Tra gli anni ***2019*** *e* ***2022*** si è assistito ad un significativo aumento delle *Segnalazioni di operazioni sospette* relative ai *Virtual asset*, passando da **732** a **5mila** *Segnalazioni*, indicando, così, una anomalia sulla circolarità e l'origine delle *cripto valute*, associate sempre più a frodi a danno di Aziende, tramite *ransomware*, **tipo di malware che limita l'accesso al dispositivo che infetta, richiedendo un riscatto da pagare per rimuovere la limitazione**.

L'**Unità di informazione finanziaria** da tempo tiene sotto osservazione il fenomeno, evidenziando nell'ultimo *Rapporto* una *crescente diffusione del fenomeno a danno di Agenzie governative e di Imprese private, con un frequente ricorso a valute virtuali nel pagamento del riscatto, motivato dalle caratteristiche di tali strumenti che ne rendono più difficoltosa la tracciabilità rispetto ai mezzi di pagamento tradizionali*.

Il **Gafi** (*Gruppo di azione finanziaria, fondato nel 1989 a Parigi*) ha programmato tutta una serie di azioni, da far adottare ai *Paesi aderenti*, per contrastare il **riciclaggio associato ai ransomware**.

Tali azioni prevedono *lo sviluppo delle cooperazioni internazionali già presenti, vista la natura transnazionale degli attacchi cyber e delle relative operazioni di riciclaggio.*

Il problema, purtroppo, è la differenza delle *Normative* tra i singoli *Paesi*, che consente agli *Hacker* la possibilità di riscuotere i riscatti in *cripto valute* e di trasferirli in *Vasp* (**Virtual asset service provider**) esteri, posizionati in *Paesi* privi di **Unità antiriciclaggio**.

Ricordiamo che le cripto valute spesso finiscono in un vortice di conversioni in altre monete virtuali, passando da Vasp in Vasp e monetizzate all'estero.