**UNIVERSITA' DEGLI STUDI DI ROMA TOR VERGATA**

***European Digital Law of the Person, of the Contract and of the Technological Marketplace* - EUDILA**
**Cattedra Jean Monnet del Progetto ERASMUS +**

# *Il telemarketing aggressivo e il fenomeno dello spoofing*

***Giuseppe Kevin Chieppa***

***0354560***

**Anno accademico 2023/2024**

# INDICE

**ABSTRACT**

Questa tesina analizza il fenomeno del telemarketing aggressivo e della pratica dello spoofing. Nel primo capitolo del lavoro verrà fatta un' introduzione generale alle pratiche commerciali scorrette, elencando brevemente le possibili categorie. Verranno introdotti i concetti fondamentali di dati personali, la loro definizione e l'importanza che ricoprono nell'economia moderna. Parleremo del GDPR (general data protection regulation), regolamento dell'Unione Europea che disciplina il modo in cui le aziende e altre organizzazioni trattano i dati personali, e dell'AGCM (autorità garante della concorrenza e del mercato) che viglia sul rispetto della normativa antitrust e sulla pubblicità ingannevole.

Nel secondo capitolo introdurremo il telemarketing, ossia tutte quelle attività promozionali o di vendita che implicano il contatto telefonico. Il telemarketing si divide in attivo (telefonare direttamente il possibile cliente) e passivo (rendere pubblico un numero telefonico alla quale ci si può rivolgere per informazioni sull'acquisto), ci concentreremo sul primo tipo, quello cioè più soggetto a possibili attività fraudolente. Parleremo del Registro delle Opposizioni, possibile soluzione al telemarketing aggressivo, e vedremo come le società di call center aggirano questo problema. Dopo aver esposto un esempio di telemarketing illegale, sanzionato dal garante della privacy, ci concentreremo sul capire come i call center acquisiscono i numeri di telefono e le possibili truffe messe in atto dagli stessi. Parleremo del nuovo Codice delle Comunicazioni introdotto dal Consiglio dei Ministri nel 2024 e del nuovo codice di condotta.

Infine, nel terzo capitolo illustreremo il fenomeno dello spoofing, cioè attacchi informatici e non, in cui un malintenzionato nasconde la propria identità fingendo di essere una fonte affidabile per ottenere accesso a informazioni riservate e dati sensibili. Analizzeremo le diverse tipologie spesso utilizzate dai truffatori, e le possibili precauzioni da adottare per non essere truffati. Faremo anche un piccolo confronto tra spoofing, phishing e vishing.

# 1. INTRODUZIONE

Nell'economia globale odierna, le pratiche commerciali scorrette rappresentano una delle problematiche più insidiose e pericolose. Oltre al danno diretto ai consumatori, esse sono in grado di compromettere gravemente la fiducia dei consumatori, distorcere la concorrenza e danneggiare l'integrità del mercato. Le pratiche commerciali scorrette sono azioni e strategie commerciali condotte da società o operatori economici che sono contrarie ai principi di equità, chiarezza e lealtà verso i consumatori e i propri concorrenti.

Queste pratiche possono manifestarsi in diverse forme, tra cui:

1. **Pubblicità Ingannevole**: Informazioni false o fuorvianti riguardo i prodotti o servizi offerti, che inducono i consumatori a prendere decisioni d'acquisto basate su informazioni false;
2. **Vendita Fraudolenta**: Vendita di prodotti non conformi alle pubblicità;
3. **Abuso di Posizione Dominante**: Imprese con una posizione di mercato dominante ostacolano la concorrenza, ad esempio attraverso prezzi predatori o pratiche esclusive;
4. **Dumping**: La vendita di prodotti a prezzi inferiori al costo di produzione nel mercato estero per eliminare la concorrenza locale;

5. **Violazione delle Norme di Sicurezza**: Commercializzare prodotti non conformi agli standard di sicurezza, mettendo a rischio la salute e la sicurezza dei consumatori.

Il codice del consumo distingue le pratiche commerciali ingannevoli da quelle aggressive:

le prime (articolo 21-23 del codice del consumo) inducono il consumatore medio in errore, falsandone il processo decisionale. Possono riguardare il prezzo, la disponibilità del prodotto, le caratteristiche del prodotto e anche pratiche che possono minacciare la sicurezza e la salute.
Le seconde (articolo 24-26 del codice del consumo) sono quelle pratiche in cui l'impresa agisce con molestie, coercizione o altre forme di indebito condizionamento.

Il codice del consumo raccoglie le principali disposizioni vigenti in materia di tutela dei consumatori, adottate anche in attuazione della normativa europea, e regola i rapporti tra gli stessi consumatori e i professionisti dettando i reciproci diritti e obblighi.

Alla luce di queste problematiche e di numerosi scandali avvenuti a livello internazionale, è evidente che una regolamentazione di queste pratiche è fondamentale per salvaguardare, in primis, i consumatori più deboli.

**AGCM**

La pratica di sorveglianza è svolta dall'AGCM, Autorità Garante della Concorrenza e del Mercato. E' un'autorità amministrativa indipendente e che prende decisioni in piena autonomia rispetto il potere esecutivo. Istituito nel 10 Ottobre 1990, è un organo collegiale e le sue decisioni vengono prese a maggioranza. Il Presidente e i componenti dell'Autorità vengono nominati dai Presidenti di Camera e Senato per una carica di 7 anni non rinnovabile.

Per contenere la spesa complessiva delle Autorità amministrative indipendenti, il legislatore ha ridotto il numero dei componenti dell'Antitrust da cinque a tre [Art. 23, comma 1, lettera d, del decreto-legge 6 dicembre 2011, convertito con modificazioni dalla legge 22 dicembre 2011, n. 214.], compreso il Presidente.

L'AGCM è un'autorità amministrativa indipendente che vigila sul rispetto della normativa antitrust e sulla pubblicità ingannevole e comparativa. Svolge attività di protezione per promuovere la concorrenza e rimuovere i vincoli alla libertà di iniziativa economica.

AGCM, inoltre, può avviare istruttorie, effettuare ispezioni e irrogazioni di sanzioni pecuniarie fino al 10% del fatturato alle imprese che violano le norme sulla concorrenza.

Coopera con le autorità garanti di altri paesi e con la Commissione Europea nell'applicazione delle regole antitrust.

## L' IMPORTANZA DEI DATI

Ad oggi la tutela del consumatore diventa ancora più complicata, grazie alla crescente globalizzazione e digitalizzazione del mondo intorno a noi. Il 65% della popolazione globale è connessa a internet, e 50 miliardi di oggetti sono su internet.

E' stato introdotto un nuovo termine alla fine degli anni 90, la new economy ( o anche net economy, dall'accorciamento di network economy) basato sull'esponenziale sviluppo delle tecnologie informatiche e digitali. Il termine si è poi evoluto con l'avvento del web 2.0, negli anni 2006-2007, andando a indicare tutta l' economia digitale, ovvero quel settore economico sviluppato grazie alla rivoluzione digitale.

Questo enorme mercato e questa enorme quantità di oggetti presenti sul web crea una mole di dati immensa, i cosiddetti BIG DATA. Le digital company sfruttano questi dati, ad oggi anche grazie all'intelligenza artificiale, per comprendere le esigenze e i desideri dei clienti., questa viene chiamata PROFILAZIONE. Questa profilazione dei clienti ha lo scopo di suddividerli in gruppi omogenei in base a gusti, interessi e comportamenti, al fine di proporre oggetti sempre più consoni con i gusti del cliente.

Si comprende, quindi, che questa profilazione dei clienti permette alle imprese di poter efficientare le strategie di marketing e poter vendere di più spendendo meno. Così i dati sono diventati il nuovo petrolio, un bene inestimabile per le aziende, ma a differenza del petrolio, i dati possono essere usati più volte e scambiati. Si stima che ogni giorno vengano rilasciati da ogni utente circa 200 megabyte di dati.

Questo scambio di dati personali che delineano il profilo della persona entra in contrasto con il diritto alla privacy, diritto fondamentale del singolo descritto dall'articolo 2 della costituzione italiana.

(ART.2: La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale.)

**DEFINIZIONE DI DATI**

È importante definire cosa si intende per dati, per dati personali si intendono le informazioni che identificano o rendono identificabile una

persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc..
Si dividono in:

1. dati che permettono identificazione diretta: dati anagrafici, immagini, ecc.

2. dati che permettono identificazione indiretta: codice fiscale, indirizzo IP, numero di targa ecc.

3. dati sensibili: quelli che rivelano le origini razziale o etnica, le convinzioni religiose, le opinioni politiche, l'appartenenza sindacale, dati genetici, dati biometrici e dati relativi all'orientamento sessuale

4. dati relativi a condanne penali e reati (giudiziari):cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato.

Con l'evoluzione delle nuove tecnologie, altri dati personali hanno assunto un ruolo significativo, come quelli relativi alle comunicazioni elettroniche (via Internet o telefono) e quelli che consentono la geolocalizzazione, fornendo informazioni sui luoghi frequentati e sugli spostamenti.

**GDPR**

Da qui nasce l' esigenza di un regolamento che protegga i dati personali di ogni individuo, il GDPR.

Il Regolamento generale sulla protezione dei dati (GDPR, dall'inglese General Data Protection Regulation) è un regolamento dell'Unione Europea che disciplina il modo in cui le aziende e le altre organizzazioni trattano i dati personali.

Entrato in vigore il 25 maggio 2018 punta a dare a ogni individuo il controllo sull'utilizzo dei propri dati, tutelando i "diritti e le libertà fondamentali delle persone fisiche". Con questa finalità, il regolamento stabilisce requisiti precisi e rigorosi per il trattamento dei dati, la trasparenza, la documentazione e il consenso degli utenti per le organizzazioni che elaborano dati personali nell'Unione Europea.

Il 4 maggio 2020 il comitato europeo per la protezione dei dati (EDPB) ha adottato delle linee guida sul consenso valido ai sensi del GDPR.

Il consenso valido di un individuo deve essere un'indicazione libera, specifica, informata e inequivocabile delle intenzioni dell'utente, vale a dire un'azione chiara e affermativa da parte di quest'ultimo. Le linee guida dell'EDPB chiariscono che lo scorrimento o la continuazione della navigazione su un sito web non costituiscono un consenso valido e che i cookie banner non possono avere caselle preselezionate. Anche i cookie wall sono stati giudicati non conformi.

L'EDPB è la massima autorità di controllo per l'applicazione del GDPR in tutta l'UE. E' composto da rappresentanti delle autorità di protezione dei dati di ogni paese membro dell'UE. Le sue linee guida e le sue decisioni sono alla base dell'attuazione del GDPR a livello nazionale.

## 2. TELEMARKETING

In questa tesina andremo a snocciolare un problema ad oggi molto diffuso in Italia, il telemarketing selvaggio. Il telemarketing selvaggio rappresenta un grave problema per la tutela dei dati personali, della privacy dei cittadini e del rischio di incorrere in qualche truffa. I call center acquisiscono illegalmente le banche dati di potenziali clienti senza il loro consenso, per poi contattarli con offerte commerciali. Questa valanga di telefonate che è possibile ricevere ogni giorno è dovuta anche al passaggio di contratti tra le società, in sostanza quando un call center riesce a sottoscrivere un contratto lo possa alla società terza, incassando una commissione. In pratica le società di call center sono società il cui unico obiettivo diventa quello di sottoscrivere contratti per poter guadagnare. Ad oggi anche l'iscrizione al Registro delle Opposizioni da parte di alcuni cittadini non ha limitato il fenomeno, in quanto si è diffuso sempre più lo spoofing, ossia l' uso di numeri di telefoni fittizi da parte dei call center per aggirare le norme.

Prima di continuare, definiamo che cosa si intende per telemarketing. Il termine "Telemarketing" si riferisce a tutte quelle attività promozionali e di vendita che implicano il contatto telefonico, diretto o indiretto, tra l'azienda e i clienti o potenziali clienti, attraverso operatori interni o call center esterni. È una tecnica di vendita che utilizza la rete telefonica sia in modo attivo, cioè telefonando direttamente ai potenziali acquirenti, sia in modo passivo, cioè rendendo pubblico un numero cui ci si può rivolgere gratuitamente per informazioni sull'acquisto di un bene o di un servizio. Questa definizione evidenzia la distinzione consolidata tra telemarketing outbound (attivo) e telemarketing inbound (passivo), analogamente alla distinzione tra outbound marketing e inbound marketing (questa tesina si concentrerà sul primo tipo). Di solito, le aziende che investono nel

telemarketing prendono l'iniziativa contattando i consumatori tramite database interni o liste condivise, per presentare il brand, la sua proposta di valore, il catalogo di prodotti o servizi, offerte temporanee e promozioni riservate.

Spesso, l'obiettivo della chiamata commerciale è promozionale e si prevede che tra i risultati del telemarketing ci siano appuntamenti negli uffici e incontri con i responsabili vendite nel caso di telemarketing B2B, o visite in negozio da parte dei clienti privati contattati telefonicamente. Quando le chiamate dei teleoperatori e dei call center sono finalizzate direttamente alla vendita, alla chiusura di contratti e alla creazione di lead (potenziali clienti) concreti, si parla più propriamente di teleselling o vendite telefoniche.

Ogni operatore telefonico ha uno script. Lo script rappresenta il fondamento della telefonata, fornendo una guida all'operatore, che può essere personalizzata per ogni cliente. Tipicamente, include una breve presentazione dell'azienda o dell'iniziativa commerciale, una fase di domande mirate al cliente (intervista), e una fase motivazionale durante la quale l'operatore outbound cerca di suscitare l'interesse del cliente basandosi sull'intervista. La fase cruciale è la chiusura, durante la quale si ottiene il consenso esplicito del cliente per l'iniziativa commerciale proposta. Altri possibili esiti della chiamata possono essere: il consenso per un ulteriore contatto, l' acquisto, l'ordine o la sottoscrizione di servizi, nonché la trasmissione di dati e informazioni necessarie.

La normativa sulla privacy ha regolamentato in modo restrittivo l' utilizzo di elenchi di numeri telefonici da parte delle aziende di telemarketing. Secondo la normativa in vigore fino al 2008, le aziende possono contattare solo i soggetti che hanno fornito il loro esplicito consenso a ricevere chiamate commerciali.

L'articolo 130, commi 1 e 2, del Codice Privacy prevede l'obbligo del consenso per l'utilizzo dei dati di contatto dei "contraenti" e degli "utenti" ai fini dell'invio di comunicazioni di marketing diretto tramite strumenti automatizzati. La definizione di "contraente" (art. 121 del Codice Privacy) include non solo le persone fisiche, ma anche tutti gli altri soggetti di diritto diversi dalle persone fisiche, come le persone giuridiche. Pertanto, anche per le persone giuridiche occorre richiedere un apposito e preventivo consenso per l'utilizzo dei loro dati di contatto a fini di marketing diretto tramite strumenti automatizzati.

**Utilizzo di strumenti non automatizzati**

Qualora invece siano impiegati, per le medesime finalità di marketing diretto, strumenti non automatizzati - come il telefono con operatore e la posta cartacea - l'utilizzo dei dati di contatto è consentito ai sensi degli articoli 6 e 7 del GDPR, nonché ai sensi di quanto previsto dall'articolo 130, comma 3-bis, del Codice Privacy. Poiché il rinvio agli articoli 6 e 7 del GDPR trova applicazione esclusiva al trattamento dei dati riferibili alle persone fisiche, non è necessario richiedere preventivamente alcun consenso alle persone giuridiche ai fini dello svolgimento di campagne di marketing diretto tramite strumenti non automatizzati.

**Diritto di opposizione per le persone giuridiche**

Resta ferma l'applicabilità alle persone giuridiche dell'articolo 130, comma 3-bis, del Codice Privacy, il quale stabilisce che l'utilizzo degli strumenti non automatizzati per finalità di marketing diretto è consentito solo nei confronti di coloro i quali non abbiano esercitato il diritto di opposizione. Tale diritto può essere esercitato mediante iscrizione della numerazione della quale sono intestatari (allo stato attuale, soltanto fissa e non mobile) e degli altri dati di cui all'articolo 129, comma 1, del Codice Privacy nel registro pubblico delle opposizioni (RPO).

Tuttavia, questa normativa ha causato problemi nell'approvazione delle liste di contatti per le aziende, che hanno dovuto intraprendere specifiche campagne di marketing per raccogliere dati personali di potenziali clienti. In genere, i clienti da contattare vengono suddivisi per età, sesso e zona geografica, in modo da adattarli al target commerciale di ciascuna campagna.

Negli ultimi tempi, sono state introdotte diverse soluzioni per impedire agli utenti di ricevere chiamate "moleste" da parte dei call center. Innanzitutto, è possibile evitare i call center utilizzando alcune funzioni di sistema previste sugli smartphone o scaricando apposite applicazioni che bloccano le chiamate in entrata riconosciute come provenienti da operatori di telemarketing. Un altro modo, come detto prima, è il servizio offerto dal Registro delle Opposizioni, che consente di autoescludersi dalle liste utilizzate dagli operatori per le loro comunicazioni. Tuttavia, esistono alcune eccezioni che ne limitano l' efficacia rispetto ad altri sistemi.

Infatti, la maggior parte dei call center opera dall'estero, il che rende più semplice per loro reperire informazioni sugli utenti da contattare. Nel frattempo, la rete è diventata un vero e proprio mercato "nero" di dati, tanto che risulta pressoché impossibile risalire a coloro che forniscono le liste. Per questo motivo, aggirare il Registro Pubblico delle Opposizioni è un'operazione piuttosto semplice. Molti utenti hanno lamentato il fatto che, pur iscrivendosi gratuitamente al servizio, non hanno risolto il problema delle chiamate indesiderate. Inoltre, il registro non offre protezione nei casi in cui un utente abbia dato il proprio consenso a ricevere attività promozionali su determinati siti web.

Molte società di vendita sono state multate dal Garante della Privacy a causa di queste pratiche scorrette (circa 256 multe dall'attivazione del GDPR), tra cui anche il fornitore Enel Energia. Il garante della privacy ha sanzionato Enel per oltre 79 milioni di euro a causa della grave carenza di

sicurezza nei suoi sistemi operativi che gestivano i dati personali dei clienti, non riuscendo così a prevenire le attività di telemarketing aggressivo esterno.

**CASO DI TELEMARKETING ILLEGALE (19 GENNAIO 2024)**

Il Garante Privacy ha sanzionato un call center operante nel settore dei contratti di energia elettrica con una multa di 60mila euro per il trattamento illecito di dati personali. La società era già stata multata di 10mila euro per non aver risposto alle richieste dell'Autorità, che è stata attivata dopo la richiesta di un utente che si lamentava di aver ricevuto telefonate promozionali senza consenso. Dopo l'accertamento ispettivo, il Garante ha riscontrato numerose violazioni:

-Il call center aveva acquisito le anagrafiche del mittente da un provider di elenchi con sede in Moldavia, dal quale aveva acquistato 100mila contatti utilizzati per oltre 32.600 telefonate, portando alla sottoscrizione di circa 300 contratti;

-Non aveva verificato l'origine dei dati, se l'informativa agli utenti era stata resa e se i consensi erano stati acquisiti regolarmente;

-Nel corso delle telefonate non vengono fornite informazioni sulla propria identità, limitandosi a richiedere di essere ricontattati;

-Non aveva effettuato le dovute verifiche nel Registro Pubblico delle Opposizioni né misure adottate per consentire il riscontro alle istanze degli utenti.

Alla luce delle gravi violazioni riscontrate e del carattere colposo della condotta, il Garante ha inflitto la multa e ingiunto di cancellare i dati acquisiti illecitamente, attivando idonee misure per il trattamento dei dati nel rispetto della normativa privacy.

## MODALITÀ DI ACQUISIZIONE NUMERI DI TELEFONO

I call center ottengono i numeri di telefono dei potenziali clienti attraverso diverse modalità, in base alle loro esigenze e strategie di marketing:

-Acquisto di elenchi di contatti da aziende specializzate che raccolgono dati personali attraverso diverse fonti, come ad esempio iscrizioni online, abbonamenti a servizi o tramite accordi commerciali. Queste informazioni vengono poi vendute legalmente ai call center che le utilizzano per le loro campagne.

-Compilazione volontaria dei propri dati in formulari online, partecipazione a concorsi o sottoscrizione a newsletter. In questi casi, spesso nei termini e condizioni (che raramente vengono letti attentamente) si autorizza la condivisione dei propri dati con terze parti, tra cui appunto i call center.

-Dialing automatico che permette ai call center di generare automaticamente combinazioni numeriche casuali e chiamare numeri a caso fino a raggiungere potenziali clienti.

-Alcune aziende possono decidere di condividere o vendere i dati dei loro clienti come parte di una strategia commerciale. Pertanto, fornendo il numero di telefono a un'azienda per un acquisto o un servizio, è possibile essere contatti da altre società affiliate o partner commerciali.

## TIPICHE TRUFFE DEI CALL CENTER

Ciò che accomuna tutte le truffe dei call center è che l'operatore fa credere a chi ascolta di chiamare per conto di una grande azienda, sia essa una compagnia telefonica o un fornitore di energia (spoofing). Non appena l'utente risponde, inizia la vera e propria truffa. Essenzialmente, ci sono due scopi principali che spingono i malintenzionati a ordire queste

truffe telefoniche: ottenere i dati personali degli utente; iscrivere gli utenti a servizi a pagamento non richiesti e non voluti.

Per poter ottenere i dati personali di un utente il procedimento seguito dai call center è molto semplice, propongono una nuova offerta vantaggiosa ma per poterla attivare richiedono dei dati, e sfruttando l'ingenuità del malcapitato riescono a ottenere IBAN o il codice di migrazione (presente sulla bolletta necessario per il cambio operatore).

Altra tipologia di truffa dei call center è quella di porre domande che possano spingere l'interlocutore a dire di sì, a quel punto tramite software di montaggio audio, utilizzano quel sì per iscrivere l'utente a servizi non richiesti. Difendersi da questo tipologia di truffa risulta complicato al momento della telefonata, l' unica cosa da fare è aspettare comunicazioni del possibile nuovo fornitore e a quel punto inviare un reclamo e sporgere denuncia alle autorità competenti (AGCM).

Altra tuffa messa in atto dai call center è quella di fingersi operatori dell'Unione Nazionale Consumatori per convincere l'utente a cambiare gestore telefonico o energetico. La truffa si divide in due telefonate:

La prima telefonata ha lo scopo di adescare la potenziale vittima, per comprendere le possibilità concrete di portare a termine la truffa. L'operatore del call center finge di essere un rappresentante della compagnia telefonica o energetica della persona chiamata e gli evidenzia che la sua tariffa è in scadenza o che sta pagando un prezzo troppo alto rispetto ai consumi. Il call center fa credere all'utente che il suo piano tariffario sia eccessivo rispetto ai prezzi di mercato e che, cambiandolo, potrebbe avere un maggiore risparmio. L'utente potrebbe rimanere sorpreso da questa comunicazione e trovarsi nella condizione di voler modificare la propria offerta.

La seconda telefonata è quella che concretizza la truffa, ovvero quella nella quale l'utente precedentemente contattato e attirato dalla

possibilità di risparmiare sulle proprie spese, entra in contatto con un nuovo operatore che si finge un consulente dell'Unione Nazionale Consumatori. Sfruttando il nome dell'associazione a tutela dei diritti dei consumatori, l'operatore del call center illustra e spiega le tariffe più convenienti di altre compagnie e aiuta il malcapitato a disdire il precedente contratto cui è legato. In questo passaggio viene solitamente detto che, grazie alla consulenza dell'Unione Nazionale Consumatori, il cliente non dovrà pagare alcuna penale per la cessazione del suo precedente accordo e il passaggio a un altro operatore o compagnia. Accettando tale procedura, il cliente è stato truffato e potrebbe ritrovarsi ad avere sottoscritto un contratto che crede godere del benestare dell'associazione dei consumatori, ma così non è.

**CODICE DELLE COMUNICAZIONI ELETTRONICHE (MARZO 2024)**

Il 20 marzo 2024, il Consiglio dei Ministri ha approvato un decreto legislativo che modifica il Codice delle comunicazioni elettroniche. Questo provvedimento introduce importanti novità per combattere il fenomeno del telemarketing selvaggio. In particolare, il decreto correttivo:

-Definisce il concetto di "call center" come "servizio specificamente organizzato per la gestione dei contatti telefonici"

-Coinvolge sia l'Autorità per le Garanzie nelle Comunicazioni (**AGCOM**) che il Ministero delle Imprese e del Made in Italy (**MIMIT**), competenti in materia e che potranno sanzionare i call center che commettono "pratiche commerciali sleali, frodi o abusi o non ottemperano agli ordini e alle diffide" con multe che vanno da 50mila a un milione di euro

-Mira a semplificare le procedure autorizzative per accelerare lo sviluppo delle infrastrutture di telecomunicazione sul territorio nazionale

Inoltre, il Codice delle comunicazioni elettroniche rappresenta il quadro normativo di riferimento per l'intero settore delle telecomunicazioni e di internet in Italia.

## NUOVO CODICE DI CONDOTTA

La percezione negativa delle incessanti chiamate indesiderate ha attirato l'attenzione delle autorità regolatorie, culminando nell'istituzione del nuovo Codice di condotta. Questo provvedimento segna una pietra miliare nella regolamentazione delle attività di teleselling e telemarketing, con l'obiettivo primario di tutelare l'utente finale dalle molestie telefoniche.

L'Organismo di monitoraggio (OdM) che rappresenta l'ultimo passaggio verso la piena applicazione di questa normativa, entrato in vigore da marzo 2024, verificherà il rispetto del codice di condotta. L'Autorità competente ha riconosciuto nell'OdM i requisiti essenziali di competenza, indipendenza e imparzialità previsti dal GDPR.

Questo accreditamento legittima l'OdM come ente di controllo sull'adesione e l'applicazione del Codice da parte delle aziende coinvolte. Le associazioni di committenti, call center, teleseller, list provider e consumatori hanno collaborato alla proposta di questo organismo, evidenziando un impegno condiviso verso un cambiamento positivo.

### Misure per assicurare la correttezza del trattamento dei dati

Gli aderenti al Codice di condotta si impegnano ad intraprendere specifiche misure per garantire la liceità del trattamento dei dati personali nell'intera filiera del telemarketing:

-Ottenere consensi espliciti per le diverse finalità del trattamento, come marketing e profilazione;

-Fornire agli utenti informazioni chiare e precise sull'utilizzo dei loro dati;

-Garantire il pieno esercizio dei diritti previsti dalla normativa sulla privacy, in particolare il diritto di opposizione al trattamento.

**Sanzioni contro i call center abusivi**

Un punto di forza del Codice è l'introduzione di sanzioni specifiche per contrastare il fenomeno dei call center abusivi. La previsione di penali o la mancata corrispondenza delle provvigioni per i contratti stipulati senza consenso valido rappresenta un deterrente significativo per sradicare le pratiche scorrette.

**Nuovo approccio al telemarketing**

Questo nuovo approccio mira a ridefinire il rapporto tra aziende e consumatori, orientandosi verso una maggiore trasparenza e rispetto della sfera personale.

La valutazione d'impatto (DPIA) richiesta per i trattamenti automatizzati, inclusa la profilazione, introduce un livello di scrupolosità che va oltre gli standard precedenti. Queste misure aspirano a ristabilire la fiducia nel telemarketing, trasformandolo da fastidio a opportunità di comunicazione diretta e personalizzata, nel pieno rispetto della privacy individuale.

## 3. SPOOFING

Concentriamoci ora sul fenomeno dello spoofing, spesso utilizzato dai call center per aggirare le norme. Parliamo prima del fenomeno in generale.

Lo spoofing è un termine che indica una vasta gamma di attacchi informatici in cui un malintenzionato nasconde la propria identità, fingendo di essere una fonte affidabile per ottenere accesso a informazioni riservate e dati sensibili. Ciò avviene aggirando i meccanismi

di autenticazione basati su indirizzi IP e nomi host, attraverso l'impersonificazione di tali elementi.

Indipendentemente dalla strategia specifica adottata, tutte le forme di spoofing hanno un elemento comune: sfruttare la fiducia delle vittime per carpire o manipolare dati, rubare denaro, eludere i controlli di accesso alle reti e diffondere malware tramite link e allegati malevoli.

Diverse sono le strategie e le tecniche che possono essere impiegate per un attacco di spoofing. Tra i più noti e utilizzati troviamo:

**-Spoofing del sito web**

In questo tipo di attacco, il criminale crea un sito web ingannevole, ma dall'aspetto credibile, replicando fedelmente layout, font, colori e loghi di un sito web reale. L'obiettivo è convincere gli utenti a inserire credenziali, dati di carta di credito e informazioni di accesso. Per rendere più efficace l'impersonificazione, gli attaccanti possono camuffare gli URL, ad esempio registrando nomi di dominio simili a quelli legittimi.

**-Spoofing della posta elettronica**

In questo caso, l'attaccante impersona indirizzi email, inviando messaggi, con lo scopo di distribuire malware o rubare dati tramite phishing.

**-Spoofing dell'ID chiamante**

Gli attaccanti sfruttano la tecnologia VoIP per personalizzare il numero di telefono e creare un ID chiamante ad hoc, al fine di ingannare la fiducia di chi risponde e avviare una truffa telefonica (vishing).

**-Spoofing degli SMS**

L'attaccante impersona l'ID chiamante alfanumerico di un contatto o di un ente per inviare SMS contenenti link di phishing o malware.

**-Spoofing IP**

L'attaccante cerca di nascondere l'identità di un server, facendo credere che le informazioni provengano da una fonte affidabile (impersonando l'indirizzo IP di un host).

**-Spoofing del server DNS**

L'attaccante compromette un server DNS, alterando la tabella degli indirizzi dei nomi, in modo da reindirizzare il traffico verso siti fraudolenti.

**-Spoofing ARP**

L'attaccante, avendo accesso diretto alla rete locale, invia messaggi ARP contraffatti per associare il proprio indirizzo hardware all'indirizzo IP di un altro host (ad esempio, il gateway), dirottando il traffico.

Gli attacchi di spoofing possono essere molto subdoli, richiedendo quindi una maggiore attenzione per difendersi efficacemente. Questa tecnica risulta particolarmente efficace quando combinata con il social engineering (cioè utilizzare metodi che hanno come scopo quello di ottenere informazioni personali tramite l'inganno) e lo sfruttamento della scarsa attenzione di molti utenti. Per questo motivo, oltre a evitare configurazioni di rete errate, è importante seguire le precauzionali consigliate, come:

-Attivare il filtro antispam

-Verificare la veridicità delle informazioni nei messaggi, contattando il presunto mittente tramite un canale fidato

-Non rispondere a email o chiamate da mittenti sconosciuti

-Impostare l'autenticazione su due fattori quando possibile

-Installare e mantenere aggiornato un programma di sicurezza completo

-Non aprire il link o allegati sospetti

-Evitare di condividere informazioni personali e riservate

-Utilizzare password diverse per ogni servizio, avvalendosi di un password manager

**SPOOFING VS PHISHING**

Vediamo ora la differenza che intercorre tra spoofing e phishing. Lo spoofing, come abbiamo già detto, consiste nell'impersonare una persona, un'organizzazione o un dispositivo legittimo al fine di ottenere accesso o informazioni non autorizzati. Questo può includere lo spoofing di email, IP spoofing, ID spoofing, ecc.

Il phishing, d'altra parte, è un attacco di social engineering che inganna le vittime per rivelare informazioni sensibili o compiere un'azione che beneficia l'attaccante, spesso impersonando un'entità di fiducia. Il phishing tipicamente utilizza tecniche di spoofing per rendere l'attacco più convincente. Le principali differenze sono:

-Lo spoofing mira a bypassare i meccanismi di sicurezza, mentre il phishing mira a rubare informazioni o accessi

-Lo spoofing non necessariamente implica frode, ma il phishing sì

-Lo spoofing può essere un componente degli attacchi phishing, ma il phishing non può essere un sottoinsieme dello spoofing

-Lo spoofing può richiedere l'installazione di malware, mentre il phishing si basa sull'ingegneria sociale

**SPOOFING VS VISHING**

Mostriamo la differenza tra spoofing e vishing. Il vishing (voice phishing) è un tipo di attacco di phishing che utilizza l'ingegneria sociale via telefono per indurre le vittime a rivelare informazioni sensibili. L'attaccante si finge un'entità di fiducia come una banca o un'agenzia governativa per manipolare la vittima affinché fornisca dati come credenziali di accesso o numeri di carte di credito. Principali differenze:

-Lo spoofing mira a bypassare i meccanismi di sicurezza, mentre il vishing mira a rubare informazioni o accessi

-Lo spoofing può richiedere l'installazione di malware, mentre il vishing si basa sull'ingegneria sociale via telefono.