

# La Cassazione aggrava le conseguenze penali della clonazione di bancomat

*Accesso abusivo aggravato per "violenza sulle cose" a chi truffa il POS.*



**C**on la sentenza n. 43755/12 depositata il 12 novembre 2012 la Corte di cassazione ha stabilito un importante principio di diritto secondo il quale clonare carte di pagamento tramite "manipolazione dello sportello bancomat" configura il reato di accesso abusivo a sistema informatico aggravato dalla violenza sulle cose.

Il processo che ha originato la sentenza ha riguardato il solito metodo di attacco di uno sportello ATM: manomissione del lettore di carte di credito (nel caso specifico, di un distributore di carburante) e riutilizzo dei codici identificativi delle carte per crearne di clonate. La difesa degli imputati ha sostenuto che, nel caso di clonazione di carte di pagamento, non c'è alcun accesso a un sistema informatico in senso tecnico, precisando, si legge nella sentenza che «le informazioni utilizzate per clonare le carte non erano state estrapolate da un sistema informatico ma da un semplice supporto fisico, quali devono intendersi le carte magnetiche» e non da un sistema informatico che sarebbe configurabile «solo se i supporti utilizzati consentono un interscambio di informazioni tra una pluralità di apparecchi ovvero se esiste una interazione «tra componenti delle apparecchiature ed elementi del programma che consente di fruire di informazioni riservate». In breve: la carta di credito non è un computer, quindi copiare i dati che contiene non può essere un accesso abusivo analogo a quello di chi buca un server. In secondo luogo, si legge sempre nella sentenza, «non è stato in alcun modo provato che i codici captati con l'inserimento del dispositivo che intercettava e memorizzava i dati dei clienti del distributore, siano proprio quelli ricollegati alle carte magnetiche predisposte dal colpevole (nome omissso, n.d.r.) e dai suoi complici e dagli stessi utilizzati per i prelievi di denaro».

Infine, si sono difesi gli imputati, anche se fossimo di fronte a un accesso abusivo mancherebbe l'aggravante di avere aggredito un sistema di interesse pubblico ed esercitato violenza sulle cose perché dopo la manomissione del POS questo ha continuato a funzionare senza problemi.

La prima linea di difesa cade, scrive la Cassazione, perché sulla base della Convenzione di Budapest sul crimine informatico, recepita in Italia con la Legge 48/2008, «le carte di debito o di credito, identificate da una banda magnetica ovvero da un chip, elementi entrambi idonei a memorizzare e trasmettere dati informatici, costituiscono un vero e proprio sistema informatico, capace di elaborare dati, rendendoli operativi, nel momento in cui si connettono all'apparecchiatura POS, consentendo l'accesso autorizzato al sistema informatico finanziario delle Banche». Dunque, ritiene la Cassazione, l'accesso abusivo non è solo quello al chip contenuto nella carta di credito, ma quello al sistema informatico bancario che autentica l'utente proprio grazie ai dati memorizzati sulla carta stessa.

**La seconda linea è stata superata** da elementi di fatto già emersi nei due gradi di giudizio precedenti: confessione del reo e prelievi eseguiti dalla sua città natale, nei Balcani, dove risiedeva sino all'arresto. Ancora una volta, quindi, non ha funzionato la difesa basata sul sostenere l'assenza di prova fra l'identità elettronica e quella fisica. Specie nei primi processi che coinvolgevano reti e computer, infatti, era frequente ascoltare difese basate su argomenti come "l'account è mio, ma non lo ho utilizzato io per commettere il reato", oppure "l'account è mio ma non c'è prova che fossi io a usarlo". Fino a quando le indagini erano fatte quasi

esclusivamente concentrandosi sulla prova informatica questi ragionamenti hanno avuto qualche successo. Ma da quando – finalmente – le forze di polizia hanno capito che alle indagini informatiche vanno affiancate sempre quelle tradizionali le cose sono cambiate. E infatti la Cassazione ha rigettato l'argomento difensivo evidenziando che, al di là degli aspetti elettronici, c'erano altri elementi che dimostravano la responsabilità del colpevole.

Anche la terza linea non ha retto all'analisi dei giudici. Per poter ottenere una pena più bassa i colpevoli hanno cercato di sostenere che il sistema finanziario non è di interesse pubblico e che, quindi, la pena sarebbe dovuta essere più mite. Ma i giudici non hanno accolto la tesi e hanno specificato che «il reato di indebita utilizzazione o falsificazione di carte di credito o pagamento ha come scopo primario la tutela dell'interesse pubblico, sia come fine di evitare che il sistema finanziario venga utilizzato a scopo di riciclaggio sia di salvaguardare, nel contempo, la fede pubblica e che solo in via mediata esso tutela il patrimonio del privato... Come logica conseguenza se ne deve arguire la natura di pubblico interesse del sistema finanziario».

Quanto alla mancanza di violenza sulle cose (altro elemento che i colpevoli invocavano per ottenere uno sconto di pena), scrivono i giudici, è vero che dopo l'installazione del chip che copiava i dati della carta il POS ha continuato a funzionare, ma la manomissione ha provocato un funzionamento anomalo e non voluto dall'utente legittimo, il che integra il requisito di «violenza sulle cose» in relazione a un sistema informatico.

Benché in molti casi la Cassazione abbia dimostrato una non perfetta conoscenza degli aspetti tecnologici dei processi che coinvolgono i computer (specie quando si parla di reti) in questo caso il ragionamento della sentenza è tecnicamente ben fondato anche, forse, visto l'elevato numero di casi del genere che ha provocato una maggior diffusione fra chi deve decidere, del funzionamento dei sistemi di pagamento. •