



Hacker etici (White Hat Hackers):

La loro situazione giuridica, i rischi correlati che si assumono e il ruolo dell'IFPDT

I.	Oggetto.....	1
II.	Contesto e definizioni.....	1
	1. Hacker etici (White Hat Hacker, WHH).....	1
	2. Divulgazione coordinata delle vulnerabilità (Coordinated Vulnerability Disclosure, CVD) ...	2
	3. La politica di CVD istituita dal NCSC	2
III.	Situazione giuridica degli hacker etici dal punto di vista della LPD	2
IV.	Rischi giuridici per gli hacker etici.....	3
	1. Rischi sotto il profilo del diritto civile (in particolare art. 15 LPD).....	3
	2. Rischi sotto il profilo del diritto penale (in particolare art. 143, 143 ^{bis} e 179 ^{novies} CP).....	4
	3. Rischi dal profilo del diritto amministrativo (IFPDT; art. 49 segg. LPD)	4
V.	Ruolo dell'IFPDT	4

I. Oggetto

- 1 Il presente promemoria si rivolge principalmente agli hacker etici per renderli attenti alla natura delle loro attività in relazione al quadro giuridico nel quale operano, in particolare dal punto di vista della protezione dei dati. Non intende esprimere un giudizio su queste attività, ma si limita a constatare l'esistenza di questi attori e a fornire loro una guida di comportamento.

II. Contesto e definizioni

1. Hacker etici (White Hat Hacker, WHH)
- 2 Si moltiplicano le notifiche all'Incaricato federale della protezione dei dati e della trasparenza (IFPDT), o ai media, riguardanti la scoperta di falle nei sistemi informatici. Spesso queste notifiche vengono fatte da persone che si definiscono hacker etici (*White Hat Hackers*, WHH). Nella sua accezione ideale un hacker etico si adopera per rilevare falle con uno spirito benevolo: non cerca di sfruttarle per trarne vantaggi, né di utilizzarle per una particolare causa (hacktivisti o ciberattivisti). Al contrario mette il gestore del sistema in condizione di correggere le falle e quindi di migliorare la propria sicurezza informatica. Va notato che gli hacker etici possono agire nell'ambito di un mandato ricevuto dal gestore del sistema, allo scopo di testarlo: questo caso non è oggetto del presente promemoria poiché *a priori* non è problematico dato che gli hacker etici agiscono d'intesa con l'obiettivo.

- 3 Le spiegazioni che seguono si rivolgono dunque agli hacker etici che agiscono fuori da qualsiasi contesto e all'insaputa del gestore del sistema, il quale sarà informato soltanto se la falla viene effettivamente scoperta. Con le loro azioni questi hacker possono rapidamente cadere nell'illegalità. Senza pretendere di essere esaustivo, questo promemoria intende fornire alcuni spunti di riflessione in modo che gli hacker etici siano in grado di meglio valutare le implicazioni delle loro azioni. L'ottica adottata è quella di un hacker etico nella sua accezione ideale ossia di «persona che vuole fare la cosa giusta»; per definizione le attività degli hacker che mirano a ottenere un vantaggio diretto (p. es. sfruttamento dei dati per scopi personali) oppure quelle degli attivisti che utilizzano queste falle a scopo di protesta (p. es. bloccare il sito Internet di un'impresa) sono *a priori* incompatibili con le prescrizioni che seguono (cfr. in particolare il concetto più ampio di hacktivisti, un concetto indipendente dalle questioni di malevolenza/benevolenza, impiegato nel [rapporto tecnico del NCSC «Minacce generali, autori e strumenti» del 16 febbraio 2021](#), n. 3.4.).

2. Coordinated Vulnerability Disclosure (CVD)

- 4 Con *Coordinated Vulnerability Disclosure* (CVD; divulgazione coordinata delle vulnerabilità) s'intende il processo di coordinamento e di condivisione di informazioni sulle vulnerabilità tra i gruppi d'interesse coinvolti (rilevatori, imprese interessate, Computer Emergency Response Teams [CERT] del Governo) allo scopo di ridurre gli effetti negativi delle vulnerabilità e informare il pubblico; una politica di CVD implica l'istituzione di piattaforme di notifica sulle quali gli hacker etici possono notificare le falle di sicurezza scoperte senza timore di essere perseguiti penalmente; inoltre, nell'ambito di una politica di questo tipo i gestori sono in genere tenuti a rimediare alle falle notificate in questo modo entro un termine definito.¹
- 5 Il concetto di CVD è essenzialmente contrario alla premessa riconosciuta e disciplinata all'articolo 2 della [Convenzione di Budapest del 23 novembre 2001 sulla cibercriminalità \(RS 0.311.43\)](#), secondo cui gli Stati firmatari adottano misure legislative per definire come reato l'accesso intenzionale a un sistema senza autorizzazione. Questo potrebbe spiegare perché i Paesi Bassi e la Francia sono gli unici Paesi membri dell'Unione europea a disporre di una politica di CVD pienamente consolidata.²

3. La politica di CVD istituita dal NCSC

- 6 In Svizzera il Centro nazionale per la cibersicurezza (NCSC) ha istituito una piattaforma per la notifica di CVD³, una scheda di buone prassi pensata per guidare gli hacker etici. Queste regole sono essenzialmente pertinenti anche dal punto di vista del diritto in materia di protezione dei dati; il presente promemoria è complementare e si concentra su aspetti più specifici della protezione dei dati.

III. **Situazione giuridica degli hacker etici dal punto di vista della LPD**

- 7 Accedere a un sistema informatico sfruttando una falla permette spesso di avere accesso ai dati in esso contenuti. Se si tratta di dati personali, si applica la legge federale sulla protezione dei dati (LPD)⁴. Qualsiasi operazione – consultazione, caricamento, comunicazione, registrazione ecc. – che l'hacker etico effettua con questi dati costituisce un trattamento ai sensi della LPD (art. 5 lett. d LPD). La LPD stabilisce diversi principi essenziali che devono essere rispettati da chiunque tratti dei dati, quindi anche dagli hacker etici.

¹ [Governance von 0-Day-Schwachstellen in der deutschen Cyber-Sicherheitspolitik - Stiftung Wissenschaft und Politik \(swp-berlin.org\)](#), pag. 32, consultato il 25 mag. 2023.

² [Governance von 0-Day-Schwachstellen in der deutschen Cyber-Sicherheitspolitik - Stiftung Wissenschaft und Politik \(swp-berlin.org\)](#), pag. 33-34, consultato il 25 mag. 2023.

³ [Coordinated Vulnerability Disclosure \(CVD\) \(admin.ch\)](#), consultato il 25 mag. 2023.

⁴ In questo promemoria, quando viene citato la LPD, si fa riferimento alla nuova legge, che entrerà in vigore il 1° settembre 2023.

8 In caso di inosservanza, gli hacker etici devono essere consapevoli che il trattamento effettuato è *a priori* illecito anche se agiscono secondo l'accezione ideale di hacker etico. Di seguito sono illustrati alcuni dei principi più pertinenti per quanto riguarda le attività degli hacker etici:

- Il principio di liceità (art. 6 cpv. 1 LPD) implica il rispetto di norme giuridiche, anche di quelle che esulano dalla LPD: un trattamento è illecito se viola una norma di diritto. Questo principio si riferisce evidentemente al diritto penale (p. es. agli art. 138 segg. o 179 segg. del Codice penale [CP]), ma in modo più ampio anche a tutto l'ordinamento giuridico (p. es. il divieto d'inganno o di minaccia secondo gli art. 28 segg. del Codice delle obbligazioni [CO]).
- Il principio della buona fede (art. 6 cpv. 2 LPD) si riferisce al comportamento generale della persona che tratta i dati. Per l'hacker etico questo implica in particolare di non avere secondi fini e di non cercare di nuocere al gestore del sistema o alle persone interessate (ossia le persone cui appartengono i dati in questione). Inoltre, non deve in particolare adottare un comportamento che ostacoli gli sforzi del gestore per rimediare alle falle scoperte e in questo modo (ri)stabilire uno stato conforme ai requisiti in materia di protezione dei dati (p. es. proferire minacce, fissare scadenze irrealiste, bloccare i sistemi ecc.).
- In base al principio di finalità (art. 6 cpv. 3 LPD) i dati non devono essere utilizzati per scopi incompatibili con quelli indicati nel momento della loro raccolta. Il fatto che i dati siano trattati da terzi, ad esempio da un hacker seppur ben intenzionato, è *a priori* incompatibile con gli scopi iniziali della raccolta e rende dunque il trattamento di principio illecito. L'hacker etico deve dunque innanzitutto astenersi dal trattare i dati personali a cui ha accesso.
- Il principio di proporzionalità (art. 6 cpv. 2 LPD) impone di non fare più di quanto necessario per ottenere lo scopo prefissato – in questo caso diagnosticare e documentare una falla (*proof of concept*). Inoltre, se nonostante la probabile illiceità di questo comportamento, un hacker etico ritiene che sia comunque necessario accedere ai dati stessi per svolgere le sue indagini, dovrà limitare i suoi trattamenti al minimo necessario – sia dal punto di vista della quantità di dati sia del tipo di trattamento. Questo implica che non dovrà conservare i dati più a lungo del necessario. La raccomandazione del NCSC di effettuare trattamenti soltanto sul proprio profilo è in questo caso particolarmente pertinente (cfr. n. marg. 6).
- Tutti questi principi vietano pure di comunicare i dati esposti oppure di divulgare l'esistenza di una falla (eccetto alle autorità di vigilanza), altrimenti si potrebbero danneggiare le persone interessate. Pertanto una divulgazione sui media è di principio incompatibile con questi principi (in particolare quando il gestore si sforza di rimediare alle falle il più rapidamente possibile). Questi principi raccomandano anche all'hacker etico di comunicare il prima possibile al gestore le proprie scoperte lasciandogli tempo a sufficienza per correggere le falle.

IV. Rischi giuridici per gli hacker etici

1. Rischi sotto il profilo del diritto civile (in particolare art. 15 LPD)

9 L'attività che può portare l'hacker etico a violare i principi sopracitati lo espone a pretese di diritto civile da parte del gestore del sistema o delle persone interessate. Se agisce in buona fede e limita i suoi trattamenti al minimo, ossia se adotta un comportamento di hacker etico ideale e cerca di rispettare i principi della LPD, si può supporre che non ci sarà un reale interesse ad agire: quando il gestore o le persone interessate saranno informati della falla l'hacker etico avrà già cancellato i dati eventualmente raccolti o sarà in procinto di farlo; non avranno inoltre subito alcun danno economico o di reputazione poiché l'hacker etico non avrà divulgato informazioni; ecc.

10 Non si può escludere il rischio di azione civile – la scelta spetta al gestore e alle persone interessate –, ma il fatto di adottare un comportamento di hacker etico ideale ridurrà al minimo questi rischi.

2. Rischi sotto il profilo del diritto penale (in particolare art. 143, 143^{bis} e 179^{novies} CP)

- 11 Oltre ai rischi in materia civile, l'hacker etico rischierà il perseguimento penale, in particolare sulla base degli articoli 143, 143^{bis} e 179^{novies} CP. Alcuni di questi reati sono per definizione incompatibili con un hacker etico (l'art. 143 cpv. 1 CP p. es. concerne il caso in cui l'hacker mira al profitto). Altri possono essere commessi anche se l'hacker si comporta in modo ideale (in particolare l'art. 143^{bis} cpv. 1 e 179^{novies} CP). Poiché questi ultimi reati sono *a priori* perseguibili soltanto a querela di parte, sono applicabili anche in questo caso le considerazioni fatte circa la mitigazione dei rischi di causa civile.
- 12 Inoltre, in presenza di un sospetto fondato di reato perseguito d'ufficio (ossia anche in assenza di querela), gli impiegati dell'IFPDT sottostanno all'obbligo di denuncia (art. 22a della legge sul personale federale [LPers]).

3. Rischi dal profilo del diritto amministrativo (IFPDT; art. 49 segg. LPD)

- 13 Nel momento in cui tratta dei dati l'hacker etico può diventare lui stesso un titolare del trattamento ai sensi della LPD. Pertanto, se il suo comportamento sembra problematico dal punto di vista della LPD, in particolare se sembra che l'hacker non abbia cercato di conformarsi ai principi sopracitati, l'IFPDT può essere indotto ad aprire un'inchiesta e disporre provvedimenti amministrativi nei confronti dell'hacker etico stesso (art. 49 segg. LPD).

V. Ruolo dell'IFPDT

- 14 La notifica all'IFPDT non è obbligatoria per gli hacker etici, pertanto non è espressamente prevista nella LPD (il titolare del trattamento è invece tenuto a notificare ogni falla che comporta un rischio elevato per le persone interessate, in particolare quando vi è da temere che sia stata sfruttata; cfr. art. 24 LPD). Se si prevede comunque una notifica vanno considerati diversi elementi:
 - Come già menzionato (cfr. n. marg. 12), in presenza di un sospetto fondato di reato perseguito d'ufficio (anche in assenza di querela: p. es. art. 143 cpv. 1 CP), gli impiegati dell'IFPDT hanno un obbligo di denuncia (art. 22a LPers).
 - Se indizi sufficienti lasciano presumere una violazione delle disposizioni sulla protezione dei dati, l'IFPDT può aprire un'inchiesta (art. 49 segg. LPD) nei confronti del titolare del trattamento ai sensi dell'art. 5 lett. j LPD (ad es. il gestore del sistema). Se sono state violate disposizioni sulla protezione dei dati, può ordinare misure amministrative per rimediare ai rischi legati alla protezione dei dati (cfr. art. 51 cpv. 3 LPD). Tuttavia, non sempre una notifica all'IFPDT sarà opportuna. Se la falla non è il frutto di una negligenza grave, se non vi sono indizi che sia stata sfruttata e se il gestore del sistema vi ha posto rimedio in modo soddisfacente, l'apertura di un'inchiesta può avverarsi superflua.
 - Notiamo infine che l'IFPDT può essere indotto ad aprire un'inchiesta (art. 49 segg. LPD) contro l'hacker stesso. Anche in questo caso non vi è garanzia di anonimato – anche se la divulgazione del nome da parte dell'IFPDT avviene sempre con un obiettivo preciso ed entro i limiti di legge.