

Come restare al sicuro (davvero) se fai giornalismo investigativo

Maria Cattini | 23/05/2025 | Open source intelligence

☐☐ Fare giornalismo investigativo oggi è un atto di coraggio

Se indaghi su criminalità organizzata, corruzione o poteri forti, sai già una cosa:

☐☐ **non basta avere prove, serve anche protezione.**

Non solo dalle minacce fisiche. Ma anche da denunce strategiche, sorveglianza digitale, attacchi legali e campagne di screditamento.

Oggi servono **strategie di sicurezza a 360°**. Pratiche, continue, condivise.

⚖️ Minacce legali: SLAPP, processi e intimidazioni

Le **SLAPP** ([Strategic Lawsuits Against Public Participation](#)) non puntano a vincere. Puntano a **zittire**.

☐☐ Sono denunce intimidatorie usate per bloccare chi indaga su temi scomodi.

☐☐ Il trucco? Far causa in paesi dove il processo è lungo, costoso, estenuante.

Cosa puoi fare:

- Non sottovalutare nessuna denuncia
- Parla subito con il tuo team legale
- Documenta tutto
- Valuta una reazione attiva: Pavla Holcová ha denunciato il primo ministro ceco... e ha vinto

☐☐ **Reporter Shield** è un'iniziativa pensata per aiutare economicamente chi finisce in tribunale per il suo lavoro.

☐☐ [Sicurezza digitale](#): non serve essere hacker, ma serve metodo

La tua identità online, i tuoi messaggi, le tue fonti... tutto può essere bersaglio.

Ecco cosa puoi fare oggi per proteggerti in modo semplice ma efficace:

☐☐ **Comunicazione:**

- Usa Signal (con messaggi a scomparsa)
- Evita linguaggio ambiguo: tutto può essere estrapolato in tribunale

☐☐ **Accesso e credenziali:**

- Usa un password manager

- Attiva la 2FA con chiavi fisiche (YubiKey)
- Riavvia il telefono ogni giorno (sì, davvero)

☐☐ Navigazione:

- Naviga solo con VPN su reti pubbliche
- Aggiorna spesso i tuoi dispositivi
- Blocca pubblicità e tracciamenti

☐☐ Profilo:

- Riduci la tua presenza sui social
- Evita “tag” e geolocalizzazione quando lavori su casi sensibili

☐☐ Sicurezza fisica: attenzione a ogni dettaglio

Non è paranoia, è sopravvivenza. Chi fa inchieste su poteri criminali è sotto osservazione, anche offline.

Checklist fisica:

- Non lasciare computer o taccuini in ufficio
- Installa telecamere nei luoghi di lavoro
- Impara a riconoscere se sei seguito
- Riporta ogni minaccia subito al team
- Organizza incontri riservati senza dispositivi, se necessario

☐☐ La **sicurezza va pianificata** all’inizio di ogni indagine, non alla fine.

☐☐☐ Gli editori devono essere parte attiva della protezione

Un buon editore:

- ☐ Valuta il rischio prima di approvare un’inchiesta
- ☐ Fornisce supporto fisico, legale, digitale
- ☐ Interviene per allontanare il giornalista in caso di pericolo

E soprattutto: **non lascia mai solo il proprio team.**

✍️ Come scrivere in sicurezza (senza autocensura)

Le parole contano. Anche nella difesa personale.

☐☐ Alcuni consigli semplici e pratici:

- Offri diritto di replica a chi citi, anche se scomodo
- Evita frasi gratuite o ironie: possono innescare reazioni violente
- Taglia i dettagli irrilevanti che possono umiliare (e provocare)

☐☐ A volte, scegliere cosa **non scrivere** è la miglior forma di difesa.

☐ In sintesi: la tua sicurezza è parte del lavoro

Fare giornalismo investigativo è rischioso. Ma **non sei solo.**

Con strumenti giusti, una rete che ti supporta e un piano ben costruito, puoi fare il tuo lavoro **senza rinunciare alla sicurezza**.

Glossario dei Termini Chiave

- **Giornalismo investigativo**: Un tipo di giornalismo che implica un'indagine approfondita e prolungata su argomenti specifici, spesso riguardanti criminalità organizzata, corruzione o poteri forti.
- **Sicurezza 360°**: Un approccio olistico alla sicurezza che considera e affronta minacce da molteplici fronti, inclusi quello fisico, digitale e legale.
- **SLAPP (Strategic Lawsuits Against Public Participation)**: Denunce strategiche contro la partecipazione pubblica; azioni legali intentate per intimidire, bloccare e esaurire finanziariamente coloro che criticano o indagano su potenti individui o organizzazioni.
- **Reporter Shield**: Un'iniziativa o organizzazione che fornisce supporto finanziario o assistenza legale ai giornalisti che affrontano azioni legali a causa del loro lavoro.
- **Open source intelligence (OSINT)**: La raccolta e l'analisi di informazioni da fonti pubblicamente disponibili per scopi di intelligence.
- **Password manager**: Software o servizio che aiuta gli utenti a generare, archiviare e gestire in modo sicuro le proprie password.
- **2FA (Autenticazione a due fattori)**: Un metodo di sicurezza che richiede due diversi tipi di credenziali per verificare l'identità di un utente, come una password e una chiave fisica.
- **YubiKey**: Un tipo di chiave di sicurezza hardware utilizzata per l'autenticazione a due fattori.
- **VPN (Virtual Private Network)**: Una rete privata virtuale; un servizio che cripta la connessione internet dell'utente e maschera il suo indirizzo IP per una maggiore privacy e sicurezza online.
- **Geolocalizzazione**: La determinazione o l'indicazione della posizione geografica di una persona o di un dispositivo.
- **Diritto di replica**: Il diritto di una persona o di un'organizzazione citata in una pubblicazione di rispondere alle affermazioni fatte.
- **Autocensura**: La pratica di limitare la propria espressione o la propria indagine per evitare possibili conseguenze negative o ritorsioni.

☐☐ **Fare giornalismo investigativo oggi è un atto di coraggio**

Se indaghi su criminalità organizzata, corruzione o poteri forti, sai già una cosa:

☐☐ **non basta avere prove, serve anche protezione.**

Non solo dalle minacce fisiche. Ma anche da denunce strategiche, sorveglianza digitale, attacchi legali e campagne di screditamento.

Oggi servono **strategie di sicurezza a 360°**. Pratiche, continue, condivise.

⚖️ **Minacce legali: SLAPP, processi e intimidazioni**

Le **SLAPP** ([Strategic Lawsuits Against Public Participation](#)) non puntano a vincere. Puntano a **zittire**.

☐☐ Sono denunce intimidatorie usate per bloccare chi indaga su temi scomodi.

☐☐ Il trucco? Far causa in paesi dove il processo è lungo, costoso, estenuante.

Cosa puoi fare:

- Non sottovalutare nessuna denuncia
- Parla subito con il tuo team legale
- Documenta tutto
- Valuta una reazione attiva: Pavla Holcová ha denunciato il primo ministro ceco... e ha vinto

☐☐ **Reporter Shield** è un'iniziativa pensata per aiutare economicamente chi finisce in tribunale per il suo lavoro.

☐☐ [Sicurezza digitale](#): **non serve essere hacker, ma serve metodo**

La tua identità online, i tuoi messaggi, le tue fonti... tutto può essere bersaglio.

Ecco cosa puoi fare oggi per proteggerti in modo semplice ma efficace:

☐☐ **Comunicazione:**

- Usa Signal (con messaggi a scomparsa)
- Evita linguaggio ambiguo: tutto può essere estrapolato in tribunale

☐☐ **Accesso e credenziali:**

- Usa un password manager
- Attiva la 2FA con chiavi fisiche (YubiKey)
- Riavvia il telefono ogni giorno (sì, davvero)

☐☐ **Navigazione:**

- Naviga solo con VPN su reti pubbliche
- Aggiorna spesso i tuoi dispositivi
- Blocca pubblicità e tracciamenti

☐☐ **Profilo:**

- Riduci la tua presenza sui social
- Evita “tag” e geolocalizzazione quando lavori su casi sensibili

☐☐ **Sicurezza fisica: attenzione a ogni dettaglio**

Non è paranoia, è sopravvivenza. Chi fa inchieste su poteri criminali è sotto osservazione, anche offline.

Checklist fisica:

- Non lasciare computer o taccuini in ufficio
- Installa telecamere nei luoghi di lavoro
- Impara a riconoscere se sei seguito
- Riporta ogni minaccia subito al team
- Organizza incontri riservati senza dispositivi, se necessario

☐☐ **Lsicurezza va pianificata** all’inizio di ogni indagine, non alla fine.

☐☐☐☐ **Gli editori devono essere parte attiva della protezione**

Un buon editore:

- ☐ Valuta il rischio prima di approvare un’inchiesta
- ☐ Fornisce supporto fisico, legale, digitale
- ☐ Interviene per allontanare il giornalista in caso di pericolo

E soprattutto: **non lascia mai solo il proprio team.**

✍️ **Come scrivere in sicurezza (senza autocensura)**

Le parole contano. Anche nella difesa personale.

☐☐ Alcuni consigli semplici e pratici:

- Offri diritto di replica a chi citi, anche se scomodo
- Evita frasi gratuite o ironie: possono innescare reazioni violente
- Taglia i dettagli irrilevanti che possono umiliare (e provocare)

☐☐ A volte, scegliere cosa **non scrivere** è la miglior forma di difesa.

☐ In sintesi: la tua sicurezza è parte del lavoro

Fare giornalismo investigativo è rischioso. Ma **non sei solo**.

Con strumenti giusti, una rete che ti supporta e un piano ben costruito, puoi fare il tuo lavoro **senza rinunciare alla sicurezza**.

Glossario dei Termini Chiave

- Giornalismo investigativo: Un tipo di giornalismo che implica un'indagine approfondita e prolungata su argomenti specifici, spesso riguardanti criminalità organizzata, corruzione o poteri forti.
- Sicurezza 360°: Un approccio olistico alla sicurezza che considera e affronta minacce da molteplici fronti, inclusi quello fisico, digitale e legale.
- SLAPP (Strategic Lawsuits Against Public Participation): Denunce strategiche contro la partecipazione pubblica; azioni legali intentate per intimidire, bloccare e esaurire finanziariamente coloro che criticano o indagano su potenti individui o organizzazioni.
- Reporter Shield: Un'iniziativa o organizzazione che fornisce supporto finanziario o assistenza legale ai giornalisti che affrontano azioni legali a causa del loro lavoro.
- Open source intelligence (OSINT): La raccolta e l'analisi di informazioni da fonti pubblicamente disponibili per scopi di intelligence.
- Password manager: Software o servizio che aiuta gli utenti a generare, archiviare e gestire in modo sicuro le proprie password.
- 2FA (Autenticazione a due fattori): Un metodo di sicurezza che richiede due diversi tipi di credenziali per verificare l'identità di un utente, come una password e una chiave fisica.
- YubiKey: Un tipo di chiave di sicurezza hardware utilizzata per l'autenticazione a due fattori.
- VPN (Virtual Private Network): Una rete privata virtuale; un servizio che cripta la connessione internet dell'utente e maschera il suo indirizzo IP per una maggiore privacy e sicurezza online.
- Geolocalizzazione: La determinazione o l'indicazione della posizione geografica di una persona o di un dispositivo.
- Diritto di replica: Il diritto di una persona o di un'organizzazione citata in una pubblicazione di rispondere alle affermazioni fatte.
- Autocensura: La pratica di limitare la propria espressione o la propria indagine per evitare possibili conseguenze negative o ritorsioni.