

# DECALOGO PER DIFENDERSI DA INTERNET

A cura di Deborah Bianchi [www.deborahbianchi.it](http://www.deborahbianchi.it)  
avvocato specializzato in Diritto dell'Internet dal 2006.

Internet ha segnato e sta segnando una rivoluzione epocale sia nell'economia sia nel sociale. Le vite di ciascuno di noi si svolgono per i  $\frac{3}{4}$  nell'ambiente digitale stimato l'impiego fattone sul lavoro e quello per intrattenere le relazioni personali. Indubbiamente Internet è un Bene Comune come l'energia elettrica, l'acqua, il gas. Una risorsa essenziale per la nostra società di cui non possiamo che essere soddisfatti. Tuttavia come ogni strumento dev'essere usato nel modo giusto e così si espongono di seguito poche semplici regole di base per evitare rischi inutili.

## PUNTO 1-SICUREZZA

Scaricare sempre l'ultimo aggiornamento dell'antivirus per fronteggiare i trojan dell'ultima ora. Password segretate e composte da molti caratteri (dagli 8 in su) in cui vi siano numeri, lettere, simboli, punteggiatura (ove consentito), minuscole e maiuscole.

## PUNTO 2-DIFFIDARE DA TUTTI

Non cedere mai la propria password o il proprio codice del cellulare neppure all'amico del cuore e men che meno al fidanzato/a.

Non cliccare mai sui LINK che giungono per e.mail perché sono inganni per piazzare virus-spia nel cellulare o nel pc. Neppure se si tratta di un avviso di pagamento di Equitalia, della bolletta del telefono e tanto meno del rinnovo delle credenziali della carta di credito. Non concedere l'amicizia sui social a soggetti sconosciuti o che comunque non hanno amici in comune con noi o ancora a soggetti che sembrano "troppo attendibili".

## PUNTO 3-INFORMARSI SEMPRE SULLE PRIVACY POLICY

Ogni volta che avviene la registrazione a una nuova piattaforma digitale controllare sempre la privacy policy. In particolare verificare se dobbiamo solo subire tutto con un unico click di consenso alla fine oppure se esistono delle opzioni che ci danno possibilità di scelta. Solo le policy con la possibilità di opzioni sono attendibili.

Settare le opzioni privacy a seconda dell'utilizzo che facciamo del social media. Se lo usiamo per parlare e condividere immagini con gli amici reali sarebbe prudente restringere l'accesso e la visibilità del nostro profilo solo agli amici veri. Se invece lo usiamo a fini di lavoro possiamo lasciare il profilo pubblico mettendo però l'opzione di controllo sui tag e sui post che non provengono dagli amici evitando così che appaiano all'improvviso sul nostro profilo.

Evitare i social media che ammettono l'anonimato.

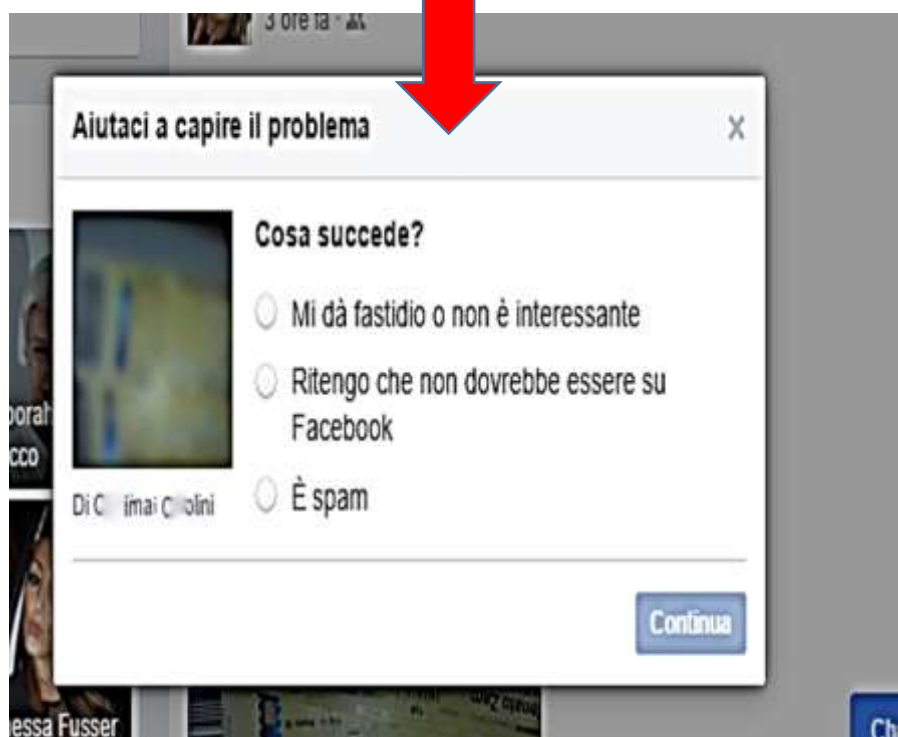
## PUNTO 4-REVENGE PORN

Attualmente la forma di denigrazione più frequente on line è il "revenge porn" ovvero la diffusione in Rete di immagini/video hard o foto intime da parte degli ex partner abbandonati che vogliono vendicarsi. Qui la prima forma di tutela sta a monte ovvero mai concedere "pagni d'amore" consistenti in foto o video intimi neppure al coniuge perché quando l'amore finisce scatta la vendetta.

## PUNTO 5-CYBERBULLISMO E CYBERSTALKING

Quando siamo oggetto di persecuzione on line dobbiamo subito attivare il tasto ANTI-ABUSO ove il social media lo preveda.

## ESEMPIO



Se la persecuzione continua e il gestore della piattaforma non si è attivato per rimuovere il post lesivo occorre DENUNCIARE alla Polizia Postale. Si può spedire la denuncia anche on line al sito: [www.commissariatodips.it](http://www.commissariatodips.it). Per emergenze chiamare i numeri 112 e 113 o rivolgetevi all'ufficio di Polizia Postale più vicino.

Se neppure la denuncia ha effetto occorre rivolgersi a un avvocato specializzato in Diritto dell'Internet e solo a quelli specializzati altrimenti si rischia di perdere del tempo prezioso. Si può poi chiedere l'AMMONIMENTO DEL QUESTORE nei confronti del persecutore.

## **PUNTO 6-DIRITTO ALL'OBLIO**

Quando vengono indicizzati dai motori di ricerca delle notizie di cronaca o dei contenuti che non sono più corrispondenti alla nostra identità personale attuale è possibile chiedere la deindicizzazione direttamente al motore di ricerca oppure al gestore del sito che ha implementato on line il contenuto non più attuale. Si raccomanda di procedere nel modo seguente:

- a) Compilare e spedire il format on line predisposto dal provider oppure utilizzare il tasto antiabuso;
- b) Se non giunge risposta entro 1 mese rivolgersi a un esperto affinché spedisca una lettera di diffida ad adempiere;
- c) Se anche la diffida non è servita occorre rivolgersi a un avvocato specializzato in Diritto dell'Internet e solo a quelli specializzati altrimenti si rischia di perdere del tempo prezioso.

## **PUNTO 7-RICORSO AL GARANTE PRIVACY**

In tutti i casi in cui si registra un trattamento dati personali, sensibili, di salute, giudiziari non autorizzato dall'interessato è possibile presentare ricorso al Garante della Privacy seguendo la procedura esposta nel prosieguo.

- a) L'interessato deve rivolgere al titolare del trattamento una richiesta senza particolari formalità (a mezzo posta, anche elettronica, o telefax), anche oralmente se ciò sia sufficiente (c.d. "interpello preventivo"). Esiste un modulo per l'esercizio dei diritti al seguente LINK: <http://www.garanteprivacy.it/home/modulistica>
- b) Se entro 15 giorni non c'è risposta si può presentare il ricorso.
- c) La proposizione del ricorso ha il costo delle competenze dell'avvocato unite al costo dei diritti di Segreteria di € 150,00. Tuttavia il ricorso può essere presentato anche senza avvocato.
- d) Il ricorso deve contenere: la sottoscrizione del ricorrente autenticata nelle forme di legge; gli estremi identificativi completi del titolare del trattamento nei cui confronti è presentato; l'indicazione del provvedimento richiesto al Garante, con esclusivo riferimento ai diritti indicati nell'art. 7 del Codice, precedentemente esercitati con istanza, alla quale il titolare non abbia fornito, entro i quindici giorni, un idoneo riscontro; gli elementi posti a fondamento della domanda; il domicilio eletto ai fini del procedimento; la copia dell'istanza rivolta al titolare; la prova del versamento dei diritti di segreteria.
- e) Il pagamento dei diritti di segreteria deve essere versato utilizzando uno dei seguenti canali: conto corrente presso Banca Popolare di Sondrio - Ag. 26 - Roma - CODICE IBAN: IT14 H056 9603 2260 0000 3900 X58 - CODICE SWIFT: POSOIT22;  
conto corrente presso Poste Italiane S.p.A., IBAN IT 75 Y 07601 03200 000096677000;  
bollettino di conto corrente postale n. 96677000.

Il versamento va intestato a: Garante per la protezione dei dati personali, Piazza di Monte Citorio, 115/121, 00186 Roma, con la causale "diritti di segreteria per ricorso".

## **PUNTO 8- MUOVERSI IN TEMPO E MAI SOTTOVALUTARE**

In tutti i casi di illecito ai danni della persona on line occorre che la vittima si muova subito perché il danno internet è come un cancro. Se vai in tempo dallo specialista riesci a debellarlo ma se aspetti si possono originare le metastasi e non c'è più nulla da fare. Ovviamente le metastasi sono la viralizzazione dei contenuti lesivi che quando sono sparsi in tutto il web non sono più raggiungibili.

## **PUNTO 9- PROPOSTA DI LEGGE SUL BULLISMO ON LINE**

In questi giorni dell'Ottobre 2016 è in corso di approvazione alla Camera la Legge sul bullismo on line. Si tratta di una normativa pensata per i minori che adesso si estenderebbe anche agli adulti ma quest'ultima modifica è tutta ancora da verificare. In sostanza l'impianto centrale della proposta di legge che probabilmente rimarrà invariato prevede per i minori tutele rafforzate. In particolare un procedimento più rapido per cancellare i contenuti lesivi così stabilito:

- Segnalazione al gestore della piattaforma e obbligo di risposta di questo ultimo entro 48 ore;
- Se non giunge risposta dal gestore, la vittima può rivolgersi al Garante Privacy che provvede entro le successive 48 ore.

## **PUNTO 10- CULTURA ETICA DIGITALE**

I mezzi di tutela elencati in questo decalogo possono servire ma il nodo cruciale della difesa della vittima nell'Internet è costituito dalla formazione dei cittadini a una cultura etica digitale. Come prima nelle scuole si insegnava educazione civica ora si dovrebbe ripetere l'insegnamento dell'educazione civica sia nella società materica sia nella società digitale. Il legislatore e la Polizia Postale si stanno molto adoperando per questo. Tuttavia il lavoro da compiere è immenso e le risorse economiche disponibili sono poche. Il consiglio dunque è quello di informarsi sempre sull'evoluzione delle nuove tecnologie digitali per restare al passo coi tempi ed evitare di essere gabbati. Nella società dell'informazione digitale, l'informazione costante e aggiornata è il mezzo di difesa principale.