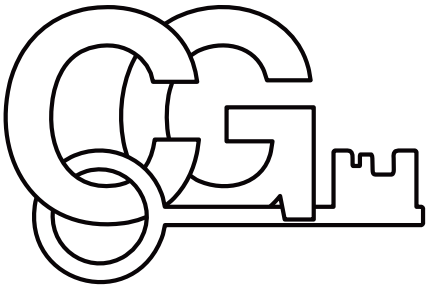
SUPPORTO DIDATTICO

# LA PROTEZIONE DELLA PRIVACY



≈

**SFERA PRIVATA - INTIMITÀ**

≈

**ARTICOLO 12**
**SFERA PRIVATA**

Nessun individuo potrà essere sottoposto a interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto a essere tutelato dalla legge contro tali interferenze e lesioni.
**DICHIARAZIONE UNIVERSALE DIRITTI UMANI(DUDU), 1948.**

## DESCRIZIONE

Un percorso per incoraggiare gli studenti a riflettere sull'importanza che riveste la protezione della sfera privata nella loro vita quotidiana e sul ruolo della legge e delle istituzioni chiamate a proteggerci.

**" Il percorso proposto mi ha permesso di interessare i miei studenti al tema della loro vita privata sui social e on-line. Insieme abbiamo ragionato sulle conseguenze e sui limiti della cessione di dati. Poter affrontare l'argomento a partire dai loro bisogni e diritti ha permesso una reale partecipazione."**

Sébastien Bandelier, professore

## COLLEGAMENTI CON IL PIANO DI STUDI

**PIANO DI STUDI PER LA SCUOLA DELL'OBBLIGO**
LIVELLO SECONDARIO I – SCUOLA MEDIA

Competenze trasversali
- Sviluppo personale
- Collaborazione
- Pensiero riflessivo e critico

Storia ed educazione civica
- Interrogare le realtà sociali in una prospettiva storica
- Capacità critica, analitica e di sintesi
- Caratteristiche di un sistema democratico

## INFORMAZIONI GENERALI

**MATERIE :** Ora di classe, informatica, italiano, civica, storia.

**SCUOLA MEDIA :** studenti classi III e IV

**DURATA :** 90–135 minuti (a seconda delle attività)

**FORMA :** Didattica partecipativa con lavori di gruppo, riflessioni individuali e approfondimenti in plenaria.

UNA INIZIATIVA DI:

AMNESTY INTERNATIONAL

# IL DIRITTO DI PROTEGGERE LA MIA INTIMITÀ

**OBIETTIVI PEDAGOGICI**

• Identificare la propria sfera privata e come l'Articolo 12 della DUDU contribuisce a proteggerla
• Sapere come il diritto alla privacy può essere violato e da chi.
• Identificare le situazioni della vita quotidiana che implicano aspetti sensibili al tema della protezione della privacy.
• Identificare le situazioni della nostra vita dove potrebbe applicarsi l'articolo 12.
• Comprendere il nostro ruolo attivo nella protezione della sfera privata e conoscere gli strumen-ti per agire.

**MATERIALE**

• Libretti DUDU ordinabili gratuitamente sul sito amnesty.ch
• Videoproiettore
• Lavagna o fogli grandi
• Presentazione in PP "Privacy"
• Approfondimenti

**SUGGERIMENTO:** Gli studenti sono consapevoli di dare informazioni personali in rete, ma lo considerano un prezzo ragionevole per l'accesso ai servizi. PPotete esplicitare che questo percorso è pensato per avere più informazioni su come funzionano questi servizi, non per convincerli a non utilizzarli.

## SVOLGIMENTO DELLE ATTIVITÀ

### "CHI DAVVERO VI CONOSCE?" (30 mINUTI)

1. Entrando all'inizio della lezione ponete tre domande particolarmente indiscrete ai vostri studenti. PPer esempio: Hai una ragazzo/,una ragazza, chi è?, "QQuanto costano le scarpe che indossi?,"I tuoi genitori hanno dei problemi di salute. Osservate le reazioni dello studente interrogato e della classe e chiedete loro se era nel vostro diritto pretendere una risposta. Spiegate che la sfera privata di ciascuno di noi è protetta dalla legge, a scuola, a livello nazionale e internazionale. È un nostro diritto non rispondere.
2. Chiedete ora agli studenti di riflettere individualmente su chi sono le persone che meglio li conoscono, che sanno le risposte alle domande inopportune che avete loro proposto. PPotete fare esempi di altre domande su situazione economica, sentimentale, religione, politica, salute.
3. Dividete ora la classe in due gruppi, ciascuno lavora intorno a un tavolo sul quale avete preparato un grande foglio con cerchi concentrici con scritto: intimità, sfera privata, sfera sociale, pubblico.
4. Gli studenti scrivono su post-it gli ambiti, le informazioni che appartengono alla loro sfera privata. Ddalle più personali a quelle di dominio pubblico. Esempi: credere in un dio, orientamento sessuale, idee politiche, situazione famigliare, piaceri, situazione economica, origini e storie famigliari.
5. Gli studenti mettono i post-it all'interno dei cerchi, a seconda di quali informazioni sono disposti a condividere con chi, discutendo arrivano a una mappa condivisa che presenteranno alla classe.
6. Mentre presentano, chiedete loro se vi è la possibilità che un'informazione passi da un cerchio all'altro e con quali conseguenze; quale sia la differenza tra "segreto" e "privato". Per evidenziare l'importanza della libertà di poter decidere quali informazioni su di noi vogliamo condividere e con chi potete portare l'esempio di un personaggio storico perseguitato sulla base di informazioni personali in mano a un potere autoritario, ad esempio Soljenitsyne.
7. Infine dite che ogni informazione su di un computer, telefono collegato alla rete è conosciuta e registrata e non cancellabile (vedi approfondimenti e link).

### DIRITTO ALLA PRIVACY (30 MINUTI)

1. Distribuite una copia del libretto con il testo della DUDU e chiedete di cercare e leggere l'articolo che protegge la nostra sfera privata. Chiedete esempi di momenti in cui questo articolo ci protegge.
2. Utlizzando la presentazione in PP, introducete le basi legali del diritto alla privacy a livello nazionale e internazionale e la teoria dei diritti umani. Importante sottolineare il dovere degli Stati di promuovere, proteggere i nostri diritti. Questo passaggio vi permette di arrivare all'attuale legislazione che protegge la nostra privacy on-line, alla questione dei "Big Data" e del controllo di massa.

### BIG DATA E CONTROLLO DI MASSA (30 MINUTI)

1. Raccontate le storie di Assange e/o Snowden e/o Chelsea Manning per evidenziare la responsabilità individuale nella possibilità di veder rispetta la nostra privacy e il livello di manipolazione al quale siano sottoposti. Oggi i "big data" e le informazioni personali sono nelle mani di poche aziende che hanno un potere enorme e operano in un contesto non regolato. Non abbiamo avuto la possibilità, il potere, la volontà di definire una regolamentazione etico forte e condivisa a livello internazionale.
2. Facoltativo: potete dare alcuni consigli, anche con i telefonini in mano, su come migliorare la privacy sul proprio dispositivo. In genere le impostazioni dei telefonini dei ragazzi e delle ragazze permettono una grande ingerenza da parte delle aziende (e dei genitori).
3. Mostrare video: Comprendere i Big Data (YouTube) e la Sorveglianza in Cina (YouTube) Video del DFA sulla privacy.

### ARGOMENTARE (45 MINUTI)

Dividete la classe in gruppi di 4 o 5 studenti e chiedete loro di scrivere esempi di non rispetto della privacy. Potete aiutarli voi suggerendo:

- telecamere in strada, che fine fanno quelle immagini?
- registrazione dei dati in uscita dalla Svizzera da parte del governo;
- colloqui di lavoro, domande personali e informazioni in rete.
- carte fedeltà dei supermercati, chi tiene i dati?
- informazioni sulla salute.

Quali sono i vantaggi di una società completamente trasparente, come quella cinese? Se chiunque sapesse tutto di noi, cosa cambierebbe?
Girate tra i gruppi chiedendo loro di fare una mappa mentale delle conseguenze che queste violazioni dell'articolo 12 della DUDU possono avere su altri diritti, sottolineate l'interdipendenza e l'universalità dei diritti.
In plenaria ogni gruppo presenta due argomenti per difendere la possibilità di mantenere una sfera privata.

### ESEMPI NEL PERSONALE (15 MINUTI)

In funzione delle reazioni degli studenti durante le discussioni e della confidenza che avete con loro, potete proporre questa parte che permette di evidenziare la differenza tra chi sono e l'immagine di sé che veicolano attraverso i social media. Preparatevi guardando i profili degli studenti sui social.
Mostrate alla classe il profilo e le foto postate da una/o di loro e analizzate sia la quantità e qualità delle informazioni personali condivise che la differenza tra la storia che raccontano i post e la vita nel mondo reale della persona.

Lo Stato e la legge hanno il dovere di proteggere la nostra privacy, ma l'attuale quadro internazionale permette alle aziende azioni che sarebbero problematiche sul territorio svizzero ed europeo.
Ma questo è possibile solo con il nostro consenso, che concediamo senza remore in modo poco informato e consapevole.

Approfondimenti

in italiano, o con sottotitoli in italiano:

Video del 2012 - Un mago indovina informazioni molto personali sui passanti, grazie a un complice collegato alla rete.
https://youtu.be/qYnmfBiomlo

In francese:

Raccolta di articoli sul tema della sorveglianza
https://www.amnesty.ch/fr/themes/surveillance

Misure di sorveglianza al tempo della pandemia
https://www.amnesty.ch/fr/themes/coronavirus/docs/2020/surveillance-digitale-coronavirus-mesures-proportionnees-meme-en-situation-etat-urgence

In inglese:
Rapporto Amnesty International del 2021:
"Uncovering the Iceberg: The Digital Surveillance Crisis Wrought by States and the Private Sector"
https://www.amnesty.org/en/documents/doc10/4491/2021/en/

Sistema del credito sociale in Cina
https://www.amnesty.org.uk/groups/cambridge/ai-surveillance-china-and-usa-10-june

La videosorveglianza a New York
https://m.facebook.com/watch/?v=498801551365557&_rdr
e
https://www.amnesty.org/en/latest/news/2021/06/scale-new-york-police-facial-recognition-revealed/

Sicurezza dei telefoni
https://www.cnbc.com/2021/07/19/apple-iphones-can-be-hacked-even-if-the-user-never-clicks-a-link-amnesty-international-says.html

Riconoscimento facciale
https://www.amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/

Esempi di sorveglianza su attivisti
https://www.amnesty.org/en/latest/campaigns/2020/10/stopspying/

# DOSSIER « SORVEGLIANZA DI MASSA»

## ECCO PERCHÈ « NON HO NULLA DA NASCONDERE » NON È LA RISPOSTA.

Quando Amnesty International ha lanciato #UnfollowMe, la campagna per vietare la sorveglianza di massa da parte dei governi, i nostri account Facebook e Twitter sono stati invasi da messaggi di persone che sostenevano che "Se non hai nulla da nascondere, non hai nulla da temere". Il ragionamento è che, se non abbiamo nulla da rimproverarci, non è un problema se i governi raccolgono tutti i nostri dati: e-mail, telefonate, impronte digitali, dati biometrici del nostro viso, impronta vocale, immagini di webcam, ricerche in rete, dal momento che non troveranno nulla di interessante. Questo è un argomento allettante, ma è sbagliato. Ed ecco perché.

Molto è stato scritto su questo tema; per proporre una sintesi interessante, abbiamo scelto in quest'occasione di proporre le risposte alle domande che abbiamo ricevuto sui profiliAmnesty dei social media e usarli per spiegare perché il "tanto non nulla da nascondere" non ènon è il modo giusto di reagire alla sorveglianzadi massa utilizzata dai nostri governi.

"**La privacy deve essere un diritto, a meno cheun atto non susciti legittimi sospetti.**» Karine Davison
Generalmente, i governi conducono una sorveglianza mirata, cioè monitorano una personao un gruppo solo per motivi specifici e legittimie per farlo hanno bisogno del permesso di un giudice. Quando parliamo di sorveglianza di massa ci riferiamo al controllo e alla registrazione dei dati di tutte le persone in un determinato territorio, senza che vi sia il sospettodi un reato. Il governo guarda a tutte e tutti come possibili sospetti e agisce in modo preventivo registrando i dati.
Ci sono poche leggi per controllare queste azioni.

**"Quindi, nessun problema se scopri una telecamera in bagno o in camera?"** Ulf Carsson

Ogni giorno facciamo cose nel nostro spazio privato che non faremmo in pubblico, o che faremmo diversamente. Questo non perché abbiamo qualcosa da nascondere, masemplicemente perché ci sono aspetti della nostra vita che preferiamo mantenere privati.
John Oliver, conduttore del programma televisivo americano Last Week Tonight, ha chiesto ai passanti a New York cosa ne pensano del fattoche centinaia di persone nelle agenzie governative hanno accesso alle loro foto private, anche di natura sessuale o molto intima.

**"Voler preservare la mia privacy non significa che ho qualcosa da nascondere."** J. Earl Walsh

La sorveglianza di massa è un'intrusione senza precedenti nella nostra vita privata. Nessuna delle generazioni precedenti ha mai dovuto permettere ai governi di sapere tutto della propria vita privata in cambio di una maggior sicurezza.
Con la pratica della sorveglianza di massa i governi stanno oltrepassando il limite invalicabile che ci garantisce libertà e diritti, e noi permettiamo loro di farlo ogni volta che diciamo: "Tanto non ho nulla da nascondere, non commetto alcun reato nella mia vita privata."

**"Nulla da nascondere, purché tu aderisca al 100% al punto di vista e alla politica del tuo governo."** Emily Kate Goulding

Proprio come nel caso della possibilità di manifestare o di esprimere la propria opinione, diventiamo consapevoli del confine della nostra sfera privata solo quando ne abbiamo bisogno. I diritti servono per proteggerci nel momento del bisogno e perché la nostra dignità sia sempre garantita. Dobbiamo continuare a difenderli in modo che ci possano proteggerci nel momento in cui ne avremo bisogno, noi o chiunque intorno anoi.
Nel corso della storia, informazioniapparentemente innocue sui cittadini sono state utilizzate per perseguitarli in tempi di crisi. Ci fidiamo del nostro attuale governo, glipermettiamo di registrare ogni nostro

movimento e comunicazione perché possa identificare e catturare chi compie azioni criminali, ma quelle registrazioni restano e le persone che vi hanno accesso potrebbero cambiare e avere altre intenzioni.
Ma cosa succede se al governo sono elette persone molto di sinistra o di destra o con idee differenti dalle nostre? Avrebbero la possibilità di utilizzare i dati a cui hanno accesso per identificare le persone o i gruppi che non condividono le loro idee o che hanno una qualche caratteristica che li disturba (religione, sesso, orientamento, colore degli occhi). Potrebbero usarle per criminalizzare chi dissente, negare loro l'accesso alle libertà e discriminare le minoranze. Non possiamo controllare da chi e dove sono registrate le informazioni, spesso si tratta di server in diversi Paesi e di grandi multinazionali private.

**"Partiamo dal presupposto che le persone dietro le telecamere di sorveglianza penseranno solo al bene dei cittadini.** Roland van der Sluijs

Non hai nulla da nascondere e nella tua vita privata non commetti alcun reato, ma nel momento in cui permetti a qualcuno di conoscere e registrare queste informazioni devi dare cieca fiducia a chi è incaricato di trattare i dati ed essere certa/o che la situazione non cambierà.
Edward Snowden lavorava per la sicurezza degli Stati Uniti d'America e aveva cieca fiducia nei suoi superiori e nel governo del suo Paese. Ma ha scoperto che le persone che avevano la responsabilità di prendere le decisioni mentivano e utilizzavano gli strumenti di sorveglianza a loro disposizione in modo illecito. "Queste persone sono alla ricerca di criminali. Puoi essere la persona più innocente del mondo, ma loro partono dall'idea che tu sia colpevole e quindi i tuoi diritti e le tue libertà sono limitati di conseguenza. Perché guardano a te come a un criminale."

**"Vuoi davvero vivere una vita di soffocante e obbedire a tutto?"** Jia Hengjian

Abbiamo prove sperimentali del fatto che un individuo che sa di essere monitorato modifica le sue azioni in base alle attese di chi lo osserva.
Nel momento in cui siamo consapevoli che il nostro governo -e i governi di altri Paesi- utilizzano algoritmi, strumenti di sorveglianza di massa e hanno accesso a data base privati per poter prevedere le attività criminale delle persone, diventiamo più cauti e sospettosi nelle nostre azioni on-line. Inizieremo con il non leggere siti e persone potenzialmente controverse, per evitare che le nostre azioni siano erroneamente interpretate.

Le società diventano così più conformiste e le possibilità di dissenso ridotte e indebolite.

**"Se non abbiamo nulla da nascondere, perché siamo sotto sorveglianza?"** Jake Lawler

In poche parole, la miglior risposta all'argomento "Ma io non ho nulla da nascondere" sarà sempre: "Se non hai nulla da rimproverarti, perché il tuo diritto alla privacy viene costantemente violato?»

**"La privacy non è – e non è mai stata – sinonimo di occultamento; è sinonimo di protezione e possibilità di libertà. Punto.»** Sam Isatlacc

**"Amico, devi vivere una vita davvero noiosa se non hai nulla da nascondere a nessuno**." Mitxel Moriana

**"Solo perché non fai nulla di sbagliato non significa che non abbia diritto a una vita privata."**Trilogia Gunby

**"Se una persona è sospettata di essere coinvolta in attività criminali, è necessario un ordine del tribunale per metterla sotto sorveglianza."** Amy Rouby

**"Se qualsiasi forma di dissenso diventa illegale, qualsiasi resistenza diventa quasi impossibile. Sono al sicuro solo coloro che non mettono mai in discussione le decisioni del governo. Evviva.»**
Roland van der Sluijs

**"Che vi piaccia o no, abbiamo il diritto di non essere spiati senza giusta causa."** Mary Shepard

# DOSSIER « SURVEGLIANZA DI MASSA » II

## DOMANDE E RISPOSTE SULLA SORVEGLIANZA DI MASSA

**Che cos'è la sorveglianza?**
Si parla di sorveglianza quando un governo o un privato osservano i movimenti e le comunicazioni di un individuo.
I governi possono dare mandato alla polizia di sorvegliare, con l'autorizzazione della magistratura, nel quadro della legislazione esistente e se si tratta di un'azione mirata, proposizionale e giustificata. Il monitoraggio delle comunicazione prevede l'osservazione dei movimenti, l'acquisizione, l'archiviazione, l'analisi e la condivisione dei dati e metadati relativi a una comunicazione e al suo contenuto. Sono detti metadati le informazioni sulla durata, il mezzo, il punto di partenza e di arrivo e il destinatario di una qualsiasi comunicazione.
Vi sono casi in cui la sorveglianza è utilizzata per intimidire e controllare una persona o un gruppo di attivisti, in generale per monitorare le attività di chi è sospettato non condividere le idee dell'autorità che osserva.

**Amnesty si oppone a ogni forma di sorveglianza, individuale e di massa?**
Amnesty International non si oppone alla sorveglianza per principio, ma rifiuta qualsiasi misura di sorveglianza di massa e indiscriminata che non sia basata su di un sospetto. La sorveglianza è giustificata solo se vi sono indizi concreti di attività illecite e la misura è mirata, necessaria, proporzionata e ordinata da un giudice.

**Quando la sorveglianza di massa si dice indiscriminata?**
La sorveglianza di massa indiscriminata è, ad esempio, la sorveglianza di Internet e delle comunicazioni telefoniche di un gran numero di persone, a volte di un intero paese, senza che le persone monitorate ne siano consapevoli o che vi siamo elementi per sospettarle di attività illegali.

**Vi è una forma legale di sorveglianza di massa indiscriminata?**
No. Anche se i governi possono legalizzare programmi di sorveglianza di massa, questi rimangono chiaramente in contrasto con il diritto internazionale che la maggior parte degli stati ha ratificato.
Secondo Amnesty International, una eccessiva sorveglianza indiscriminata non può mai essere una violazione giustificata e proporzionata dei diritti umani.

Quando la sorveglianza diventa legale?
La sorveglianza, per essere legale, deve soddisfare sei condizioni:

1. Deve avere una base giuridica chiara; vale a dire, deve essere regolata da disposizioni giuridiche accessibili a tutti.
2. Deve essere autorizzata con una decisione specifica, pronunciata da un giudice o da un'altra autorità indipendente.
3. Deve essere istituita per tutelare un legittimo interesse pubblico, ad esempio per chiarire un'indagine penale o per garantire la sicurezza nazionale.
4. Deve rivolgersi a una persona specifica, a un gruppo di persone o a un luogo ben definito per raggiungere un obiettivo legittimo.
5. Deve essere necessario, cioè non ci devono essere altri mezzi meno intrusivi per raggiungere l'obiettivo desiderato.
6. Deve essere proporzionata, vale a dire che la violazione dei diritti umani deve essere proporzionata allo scopo legittimo perseguito.

La sorveglianza delle comunicazioni di un intero paese – come praticata dalla NSA negli Stati Uniti– è totalmente illegale. Tale sorveglianza è sproporzionata e i governi non sono stati in gradodi fornire prova della sua necessità. Molti programmi di sorveglianza sono, inoltre, autorizzati da vaghe norme legali che sia i giudici che i legislatori trovano difficili da interpretare. In molti paesi, la sorveglianza è ordinata da decisioni segrete e senza alcuna trasparenza.

**Quali sono le protezioni giuridiche contro la sorveglianza di massa indiscriminata?**
L'articolo 17 del Patto internazionale sui diritti civili e politici protegge tutti da "interferenze arbitrarie o illegali con la loro vita privata".
L'articolo 19 dello stesso testo tutela il diritto alla libertà di espressione, che include "la libertà di

cercare, ricevere e mettere in evidenza informazioni e idee di ogni tipo, senza riguardo per i confini".
I diritti umani riconosciuti a livello internazionale proteggono la sfera privata e la libera espressione. Gli Stati hanno l'obbligo di rispettarli e proteggerli. Il diritto internazionale consente ai governi di limitare questi diritti in determinate circostanze e poter quindi effettuare un monitoraggio delle comunicazioni. Come ogni limitazione dei diritti umani fondamentali, questo può essere fatto solo per proteggere un interesse superiore e deve essere già prevista la fattispecie specifica nella legge. Significa che le misure di sorveglianza devono seguire le sei condizioni che abbiamo elencatonella risposta precedente.

**Qual'è il rapporto tra il diritto nazionale e quello internazionale nel caso della sorveglianza?**
I poteri di vigilanza sono disciplinati dal diritto nazionale. Ma il fatto che la sorveglianza sia regolata da una legge non la rendeautomaticamente legale. Gli governi sono tenuti a seguire, oltre alla propria legislazione, gli obblighinei confronti degli standard internazionali in materia di diritti umani. Una misura disorveglianza non compatibile con i diritti umani è illegale. La sorveglianza delle comunicazioni è una violazione del diritto alla vita privata e alla libertà di espressione, due diritti garantiti, tra l'altro,dalla CEDU.

**Perchè le rivelazioni di Eduard Snowden sono state importanti?**
Le rivelazioni di Edward Snowden hanno dimostrato ciò che in molti temevano: il governo Inglese e statunitense hanno segretamente registrato e analizzato i dati personali e le comunicazioni di milioni di persone, sia sul loro territorio che all'estero. Senza alcun quadro legale definito o trasparenza. Grazie alle rivelazioni Snowden, ex-funzionario della NSA statunitense, ora conosciamo l'entità della sorveglianza effettuata dai servizi segreti statunitensi e britannici. Alcuni esempi:
I servizi segreti degli Stati Uniti consegnano ogni giorno 200 milioni di note scritte ai servizi britannici.
I servizi segreti degli Stati Uniti e del Regno Unito sono in grado di accendere la telecamera eil microfono del tuo cellulare o della tua TV per ascoltarti anche quando sono spenti e scollegati. Gli stessi servizi registrano le immagini da milioni di telecamere di telefoni cellulari in tutto il mondo, senza che i proprietari ne siano consapevoli e senza che su di loro vi sia alcun sospetto di essere coinvolti in attività illecite.

**Sono sorvegliata/o?**
Usi un telefono cellulare o internet? In questo caso, vi sono buone probabilità che tu venga monitorato. Programmi di sorveglianza come "Prism" eUpstream" utilizzati dalla NSA o "Tempora" utilizzatidal British Government Communication Head (GCHQ), hanno accesso ai metadati delle principali società che operano on-line, come Google, Facebook e Yahoo. Inoltre, intercettano i dati direttamente dai cavi di rete e le comunicazioni telefoniche. A livello nazionale, il governo svizzero registra tutti i dati in uscita verso l'estero sui cavi di rete. Anche se qualcuno domiciliato in Svizzera invia un'e-mail a un'altra persona in Svizzera tramite il proprio account GMail, Yahoo o simili il messaggio utilizza un server all'estero, e questo autorizza la possibilità di registrarlo anche se sia mittente che destinatario si trovano in Svizzera. Purtroppo, non siamo altroche un numero di telefono, un indirizzo e-mail o un IP memorizzato nei data center.

**Quali dati raccolgono su di me?**
I dati personali vengono generati ogni volta che autorità, aziende o individui utilizzano la tecnologia digitale, prelevano denaro dal bancomat, navigano su Internet, passano davanti a telecamere di sorveglianza o tutti i nostri dati in possesso delle autorità fiscali, dell'amministrazione, degli istituti e casse che si occupano si sanità come ospedali e casse malati.
I programmi di monitoraggio registrano e analizzano la cronologia del tuo browser Internet, le tue ricerche, le tue e-mail, le tue informazioni istantanee, le tue conversazioni da comunicazioni video e telefonate. Raccolgono anche metadati (dati sui dati): con chi, quando, per quanto tempo e da dove hai comunicato?

**Cosa succede ai miei dati?**

...

Nessuno sa esattamente cosa succede ai nostri dati personali e non puoi far nulla per impedire la loro diffusione. Quel che è certo è che i dati vengono archiviati in gigantesche banche dati e analizzati utilizzando potenti algoritmi. I dati registrati sono scambiati tra diversi Stati e messi a disposizione di diversi servizi di intelligence.

**Perché la raccolta di questi dati è pericolosa?**

Presi separatamente, i dati e frammenti di informazioni raccolte non hanno un grande valore. Ma oggi i dati sono scambiati, registrati, analizzati da potenti algoritmi, non restano fermi in un server al sicuro. Sono utilizzati per eseguire profili personali molto dettagliati, con opinioni politiche, preferenze sessuali, stile di vita, ambiente sociale, livello di istruzione, situazione di salute fisica e psicologica. Questi profili, costruiti in modo automatico da un algoritmo, sono alla base di indagini e azioni di discriminazione e violazione dei diritti e delle libertà di persone o gruppi di persone.

**In che modo la sorveglianza può avere conseguenze sulla libertà di opinione?**

Sapere di essere monitorati da un'autorità porta all'autocensura. Come una spada di Damocle, la sorveglianza influenza la libertà di opinione e di riunione.

Coloro che hanno paura di essere monitorati sono meno disposti a esprimere la loro opinione e non utilizzano la rete per promuovere una manifestazione o per avere informazioni su di un argomento di loro interesse. Il diritto ad avere il nostro spezio di riservatezza, intimità è una condizione necessariaper l'esercizio di molti altri diritti come la libertà di opinione e d'informazione, il diritto a assemblee pacifiche e pacifiche, il divieto di discriminazione.

Come i governi utilizzano lo sorveglianza come strumento di repressione?

Le piattaforme online e i social sono sempre più utilizzati per promuovere manifestazioni e proteste. Le "primavere arabe" sono state un esempio di questo uso. Molti governi in tutto il mondo stanno limitando i social e le ricerche sulla rete per indebolire gli strumenti di comunicazione e sensibilizzazione in mano agli attivisti e a chi non condivide le loro opinioni. La violazione della libertà di espressione è palese nella censura diYouTube e Twitter da parte del governo turco o la sorveglianza globale alla quale sono sottoposte lepersone in Cina.

Durante le proteste di Maidan a Kiev nel 2014, tutti i manifestanti e le persone che si trovavano nelle vicinanze hanno ricevuto il seguente messaggio: "Ti abbiamo registrato come persona che ha partecipato

**Perché dovrei preoccuparmi della sorveglianza di massa se non ho nulla da nascondere?**

La domanda è formulata male e ci si dovrebbe piuttosto chiedere: "Perché la mia privacy viene violata se non ho fatto nulla di sospetto? Non accetteremmo mai che il governo inserisca videocamere nelle nostre case, apra la nostra corrispondenza e ascolti tutte le nostre discussioni con i nostri amici. Eppure, è questo ciò che fa con la sorveglianza di massa.

Una società che rispetta la libertà e lo stato didiritto deve rispettare la privacy dei suoi cittadini, a meno che non vi siano sospetti basati su indicazioni concrete che essi siano coinvolti in attività criminali. In caso contrario, tutti i cittadini sono presunti colpevoli fino a quando non sono stati in grado di dimostrare la loro innocenza.

Alcuni governi usano i dati sensibili per intimidire, opprimere e mettere a tacere gli oppositori. Oggi qui da noi non accade, ma nessuno stato è immune da un cambio di regine o alle pressioni di potenti alleati. Se non ci proteggiamo, corriamo il rischio di una società futura in cui la privacy sarà assente.

**Perché dovrei preoccuparmi della sorveglianza di massa da parte di un governo se le grandi aziende che operano in rete hanno già tutti i miei dati?**

Dovremmo preoccuparci anche di come queste grandi aziende usano I nostril dati. Sono tenute a proteggerli e non sono autorizzate a usarli per qualcosa di diverso da quello per cui sono stati raccolti. Detto questo, c'è un'enorme differenza tra i dati raccolti da Facebook e quelli raccolti dal governo: decidi liberamente se iscriverti a un servizioe sei tu a decidere quali dati condividere con ilmondo, mentre i servizi informativi raccolgono questidati a nostra insaputa. Infine, le aziende non sono in grado di raccogliere dati da tutti ma solo dalle persone che utilizzano i loro prodotti.