COME SFUGGIRE AL CONTROLLO INFORMATICO

I cambiamenti che cominciamo a scorgere nell'organizzazione degli strumenti di repressione, in questa fase del capitalismo, sono senz'altro orientati all'utilizzo sempre più massiccio della tecnologia, come dispositivo di controllo remoto, di sorveglianza a distanza o addirittura di dissuasione e previsione del disordine sociale e del conflitto. Dal braccialetto elettronico, a strumenti amministrativi quali il Daspo, il foglio di via, l'obbligo di dimora o di firma, al controllo delle attività compiute attraverso la rete internet, stiamo assistendo alla messa in campo di un'azione complessiva tesa ad imporre una sorveglianza onnipervasiva sulla nostra vita quotidiana. Questo va di pari passo alla puntualità con la quale le aziende che offrono servizi in rete (accesso a internet, mail, social network) sono in grado di profilare ed entrare in possesso di una mole infinita di dati riguardanti ognuno ed ognuna di noi. Le macchine che usiamo quotidianamente per comunicare e per entrare in relazione con gli/le altre/i (computer, smartphone, tablet, telefoni) rischiano di essere il cavallo di Troia attraverso cui l'azione repressiva trova luogo.
Se da un lato è impossibile fare a meno di tutti questi strumenti, dall'altro è necessario comprendere la portata del problema, avere un approccio critico riguardo alle tecnologie che utilizziamo ed adottare alcune contromisure, anche piccole ma essenziali, per evitare di diventare noi stessi la prima fonte di informazione delle polizie di tutto il mondo.
La prima cosa da fare è abbandonare completamente i sistemi operativi Windows e Apple MacOsX, optando per l'utilizzo di GNU/Linux o di sistemi portatili, che girano su penne USB, quali Freepto e Tails.
Una menzione importante va data ai programmi che utilizziamo per comunicare. Spesso pensiamo che alcuni programmi siano più "sicuri" di altri o che comunque ci diano una maggiore tranquillità, come ad esempio l'utilizzo di sistemi di cifratura o di crittografia nello scambio di mail o di altre informazioni. Ricordiamoci che utilizzare programmi sicuri su un computer non sicuro è poco utile: nessuna tecnica crittografica ci proteggerà
da una password banale. Una porta blindata è inutile, se lasci la chiave sotto lo zerbino. La nostra sarà quindi una panoramica sulla "repressione tecnologica" e su alcuni rimedi per combatterla.

Chi ha qualcosa da nascondere?
Ognuno e ognuna di noi.
Sul tuo computer transitano un mare di informazioni delicate: i siti che visiti, le persone con cui parli, i messaggi che ti scambi sono monitorati in modo sistematico, per meglio "classificarti". Discorso analogo vale per smartphone e tablet. Con un pò di analisi e possibile sapere chi sei, dove vivi, chi frequenti, la tua routine, il tuo "carattere". Questi dati possono rivelare tanto i tuoi gusti musicali quanto le tue tendenze politiche: la profilazione commerciale va a braccetto con una schedatura di massa.
Non si tratta però solamente di proteggere la propria identità, o fatti specifici legati a reati: monitorando la rete, la polizia cerca soprattutto di capire quali sono i soggetti più attivi all'interno di un gruppo, al fine di rendere più facile un'attività di contrasto.

I miei dati sono al sicuro?
La sicurezza informatica e una materia complessa, proviamo quindi a districarla. Il tuo computer *contiene* dei dati. Chi controlla il tuo computer ha il pieno accesso ai tuoi dati. Non è così improbabile che qualcuno lo faccia: accessi fisici (computer lasciati incustoditi) o software (attraverso internet) avvengono quotidianamente.
Il tuo computer *comunica*. Ogni volta che chatti, videochiami, scrivi email, ti connetti a dei social network, invii foto o ascolti musica, il tuo computer scambia messaggi con altri computer e server. Qualcuno potrebbe *ascoltare* queste comunicazioni. Molti dei *servizi* che usi su internet controllano i tuoi dati. Le aziende (google, facebook, microsoft, yahoo…) tengono traccia di ogni possibile informazione su di te, e puoi stare certo che le inoltreranno alle autorità non appena richiesto. Stai quindi delegando i tuoi dati alla loro gestione. Ti fidi di loro?
Per finire, ricorda che la gestione della tua sicurezza è principalmente un approccio mentale. Spesso è necessario prestare particolare attenzione: ad esempio nell'usare il computer di un tuo amico o quelli di un *internet point* potresti lasciare lì le tue password, permettendo ai visitatori successivi di vedere i tuoi dati.

Malware
Tutti sappiamo cos'e un virus per il computer, se non altro per esserne stati/e infettati/e qualche volta ed aver visto diventare il sistema operativo incontrollabile, oppure preda di azioni esterne. Un Malware è un programma simile a un virus che ha lo scopo di ottenere il controllo

del tuo computer, trasformandolo in una sorta di microspia altamente tecnologica.
Questa tecnica è sempre più usata dalle polizie di tutto il mondo, ed è decisamente la più potente. Ci si può proteggere dai Malware, innanzitutto, smettendo di utilizzare sistemi operativi proprietari (Microsoft Windows ed Apple Mac OSX) visto che sono decisamente più controllabili rispetto ad esempio a GNU/Linux (sebbene anche un utilizzo sconsiderato di Linux possa comportare dei rischi). Problemi simili si riscontrano anche nelle applicazioni, un esempio significativo è Skype: è infatti noto che questo programma non solo è monitorato dalle polizie, ma viene addirittura utilizzato per controllare tutte le attività del computer. Possiamo quindi dire che Skype e un malware.

Sequestro
Con un mandato, la polizia può sequestrare materiale informatico a scopo di indagine. Nel dubbio, la polizia sequestra tutto quello che può (computer, telefoni, smartphone, penne USB, fotocamere, registratori, etc).
Dopo il sequestro, la polizia prende possesso di tutto ciò che trova su computer e hard disk. Se i dati del computer non sono cifrati, la polizia può facilmente accedere alle password che hai salvato sul tuo computer, ai tuoi documenti, alla cronologia (del browser, delle chat etc.) e, se usi un client di posta, alle tue e-mail.
La migliore soluzione contro questo attacco è criptare il proprio disco, oppure utilizzare sistemi operativi installati direttamente su una penna USB (come Freepto o Tails), in modo da non lasciare mai dati sensibili sul proprio computer

La perquisizione informatica
Se ti trovi in un luogo pubblico è possibile per la polizia chiedere di controllare il tuo computer (o smartphone) senza necessità di mandato o giustificazione.

Come comportarsi
Per quanto riguarda il portatile, una semplice soluzione è abbassare lo schermo: la maggior parte dei sistemi chiede una password per sbloccare lo schermo. A quel punto, se la password non è troppo facile (ad esempio uguale al nome utente) difficilmente sarà possibile accedere al sistema con una semplice perquisizione.
Ricordati che non sei tenuto a dire la password, oltre al fatto che è

sempre ammessa l'eventualità di non ricordarla. Per gli smartphone sono disponibili metodi simili per mettere un blocco allo schermo, spesso in modo molto semplice.

Il sequestro

Il caso del sequestro è differente: si tratta tipicamente di un evento organizzato in cui la polizia entra in un domicilio per sequestrare oggetti utili alle indagini. La perquisizione di domicilio necessita, normalmente, di mandato. E' pero possibile subire una perquisizione domiciliare senza mandato se finalizzata alla ricerca di armi o droga; in questo caso la polizia non può sequestrare nulla che non sia armi o droga.
Ecco alcune raccomandazioni:

- Spegnere i computer o "bloccarli" (ad esempio attivando lo screensaver del portatile): questo, più che per il sequestro in sè, serve ad evitare che sia condotta *anche* una perquisizione.
- Verificare che siano posti i sigilli su tutto il materiale sequestrato, compresi computer, hard disk,etc. se questo non avviene, chiedere che sia messo a verbale.
- Richiedere la presenza di un perito di parte durante il sequestro. Chiunque può esserlo (ovviamente una persona con competenze informatiche risulta maggiormente credibile).
- Richiedere la presenza di un avvocato.
- Se ti vengono richieste le password non sei obbligato a darle. Non ricordare è meglio che negare e porsi in un atteggiamento ostile. Considera però che se il computer non è cifrato, tutte le password ivi memorizzate saranno violate con estrema semplicità, ad esempio quella di avvio di Windows oppure la password del tuo servizio on line preferito.
- Se il tuo computer è già acceso e viene usato da polizia o periti durante il sequestro, chiedi che sia messo a verbale. A maggior ragione se era spento e viene acceso. Dopo il dissequestro (ovvero alla riconsegna del materiale) **non** accendere per nessun motivo i dispositivi, per non precludere la possibilità di una eventuale controperizia. Avvisa invece un esperto informatico di tua fiducia.

Ricette per la tua sicurezza

Password

Spesso, per pigrizia, si imposta una stessa password per più contesti, o una password semplice per paura di dimenticarla. Password semplici

possono essere indovinate da programmi appositi.
Prendere la prima lettera di ciascuna parola di una frase molto lunga (almeno 12 parole) può essere un buon metodo per generare una password sufficientemente sicura e facile da ricordare. Ad esempio, la frase “ogni mattina mi alzo e ascolto la rassegna stampa di radio onda rossa” si trasforma nella password: ommasealrsdror Non bisogna usare password importanti in contesti non sicuri (internet point, computer di persone non fidate o di persone di cui ti fidi “personalmente” ma non tecnicamente o in luoghi dove ci sono telecamere); comunque, a volte questo succederà. In questi casi, e importante cambiare la password da un computer fidato appena possibile. Non condividere le password, se questo è necessario, cambia le password appena possibile.
• Diversifica il più possibile le password e comunque utilizza sempre password diverse per contesti diversi (ad esempio utilizza password diverse per la mail di lavoro, per la mail su server commerciali e per la mail su server autogestiti come Autistici/Inventati o Riseup).
• Se il tuo computer non è cifrato, le password che memorizzi sul tuo browser saranno registrate in chiaro; valuta quindi di non salvare affatto quelle particolarmente sensibili (o meglio, cifrati il disco!).

Comunicare
Le comunicazioni personali e quotidiane sono le operazioni più sensibili che fai in rete e, probabilmente, sono già state osservate dal tuo provider adsl o di posta elettronica. Quindi, o ti trovi un provider meno impiccione oppure fai in modo che il provider non possa leggere le tue comunicazioni. Ti consigliamo di seguire entrambi questi consigli.

Usare servizi autogestiti
Difficoltà di configurazione: facile
Difficoltà quotidiana: facilissima
Utile contro: identificazione, richiesta dati al fornitore di servizi, profilazione
I servizi autogestiti sono delle piccole isole nella rete, spazi aperti dove individualità e collettivi forniscono strumenti e servizi di comunicazione liberi. Questi servizi sono gratuiti per tutti/e, ma hanno un costo per chi li rende disponibili: sostienili con benefit e donazioni! I servizi autogestiti (riseup.net, autistici.org, indivia.net, tracciabi.li) prendono contromisure per evitare di fornire informazioni su di te alle autorità. Inoltre questi servizi mettono al centro delle priorità l’utente invece dei profitti.

Questo li porta a fare scelte molto migliori nei tuoi confronti. Ad esempio, Gmail ti "sconsiglia" di cancellare le email, altri servizi commerciali ti incentivano ad abbinare un numero di cellulare al tuo account.
Nessun server autogestito di chiederà mai di fare cose simili. Utilizzare servizi autogestiti e veramente semplice: per richiedere una email su autistici.org vai su https://services.autistici.org/ e compila il modulo. Dopo qualche giorno la tua email verrà attivata.

Chat sicura
Gli strumenti più diffusi per l'Instant Messaging (Skype, Google hangout, Facebook Chat, etc) si vantano molto della loro sicurezza, ma questa e solo propaganda: in realtà la privacy e semplicemente delegata a delle aziende; non c'è alcun buon motivo per credere che di fronte alla richiesta della magistratura queste difendano la privacy dei propri utenti.
Esistono però delle soluzioni: i server autogestiti A/I e Riseup offrono ai loro utenti Jabber (XMPP), uno strumento molto diffuso di Instant Messagging, che puoi usare con Pidgin. Peraltro, il servizio viene automaticamente attivato per chiunque abbia una mail con uno di questi server autogestiti. Nella nostra esperienza, Jabber e lo strumento più sicuro e più semplice da imparare ad usare continua online

Navigare in rete
Tutta la tua attività in rete può essere tracciata facilmente. La maggior parte dei siti web tiene traccia degli indirizzi IP dei loro visitatori. Questi dati possono essere utilizzati a posteriori per identificare l'autore di un contenuto pubblicato su Internet. Per questo motivo non è sufficiente utilizzare uno pseudonimo per proteggere la nostra reale identità.
Esistono software che ci danno la possibilità di rimanere anonimi durante la navigazione con il browser su internet: TorBrowser e una versione modificata di Firefox già configurata per utilizzare la rete Tor. Tor fa rimbalzare il traffico internet da una nazione all'altra prima di giungere a destinazione. Questo processo rende molto difficile l'identificazione di chi lo usa attraverso l'indirizzo IP.

Sicurezza del tuo telefono
Tutti i cellulari si appoggiano alla rete GSM. Questo ha già delle implicazioni di sicurezza. Quando usi il cellulare la tua posizione viene continuamente comunicata al tuo operatore con un'approssimazione di

circa 50 metri. Inoltre esistono sistemi di monitoraggio “preventivo”, in grado cioè di rilevare i movimenti di un dispositivo in tempo reale interpretando i comportamenti abituali e “anomali” e allertando le autorità nel caso di aggregazioni di soggetti attenzionati. I tabulati telefonici e gli sms di ciascun cittadino sono archiviati per almeno 2 anni (spesso di più) e sono accessibili in qualsiasi momento dalla polizia. Questi dati, apparentemente innocui, sono in realtà utilissimi anche semplicemente per individuare nuovi soggetti da sorvegliare.
Tutte le telefonate effettuate sono intercettabili dagli operatori e di conseguenza da polizia e magistratura. Tale possibilità nella realtà viene ampiamente sfruttata: benché solo una piccola parte delle intercettazioni sia utilizzabile come prova in sede processuale, le intercettazioni sono particolarmente diffuse a scopo investigativo, anche nei confronti di chi non e indagato. Sebbene le telefonate siano molto monitorate, sono leggermente preferibili agli sms.

Smartphone
Non tutti i cellulare sono uguali, alcuni sono più evoluti di altri. Parliamo di smartphone, includendo non solo android windows e iPhone, ma tutti i cellulari evoluti su cui puoi installare applicazioni. Questi dispositivi, che sono veri e propri computer leggeri ed estremamente portatili possono comunicare in rete (wifi/3G/4G) e possono essere “estesi” attraverso l’installazione di nuove applicazioni.
Gli smartphone offrono modalità di comunicazione aggiuntive rispetto ai vecchi cellulari quali email, chat, social network. Queste possibilità si possono tradurre in minacce. Ad esempio, le applicazioni che installiamo con tanta facilità potrebbero rivelarsi dei malware e trasformare il nostro smartphone in una microspia ultra portatile: questa eventualità si è già tradotta in realtà in molte occasioni. Occorre quindi cautela nello scegliere quali applicazioni installare, evitando l’installazione compulsiva. Non solo le app possono avere secondi fini: lo stesso “store” e in realtà un sistema capace di installare ciò che vuole di sua iniziativa sul nostro dispositivo. Questo dà un potere enorme alle aziende che lo controllano, e non può tranquillizzarci.
La localizzazione degli smartphone è ancora più precisa (raggiungendo una precisione di pochi metri) che con il GSM: grazie all’utilizzo di GPS e reti WiFi, qualsiasi applicazione può ottenere informazioni molto dettagliate sui tuoi spostamenti.
Uno smartphone è a tutti gli effetti un computer tascabile, e se utilizzato

in maniera opportuna può avere diversi vantaggi rispetto ad un cellulare tradizionale: la possibilità di scattare foto e metterle online rapidamente, ad esempio, e di grande utilità per un attivista; anche la disponibilità di chat cifrate e sicuramente più attraente degli SMS, ma dobbiamo ricordarci che gli smartphone non possono essere considerati uno strumento sicuro. In particolare, ci sentiamo di sconsigliare fortemente gli smartphone BlackBerry ed Apple (iPhone e iPad). Anche gli smartphone Android non sono esenti da problemi, ma lasciano la possibilità di un uso abbastanza sicuro ad un utente cosciente.
Forniamo qui delle ricette per usare gli smartphone a fini di mediattivismo o per ottenere un livello di sicurezza tale da poter essere violato ma solo con un considerevole investimento di tempo e denaro.

ObscuraCam: anonimizzare le immagini
Se scatti delle foto con il tuo smartphone durante un corteo faresti bene ad editarle in modo da rendere i volti delle persone irriconoscibili se pensi di conservarle o se pensi di condividerle su un social network. Nei processi contro gli attivisti i riconoscimenti attraverso le foto rappresentano spesso una prova decisiva. Inoltre ricorda che spesso non e sufficiente coprire solamente il volto, ma e necessario anonimizzare anche: spille, indumenti e tutti gli altri accessori utilizzabili per l'identificazione. Inoltre sia Facebook che Google utilizzano software capaci di riconoscere automaticamente il volto delle persone fotografate ed associargli un'identità reale.
Non sempre puoi prevedere l'esito di un corteo, per questo motivo se pubblichi "in diretta" le tue foto sui social network ricorda sempre che possono mettere in pericolo le persone coinvolte anche se stai fotografando una situazione al momento tranquilla; ad esempio potrebbe succedere di fotografare una persona che si è assentata dal posto di lavoro per essere in piazza, e la diffusione di questa foto potrebbe causargli molti problemi. Inoltre ricorda che durante un corteo il tuo materiale fotografico può essere posto a sequestro se vieni fermato dalle forze dell'ordine, quindi se le tue foto possono mettere in pericolo delle persone evita di farle.
Obscuracam è una app per Android che rende semplicissimo l'offuscamento delle facce e ti permette di editare velocemente le foto prima di pubblicarle online. E' pero molto importante che l'oscuramento sia effettuato al momento dello scatto; non bisogna quindi scattare una foto e dopo correggerla con obscuracam.

Carte telefoniche prepagate
In molte nazioni è possibile acquistare carte SIM prepagate senza fornire obbligatoriamente un documento di identità. Tutti i telefoni posseggono pero un identificativo chiamato IMEI che viene trasmesso durante ogni telefonata. Cambiare la scheda telefonica che usate quotidianamente con una acquistata in maniera anonima potrebbe non garantire il vostro anonimato, dal momento che potrebbe essere comunque possibile identificare il vostro telefono. Serve quindi abbinare una scheda anonima con un cellulare non associato alla vostra identità.

Utilizzare computer pubblici
A volte, non è possibile utilizzare il proprio computer. Per controllare la posta o navigare su internet vengono usati computer "pubblici", ad esempio in un internet point. In queste occasioni è importante ricordarsi di:

- usare il **"private browsing"** (anche detto Incognito Mode in google chrome), una modalità in cui la cronologia e le password non vengono salvate.
- **fare logout** dai tuoi account, altrimenti il successivo utilizzatore del computer avrà accesso ai tuoi dati!
- ricorda che un computer pubblico è **inaffidabile** per definizione: meglio non far passare password o dati sensibili su di esso.