovere e coordinare la collaborazione nel campo delle indagini sulla cybercriminalità. Questo si riflette anche nel suo mandato di prevenzione che consiste nel sostenere l'attività di prevenzione operativa e le organizzazioni coinvolte nella cyberprevenzione nazionale. All'inizio del 2021, la rete NEDIK ha quindi deciso di intensificare la propria collaborazione con la Prevenzione Svizzera della Criminalità, una delle principali organizzazioni di prevenzione nel nostro Paese. Le due entità scambiano informazioni in questa rete per coordinare le misure preventive e repressive, condividere conoscenze specialistiche e adattare i corsi di formazione di base e continua in quest'ambito.

Grazie al "cyber patrolling" attuato in assenza di sospetti, le forze di polizia svizzere registrano molti successi al loro attivo. Queste operazioni permettono di identificare, localizzare, arrestare e perseguire penalmente gli individui coinvolti in affari illegali. La combinazione di misure repressive e preventive è quindi determinante per combattere la cybercriminalità. E la rete NEDIK svolge un ruolo importante in quest'ambito, poiché è incaricata di promuovere la collaborazione nel settore delle indagini sulla cybercriminalità informatica. Affinché gli interventi in quest'ambito siano coronati da successo, è essenziale che le varie autorità collaborino e si coordino allo scopo di agire con efficienza e pragmatismo. Lo spazio digitale globalizzato permette agli internauti di navigare a livello planetario e di avere moltissimi contatti in rete. Per questo motivo, anche le forze di polizia svizzere devono poter attingere a risorse globalizzate e a una solida rete di collaborazioni, sia a livello intercantonale che internazionale. Solo in questo modo si potrà combattere con successo la cybercriminalità, questa galassia complessa e sconfinata.

123RF/Kirill Makarov

*«Grazie al 'cyber patrolling' attuato in assenza di sospetti, le forze di polizia svizzere registrano molti successi al loro attivo.»*

* NCMEC = National Center for Missing and Exploited Children (Centro nazionale per i bambini scomparsi e sfruttati)

Street-Art in Gloucestershire

*«Le difficoltà sono di due generi: da un lato, le difficoltà tecniche e, dall'altro, la comprensione del contenuto delle conversazioni.»*

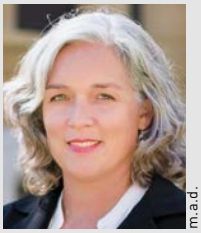
# Sorvegliare ricorrendo ai mediatori linguistici: una pratica in cerca di norme

La sorveglianza delle telecomunicazioni in tempo reale, in certi casi tecnicamente possibile e lecita, può aiutare a prevenire o elucidare reati penali. Ma può anche fallire se il contenuto delle conversazioni non viene capito. Le autorità di perseguimento penale dipendono moltissimo dai mediatori linguistici. Eppure, il loro ruolo nell'ambito dei procedimenti penali è poco studiato. Un progetto di ricerca dell'Università di Neuchâtel sta contribuendo a cambiare questa situazione.

La sorveglianza segreta delle telecomunicazioni è praticata da quando sono stati posati i primi pali del telegrafo nel 1840. Da allora, ogni invenzione in quest'ambito ha permesso di sviluppare nuovi dispositivi di sorveglianza, mentre i progressi realizzati nello stesso periodo nel campo delle tecniche di crittografia hanno reso più difficile alle autorità di perseguimento penale l'accesso al contenuto delle conversazioni. Di conseguenza, è sensazionale quando gli inquirenti di polizie straniere riescono ad accedere a reti criptate come *IronChat, Sky ECC* e *EncroChat.* I dati riguardanti l'operazione *Sky ECC* sono sbalorditivi: a livello mondiale, gli investigatori avrebbero intercettato circa un miliardo di messaggi criptati provenienti da oltre 170 000 utenti in Europa, Nord America, Sud America e Medio Oriente. Per le autorità incaricate dell'inchiesta penale, questo volume di dati pone già di per sé un problema di capacità ai limiti della gestibilità.

Raramente, tuttavia, si pone in questo contesto la domanda che segue, nonostante la sua pertinenza: cosa succede quando i messaggi sono scambiati in una lingua sconosciuta alle competenti

**Autrice**



m.a.d.

**Nadja Capus**
Prof. Dr. iur.
Cattedra di diritto penale e diritto processuale penale
Università di Neuchâtel

rdi

*«L'attività di mediazione linguistica richiede competenze altamente specifiche: ci si esprime infatti nella lingua parlata tutti i giorni, nei dialetti, nelle lingue regionali o addirittura in un linguaggio codificato utilizzato negli ambienti delle persone intercettate.»*

(Foto: Nicole Kidman in "The Interpreter", 2005)

autorità di perseguimento penale? Emerge rapidamente che le difficoltà sono di due generi: da un lato, le difficoltà tecniche e, dall'altro, soprattutto la comprensione del contenuto delle conversazioni. Quest'ultima difficoltà è ancora più problematica quando non si tratta di comunicazioni scritte, ma di conversazioni orali. Il primo e più importante sorvegliante è quindi l'interprete o, come definiamo questa specifica figura professionale, il mediatore linguistico o la mediatrice linguistica. Spesso, infatti, si ignora quanto le autorità di perseguimento penale dipendano da queste persone.

## Conseguenze fatali di una mediazione linguistica inadeguata

Una sorveglianza segreta delle telecomunicazioni può avere conseguenze fatali se ci sono troppo pochi mediatori linguistici, se questi ultimi sono troppo poco o per nulla formati e/o se le istruzioni fornite loro sono insufficienti. Quante perdite di tempo se le traduzioni contestate devono essere controllate da un'altra persona, se gli errori commessi non permettono di utilizzare come mezzo di prova le sequenze sorvegliate, registrate e tradotte.

Qui è importante sottolineare che dopo l'11 settembre, l'intera indagine condotta dall'FBI sugli attentati terroristici negli Stati Uniti non riusciva a progredire proprio a causa delle capacità insufficienti dei mediatori linguistici. In Austria, in un caso di tratta degli esseri umani, è emerso che la mediatrice linguistica, d'intesa con la polizia, aveva in parte scritto nel verbale dichiarazioni completamente diverse da quelle che si trovavano sul nastro ascoltato, in modo da "farle apparire meglio" *(Der Standard,* 6.5.2014). In Svizzera, alcuni procedimenti giudiziari hanno messo in evidenza il fallimento delle cooperazioni tra polizia e mediatori linguistici e l'inadeguatezza delle prestazioni di questi ultimi (vedere Decisioni del Tribunale federale del 28.1.2005 e del 23.9.2013). Le condanne hanno così dovuto essere annullate e i casi sono stati rinviati al Tribunale di primo grado con l'obbligo, per ogni registrazione che si voleva utilizzare, di documentare il metodo impiegato per convertire la registrazione della conversazione telefonica in lingua straniera nella lingua del procedimento. Il tribunale doveva inoltre rivelare l'identità di ogni persona che aveva partecipato all'operazione, così come le istruzioni impartite ad ognuno di loro. E infine doveva dimostrare che ognuno di loro era stato sufficientemente informato sulle conseguenze penali contemplate nell'articolo 307 CP in caso di falsa dichiarazione o traduzione. In assenza di queste informazioni, i verbali della traduzione scritta delle telecomunicazioni sorvegliate in segreto non potevano semplicemente essere utilizzati come mezzo prova.

Questo è – in sintesi – lo standard rudimentale delle norme stabilite dal Tribunale federale nel 2002 nella sua

decisione principale DTF 129 I 85. Ma questo standard è applicato nei cantoni? È sensato? Dovrebbe essere ampliato? Cosa succede effettivamente nella pratica? E le persone coinvolte come vivono questa situazione? Il nostro progetto di ricerca è fra l'altro incentrato proprio su queste domande.

## Un oggetto di ricerca ben poco accessibile

Il ricorso a servizi di interpretariato, traduzione e mediazione linguistica nei procedimenti penali non è una rarità. L'interprete riporta a voce nella lingua d'arrivo quanto viene detto o scritto nella lingua di partenza, lavorando sotto pressione e in tempi ristretti. L'attività di traduzione, invece, equivale per esempio a trascrivere direttamente conversazioni intercettate o anche documenti scritti nella lingua d'arrivo. Nel contesto della sorveglianza segreta delle telecomunicazioni, si possono svolgere entrambe le attività, motivo per cui usiamo il termine di mediazione linguistica. Anche se quest'attività avviene in una fase importante di un'istruzione penale, pochi studi primari hanno analizzato la sua funzione al di fuori della Svizzera, perché l'interesse a mantenere il segreto è ovviamente enorme.

Dal dicembre 2019, il Fondo nazionale per la ricerca scientifica finanzia il nostro progetto di ricerca interdisciplinare dedicato allo studio dei contributi di mediazione linguistica dal punto di vista delle loro condizioni di produzione e del loro impiego nel contesto della sorveglianza segreta delle telecomunicazioni. Da allora, diverse autorità di polizia e i ministeri pubblici di vari cantoni (ma non il Ministero pubblico della Confederazione), ci hanno facilitato, grazie a collaborazioni fruttuose, l'accesso a questo settore dov'è difficile riunire le condizioni di ricerca.

Per poter esaminare più da vicino le attività dei mediatori linguistici, abbiamo dei colloqui con questi ultimi e con gli investigatori della polizia di alcuni di questi cantoni. Conduciamo inoltre un sondaggio online a livello nazionale fra i mediatori linguistici reclutati dalla polizia. Obiettivo: raccogliere informazioni sulla loro formazione, sulle loro competenze linguistiche e di traduzione e sulle loro esperienze professionali. I dati raccolti saranno completati da osservazioni fatte direttamente sul campo. Inoltre, il progetto si focalizza sui prodotti del lavoro dei mediatori linguistici: in base ad un'analisi di 22 incarti penali provenienti da quattro cantoni, si tratta di stabilire, dal punto di vista giurisprudenziale e giuridico-sociologico, come il lavoro dei mediatori linguistici è integrato nelle indagini penali e com'è documentato. Infine, si analizzeranno le registrazioni audio e i relativi verbali dal punto di vista traduttologico. Qui ci si focalizzerà sulle strategie e sui metodi di lavoro adottati dai mediatori linguistici. Il progetto ripercorre anche le fasi di sviluppo di un mezzo di prova che risulta da una conversazione intercettata e che viene aggiunta all'incarto come mezzo di prova scritto.

## Primi risultati

La consapevolezza del problema è molto aumentata negli ultimi anni, in quanto si sono fatti sforzi sia a livello europeo che cantonale (eccezion fatta per la Confederazione) per migliorare la qualità dei servizi linguistici e per inserirli nei procedimenti penali a titolo di documentazione, verifica e possibilità di contestazione. Tuttavia, da una delle nostre analisi emerge che questi sforzi si focalizzano in primo luogo sugli interpreti più visibili, ossia quelli che sono presenti durante i procedimenti giudiziari o gli interrogatori. Eppure l'attività di mediazione linguistica richiede strategie di traduzione molto diverse e competenze altamente specifiche. Ci si esprime infatti nella lingua parlata tutti i giorni, nei dialetti, nelle lingue regionali o addirittura in un linguaggio codificato utilizzato negli ambienti delle persone intercettate. Da notare che l'intercettazione viene effettuata ricorrendo a dispositivi tecnici in circostanze talvolta difficili, ciò che può compromettere la percezione acustica. Si tratta di dialoghi telefonici o (nel caso del collocamento di microfoni in veicoli o locali) anche di conversazioni tra più persone che il mediatore linguistico però non vede mentre ascolta. Le sue capacità di ascolto sono quindi primordiali quando si tratta di riconoscere voci diverse o un cambiamento di lingua. L'alto grado di spontaneità di questi mandati, oltre al fatto che si debba svolgere un'attività ibrida di interpretariato e traduzione, richiede anche ai mediatori linguistici di avere una grande capacità di anticipazione e conoscenze di base specialistiche. Tenuto conto della diversità delle competenze richieste, sorprende che si accetti generalmente (anche da parte del Tribunale federale) che basti essere bilingue per svolgere questa attività molto particolare e impegnativa.

Il trattamento riservato alle informazioni e alle prove ottenute grazie alla mediazione linguistica non tiene conto di queste particolarità, come dimostra l'analisi della letteratura dedicata a questo tema, della giurisprudenza del Tribunale federale e degli atti processuali. La nostra analisi di questi atti (per il momento solo la metà è stata studiata) evidenzia che i criteri di validità stabiliti dal Tribunale federale non sono generalmente soddisfatti nella pratica. Per esempio, né l'identità degli interpreti, né le informazioni sul metodo di traduzione applicato all'interpretariato e neppure le istruzioni impartite ai mediatori linguistici figurano negli incarti analizzati. È relativamente raro trovare l'indicazione che i mediatori linguistici sono stati informati sull'art. 307 CP, ed è ancora più raro che siano stati informati sull'art. 320 CP.

È importante rilevare che l'attività dei mediatori linguistici avviene ad un punto d'intersezione sensibile tra accertamento dei fatti e la loro interpretazione giuridica, motivo per cui le forme informali di cooperazione possono assumere rapidamente una notevole importanza. Dai dati che abbiamo

raccolto finora, emerge tuttavia che vi sono notevoli divergenze riguardanti l'assegnazione dei ruoli definiti dalle autorità, l'autovalutazione dei mediatori linguistici, così come il modo in cui questi ultimi sono istruiti sul caso e sui metodi di lavoro.

È interessante notare che il Tribunale federale – che come abbiamo visto, ha svolto un ruolo importante nel fissare le prime norme in materia – stabilisce una giurisprudenza in pratica contraddittoria. Da un lato, quest'ultimo esige infatti che l'identità dei mediatori linguistici, le istruzioni impartite loro e l'attuazione del loro lavoro siano più visibili. Dall'altro, le sentenze pronunciate permettono di relegare nell'ombra il contributo dei mediatori linguistici alla raccolta e alla selezione delle informazioni ritenute pertinenti per il procedimento, così come la grande responsabilità che incombe loro. Molte delle informazioni indispensabili agli investigatori devono quindi essere trasmesse in via informale tra i mediatori linguistici e la polizia.

## Prospettive

Abbiamo visto che i problemi derivanti da interventi di mediazione linguistica carenti possono causare costi, portare alla perdita di prove, indebolire gli elementi a carico o a discarico, e quindi contribuire al fallimento dei procedimenti penali o causare ritardi che aumentano il rischio di prescrizione. Il nostro progetto di ricerca interdisciplinare, che si concluderà nel novembre 2022 dopo un periodo di tre anni, mira a contribuire a colmare le suddette lacune di ricerca e, nell'ambito degli scambi con i rappresentanti del settore, a trarre insegnamenti che aiuteranno la polizia e i pubblici ministeri a sviluppare "buone pratiche" in materia di selezione e impiego di mediatori linguistici nell'ambito dei casi di sorveglianza segreta delle telecomunicazioni. L'obiettivo è anche di fornire ai tribunali una guida sulle norme auspicabili in materia di raccolta e utilizzo delle prove. Per il suo successo, questo progetto di ricerca beneficia della generosa cooperazione delle autorità di polizia, dei ministeri pubblici e dei tribunali.

**Per ulteriori informazioni** consultare il sito del *Centre romand de recherche en criminologie* dell'Università di Neuchâtel: www.unine.ch/crrc/intercept-interpret.
La professoressa Dr.ssa Nadja Capus (nadja.capus@unine.ch, 032 718 13 05 o 079 536 50 52), responsabile del progetto, il Dr. Damian Rosset (damian.rosset@unine.ch), la Dr.ssa Cornelia Griebel (cornelia.griebel@unine.ch), la Dr.ssa Ivana Havelka (ivana.havelka@unine.ch) e la MLaw Elodie Bally (elodie.bally@unine.ch) saranno lieti di fornirvi maggiori informazioni al riguardo.

# L'uso della sorveglianza elettronica in Svizzera

Oggi, in Svizzera, la sorveglianza elettronica è principalmente utilizzata nell'ambito dell'esecuzione delle pene detentive. Questa pratica permette soprattutto di rilevare a posteriori l'inosservanza delle disposizioni imposte dalle autorità e di verificare la capacità della persona condannata di assumere e mantenere gli impegni presi. Nella sua applicazione attuale, la sorveglianza elettronica costituisce quindi una forma alternativa di sanzione e non serve a prevenire i reati. Ci sono però alcune innovazioni.

Già dal 1999, la possibilità di portare un braccialetto elettronico alla caviglia ha in parte sostituito, in Svizzera, l'esecuzione di una pena in uno stabilimento penitenziario. Nell'ambito di un progetto pilota, la Confederazione aveva all'epoca autorizzato sei cantoni – Basilea Città, Basilea Campagna, Berna, Ginevra, Ticino e Vaud, a cui si è poi aggiunto anche Soletta nel 2003 – ad eseguire alcune pene privative della liberà ricorrendo alla sorveglianza elettronica (SE). Dopo aver sperimentato per circa dieci anni l'utilizzo della sorveglianza elettronica, i feedback di questi cantoni sono stati generalmente positivi. A partire dal 1° gennaio 2018, data della sua entrata


## Autori

**Janine Repetti-Dittes**
Segretaria Generale dell'Associazione *Electronic Monitoring*


m.a.d.

**Alain Hofer**
Segretario Generale supplente, Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia (CDDGP)


m.a.d.

123RF/stocksolutions

*«La sorveglianza elettronica è presa in considerazione solo quando il rischio di fuga o di recidiva sono praticamente nulli.»*

nel Codice penale, questa pratica è contemplata nel diritto federale. Da allora, i cantoni sono tenuti a proporre la sorveglianza elettronica come forma di esecuzione delle pene privative della libertà.

A certe condizioni, la sorveglianza elettronica può essere utilizzata per l'esecuzione di brevi pene privative della libertà da 20 giorni a 12 mesi *(la cosiddetta SE frontdoor)*. Inoltre, si può utilizzare la sorveglianza elettronica per un periodo da tre a dodici mesi *(la cosiddetta SE backdoor)* su persone che stanno per beneficiare di una liberazione condizionale alla fine di lunghe pene detentive. La sorveglianza elettronica è presa in considerazione solo quando il rischio di fuga o di recidiva sono praticamente nulli. Inoltre, la persona che si sottopone alla sorveglianza elettronica deve avere un domicilio fisso e una vita quotidiana strutturata (lavoro, formazione), e deve anche essere d'accordo con questa forma d'esecuzione della pena e con il piano d'esecuzione proposto. La persona deve inoltre dimostrare di essere capace di assumere e mantenere gli impegni presi, e le persone adulte che vivono nella sua stessa economia domestica devono essere d'accordo con questa forma d'esecuzione della pena. Se si presume che una persona continui a costituire un pericolo, la sorveglianza elettronica non viene invece presa in considerazione nel periodo di privazione della libertà.

Gli obiettivi e i vantaggi dell'esecuzione di pene privative della libertà ricorrendo alla sorveglianza elettronica sono evidenti: nel caso di pene detentive di breve durata, fino a un anno, questa pratica evita ampiamente la stigmatizzazione associata all'esecuzione di pene privative della libertà in uno stabilimento penitenziario. La persona condannata non viene infatti "tagliata fuori" dal suo contesto familiare e dalla sua vita quotidiana. Può continuare a lavorare e a frequentare il proprio ambiente professionale e privato. Dato che però la persona sorvegliata può lasciare il proprio domicilio solo a determinati orari e deve trascorrere il proprio tempo libero agli arresti domiciliari, la pena privativa della liberà mantiene tutto il suo carattere punitivo. Utilizzata alla fine di una lunga pena detentiva, la sorveglianza elettronica può facilitare il reinserimento controllato nella società. Di conseguenza, questa soluzione riduce significativamente i costi di esecuzione della pena e di reinserimento per la collettività.

## Campi d'applicazione della sorveglianza elettronica

Nel frattempo, però, altri campi d'applicazione della sorveglianza elettronica si sono aggiunti a quello dell'esecuzione

delle pene privative della libertà. Dal 1° gennaio 2011, il Codice di procedura penale svizzero ha adottato questa soluzione come pratica per sorvegliare le misure sostitutive in alternativa alla carcerazione preventiva e alla detenzione per motivi di sicurezza. Dal 1° gennaio 2015, il Codice penale prevede inoltre la sorveglianza elettronica per l'esecuzione dei divieti di avere contatto e di accedere a determinate zone. Dal 1° gennaio 2022, anche il diritto civile ricorrerà alla sorveglianza elettronica per proteggere le persone vittime di violenza. Altri campi d'applicazione sono attualmente al vaglio. Per esempio, la sorveglianza elettronica è anche prevista nell'ambito delle misure di polizia per combattere il terrorismo. Infine, si discute l'uso della sorveglianza elettronica anche nel settore delle misure coercitive nell'ambito del diritto sugli stranieri.

## Requisiti tecnici e generi di sorveglianza

Questi nuovi campi d'applicazione hanno anche cambiato le aspettative e i requisiti posti alla tecnologia. Nell'ambito dell'esecuzione delle pene privative della libertà, per esempio, di regola non si cerca di sapere dove si trova esattamente la persona sorvegliata quando non è a casa. Ci si limita a verificare se la persona si trova o meno in casa negli orari prescritti e quindi a stabilire la sua presenza o assenza in un determinato luogo. Questo genere di sorveglianza non richiede quindi un monitoraggio GPS per determinare la posizione esatta della persona sorvegliata, perché la sua localizzazione è meno importante. Si misura solamente la distanza tra il trasmettitore, fissato in modo permanente alla caviglia della persona condannata, e il ricevitore installato al suo domicilio. Il segnale è trasmesso tramite la rete telefonica al servizio competente che confronta i dati ricevuti con i dati del programma della persona sorvegliata. Se le assenze non corrispondono agli orari impostati o se la persona sorvegliata tenta di manipolare o rimuovere il braccialetto elettronico, scatta un allarme. Attualmente, la cosiddetta sorveglianza RF (= radiofrequenza) è l'opzione più utilizzata in Svizzera.

Negli altri campi d'applicazione, si pongono in parte requisiti diversi alla tecnologia. Quando si ricorre alla sorveglianza elettronica nell'ambito del diritto civile per proteggere vittime di violenza, si richiede per esempio di determinare e registrare costantemente il luogo in cui si trova la persona sorvegliata. Occorre in tal caso utilizzare la tecnologia GPS. Questa sorveglianza GPS (= *global positioning system*, ossia sistema di posizionamento

Adobe Stock/toya_uz

*«In futuro, il campo d'applicazione della sorveglianza elettronica dovrà essere ampliato, soprattutto nella sfera di competenza della polizia, in particolare per combattere la violenza domestica e lo stalking.»*

globale) permette di controllare di continuo la posizione della persona sorvegliata e di creare profili di movimento. Tecnicamente, esistono varie soluzioni per praticare una sorveglianza GPS.

Dato che questa tecnologia assicura una localizzazione in tempo reale, la sorveglianza con il GPS ha anche un ulteriore effetto preventivo. La persona sorvegliata è infatti consapevole che può essere rintracciata in qualsiasi momento e quindi che la probabilità di essere scoperta in caso d'infrazione è molto alta.

La sorveglianza GPS ha però anche delle limitazioni tecniche. In determinati luoghi, come all'interno di grandi centri commerciali, nei seminterrati o nelle gallerie, la ricezione satellitare è limitata. In questi luoghi inaccessibili ai segnali GPS, il sistema può allora essere integrato dalla rete mobile, localizzando la persona in funzione della sua distanza dal più vicino palo della telefonia mobile. La precisione della localizzazione dipende tuttavia dal grado di copertura della zona con antenne di telefonia mobile.

La tecnologia GPS permette di controllare i movimenti della persona sorvegliata sia a posteriori (la cosiddetta sorveglianza passiva) che in tempo reale (la cosiddetta sorveglianza attiva). Nel caso della sorveglianza passiva, i dati dei movimenti sono principalmente analizzati dall'autorità competente durante le ore d'ufficio. Nel caso della sorveglianza attiva, la localizzazione avviene in tempo reale e la persona è sorvegliata 24 ore su 24. Non appena la centrale di sorveglianza riceve un messaggio d'allarme, si ordina immediatamente un intervento predefinito che può consistere in una presa di contatto telefonica con la persona sorvegliata o anche in un intervento di polizia. Il ricorso alla sorveglianza elettronica non deve tuttavia far credere che questa soluzione sia un mezzo affidabile per prevenire i reati. Dato che l'uso della sorveglianza attiva può suscitare aspettative che non si possono soddisfare, occorre essere prudenti quando si ricorre a questa soluzione e pianificare con attenzione il suo uso. È infatti problematico se la polizia deve intervenire immediatamente per prevenire un possibile reato quando la persona condannata non rispetta gli obblighi stabiliti.

## Cooperazione intercantonale: il punto della situazione

Le esperienze fatte nell'ambito dell'applicazione della sorveglianza elettronica hanno evidenziato che non è sensato per ogni cantone dotarsi delle proprie strutture per seguire i casi di sua competenza. La Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia (CDDGP) ha quindi commissionato già nel 2013 i lavori di armonizzazione della sorveglianza elettronica. Infine, nell'autunno 2019, è stato costituito il "Verein gesamtschweizerisches Electronic Monitoring – Investition und Betrieb" (Associazione svizzera per la sorveglianza elettronica – investimento e gestione), il cui obiettivo è di offrire ai cantoni membri un sistema unitario di sorveglianza elettronica a livello nazionale che tenga conto delle esigenze di ogni cantone per quanto riguarda le varie applicazioni in quest'ambito. A tutt'oggi, 22 cantoni hanno aderito all'associazione.

In occasione dell'assemblea autunnale della CDDGP nel novembre 2020, i cantoni membri hanno deciso di non dotarsi, per il momento, di una centrale di sorveglianza comune nell'ambito del progetto attuale. In una prima fase, il nuovo sistema non permette quindi di attuare una sorveglianza attiva in tutti i cantoni membri. In quella stessa occasione, la CDDGP ha ribadito che le soluzioni prese in considerazione permetteranno però di farlo in futuro. Questo darà la possibilità di introdurre agevolmente la sorveglianza attiva in un secondo tempo, cioè quando i cantoni, che già cooperano con una centrale di sorveglianza e che praticano la sorveglianza attiva, disporranno di un'esperienza sufficiente in materia.

Nel febbraio 2021 è stata lanciata una gara d'appalto pubblica per trovare un operatore che offra una soluzione nazionale in grado di soddisfare le condizioni e i requisiti elaborati dai rappresentanti cantonali e dai vari gruppi d'interesse nella fase di concezione del progetto. Attualmente, tre cantoni pilota stanno ampiamente testando gli apparecchi dei vari fornitori. Il nuovo sistema dovrebbe essere introdotto in tutti i cantoni nel corso del 2022 ed entrare in funzione entro il 1° gennaio 2023 al più tardi.

## Conclusioni e prospettive

Oggi, in Svizzera, la sorveglianza elettronica è utilizzata principalmente nel campo della privazione della libertà. Scopo principale: rilevare a posteriori le violazioni degli obblighi imposti dall'autorità e verificare la capacità della persona condannata di assumere e mantenere gli impegni presi. Le violazioni sono comunicate ai servizi competenti e sanzionate, se necessario. Nella sua applicazione attuale, la sorveglianza elettronica costituisce quindi una forma alternativa di sanzione, ma non serve a prevenire i reati.

In futuro, il suo campo d'applicazione dovrà essere ampliato, soprattutto nella sfera di competenza della polizia, in particolare per combattere la violenza domestica e lo stalking. In quest'ambito, si vuole testare l'uso della sorveglianza elettronica in combinazione con altri strumenti di protezione dalla violenza per acquisire esperienze in materia. La strategia più promettente sembra appunto essere la combinazione di misure di sorveglianza elettronica con una gestione efficace delle minacce.

L'intento dell'Associazione *Electronic Monitoring* è di fornire ai cantoni una soluzione unica e pragmatica per mettere in pratica la sorveglianza elettronica. L'obiettivo è di garantire che la sorveglianza elettronica e le possibilità tecniche ad essa associate siano sempre utilizzate dove generano un reale valore aggiunto.

# «Occorre sempre soppesare le cose»

## Conversazione con Jürg Halter sulla correlazione tra sorveglianza privata o statale e crisi del coronavirus, digitalizzazione, democrazia, desiderio di risposte semplici e linguaggio.

© by Rob Lewis

*Jürg Halter, pluripremiato scrittore e interprete di arte oratoria, vive e lavora a Berna. Esprime regolarmente le sue opinioni su temi socio-politici nei media sia tradizionali che sociali. Recentemente, la sua raccolta di poesie "Gemeinsame Sprache" è stata pubblicata dalla casa editrice Dörlemann Verlag.*

***Signor Halter, all'inizio di quest'anno lei è stato ospite della trasmissione "Literaturclub" (club letterario) in onda sul canale televisivo SRF dove ha presentato una nuova traduzione del romanzo "1984" di George Orwell, probabilmente il romanzo più famoso sul tema della "sorveglianza". Quali aspetti di questa tematica la interessano in particolare?***

Nel suo romanzo, pubblicato nel 1949, Orwell illustra in modo esemplare fin dove può arrivare uno Stato quando controlla tutto e tutti e sorveglia ogni dichiarazione, perché in questo racconto tutte le persone sono sorvegliate 24 ore su 24. Ci sono teleschermi che istruiscono la popolazione su quando andare a letto e quando alzarsi, e la sorvegliano sul lavoro. E c'è una psicopolizia che usa i teleschermi per interpretare le espressioni del volto e capire per esempio se qualcuno sta pensando qualcosa contro lo Stato o una delle sue leggi. In quel caso, le persone sono risvegliate dal loro sonno, arrestate e semplicemente fatte sparire. Oppure subiscono un lavaggio del cervello e vengono poi, per così dire, purificate, o meglio lobotomizzate prima di essere reinserite nella società. Da un lato, si potrebbe dire che si tratta di un'esagerazione, ma dall'altro, Orwell si è ovviamente ispirato alle vere e proprie dittature dell'epoca, in particolare allo stalinismo e, naturalmente, al nazismo. L'aspetto affascinante e spaventoso di questo romanzo è quanto sia ancora d'attualità.

***...o nuovamente d'attualità. Perché per la prima volta le possibilità tecniche non sono mai state così simili a quanto descritto nel romanzo. La sorveglianza della micromimica, per esempio, potrebbe ben presto essere tecnicamente fattibile.***

Proprio così. Da un lato, il romanzo riflette l'epoca in cui è stato scritto e, dall'altro, è così spaventoso perché fa predizioni per molti versi alquanto azzeccate. E forse tutto questo diventa ancora più angosciante se si considera che oggi la tecnologia è molto più avanzata di quanto fosse allora immaginabile. Penso per esempio ai "deep fake", cioè alla possibilità di utilizzare poche riprese video di una persona per farle dire qualcosa che non ha mai detto per poi incriminarla sulla base di questo video. Una grande differenza con la pratica della sorveglianza nel romanzo è che oggi molte persone si autosorvegliano volontariamente, o apparentemente volontariamente, con i loro smartphone e smartwatch. Quando fanno jogging, per esempio, hanno con sé questi dispositivi con cui misurano le pulsazioni, la frequenza cardiaca, ecc. Trasmettono poi i dati rilevati alla società d'assicurazione, la quale concederà loro eventualmente riduzioni di premio. Ma la maggior parte dei dati oggi raccolti da noi e su di noi dai nostri smartphone, computer, ecc., saranno potenzialmente utilizzati nel nostro interesse o contro di noi solo in futuro. Per il momento, la maggior parte di questi dati non è ancora stata analizzata.

***Noi in Svizzera viviamo – si è quasi propensi a dire – in una delle ultime democrazie rimaste, molto lontana da una società distopica orwelliana. Secondo lei, quindi, quanto è sentito il problema da noi? Quanto è grande per noi il pericolo che improvvisamente le nostre conquiste democratiche siano del tutto annullate per vie traverse dalla tecnologia?***

Fondamentalmente, vedo due tipi di minacce possibili: da un lato, quella dei giganti tecnologici globalizzati che raccolgono costantemente dati e, dall'altro, quella dello Stato, ma in questo caso per via piuttosto della sua passività. Lo Stato, infatti, si mostra spesso completamente impotente di fronte ai gruppi internazionali, anche se ci sono possibilità legali per limitare la sorveglianza fatta dai gruppi tecnologici. Ma questo funziona solo se tutti i paesi dell'Unione Europea adottano le necessarie risoluzioni in materia. Un solo paese può fare poco. Un grande pericolo consiste anche nell'atteggiamento ingenuo di molte persone che tendono spesso a dichiarare: "se non si fa niente di male, non può succedere niente". Ma la domanda da porsi è sempre: chi definisce cos'è sbagliato e cos'è giusto? Quando un sistema cambia, può succedere rapidamente che quello che si pensava fosse giusto venga improvvisamente considerato sbagliato. Allora la situazione diventa davvero pericolosa! A mio avviso, la digitalizzazione viene ancora presentata in modo troppo positivo, ossia parlando quasi esclusivamente di aumento della libertà. Eppure la digitalizzazione rende le persone sempre più trasparenti, e quindi anche sempre più vulnerabili. E se l'individuo diventa sempre più vulnerabile, allora l'intera società e la democrazia stessa sono sempre più a rischio, perché la democrazia prospera grazie alla fiducia.

***Qual è esattamente la relazione tra il progresso della digitalizzazione e la perdita di fiducia? Nell'attuale situazione dovuta al coronavirus, si osserva che la fiducia nelle misure prese dallo Stato è andata persa in molti ambiti. Anche diversi suoi colleghi di spicco della scena culturale esprimono scetticismo, vedono cospirazioni o parlano addirittura di una dittatura del coronavirus. Qual è la sua opinione in proposito?***

Fondamentalmente, quando si pone loro una domanda e si dà loro un microfono in mano, molte persone tendono a rispondere, anche se non hanno la competenza per farlo. Anche gli operatori culturali non sono immuni alla stupidità e come gli altri sono inclini a credere a risposte troppo semplicistiche, a presunti nemici e a teorie del complotto. È vero, ci sono alcuni stati che non potevano più essere definiti democrazie anche prima della crisi del coronavirus e che hanno usato le misure contro la pandemia come un'opportunità per limitare ulteriormente la libertà dei loro cittadini. Questo è realmente accaduto. Per contro, è ridicolo parlare di una dittatura del coronavirus qui in Svizzera, perché le misure adottate erano sostanzialmente facili da capire e sono state comunicate in modo comprensibile. Tuttavia, non ci si può aspettare che tutte le misure siano di primo acchito sempre coerenti e non abbiano alternative, poiché questa crisi sanitaria è nuova per tutti noi e si deve poter reagire con flessibilità. Anche se molte persone non hanno più la consapevolezza dello Stato, se non quando devono pagare le tasse, il fatto che lo Stato abbia riacquistato così tanto potere in così poco tempo è stato del tutto inaspettato, ma probabilmente non c'è altro modo di reagire ad una catastrofe naturale. Se le misure fossero state dapprima sottoposte a votazioni popolari, il numero di vittime sarebbe stato molto più alto e la catastrofe molto più grande. Ma molte persone cercano spiegazioni semplici, sospettano che dietro il coronavirus si celi un potere malvagio, credono che la pandemia sia solo una manovra diversiva, ecc. Queste teorie del complotto sono sempre esistite, ma ora la digitalizzazione permette una loro diffusione molto più veloce, e le persone che ci credono entrano in contatto molto più facilmente e rapidamente tra loro.

***Che ruolo svolgono i media in questo contesto?***

I media, che naturalmente guardano anche al numero di click che generano, spesso danno maggiore spazio alle voci più forti, anche se queste raramente rappresentano la maggioranza della popolazione. A mio avviso, anche i media qui hanno una loro responsabilità, per esempio perché utilizzano erroneamente il termine *scettico,* che in realtà è chiaramente definito. Chiunque neghi l'esistenza o la pericolosità del virus non è uno scettico, bensì è un negazionista. Scettico è invece chi critica le misure argomentandole. Ma nei media c'è spesso una totale confusione fra questi termini. Direi allora ai media: prestate maggiore attenzione a quelle persone disposte ad esprimersi criticamente ma che sono anche in grado di motivare le loro critiche con argomenti razionali, piuttosto che a quelle che mentono e diffondono teorie complottiste. A proposito, alle persone che dicono seriamente che qui abbiamo vissuto in una dittatura, sarei felice di acquistare un biglietto aereo per la Bielorussia o la Corea del Nord, così che possano sperimentare lì la loro idea di libertà!

***O in Austria? Scherzi a parte. Sembra che in passato fosse più facile accordarsi su ciò che è un fatto e su ciò che non è, e poi discutere su come valutare questi fatti. Oggi sembra che per ogni fatto ci sia un fatto alternativo. Ognuno può credere quello che vuole e dichiarare che si tratta di un fatto. Come mai?***

La tecnologia digitale dà a molte persone la sensazione di poter dire la loro quando prima solo le cosiddette élite potevano esprimersi. Da un lato, questo è positivo, ma dall'altro è altamente problematico, perché questo ha estremamente abbassato la soglia d'inibizione per esprimersi. In passato, per esempio, bisognava fare uno sforzo per

scrivere a macchina o a mano una lettera dei lettori, poi affrancarla e spedirla all'editore di un giornale. C'erano diversi ostacoli da superare. E poi c'era sempre una redazione che decideva se questa lettera doveva essere data alle stampe o meno. Oggi, basta un clic per far pubblicare la propria opinione, cosa allettante, naturalmente. Ognuno diventa il proprio mezzo di comunicazione. E qui si verificano molte contraddizioni: persone che, da un lato, pubblicano costantemente fatti personali e foto di se stessi sui media sociali e, dall'altro, si indignano per la registrazione dei loro dati nei ristoranti perché si sentono minacciati nella loro libertà. Credo che queste contraddizioni riguardino un po' tutti noi: esigiamo il rispetto del nostro anonimato e della nostra sfera privata da un lato, mentre con il nostro stesso comportamento inganniamo noi stessi dall'altro.

Per quanto riguarda l'opposizione tra fatti e affermazioni, opinioni, fake news, ecc., trovo che assistiamo ad un'evoluzione problematica, perché anche in questo caso non si fa alcuna differenziazione. In effetti, si può credere nella scienza e nei fatti, ma essere comunque critici nei confronti di certi sviluppi scientifici. Per esempio, se si legge uno studio sul tenore di zucchero negli alimenti e che dopo essersi informati in modo più approfondito in materia, ci si rende conto che lo studio è stato commissionato da un'azienda alimentare, allora si dovrebbe analizzare lo studio in questione con spirito critico. Occorre sempre soppesare le cose. Ma molte persone vogliono risposte chiare e non sopportano i pareri contraddittori. Come se ci fosse sempre e solo una risposta giusta o sbagliata, un atteggiamento a favore o contrario.

***Eccolo di nuovo, il principio digitale: sì o no, zero e uno! Già negli anni settanta e ottanta, persone avvedute temevano che la permeazione delle nostre vite e del nostro pensiero con la digitalità ci avrebbe alla fine reso vittime di quest'ultima, al punto da non essere più nemmeno in grado di immaginare che sia necessario avere anche un "sia l'uno che l'altro", un "né l'uno, né l'altro" e un "forse".***

Questo è il punto cruciale: la digitalizzazione ha davvero un impatto sul nostro pensiero. Lo si può anche osservare, per esempio, nel sistema educativo con i test a scelta multipla: non si deve più essere in grado di formulare e soppesare le cose autonomamente. Oggi basta cliccare su questo o quello, ed è fatta. Questo è pericoloso perché una democrazia degna di questo nome vive di diversità e differenze, di tolleranza e rispetto delle opinioni e dei punti di vista altrui. La democrazia ha anche bisogno che si trovi il consenso su certe cose, per esempio sul funzionamento della democrazia stessa! Uno Stato di diritto vive di tutto questo. Ma la digitalizzazione, così come si è sviluppata finora, ci porta a credere che si deve sempre decidere per una o per l'altra cosa. Alla fine, questo porta ad una frammentazione della società in compartimenti sempre più stagni di persone che la pensano allo stesso modo.

***Una volta, Jean Ziegler l'ha definita una "voce politica importante" nel nostro Paese. Qual è il legame tra la sua attività di scrittore e artista dell'oratoria e il suo impegno politico?***

Dato che la lingua è il mio strumento d'espressione, cerco sempre di essere consapevole di ciò che posso farne, e non solo nell'arte, bensì anche in tutta la società. La lingua è spesso anche lo strumento con cui una democrazia viene dapprima attaccata ma poi anche difesa. Dato che la lingua è usata come mezzo di propaganda, mi interessa non solo scrivere bei libri o poesie, ma in generale anche conoscere il suo funzionamento: sapere cosa viene detto o meno, da chi e come, cosa viene nominato e cosa viene evitato in una formulazione. Ecco perché mi piace anche analizzare i discorsi di politici o capi d'azienda, per esempio. Spesso è proprio ciò che non si dice a dire molto di più di ciò che si dice. Anche i giuristi sono spesso persone molto attente alla lingua, perché è estremamente importante il modo di formulare qualcosa nel linguaggio giuridico. Prendiamo per esempio il termine "soggetto pericoloso": si tratta di una nozione molto vaga e, a seconda del sistema in cui si vive o del modo in cui questo termine viene definito, un "soggetto pericoloso" può già essere inteso come qualcuno che semplicemente pensa in modo critico e che poi potrebbe essere da sorvegliare.

***Si tratta solo di affermazioni formulate in modo vago o che non sono affatto formulate? O non siamo già andati oltre, ossia ad uno stadio in cui molti termini hanno assunto un nuovo significato? Penso a questa frase attribuita ad Adorno che dichiara: "Non ho paura del ritorno dei fascisti come fascisti, ma del loro ritorno come democratici". È esattamente quello che si osserva ora, per esempio, con il termine "terrorismo". Nel frattempo, i dittatori e gli autocrati intorno a noi di riflesso accusano di "terrorismo" i manifestanti pacifici, i giornalisti investigativi e altri oppositori politici, perché considerano che chi fa arrestare i terroristi è nel giusto. Ma in realtà si tratta solo di una sfacciata ridefinizione del termine, e non di una vaga bugia, bensì di una falsità formulata con precisione. Come si combatte questa situazione?***

A mio avviso è molto pericoloso cambiare il significato delle parole e, nel peggiore dei casi, assegnare loro un senso contrario, allo scopo di limitare le libertà. Questo può avvenire a livelli molto diversi, per esempio quando si descrive la crescente sorveglianza come strumento per difendere la libertà, tralasciando però semplicemente di esporre l'altra metà della verità. La mia missione come scrittore, rispettivamente come persona che esprime pubblicamente delle critiche, consiste nell'ascoltare attentamente – e nominare – ciò che viene effettivamente detto. Si capisce ciò che viene effettivamente detto o invece si suggerisce il contrario senza esprimerlo? Per respingere critiche sgradevoli, si usano spesso ter-

mini per screditare i critici, per dipingerli come cattivi, oppure si annacquano linguisticamente i fatti sgradevoli. Così, una critica alla limitazione della libertà sarà ridefinita come un attacco alla libertà. Il modo migliore per contrastare tutto questo è quello di non stancarsi mai di denunciare le manipolazioni e le distorsioni linguistiche in quanto tali e di informare la gente al riguardo.

***Ancora una domanda personale: si sente veramente sorvegliato?***

So di essere molto sorvegliabile, già per il solo fatto di usare i computer, e ogni volta che ci penso, mi spavento di quanto sono probabilmente sorvegliato. Sapendo quanti dati rivelo, in realtà sono molto negligente in quest'ambito. Ecco perché penso che sia sbagliato che lo Stato scarichi questa responsabilità sui suoi cittadini. È compito dello Stato porre dei limiti ai gruppi tecnologici in modo che non abbiano affatto la possibilità di scoprire più informazioni sulle persone di quanto sia loro legalmente consentito. È illusorio pensare che l'utente assuma questa responsabilità. E anche lo Stato dev'essere sorvegliato da organismi indipendenti che controllino come utilizza i dati dei propri cittadini. Se lo Stato sorveglia, a sua volta dev'essere sorvegliato. Più uno Stato sorveglia, più diventa paranoico, e meno fiducia risponde nei suoi cittadini.

***La sorveglianza va bene, la fiducia è meglio?***

Per giustificare la sorveglianza, si invoca spesso la necessità di garantire la sicurezza. Occorre trovare un equilibrio tra sicurezza e libertà. La sicurezza assoluta è forse possibile, ma in quel caso non c'è più libertà. Non è una questione di "o uno, o l'altro", ma di "sia l'uno che l'altro"! In linea di principio sono naturalmente favorevole a trattare la questione in modo democratico e trasparente.

*Jürg Halter, grazie mille per l'interessante conversazione!*


Weber & Partner

*Manifesto dell'UFSP scarabocchiato nella città vecchia di Berna nell'aprile 2021.*

# Cittadini e polizia: chi può filmare chi nei luoghi pubblici?

In Svizzera, le *bodycam* in dotazione alla polizia sono al centro di polemiche e non fanno ancora parte del equipaggiamento standard delle forze dell'ordine. A differenza degli Stati Uniti, nel nostro Paese, il principio di trasparenza non si applica alle registrazioni video della polizia. Nel contempo, chiunque – giornalisti inclusi – filmi delle operazioni di polizia, si espone a delle sanzioni. Per questo motivo, in un'epoca in cui le telecamere sono onnipresenti, sarebbe utile, per tutte le parti coinvolte, rafforzare e perfezionare la giurisprudenza in materia.

Conoscete *Audit the Audit*, il canale YouTube americano che analizza "le interazioni giuste o sbagliate della polizia"? Sulla base di registrazioni video, questo canale valuta il comportamento delle persone coinvolte – agenti di polizia e altri funzionari da un lato, e cittadini dall'altro – durante i vari interventi. Le interazioni sono commentate sulla scorta delle basi legali e della relativa giurisprudenza. Infine, si dà un voto alle persone coinvolte. Così, una poliziotta che si comporta in modo esemplare e conformemente alla legge può ricevere il voto più alto, ossia "A+", mentre un cittadino che si comporta in modo scorretto riceve una "F" corrispondente a una nota insoddisfacente.

## Il diritto di filmare la polizia negli Stati Uniti

Le registrazioni video provengono da smartphone e videocamere di cittadini, così come dalle *bodycam* (videocamere portatili posizionate su una persona) e dalle *dashcam* (videocamere installate sui veicoli) in dotazione agli agenti di polizia. Negli Stati Uniti, i cittadini hanno di regola il diritto di filmare le operazione di polizia, anche se sono direttamente coinvolti, per esempio durante un controllo della circolazione. Nel contempo, molti corpi di polizia filmano sistematicamente i loro interventi con le loro telecamere. Queste riprese sono considerate *Public Record* (documenti pubblici) e sono generalmente accessibili a tutti. Lo stesso vale per le fotografie e le registrazioni audio. A livello federale, la base legale è fornita dal *Freedom of Information Act* (FOIA), ossia la legge sulla libertà d'informazione, e da leggi simili in vigore nei vari stati americani. Filmare la polizia è un *First Amendment Right* (diritto del primo emendamento) che negli Stati Uniti fa parte della libertà di opinione e di parola *(Freedom of Speech)*. È d'altronde grazie ai *First Amendment Audits* (Audit del Primo Emendamento) che vari attivisti – dal comportamento più o meno "simpatico" – verificano se la loro libertà di parola è effettivamente garantita.

L'importanza di tali registrazioni video è stata recentemente dimostrata in occasione della morte di George Floyd durante un intervento della polizia a Minneapolis. Le riprese realizzate dai testimoni e dalla polizia hanno fatto scalpore in tutto il mondo e sono state messe agli atti come base importante per il procedimento penale.

In Svizzera, le *bodycam* della polizia sono politicamente controverse e il loro impiego non è ancora ufficiale. A differenza degli Stati Uniti, il principio di trasparenza non si applica alle registrazioni video della polizia, né a livello federale, né a livello cantonale.

Nel contempo, chiunque – giornalisti inclusi – filmi delle operazioni di polizia in Svizzera, si espone a delle sanzioni. Capita spesso, infatti, che le persone che filmano operazioni di polizia siano arrestate e costrette a cancellare le registrazioni video o addirittura a consegnare il proprio smartphone. Il 1° maggio 2021, a Zurigo, alcuni professionisti dei media sono stati in parte ostacolati nello svolgimento del loro lavoro d'informazione.

## Filmare nei luoghi pubblici: una realtà in contrasto con l'ordinamento giuridico in vigore

Indipendentemente dalle operazioni di polizia, filmare nei luoghi pubblici sta diventando un'attività sempre più diffusa. Da un lato, quasi tutti hanno a portata di mano, in qualsiasi momento, una potente videocamera grazie al proprio smartphone e, dall'altro, si può fare scalpore con le registrazioni video girate in luoghi pubblici pubblicandole su TikTok e altre piattaforme di media sociali. Il boom di canali dedicati, come "Szene isch", lo dimostrano bene. Anche le *dashcam* nei veicoli stanno diventando sempre più popolari. D'altronde, questa categoria comprende ormai più di cento prodotti acquistabili online in qualsiasi momento.

Eppure, filmare nei luoghi pubblici e pubblicare le registrazioni fatte è una realtà in contrasto con l'ordinamento giuridico svizzero in vigore. La polizia può generalmente contare sul fatto che

**Autore**


m.a.d.

**Martin Steiger**
Lic. iur. HSG
Avvocato specializzato in diritto nello spazio digitale, Zurigo

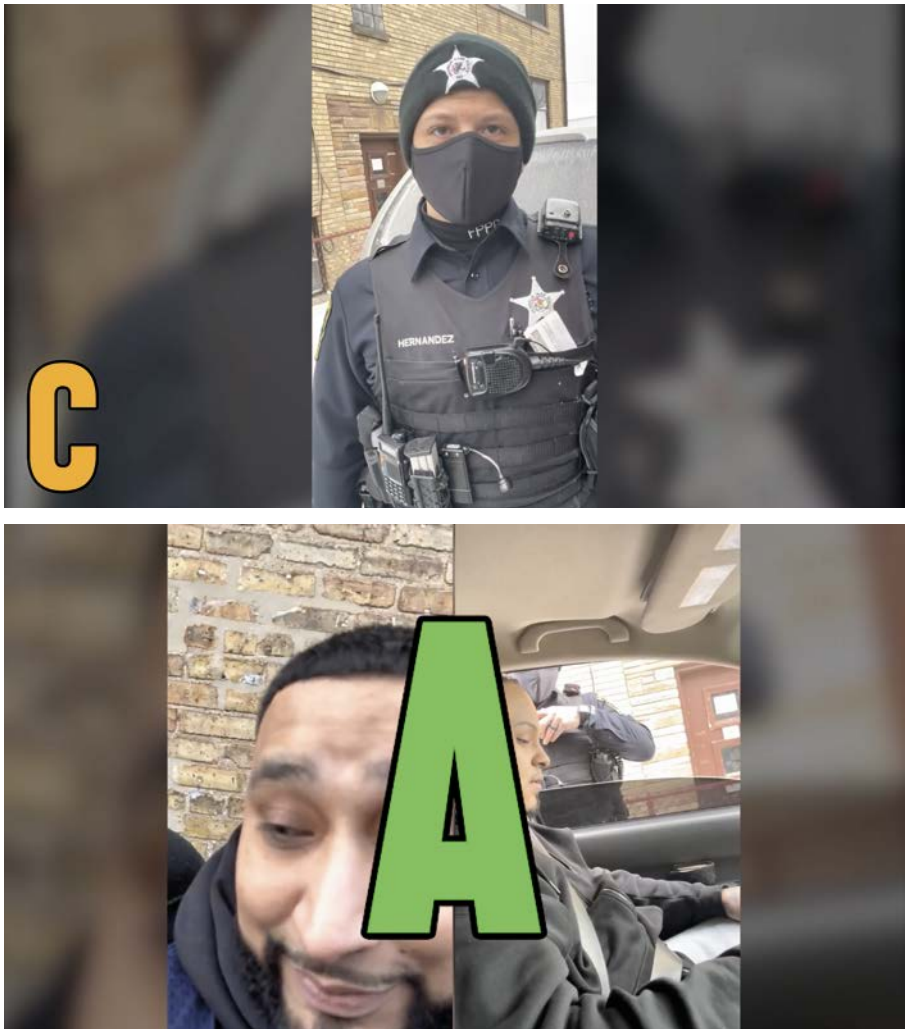
la giurisprudenza non solo vieta la registrazione dei suoi interventi, bensì rifiuta anche l'utilizzo delle registrazioni effettuate con *dashcam* per perseguire infrazioni e delitti, e quindi la stragrande maggioranza delle presunte violazioni del codice stradale. Anche il solo fatto di filmare senza successiva pubblicazione delle riprese può violare i principi della protezione dei dati e della personalità, in particolare in relazione al "diritto alla propria immagine". Dalla sentenza del Tribunale federale nel caso Google Street View del 2012, è emerso chiaramente che anche le persone "accessorie" devono in linea di principio acconsentire ad essere filmate nel caso di registrazioni digitali.

Dato che per le persone filmate contro la loro volontà è molto complicato sporgere denuncia, la protezione della personalità può essere invocata quasi solo dal proprio difensore nell'ambito di un procedimento penale. Questo è probabilmente uno dei motivi per cui molti agenti di polizia tentano di impedire fin dall'inizio la registrazione dei loro interventi. A ciò si aggiunge il fatto che il "diritto alla propria immagine" non gode di alcuna protezione nell'ambito del diritto penale, bensì dev'essere fatto valere nel quadro di un'azione civile che – per una volontà politica esplicita – è onerosa e non funziona senza l'assistenza di un avvocato.

## Moltiplicazione delle registrazioni nei luoghi pubblici

Le registrazioni video nei luoghi pubblici – specialmente di operazioni di polizia – si moltiplicano sempre più. È ormai evidente che la polizia adotta approcci molto diversi per combattere le presunte violazioni del diritto nell'ambito di manifestazioni. Quando vi sono manifestazioni della sinistra, la polizia agisce sempre in modo repressivo, anche nei confronti dei professionisti dei media. Nel caso di alcune manifestazioni contro le misure di protezione anti COVID-19, invece, non solo la polizia ha ampiamente rinunciato a procedere in modo repressivo, in nome della presunta "proporzionalità", ma ha addirittura dovuto talvolta lasciarsi letteralmente prendere in giro dai manifestanti, mentre altrove si sono persino verificate scene di fraternizzazione. Le registrazioni video permettono di avviare il dibattito su questa disparità di trattamento, dibattito che dovrebbe essere scontato in uno Stato di diritto democratico, ma che troppo spesso avviene solo sulla base di "prove" costituite dalla pubblicazione di queste registrazioni video.

Questo dibattito aiuta, tra l'altro, quei membri delle forze di polizia che non sono d'accordo con la procedura scelta, ma che non possono o non vogliono esprimersi criticamente.




*«Conoscete* Audit the Audit, *il canale YouTube americano che analizza 'le interazioni giuste o sbagliate della polizia'?»*

Per me è chiaro che le operazioni di polizia nei luoghi pubblici debbano poter essere filmate, a condizione di non violare il diritto della personalità dei poliziotti coinvolti. Da un punto di vista legale, l'interesse pubblico superiore giustifica un controllo rigoroso delle attività della polizia. Inoltre, non c'è motivo di privilegiare inutilmente i professionisti dei media, perché nello spazio digitale ogni cittadino può fregiarsi in qualsiasi momento del titolo di giornalista, mentre nei media tradizionali i confini tra i ruoli professionali e privati si confondono. Tuttavia, le registrazioni video e la loro pubblicazione raggiungono i loro limiti quando i singoli agenti di polizia si ritrovano, a loro scapito, sotto i riflettori solo per via

*«Per quanto riguarda le operazioni di polizia, si dovrebbe chiarire – a livello legale o in via giudiziaria – che esiste in linea di principio un* Right to Record the Police *secondo il modello americano.»* (Foto: 1° maggio 2021 a Zurigo, video YouTube di Harp Lover)

della loro professione. Anche se i singoli agenti di polizia hanno molto potere e rappresentano il monopolio dell'uso della forza da parte dello Stato, essi appartengono fondamentalmente alle forze dell'ordine nel loro insieme quando intervengono. Al contrario, gli agenti di polizia dovrebbero poter filmare i loro interventi con le *bodycam* – nell'ambito di condizioni quadro chiare – ed eventualmente dovrebbero anche essere obbligati a farlo. Nei casi in cui si deve filmare, tutte le registrazioni dovrebbero fondamentalmente sottostare al principio della trasparenza. I diritti delle persone filmate potrebbero essere esaminati e adeguatamente garantiti al momento della pubblicazione delle registrazioni.

## Sicurezza giuridica per le riprese video in luoghi pubblici

Per autorizzare in generale i cittadini a filmare nei luoghi pubblici, occorre creare una sicurezza giuridica almeno in alcuni ambiti. Per esempio, l'uso delle *dashcam* potrebbe essere disciplinato in modo costruttivo nell'interesse della sicurezza stradale. Certo, le critiche nei confronti delle registrazioni video rispettivamente della videosorveglianza sono per lo più giustificate perché il fatto di sapere di essere filmati o anche di credere di essere filmati influenza il comportamento umano. Una tale "pressione dovuta alla sorveglianza" non è ampiamente tollerata in una società libera, tranne in alcuni casi come per esempio nel traffico stradale. Regolamentare l'uso delle *dashcam* potrebbe tra l'altro significare conservare solo certi eventi della durata di pochi minuti che le autorità potrebbero poi utilizzare. Al contrario, la conservazione immotivata di ore di registrazione, com'è oggi il caso, sarebbe vietata.

Un quadro giuridico più chiaro contribuirebbe anche a chiarire chi è autorizzato a filmare chi nei luoghi pubblici e a quali condizioni. Inoltre, tenendo conto del consenso sociale mutato a seguito dell'onnipresenza degli smartphone, l'azione giuridica sarebbe molto più efficace di un inutile divieto. Chi non dovrebbe essere assolutamente autorizzato a filmare trova in ogni caso sempre il modo di farlo. Per esempio, i manifestanti hanno comunque iniziato a capire che non è saggio filmare con il proprio smartphone la manifestazione a cui partecipano. Per essere sicuri di poter pubblicare le loro registrazioni video e di evitare che la polizia le sequestri, i manifestanti devono trasmettere le immagini in diretta in Internet o effettuare le riprese di nascosto. Se invece l'obiettivo è documentare interamente una manifestazione in tutta sicurezza, è consigliabile avvalersi di squadre specializzate che staranno ad una distanza sufficiente, analogamente alle forze dell'ordine durante certi eventi.

Per quanto riguarda le operazioni di polizia, si dovrebbe chiarire – a livello legale o in via giudiziaria – che esiste in linea di principio un *Right to Record the Police* (diritto di filmare la polizia) secondo il modello americano. Chi non interferisce con le operazioni di polizia e non mette in pericolo né se stesso né gli altri deve avere il diritto di filmare. Per la pubblicazione si applicano le disposizioni correnti in materia di diritto della personalità, cioè in caso di controversia, occorre soppesare gli interessi in gioco. Per le persone coinvolte dovrebbe così essere più facile adire le vie legali. Questo permetterebbe da un lato di proteggere efficacemente i diritti delle singole persone e, dall'altro, di perfezionare la pratica giuridica attraverso una giurisprudenza differenziata. E per quanto riguarda gli agenti di polizia, questi ultimi dovrebbero naturalmente poter contare sul sostegno dei loro corpi di polizia quando desiderano difendersi.

# I suricati e i cani...

... sono un esempio emblematico di come si può essere molto concentrati e vigili, ma non capire nulla. I suricati, ritti sulle loro zampe, sorvegliano costantemente tutta la prateria facendo con la testa movimenti rapidissimi e a scatti, prima di crollare dalla stanchezza per lo sforzo e addormentarsi. I cani abbaiano frustrati credendo erroneamente che qualcuno avesse lanciato loro un bastone per giocare. Ci vuole ben altro per una sorveglianza riuscita.

Il fatto di avere una guardia che sorveglia mentre gli altri dormono è probabilmente una necessità atavica dettata dal bisogno di sopravvivenza. In questo senso la sorveglianza, e il sentimento di sicurezza che infonde, sono un aspetto fondamentalmente positivo: la guardia sorveglia per conto delle persone che dormono e svolge quindi una funzione protettiva. Dev'essere in grado di riconoscere i pericoli, e anche sapere cosa fare quando incombe il pericolo, ossia prima di tutto svegliare chi dorme. In questo caso, quindi, sorvegliare significa proteggere. E a questa immagine di sorveglianza protettiva si associa il buon vecchio vigile, il guardiano notturno che fa la sua ronda, come in un dipinto del XIX secolo.

La parola sorveglianza contiene il termine "veglia". Dal canto suo, il prefisso "sor" (ossia sopra) in sorveglianza potrebbe teoricamente esprimere un eccesso di "vigilanza" o un superamento dei limiti come nei termini "sopraeccedere" o "sopraccaricare". In realtà, questo termine significa piuttosto vegliare su tutto allo scopo di proteggerlo, godere di una copertura completa, vigilare sulla totalità dell'oggetto, ossia avere una "visione d'insieme". Naturalmente, si può anche avere una "visione d'insieme" eccessiva, ciò che porta a chiedersi se, in materia di sorveglianza, ci saranno "terre rare" a sufficienza per continuare con l'attuale pratica di raccolta dei dati nei prossimi decenni. La raccolta di dati non costituisce di per sé una sorveglianza, ma rappresenta comunque uno dei suoi strumenti. La sorveglianza inizia quando qualcuno vuole per esempio sapere qualcosa di specifico su un'altra persona basandosi sui dati raccolti, con lo scopo (e il potere!) di sanzionarla in qualche modo, se è riuscito a trovare quello che cercava.

E proprio qui sta il problema: quando le squadre investigative antidroga sorvegliano i gruppi di narcotrafficanti, si auspica che dispongano della migliore tecnologia possibile e dei più abili mediatori linguistici (vedere a pag. 13) per evitare qualsiasi malinteso e poi arrestare, accusare e giudicare questi criminali. Quando invece gli stati totalitari utilizzano in modo improprio la "mostruosa macchina di raccolta dei dati" per rintracciare, arrestare e torturare i dissidenti e gli oppositori politici, si desidererebbe che la tecnologia non si fosse mai evoluta così tanto. È risaputo che ogni conquista tecnologica può essere usata in modo sensato o improprio.

Qui c'è un altro aspetto importante da considerare: chi viene sorvegliato *sa* di essere sorvegliato o no? Nel traffico stradale, per esempio, i radar e i rivelatori di radar si confrontano in un'accesa competizione da anni. Analogamente, chi sa di essere sorvegliato potrebbe anche sviluppare strategie per ingannare o addirittura far cadere in trappola chi sorveglia. Per esempio, le serie televisive "The Wire" e "Narcos", ci hanno fatto scoprire gli stratagemmi spettacolari messi in atto dai trafficanti di droga. Nell'ex DDR, invece, gli artisti critici nei confronti del regime sapevano che la censura avrebbe vagliato minuziosamente i loro testi, perciò vi includevano i cosiddetti "elefanti rosa", cioè contenuti così palesemente critici nei confronti del regime – e quindi sempre censurati – a cui facevano poi seguito critiche molto più sottili e velate contro il regime che invece sfuggivano agli occhi della censura.

Per il momento, chi possiede una carta Cumulus della Migros o una Supercard della Coop non deve temere che la polizia si presenti improvvisamente alla porta di casa per via dei suoi ultimi acquisti. Tuttavia, chi possiede una simile carta dovrebbe sempre essere consapevole che tutti gli acquisti fatti sono registrati a tempo indeterminato. Chi poi acquista solo prodotti "M-Budget" e "Prix Garantie" potrebbe essere considerato una persona avara o indigente. E questo potrebbe diventare un problema, se la Svizzera un giorno decidesse di intraprendere un'azione mirata sia contro l'avarizia (una peculiarità dei ricchi, tra l'altro) che contro la povertà che imperversa fra la propria popolazione. Per il momento, però, possiamo stare tranquilli, perché è improbabile che questo accada presto.

*Volker Wienecke*
Contatto: redaktion@skppsc.ch

### Rilancio della campagna sul coraggio civile

Nel 2019, la PSC ha lanciato la sua campagna di sensibilizzazione "Coraggio civile – Sulla strada giusta". In brevi video, vari membri dei corpi di polizia di tutta la Svizzera spiegavano come dar prova di coraggio civile e quando è il caso di intervenire nelle più svariate situazioni. Dato che a tutt'oggi questo tema non ha perso nulla della sua attualità, la PSC ha deciso di rilanciare questa campagna. Dall'inizio di giugno e fino alla fine del 2021, ogni settimana si attirerà l'attenzione su uno dei temi presentati in questi video. Verranno inoltre pubblicati sui media sociali dei sondaggi sui vari comportamenti da adottare in funzione delle situazioni. Il rilancio sarà abbinato ad illustrazioni in bianco e nero create appositamente per l'occasione e concepite per essere facilmente identificabili.


## LA CRIMINALITÀ CON UN TOCCO DI COMICITÀ

**IN VENDITA:**

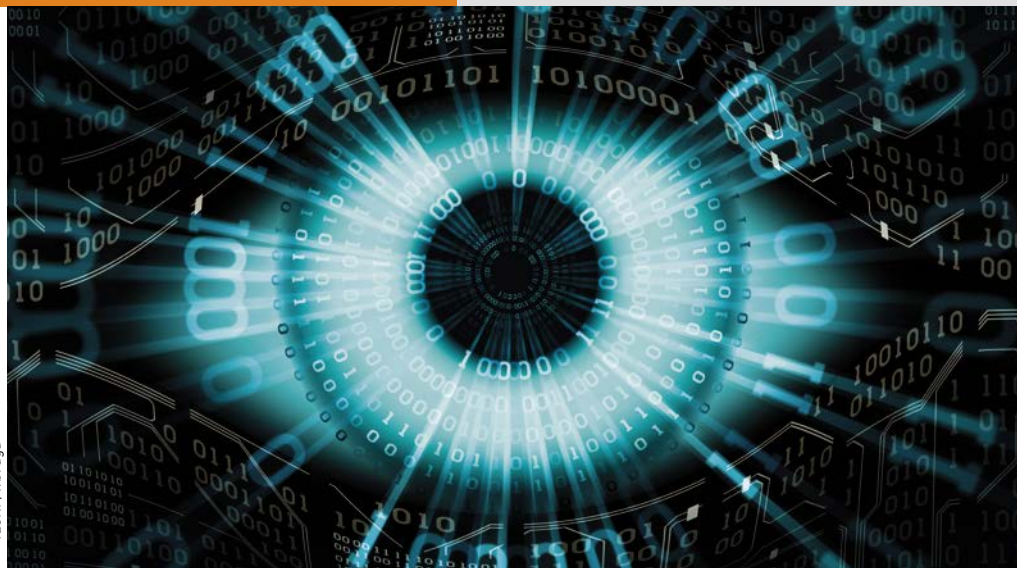
3 vecchie telecamere di sorveglianza, ma ancora perfettamente funzionanti.

Disegno: Agnes Weber

SKPPSC

Prevenzione Svizzera della Criminalità
Casa dei Cantoni
Speichergasse 6
Casella postale
CH-3001 Berna

**www.skppsc.ch**



123RF/wbraga