

Il Passaparola di [Richard Stallman](#), programmatore, informatico e attivista statunitense.

Ciascuno è libero di far operare il proprio computer come vuole



Richard Stallman: Sono Richard Stallman. Ho lanciato il movimento per il Software Libero, che in inglese ha un nome ambiguo, Free Software, ma che riguarda la libertà, non il prezzo; ho guidato lo sviluppo del sistema operativo GNU che oggi, insieme al kernel Linux, è utilizzato come sistema GNU+Linux su milioni di computer, e che permette all'utente di avere il controllo sulle proprie attività informatiche e sul software che usa, anziché il contrario. Se si utilizza software non libero, proprietario, "soggiogante", allora è il programma che controlla l'utente, tutti gli utenti, e c'è un proprietario che controlla il programma, il che significa che quel programma è uno strumento che dà al proprietario potere nei confronti dell'utente. E' un'ingiustizia; ecco perché dobbiamo farla finita col software non libero.

Intervistatore: Non è quindi solo una questione di prezzo.

Richard Stallman: Non è assolutamente una questione di prezzo. Il prezzo, in definitiva, è solo un dettaglio; non c'è nulla di sbagliato nel pagare dei programmatori per il lavoro che svolgono. Io sono stato un programmatore, non mi offendeva essere pagato per il mio lavoro.

Il punto non è questo ma piuttosto: sei tu che controlli il software che utilizzi o è questo a controllare te? Queste sono le uniche due possibilità; con il software o sono gli utenti a controllare il programma o è il programma che controlla gli utenti. Ora, cosa determina quale situazione ricorre? Nel primo caso, in cui gli utenti controllano il programma, si tratta di free software: perché gli utenti abbiano un controllo effettivo sul programma, essi hanno bisogno di alcune libertà fondamentali; queste quattro libertà fondamentali sono i criteri guida del software libero.

La libertà zero è la libertà di eseguire il programma come desideri.

La libertà uno è la libertà di studiare il codice sorgente del programma - cioè gli schemi del programma, presentati in una forma comprensibile per l'essere umano - e poi modificare il programma in modo che operi nel modo che desideri.

Con queste due libertà ogni utente, individualmente, ha il controllo del programma; con queste due libertà ciascuno è libero di far operare il proprio computer come vuole. Ma il controllo individuale non è sufficiente, perché la maggior parte degli utenti non sa come programmare, svolge altre professioni, altre attività e se uno non è capace di programmare non sa come esercitare la libertà uno; non saprebbe comprendere la sorgente né tantomeno modificarla.

Quindi non è ancora abbastanza. Gli utenti hanno bisogno anche di un controllo collettivo, vale a dire che qualsiasi gruppo di utenti può decidere di lavorare insieme, che si tratti di due persone o di un intero paese; possono lavorare insieme, esercitando il controllo perché il computer faccia ciò che loro, collettivamente, vogliono che faccia.

Nel gruppo, quindi, ci saranno alcuni programmatori, che faranno materialmente le modifiche. Ma gli altri possono utilizzare quella versione e decidere di cooperare perché condividono degli obiettivi. Il gruppo potrebbe poi invitare il pubblico, offrire copie a tutti oppure no, è una loro scelta.

In sintesi, per esercitare un controllo collettivo sul programma c'è bisogno di due altre libertà fondamentali: la libertà due che è la libertà di ridistribuire copie identiche ad altri, mentre la libertà tre consiste nel poter distribuire le copie modificate, se lo desideri.

Queste due libertà consentono alle persone di formare un gruppo per far fare al programma quello che collettivamente vogliono e fornirne copie ad altri, in pratica invitandoli a far parte del gruppo.

Se gli utenti non godono delle quattro libertà, allora non controllano il programma. E' il programma che controlla gli utenti, e il proprietario controlla il programma. Il proprietario esercita il proprio potere sugli utenti per mezzo del programma.

In genere il proprietario è una grande compagnia, ed il proprietario comprende bene il potere che possono esercitare ed è alla costante ricerca di nuovi, astuti metodi per trarre vantaggio da quel potere a danno degli utenti.

Si possono inserire funzionalità maligne, ad esempio, che spiano gli utenti. Che limitano intenzionalmente ciò che gli utenti possono fare con i dati a disposizione. Esistono persino delle "back doors" in grado di ricevere comandi remoti, che effettuano delle operazioni sull'utenza senza richiedere l'autorizzazione e senza informare l'utente di ciò che stanno facendo.

Queste sono cose che accadono normalmente nel software non libero. Sappiamo che in Microsoft Windows ci sono delle specifiche funzionalità maligne. In Mac OS. Nel software degli i-oggetti di Apple. In Flash Player. In "Angry Birds". Nel Kindle di Amazon. Nella Playstation 3, e in quasi tutti i telefoni cellulari. Questo significa che, se tu stai usando software non libero, sei quasi certamente soggetto a qualche funzionalità maligna.

E cosa c'è da aspettarsi, quando si dà alle grandi compagnie potere sulle persone, cosa ne faranno? Ne approfitteranno! Compiono ricerche su come far del male alla gente. La mia risposta è: " Non provate a farli smettere di trattar male la gente. Toglietegli tutto il potere di cui godono." Con il software libero gli togliamo il potere, almeno in un campo della vita, naturalmente; ci sono altri campi che richiedono altre soluzioni.

Uno dei maggiori utenti di software è lo stato. Molte agenzie dello stato e altre entità statali usano software. Di solito si tratta di software non libero, il che significa che queste entità non controllano i propri computer. Il che viola la sovranità informatica dello stato.

Se usi un programma non libero e perdi il controllo del tuo computer, è peggio per te. Sei tu che ci perdi. Non ti condanno, perché non mi hai danneggiato in alcun modo. Hai danneggiato te stesso. Mi dispiace per te. Posso provare ad aiutarti, se vuoi. Quando è lo stato a perdere il controllo sul proprio computer, è molto peggio. Perché

lo stato non fa operazioni informatiche per il proprio piacere, lo fa per le persone. Lo Stato ha il dovere morale di mantenere il controllo su quelle operazioni informatiche, in modo che non vadano a finire nelle mani di terze parti.

Ciò significa che le entità statali non devono usare software proprietario. Devono usare esclusivamente software libero, e lo stato deve mantenere il controllo delle operazioni informatiche che compie per noi. Lo stato deve adottare politiche atte a liberarsi del software non libero che sta utilizzando, e naturalmente fare in modo che non ne venga introdotto altro.

Come si realizza questo? Prima di tutto, quando lo stato acquista lo sviluppo di una soluzione informatica, il contratto deve prevedere che la soluzione sia fornita come software libero, e che venga disegnata in modo da poter operare in ambienti liberi. Può essere portabile, può essere in grado di girare anche su altri ambienti, non importa. Il punto è che il contratto sia vincolato ad una soluzione che non allontani lo stato dal recuperare la propria sovranità.

Nel tempo, lo stato deve sostituire le soluzioni non libere esistenti con del software libero. Inoltre, quando lo stato acquista dei computer, deve comprare dei modelli che funzionino con il software libero, o almeno che ci si avvicinino il più possibile tra i modelli in vendita al pubblico.

In questo modo, lo stato farà pressione sulle compagnie perché vadano nella direzione di rendere i loro computer utilizzabili senza alcun software non libero, e sarà sicuro che i computer che sta acquistando non diventino un ulteriore ostacolo al recupero della sovranità informatica.

Se lo stato non ha la sovranità informatica, è vulnerabile agli abusi. Ricordate che alcuni programmi non liberi hanno delle "backdoors" che ricevono comandi remoti e fanno delle cose all'utente. Tra questi c'è Microsoft Windows, il software degli i-oggetti, e la maggior parte dei cellulari.

Se un'agenzia statale svolge un compito importante, la presenza di software non libero in quella agenzia costituisce una minaccia per la sicurezza nazionale. Io faccio riferimento ai casi conosciuti di backdoors, ma in tanti altri casi noi non sappiamo nulla, e non siamo in grado di scoprire nulla, quindi l'utilizzo di software non libero significa che lo stato rischia di avere delle backdoors. Che possono venire utilizzate per attaccare lo stato stesso.

E' già stato fatto.

Un esempio italiano

Intervistatore: Richard, il tuo consiglio su ciò che il prossimo governo italiano dovrebbe fare per il software libero.

Richard Stallman: Quali sono i miei consigli? Ho già fatto due proposte, ma ne ho altre. del benessere e della libertà delle persone. Si tratta di una missione molto ampia. Una parte di essa riguarda l'informatica per le persone. Lo stato dovrebbe aiutare la gente a diventare libera nell'utilizzo del computer. Aiutare la gente a muoversi all'uso del software libero. Non dovrebbe mai fare l'opposto, spingere i cittadini ad usare programmi non liberi. Ciò implica che alcune cose devono essere cambiate. Innanzitutto, quando lo stato distribuisce del software, esso deve sempre essere libero. Quando entità statali esortano il pubblico ad usare del software, deve essere sempre libero. La Rai diffonde dei video in un formato che prima era segreto; ora credo che non lo sia più ma il software di cui incoraggiano l'utilizzo non è libero. Questo deve finire.

Inoltre, molti siti web del governo, come molti altri siti web, spediscono del software al computer dell'utente. Software che è incluso, o richiesto, dalle pagine web. Di solito

è scritto in linguaggio JavaScript, che di solito non è libero. I siti web del governo dovrebbero assicurarsi che tutto il codice JavaScript che spedisce all'utente sia software libero.

L'influenza più grande che lo stato esercita sul pubblico è attraverso la scuola. La scuola insegna agli studenti ad usare il software. E' software libero, rispettoso della libertà, o proprietario? Bene, dovrebbe essere tutto software libero. Lo stato deve fare in modo di convertire le scuole al software libero.

Esiste in Italia un esempio di un sistema scolastico che ha adottato, in qualche misura, il software libero. E' la scuola italiana di Bolzano, che ha deciso di convertirsi al software libero. Tutti i sistemi scolastici italiani dovrebbero spostarsi sul software libero. Le scuole, come ogni altra attività educativa, hanno una missione sociale, che consiste nel formare buoni cittadini per una società forte, capace, indipendente, cooperante e libera.

In informatica, questo significa formare le persone a diventare utenti capaci di utilizzare software libero. Pronti ad essere parte attiva di una società digitale libera. Le scuole non dovrebbero mai insegnare un programma proprietario, perché questo significa insegnare dipendenza da una compagnia. E questo va contro la missione sociale di una scuola. Non si deve mai fare.

C'è poi una ragione più profonda. Per l'educazione morale. Educazione e cittadinanza. Le scuole devono fare di più che insegnare fatti e abilità. Le scuole devono insegnare lo spirito di benevolenza: l'attitudine ad aiutare altre persone. Quindi, in ogni classe deve valere questa regola: studenti, se portate un programma in classe, non potete tenerlo per voi. Dovete condividere le copie in classe con tutti quelli che le desiderano. E anche il codice sorgente, gli schemi matematici, algebrici del programma, nel caso che qualcuno voglia imparare. Perché la classe è un luogo in cui condividiamo la nostra conoscenza, quindi portare in classe del software proprietario non è permesso. La scuola deve dare il buon esempio seguendo la propria regola, quindi deve portare in classe solo software libero, e dividerne le copie con tutti, incluso il codice sorgente.

Non si tratta soltanto di come fare educazione in maniera un po' migliore, o un po' più efficiente. Si tratta di fare della buona educazione invece che una educazione cattiva, sbagliata.

Il modello migliore, a livello mondiale, di conversione delle agenzie statali al software libero è l'Ecuador, dove il Presidente Correa ha messo in atto una politica per cui qualsiasi agenzia voglia continuare ad usare del software proprietario deve richiedere un'eccezione, presentando motivazioni convincenti a sostegno della richiesta.

Altrimenti deve spostarsi sul software libero.

Una volta ottenuta l'eccezione, questa resta valida per qualche anno, poi viene riconsiderata, per valutare se sia nel frattempo divenuta possibile l'adozione di software libero. Ecco come si implementa un sistema efficace per allontanare lo stato dal software proprietario.

Va detto che oggi c'è un altro modo di perdere il controllo delle proprie attività informatiche, sia da parte degli individui, che di compagnie o agenzie di stato, e consiste nel lasciare che altri le facciano per noi sul proprio server. Se le vostre attività si svolgono sul server di qualcun altro, con software scelto da quella persona, voi non siete in controllo delle vostre attività. Questo fenomeno si chiama "software come servizio", ed è profondamente scorretto.

Le agenzie di stato devono rifiutare anche il software come servizio, a meno che non stiano utilizzando un server che è operato dallo stato a quello scopo; che va bene, in quel caso è solo un altro pezzo dello stato, che può quindi svolgere i servizi al cittadino.

Intervistatore: gli stati non devono avere software nella nuvola?

Richard Stallman: Non uso il termine "nuvola informatica", lo trovo nebuloso. Implica diverse cose, che sollevano questioni differenti. Se si utilizza quell'espressione non si sa più di cosa si stia parlando. Io preferisco usare espressioni più specifiche, come "software come servizio". Un'altra cosa che si potrebbe intendere è "servizi di archiviazione dati remoti".

Lo stato non dovrebbe mai servirsi di servizi di archiviazione remota di altre entità, mentre può fornire un centro di archiviazione remota che venga utilizzato dalle altre agenzie statali.

La tecnologia digitale ha reso possibile una sorveglianza tale che Stalin poteva solo sognarsela. E' incredibilmente pericolosa.

Può darsi che la tecnologia digitale sia una maledizione per l'umanità per il livello di sorveglianza che rende possibile. Qualcuno nella ex-Germania Est (credo) ha utilizzato non so quale cavillo di legge irlandese per chiedere che Facebook in Irlanda gli consegnasse tutti i dati che lo riguardavano. Ha ottenuto centinaia o migliaia di pagine, non ricordo più.

Ha detto che la Stasi, la polizia segreta, non avrebbe avuto un dossier così vasto su una persona che non fosse coinvolta nella politica o in affari criminosi. Lui non era particolarmente coinvolto in alcunché di politico o di criminoso, eppure Facebook aveva un dossier gigantesco su di lui.

Questo è solo un esempio della portata della sorveglianza digitale. Parte della sorveglianza digitale viene fatta attraverso elementi di sorveglianza nei programmi che utilizziamo, principalmente nel software non libero.

Se abbiamo il controllo del nostro software, abbiamo il potere di assicurarci che non contenga elementi di sorveglianza, ma ci sono altri modi in cui questa sorveglianza viene attuata. Tantissimi siti web sorvegliano la gente che li visita e anche quella che non li visita.

Facebook è il principale esempio di sorveglianza su persone che non sono suoi utenti e non visitano il suo sito. Funziona grazie ai tasti 'Mi piace'. Se visitate una pagina con su il bottone 'Mi piace', Facebook sa immediatamente che il vostro computer ha visitato quella pagina. Ecco come.

L'immagine di quel tasto 'Mi piace' viene da una server di Facebook. Quando il vostro browser guarda la pagina, vede il riferimento a quell'immagine e dice al server di Facebook: " Dammi quell'immagine". Dice anche: "Lo chiedo per questa pagina".

Il server di Facebook sa che il tuo computer ha richiesto l'immagine per questa pagina. Se sa che quel computer è usato principalmente da te, Facebook sa che hai visitato quella pagina, anche se tu non hai mai usato Facebook in vita tua.

Bene, noi del progetto GNU stiamo lavorando ad un browser che sarà in grado di bloccare queste immagini, in modo che Facebook non possa più sorvegliare le persone in quel modo. Ma ciò che occorre veramente è che tali pratiche siano proibite per legge.

L'Unione Europea ha una direttiva per la protezione dei dati, all'epoca pionieristica, peccato che appartenga ad un'altra era. Quando ci si aspettava che le compagnie acquisissero e immettessero informazioni nelle proprie banche dati perché voi avevate spedito un pezzo di carta con delle informazioni, che poi loro copiavano e archiviavano nei propri computer.

La direttiva per la protezione dei dati funziona molto bene per quel caso specifico, solo che oggi le pratiche informatiche sono cambiate. Oggi una compagnia molto probabilmente acquisisce dati personali attraverso una pagina web. Quando guardi quella pagina web, molto probabilmente questa fornisce informazioni su di te anche ad altre compagnie.

Per esempio a Facebook, se c'è un tasto 'Mi piace'. A compagnie pubblicitarie che forniscono la pubblicità al sito. E così via. Bene, quell'informazione è stata efficacemente fornita dalla ditta con cui tu stai cercando di interagire ad altre

compagnie, secondo una modalità che aggira i dettami della direttiva sulla protezione dei dati.

Dettami che devono essere estesi se vogliamo che questo comportamento venga trattato come se quella compagnia avesse fornito i tuoi dati ad altri, cosa che non sarebbe stata permessa. Ma è anche peggio di così. Oggi, il sito web di quella ditta potrebbe non trovarsi sul computer della ditta stessa. Potrebbe trovarsi su un server virtuale preso in affitto da un'altra ditta. La quale a sua volta è ora in possesso dei vostri dati.

E se quella ditta fosse negli Stati Uniti? Se il server fosse negli Stati Uniti? A quel punto i vostri dati si trovano in un posto dove manca del tutto una legge sulla protezione dei dati. Gli Stati Uniti hanno un sistema di protezione dati che si applica solo ad alcuni campi particolari. Nella maggior parte dei casi, non si applica.

Questo non deve essere permesso. Le ditte europee non devono poter prendere dati e immagazzinarli in un luogo che non è soggetto a regole per la protezione dei dati equivalenti. Se i dati trasmessi dalla compagnia al proprio server attraversano gli Stati Uniti, questi copiano tutto il traffico dati che attraversa il confine.

Così stabilisce il famoso, illegale provvedimento sulle intercettazioni di Bush, che egli riuscì poi a far legalizzare dal Congresso. Si chiama "FISA Amendments Act", credo. Stabilisce che qualora avvenga una comunicazione tra una persona degli Stati Uniti e una persona non degli Stati Uniti, questi hanno la facoltà di copiarla. E lo fanno.

E' chiaro che se lo scopo è la protezione dei dati, non si può consentire a soggetti europei di inviare dati attraverso confini dove si sa che verranno spiati. La direttiva sulla protezione dei dati viene adesso ridisegnata. Le ditte che fanno pubblicità su Internet stanno facendo lobby in maniera molto pesante per impedire che assolve alla propria funzione.

Ecco un campo in cui gli europei devono attivarsi subito. La legge è sotto esame al parlamento europeo e va velocemente. Ho tenuto lì una conferenza all'inizio di Febbraio. Spero di aver influenzato qualcuno, ma io sono straniero. Non sono uno straniero ricco, quindi non mi daranno grande ascolto.

Questa battaglia tocca a voi.