COME ACQUISIRE LA PROVA DIGITALE
DURANTE L'ATTIVITÁ INVESTIGATIVA

Carissimi, facendo seguito alle precedenti pubblicazioni in relazione agli argomenti trattati nel corso dell'ultima edizione delle Giornate di Polizia Locale e Sicurezza Urbana (settembre 2021), desidero segnalare alla Vostra attenzione un piccolo contributo relativo all'acquisizione della prova digitale durante l'esercizio dell'attività investigativa.

Gli agenti e gli ufficiali di Polizia Locale, ai sensi dell'**art. 57 c.p.p.,** rivestono come noto anche funzioni di agenti di Polizia Giudiziaria e, per tale ragione debbono, anche di propria iniziativa, prendere notizia dei reati e compiere gli atti necessari al fine di assicurare le fonti di prova.
Relativamente a quest'ultimo aspetto si è focalizzata la relazione del 16 settembre 2021 tenuta da **Marco Luciani**, Responsabile Polizia Giudiziaria della Polizia Locale di Milano.
Nello specifico, l'argomento affrontato dal Relatore ha riguardato l'acquisizione della prova digitale.
Qual è la ragione di ospitare uno spazio di riflessione su questo specifico argomento?
La ragione principale risiede nel fatto che la prova digitale ed informatica comporta maggiori difficoltà sotto il profilo della raccolta e della conservazione rispetto agli ordinari mezzi probatori.
Difatti, i dispositivi elettronici, di qualsiasi natura essi siano (*smartphone*, *laptop*, *pc*, ecc.), sono dotati di una memoria interna contenente dati.
Il processo di raccolta e di conservazione di detti è complesso tanto sotto il profilo tecnico, quanto sotto il profilo giuridico.
In quest'ultimo senso, la l. 48/2008, in tema di criminalità informatica, ha introdotto nel codice penale fattispecie di reato volte a sanzionare comportamenti lesivi dell'integrità dei dati informatici, nella cui commissione

può, in astratto, incorrere anche l'operante di P.G. durante la ricerca della prova digitale.

Nello specifico:

- **a)** L'art. 615-*bis* c.p., rubricato "Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico"
- **b)** L'art. 635-*bis* c.p., rubricato "Danneggiamento di informazioni, dati e programmi informatici"
- **c)** L'art. 635-*ter* c.p., rubricato "Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità"
- **d)** L'art. 635-*quater,* rubricato "Danneggiamento di sistemi informatici o telematici"
- **e)** L'art. 635-*quinquies,* rubricato "Danneggiamento di sistemi informatici o telematici di pubblica utilità"

È dunque compito dell'operante di P.G. **garantire la conservazione dei dati originali ed impedirne l'alterazione,** non solo al fine di evitare di incorrere nelle responsabilità penali suddette, ma anche al fine di rendere le prove digitali raccolte immuni da eventuali censure.

A tal proposito, per venire incontro alle esigenze di conservazione e di genuinità della prova digitale, sempre per il tramite della novella del 2008, il Legislatore ha inserito nel Codice di procedura penale un'apposita previsione, **l'art. 254-*bis*,** rubricato "Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni", con cui viene disciplinata l'ipotesi del **sequestro di dati informatici.**
Detta disposizione prevede la possibilità per l'Autorità giudiziaria di acquisire i dati mediante c.d. **copia forense**.

L'estrazione dei dati mediante copia è assoggettata ad una rigorosa procedura che ha come principale obiettivo quello di **garantire la conformità della copia con l'originale.**

A tal fine, per l'operatore è fondamentale, nell'atto di sequestro, sia nelle forme ordinarie, sia tramite copia, effettuare le operazioni in maniera corretta e trasparente, redigendo il **verbale di sequestro** in forma **completa** ed **esaustiva.**

Ad esempio, se oggetto del sequestro dovesse essere uno *smartphone*, sarà necessario:

1) Individuare il **numero di telefono**
2) Individuare e dare atto di **tutti** gli elementi del dispositivo, in particolar modo delle ***memory card*** esterne. Difatti, non è affatto raro che molti dati (foto, video, documenti) siano contenuti all'interno di questi supporti esterni, pertanto a fini processuali è necessario che ne venga data attestazione nel verbale, pena la loro inutilizzabilità
3) Richiedere la **chiave di accesso (*password*)** al soggetto raggiunto dal sequestro. Pur non essendo quest'ultimo tenuto a fornirla, ottenere la *password* per un agente di P.G. consente all'amministrazione giudiziaria di risparmiare risorse sia economiche che temporali, dal momento che la ricerca della chiave di accesso comporta il ricorso a specifiche società di consulenza informatica.

In ultima istanza, è bene richiamare l'attenzione su una questione che è stata plurime volte affrontata dalla Giurisprudenza, ovvero la **natura di accertamento ripetibile o meno** dell'estrazione di un *file* mediante copia forense.

La risoluzione della *vexata quaestio* comporta effetti pratici non irrilevanti. Qualora si ritenesse infatti, che la complessità dell'accertamento della prova digitale e della conservazione dei dati raccolti, possa essere considerata sufficiente per l'applicazione del disposto di cui all'art. 360 c.p.p. (accertamenti

tecnici non ripetibili), il verbale di sequestro non formerebbe solo atto di indagine, bensì andrebbe ad integrare il fascicolo per il dibattimento (art. 431 c.p.p.), fungendo a tutti gli effetti da prova utilizzabile ai fini della decisione finale.
Seppur in contrasto con la dottrina, gli insegnamenti provenienti dalla giurisprudenza attestano che l'estrazione di un *file* **non** costituisce un atto irripetibile, dal momento che non comporta alcuna attività di carattere valutativo su base tecnico-scientifica, né determina alcuna alterazione dello stato delle cose, tale da recare un pregiudizio alla genuinità del contributo conoscitivo in ottica dibattimentale. Di conseguenza, sarebbe assicurata, in ogni caso, la riconducibilità di informazioni identiche a quelle contenute nell'originale (cfr. Cass. Pen., Sez. III, n. 15133/2018 e Cass. Pen., Sez. V, n. 11905/2016).

In conclusione, la prova digitale è una prova che viene definita "fragile" e che richiede sforzi e attenzioni maggiori rispetto alle altre prove, essendo necessario, prima di tutto, **garantirne l'autenticità** e, in ragione di ciò, gli atti posti essere dall'Operatore di P.G. nella fase della sua acquisizione sono sicuramente determinanti.
Tanto dovevo.

Massimo Biffa

Ottobre 2021