L'INCHIESTA

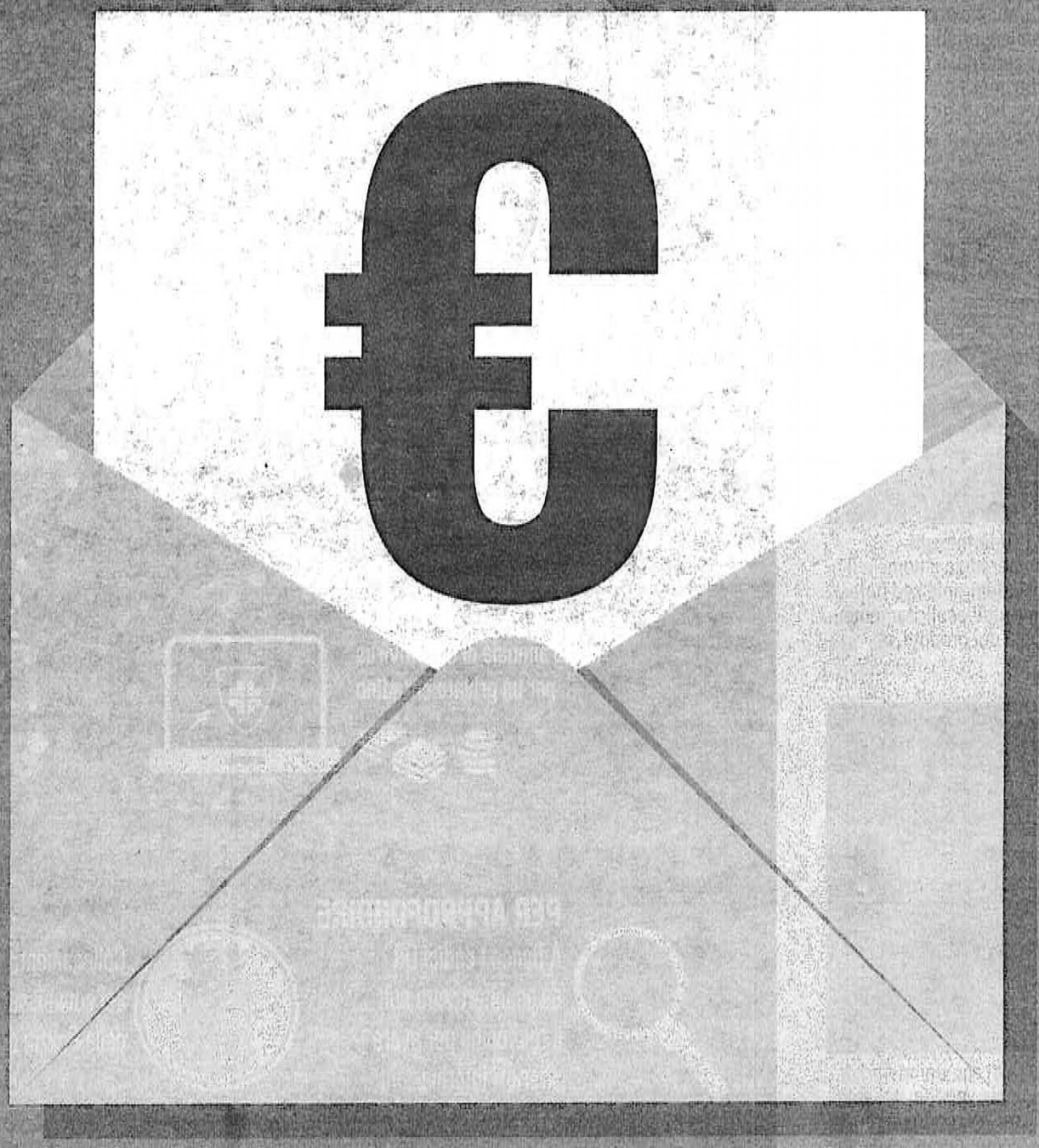
AL MERCATO DELLE MAIL

Un indirizzo di posta elettronica vale (come minimo) 5 centesimi e viene venduto in pacchetti da mille euro. Chi li compra? Le aziende che vogliono ficcare il naso nelle nostre abitudini

di **Michelangelo Bonessa**

La posta non è mai stata così preziosa da quando è diventata digitale. Se nell'era della carta era importantissima, tanto che gli Stati l'hanno sempre controllata tanto in pace quanto in guerra, oggi la casella email è diventata una finestra su un nuovo mondo in cui i dati personali hanno assunto tutto un altro valore. Il web ha assegnato un prezzo a ogni pezzo della nostra vita. A partire proprio dalla fatidica chiocciolina. Milioni e milioni di indirizzi di posta elettronica vengono venduti in continuazione in tutto il mondo (...)

segue a pagina **20** e **21**



segue da pagina 19

A CACCIA DEI CONSUMATORI

Tessere fedeltà e posta Così le aziende ci spiano

(...) per gli scopi più diversi. Per capire quanto sia rilevante a livello globale questo traffico basti pensare che ogni minuto si scambiano 200 milioni di messaggi di posta elettronica per un totale giornaliero di 290 miliardi. Un flusso immenso da cui tanti cercano di trarre profitto: solo l'e-mail marketing, cioè il business delle pubblicità via mail, secondo alcune stime, ha un giro d'affari di 20 miliardi di dollari.

Ma il valore della singola e-mail varia molto. Si trovano pacchetti a 5 centesimi ciascuna ma gli elenchi in vendita contengono migliaia di contatti e si vendono a pacchi da mille o duemila euro.

Le cifre variano molto a seconda della profondità delle informazioni: se a una casella di posta sono associate informazioni come l'età dell'utente, la zona di residenza, la professione svolta o qualunque altro dettaglio, il valore dell'informazione finisce per moltiplicarsi.

Se infatti un'azienda è in grado di stabilire con più precisione chi siano le persone a cui vendere i propri prodotti, può incrementare molto i propri guadagni. Ad esempio: se so che mille persone di un certo quartiere di Milano prediligono i mocassini blu e li comprano ogni sei mesi, non avrò bisogno di distribuirli in cento negozi a caso, ma lo farò solo in quelli del quartiere dove vivono le persone interessate inviandogli magari una e-mail con le nuove offerte.

È in sostanza buona parte del business di Facebook e dei siti simili che per accedere ai servizi richiedono una e-mail. Di solito offrono servizi gratuiti perché ricavano soldi dalla vendita di dati personali degli utenti. Non serve per forza che siano il nome e il cognome, alle aziende bastano anche informazioni più generiche per organizzare i propri affari. Spesso interessano i cosiddetti « *inferred data*», cioè i dati con le informazioni generate da un sistema e non ceduti esplicitamente da un utente.

Per capirsi: quando ci spostiamo in metropolitana ci sono sistemi automatici che contano quante persone hanno timbrato il biglietto, a che ora, da dove partono e dove scendono.

Possono essere dati preziosissimi, come sanno bene i supermercati che studiano i propri clienti con uno strumento a prima vista inoffensivo come le tessere-fedeltà, che segnalano abitudini di acquisto (dai prodotti agli orari). Sono conoscenze che valgono patrimoni e per avere un'idea di quante aziende stiano lavorando su di noi esistono diversi siti internet, uno abbastanza completo è *youronlinechoices.eu*. Anche se ora, a mettere dei paletti a questo genere di commercio ci ha pensato la normativa europea sulla privacy ache va sotto il nome di General Protection Data Regulation.

L'ALTRO LATO DELLA MEDAGLIA

Ma qui finisce la parte legale dell'uso delle e-mail. Perché ci sono aziende che acquistano le email per tempestarci di pubblicità, ma anche organizzazioni criminali che le comprano per acquisire informazioni come i codici di accesso ai conti bancari o alle carte di credito. O per far firmare contratti per servizi aggiunti-

Al momento della registrazione i siti chiedono una mail: merce preziosa che viene venduta alle aziende e serve a «mirare» i messaggi pubblicitari

Ma i pacchetti di indirizzi fanno gola anche alle organizzazioni criminali che tentano di intercettare i codici delle carte di credito o tendono trappole spilla-soldi

vi a pagamento. Sul *dark web*, cioè quella parte di Internet fuori dai comuni motori di ricerca, si trovano milioni di carte di credito in vendita, nel solo 2019 erano 99 milioni (per il 65% americane) secondo un report della società di cyber sicurezza *Sixgill*. Anche in questo caso si parte da poche decine di euro per arrivare a cifre molto più alte a seconda dei proprietari, della consistenza del conto e di mille altri parametri.

Come si ottengono password e codici di accesso? Dalla posta elettronica delle persone grazie a tecniche che vanno sotto il nome di *phishing* e *social engeneering*. La prima consiste nel «pescare» contatti con massicci invii di messaggi fraudolenti. Alcuni esempi sono quelli bancari, come una (falsa) e-mail che avverte l'utente della necessità di cambiare le credenziali di accesso al conto online. Magari spedita in un orario in cui la persona media è stanca o disattenta. L'utente vede, si agita e inserisce le credenziali. In breve gli arriva un messaggio rassicurante e non ci pensa più fino a quando qualcuno non gli si svuota il conto corrente. Oppure un altro esempio è la firma di contratti per servizi aggiuntivi a pagamento, di recente in una truffa simile è finito anche il Procuratore di Milano Francesco Greco: 20 euro al mese addebitati senza richiesta.

IL VOLTO DELLA TRUFFA

Ma quali sono i limiti del lecito? A spiegarlo è Daniele Loglio, avvocato esperto di cyber dello studio Pulitanò Zanchetti: «Perché sia configurabile un determinato reato, il nostro ordinamento richiede che sussistano tutti gli elementi costitutivi. Il delitto di truffa richiede che l'autore del reato abbia indotto in errore un soggetto (ad esempio l'utente della rete internet) con artifici o raggiri, portandolo a compiere un atto (l'abbonamento ad un servizio) che cagioni un danno ingiusto al truffato e da cui derivi un vantaggio per altro soggetto – spiega il legale - Ma se ad essere ingannato è un sistema informatico, allora il reato configurabile potrà essere la frode informatica ex art. 640. Si tratta di una fattispecie introdotta nel nostro ordinamento nel 1993 per punire condotte che, prima di quel momento, non erano perseguibili poiché non ricadevano nella classica truffa. Sotto un profilo civilistico, un contratto frutto di una frode è nullo».

Per dare un'idea del fenomeno del *phishing*, si stima che sia pari al 52% delle email mondiali. Un dato in realtà in calo, perché vent'anni fa la percentuale era molto più alta. Ma gli attacchi alle e-mail sono i più vari e in continua evoluzione. Secondo la Polizia Postale i pericoli hanno nomi esotici: al momento «i più frequenti si chiamano mail *bombing, botnet, phishing, spyware, Ransoware, Adware, cookie, DDoS, Men in the middle* - spiegano i cyber poliziotti - di solito sono associazioni dell'est Europa la maggior parte degli attacchi hanno l'obiettivo di estorsione, altre semplicemente per bloccare l'accesso alla rete per altri scopi». Nella gran parte dei casi questi attacchi hanno scopi estorsivi, come sottolinea la Postale. Creano cioè dei problemi al computer grazie a una e-mail e per risolverli chiedono un riscatto.

Michelangelo Bonessa