ESTUDO – PRINCIPAIS MEDIDAS PARA COIBIR TELEMARKETING ABUSIVO E CHAMADAS DE ROBOCALL – BENCHMARKING INTERNACIONAL

Superintendência de Relações com Consumidores – SRC

Gerência de Interações Institucionais, Satisfação e Educação para o Consumo – RCIC

Processo de Inteligência e Diagnóstico – RCIC2

Brasília/DF, Setembro-Outubro/2022

O presente trabalho relaciona as principais medidas adotadas por Administrações e Órgãos Reguladores de outros países para coibir o telemarketing abusivo e as chamadas de robocall. Além de atualizar o Estudo de benchmarking internacional produzido em 2019, realiza-se uma análise contextualizada dessas medidas frente às soluções empregadas nos últimos anos por esta Agência para o combate dessas práticas lesivas aos consumidores dos serviços de telecomunicações.

*Esta análise foi desenvolvida no contexto de Tópico Prioritário de Inteligência (*Key Intelligence Topic - KIT*), definido no âmbito das competências da Superintendência de Relações com Consumidores (SRC) na execução das atividades do macroprocesso de Inteligência Institucional da cadeia de valor da Anatel. Ela foi produzida pela equipe da SRC com o objetivo de contribuir para o detalhamento do quadro das relações de consumo no setor de telecomunicações, a fim de subsidiar ações regulatórias relacionadas ao tema. As considerações ora apresentadas não representam, necessariamente, a posição final da Agência a respeito da matéria.*

Elaboração: Egon Cervieri Guterres e Humberto Bruno Pontes Silva.

Revisão: Alexandre Magnus Queiroz Gameiro.

Colaboração: Isadora Moreira Firmino.

Nos últimos anos, as chamadas e mensagens telefônicas indesejadas deixaram de ser apenas um incômodo ocasional e se tornaram um grande e recorrente transtorno para os consumidores dos serviços de telecomunicações.

O imenso crescimento dos volumes diários de ligações de telemarketing abusivo (*spam*) e de chamadas fraudulentas (*scam*), impulsionados por mudanças tecnológicas e de comportamento – particularmente após a deflagração da pandemia do novo coronavírus –, fez com que diversos países, o Brasil incluído, adotassem estratégias e medidas regulatórias para mitigar os impactos dessas práticas sobre os consumidores.

Nessa linha, o presente Estudo procura responder às seguintes indagações: (i) quais as principais soluções técnicas e medidas regulatórias utilizadas nos outros países para coibir as ligações indesejadas? (ii) Quais dessas ações se mostraram mais efetivas e apresentaram

melhores resultados, em especial nos últimos anos? (iii) Quais delas têm compatibilidade com o contexto brasileiro e poderiam vir a ser adotadas pelo Brasil no combate a esse problema?

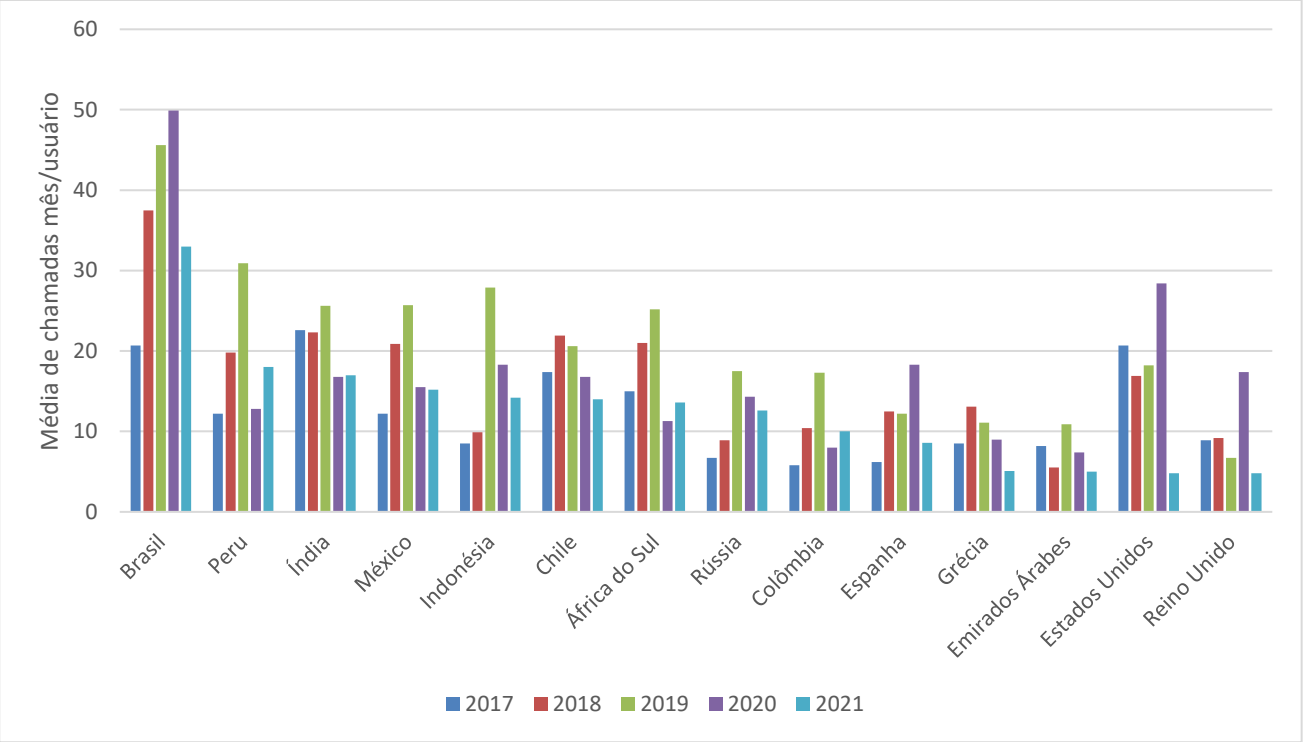
Para promover tal análise, este Estudo relaciona as principais medidas adotadas por Administrações e Órgãos Reguladores de outros países para coibir o telemarketing ativo de publicidade abusiva e as chamadas de *robocall* (discadores automatizados de ligações de curta duração). Além de atualizar o Estudo de benchmarking internacional produzido em 2019, realiza-se uma análise contextualizada dessas medidas frente às soluções empregadas nos últimos anos por esta Agência para o combate de tais práticas lesivas aos consumidores dos serviços de telecomunicações.

Procura-se, assim, oferecer uma visão, ainda que simplificada, das mais recentes tendências globais no tocante às medidas de enfrentamento dos emergentes desafios de gerenciamento de chamadas indesejadas e importunas. Ao cotejar nossas escolhas institucionais e regulatórias frente às diferentes abordagens e soluções que estão sendo discutidas e adotadas nos outros países, espera-se descobrir *insights* e subsídios úteis para o desenvolvimento e aprimoramento das ações empregadas pela Anatel.

1. INTRODUÇÃO

As ligações indesejadas são hoje um problema global e generalizado. Conforme relatórios da empresa sueca Truecaller (fornecedora de um aplicativo de mesmo nome, para *smartphones*, especializado no bloqueio dessas chamadas), o Brasil ocupa com larga vantagem o topo do *ranking* de países afetados por chamadas de *spam* e *scam* há quatro anos[1]. A situação dos demais países que se destacaram nos últimos cinco anos pelo grande volume de chamadas desse tipo pode ser visualizada no gráfico a seguir. As informações foram coletadas dos usuários do aplicativo, e representam o número médio de chamadas mensais, por usuário, ao longo dos anos.

Gráfico 1 – Países que se destacam em ligações de spam/scam 2017-2022, segundo a Truecaller.



FONTE: elaboração própria a partir de: TRUECALLER, *Global Spam&Scam Reports* 2017, 2018, 2019, 2020 e 2021.

De modo geral, depreende-se do gráfico que vários países, após alcançarem um pico nos anos de 2019-2020, obtiveram relativo êxito em reduzir o volume de chamadas não desejadas ou, pelo menos, dão indícios de alcançar uma situação de estabilidade e avançar nesse sentido.

Neste Estudo, a atenção será concentrada na análise da experiência regulatória recente (entenda-se, aproximadamente nos últimos cinco anos) dos países que intensificaram e ampliaram suas medidas de combate ao telemarketing abusivo e às chamadas de *robocall*.

Como *framework* de análise será utilizado o artigo de Tu, Doupé e Zhao (2016)[2], "*SoK: Everyone Hates Robocalls: A Survey of Techniques Against Telephone Spam*", que investigou técnicas de combate ao *spam* telefônico. Ele será apresentado na próxima seção.

Na seção seguinte, serão brevemente resumidas as medidas recentes adotadas pelos países selecionados. Informações adicionais estão disponíveis nos Anexos deste documento, um para cada país. Cabe mencionar que o presente Estudo constitui uma atualização de informações presentes no Estudo de Tópicos Prioritários de Inteligência "Ligações indesejadas – Benchmarking Internacional"[3], produzido em dezembro de 2019 por esta mesma Gerência de Interações Institucionais, Satisfação e Educação para o Consumo – RCIC, da Superintendência de Relações com Consumidores – SRC.

No Estudo de 2019, foram relacionadas as medidas adotadas por sete países (a saber: Alemanha, Austrália, Estados Unidos da América, França, Índia, Itália, e Reino Unido), esclarecendo seu contexto, estratégia utilizada e arranjo institucional correspondente. Aqui, apenas serão tratadas as atualizações mais relevantes, para estes e outros países, escolhidos pela relevância e representatividade das medidas adotadas.

Adicionalmente, esta Gerência recentemente concluiu e publicou o Estudo de Tópicos Prioritários de Inteligência "Diagnóstico em Qualidade da Informação e Desinformação – Medidas Regulatórias para Coibir Telemarketing Abusivo e Chamadas de Robocall"[4]. Ele discorre, de forma sintética e sistemática, sobre as principais medidas regulatórias relativas ao tema adotadas pela Anatel a partir de 2019.

As informações constantes de ambos os supramencionados Estudos, aliás, são bastante relevantes para a compreensão do que se discutirá nas próximas seções do presente trabalho, particularmente para fins de comparação e evolução das abordagens, sendo sua prévia leitura fortemente recomendada. As respectivas referências encontram-se ao final deste documento.

Além disso, em complementação, neste Estudo também serão apresentadas recentes iniciativas europeias no sentido de se estender a aplicabilidade e o alcance das medidas de combate ao telemarketing abusivo e chamadas indesejadas às plataformas digitais e aplicações de comunicação *Over-the-Top* (OTT) – nas quais tais problemas têm galgado cada vez maior relevo ultimamente.

Na sequência, após o relato dos novos achados/atualização de *benchmarking*, será realizada análise cotejando-os ao atual contexto brasileiro e dialogando com as medidas regulatórias recentemente adotadas pela Anatel. A análise terá por foco de avaliação a experiência dos consumidores de serviços de telecomunicações, considerando seus direitos e obrigações, bem como os respectivos ônus, vantagens e impactos de cada alternativa, conforme linha delineada pelo *framework* de análise escolhido. Ao final, serão trazidas considerações sobre as medidas investigadas e sua possível adoção e aplicabilidade no contexto brasileiro.

1.1 TÉCNICAS CONTRA O SPAM TELEFÔNICO

O artigo de Tu, Doupé e Zhao (2016), "*SoK: Everyone Hates Robocalls: A Survey of Techniques Against Telephone Spam*", como mencionado, aqui serve de substrato de análise e comparação das medidas regulatórias de combate às chamadas abusivas. Ele investiga e categoriza uma série de técnicas empregadas para esse fim, detalhando no que consistem e suas principais mecânicas, além de avaliar, entre outras coisas, os desafios que essas técnicas pretendem endereçar, sua aplicabilidade, usabilidade e robustez.

Os autores ressaltam que o primeiro passo para analisar esse problema generalizado consiste em compreender como o "ecossistema do *spam* telefônico" funciona – em particular, quais são os principais atores envolvidos e como acontece o fluxo de dinheiro nesse sistema (entenda-se, a remuneração pelo uso das redes e a receita de *mailing lists*, as listas com os números de telefones dos clientes).[5]

A Tabela 1, a seguir, enumera os quatro principais atores envolvidos nesse processo.

Tabela 1 – Atores-chave do Ecossistema de *Spam* Telefônico

Spammer	Originador das chamadas indesejadas. Pode ser parte de uma organização ou um terceiro contratado especializado neste serviço. As chamadas são geralmente realizadas para a prática do telemarketing ativo abusivo, de fraudes (*scam*) e de campanhas de assédio. Para maior eficiência nos custos, as ligações são realizadas com o uso de discadores automatizados (*autodialer*).
Internet Telephony Service Provider (ITSP)	Ou prestador/transportador de VoIP, responsável por converter/carregar as chamadas realizadas na rede TCP/IP pelo discador automatizado, para prestadora de telecomunicações de telefonia comutada (*Public Switched Telephone Network* – PSTN, ou Serviço Telefônico Fixo Comutado – STFC, no nosso caso). Geralmente remunerado conforme o volume de chamadas.
Interexchange Carrier (IXC)	Responsável pelo transporte das chamadas e interconexão das redes de telefonia. No faturamento das chamadas, são remunerados pelo uso de suas redes conforme diversos fatores, tais como origem, distância, tipo de tráfego etc.
Termination Carrier	Responsável pela terminação (destino final) da chamada, sendo remunerado por essa última etapa da ligação. É a prestadora de serviços de telecomunicações da qual pessoas e empresas são assinantes.

FONTE: elaboração própria, a partir de Tu, Doupé e Zhao (2016).

A operação do *spammer* possui três elementos básicos: a lista de contatos, a "mensagem" e o canal de distribuição maciça. O conteúdo da mensagem é tipicamente um extrato de áudio pré-gravado ou gerado por programas sintetizadores de texto em fala (*text-to-speech synthesizer*), muito embora também sejam bastante comuns os sistemas de resposta interativos (*Interactive Voice Response* – IVR). O conteúdo varia conforme os diferentes tipos de *spam*, tais como telemarketing,

cobrança, tentativas de fraude, campanhas políticas e "*one-ring scams*". Para a distribuição das mensagens, é usual o uso de serviços de VoIP e discadores automatizados.[6]

Por oportuno, cabe um rápido esclarecimento. As *one-ring scams*, como o nome sugere, são as chamadas que desligam após tocar uma ou duas vezes, ou mesmo são encerradas, pelo originador, poucos segundos após o atendimento. Seu objetivo é verificar se o número telefônico discado está em uso ("prova de vida") e se o usuário está disposto a atender às ligações, para fins de se elaborar e refinar as *mailing lists*. No Brasil, assim como em diversos países, esse tipo de chamada também é conhecido como "chamadas de *robocall*".

Tu, Doupé e Zhao também acrescentam a possibilidade de existir um quarto elemento na operação de *spamming* especificamente para a circunvenção de defesas e barreiras, o que torna o processo muito mais robusto, sofisticado e difícil de combater. Há duas técnicas mais comuns, o *Voicemail Injection* (a mensagem pré-gravada vai diretamente para a caixa postal do destinatário) e o *Caller ID Spoofing*. Esta última, cada vez mais utilizada, compreende técnicas de mascaramento/falsificação do número originador da ligação, o que é particularmente eficiente em driblar os bloqueadores de chamadas e na realização de diferentes tipos de fraude.[7]

1.2 DESAFIOS

Isso considerado, os desafios a serem superados para o combate do *spam* telefônico – que são substancialmente diferentes do combate do *spam* de correio eletrônico, como se verá – são tanto técnicos quanto regulatórios. A Tabela 2, abaixo, sintetiza os principais desafios apontados pelos autores:

Tabela 2 – Principais Desafios do Combate ao *Spam* Telefônico

***Immediacy Constraint* (Imediatismo)**	Diferentemente do *spam* de e-mail, que pode entrar em uma fila de processamento e ser avaliado posteriormente, o *spam* telefônico requer ação imediata de avaliação, no momento em que ocorre a chamada. Um sistema anti-*spam* telefônico possui uma pequena janela de tempo para agir. Se há demora nessa avaliação, um originador legítimo pode pensar que o destinatário se encontra impossibilitado de atender a chamada naquele momento.
***Difficulty of Working with Audio Streams* (Dificuldade de se trabalhar *streams* de áudio)**	O conteúdo de texto dos e-mails não apenas é mais fácil de analisar por um sistema de verificação automatizado, como também tal processo não afeta originador e destinatário. Além de ser muito mais difícil analisar um *streaming* de áudio, o conteúdo da chamada de voz somente é revelado após o atendimento da ligação.
***Lack of Useful Header Data* (Ausência de informações úteis no cabeçalho)**	Novamente, o e-mail leva vantagem neste quesito, pois o cabeçalho das mensagens de correio eletrônico possui várias informações úteis e bem definidas, além de ser comparativamente mais complexo omitir o domínio e o IP do remetente. Nas ligações telefônicas, as informações do cabeçalho da chamada podem ser facilmente alteradas e omitidas pelo *spammer*.

Hard to Gain User Acceptance **(Difícil aceitação pelo usuário)**	As chamadas telefônicas são vistas pelos consumidores como mais urgentes e importantes do que os e-mails, o que faz com que eles tenham menor tolerância aos falsos positivos (isto é, uma chamada erroneamente bloqueada pode ter severas consequências). Assim, é mais difícil que aceitem e confiem nos sistemas anti-*spam* telefônicos.
Caller ID Spoofing **(Falsificação da identidade do chamador)**	As informações de identificação do originador da chamada podem ser muito úteis para o bloqueio das chamadas indesejadas. Todavia, como não existe no sistema telefônico um mecanismo de autenticação, essas informações podem ser facilmente adulteradas. Além disso, com a proliferação dos serviços VoIP, nunca foi tão fácil e barato executar tais técnicas de mascaramento dos originadores das chamadas.
Difficulty of Tracing Spam Calls **(Dificuldade em rastrear chamadas de *spam*)**	É difícil localizar a origem de uma chamada depois de iniciada, pois apenas o número de destino é utilizado nas tabelas de encaminhamento e na comutação de circuitos telefônicos. A menos que haja colaboração entre os elos de transporte da chamada, o rastreamento é muito difícil. Se a chamada é realizada na rede TCP/IP, o *spammer* pode se esconder atrás de *proxies*, VPNs e redes Tor, ou mesmo distribuir as chamadas em *botnets*, tornando o rastreamento praticamente impossível.
Entrenched Legacy Systems **(Sistemas legados arraigados)**	A infraestrutura dos núcleos de rede de telefonia evoluiu muito ao longo das décadas e hoje opera em sistemas com base IP. Os protocolos de sinalização telefônica e encaminhamento das chamadas de voz, por outro lado, pouco mudaram nesse período, como forma de se assegurar a plena compatibilidade com as redes legadas. A revisão desses protocolos, por opções mais eficientes, robustas e confiáveis, implica em atualizações e ajustes sistêmicos que afetam toda a rede de telefonia, com grande implicação para sistemas legados. Enquanto isso, os *spammers* se aproveitam das fraquezas e lacunas das tecnologias legadas (como, por exemplo, a falta de verificação do originador).
Lack of Effective Regulations **(Ausência de regulações efetivas)**	No caso do correio eletrônico, há considerável incentivo para o setor adotar as soluções tecnológicas e participar dos esforços de combate ao *spam*. Isso porque, ao fazê-lo, os provedores estão purgando de suas redes e sistemas algo que apenas lhes acarreta custos e desperdícios. Esse não é o caso do *spam* telefônico, pois as empresas de telefonia que participam deste ecossistema são remuneradas pelo uso dos seus recursos de rede. O único que não se beneficia nessa cadeia é o consumidor. Uma prestadora de serviços de telecomunicações que implementa salvaguardas de proteção para seus consumidores até pode se beneficiar indiretamente (com uma melhor imagem pública ou cobrando por um serviço adicional de filtragem de chamadas de *spam*, por exemplo), todavia, o desincentivo da perda de remuneração do uso de sua rede permanece.
Lack of Globalized Enforcement **(Ausência de *enforcement* globalizado)**	Muitas Administrações federais/centrais e suas Unidades/Estados membros possuem legislações e regulações, em diferentes esferas, tratando do tema (por exemplo, tornando ilegais a prática do *spoofing* e a realização massiva de chamadas com o uso de *robocall*). Com o avanço tecnológico e a globalização, todavia, as redes de telefonia passaram de um ecossistema local para um global e, deste modo, muitos *spammers* começaram a operar fora da jurisdição das autoridades nacionais. Para que as medidas de controle do *spam* telefônico sejam efetivas, é preciso que haja um *enforcement* globalizado.

FONTE: elaboração própria, a partir de Tu, Doupé e Zhao (2016).

1.3 TÉCNICAS DE PREVENÇÃO

Na sequência, os autores relacionaram as técnicas básicas de prevenção do *spam* telefônico (e do *spam* de correio de voz), agrupadas em três categorias:

1. *Call Request Header Analysis* (Análise do Cabeçalho de Requisição da Chamada);
2. *Voice Interactive Screening* (Triagem Interativa de Voz);
3. *Caller Compliance* (Conformidade do Originador).

A primeira delas, *Call Request Header Analysis*, reúne técnicas de filtragem das ligações com base no cabeçalho da requisição de chamada, como o nome indica. Justamente por depender da fidedignidade dessas informações, essas técnicas, isoladamente consideradas, são vulneráveis ao *spoofing* e à omissão de informações do cabeçalho.[8]

A segunda categoria, *Voice Interactive Screening* (Triagem Interativa de Voz), é composta por técnicas que forçam o originador da chamada a interagir, ativa ou passivamente, com um sistema interativo de entrada de voz. No caso ativo, o chamador deve realizar alguma tarefa específica; no passivo, o sistema acompanha a interação silenciosamente e sem passar qualquer informação explícita ao originador. Tais sistemas não dependem do *Caller ID* ou dados do cabeçalho de requisição da chamada, o que amplia sua resiliência contra técnicas de *spoofing*. Por outro lado, sua implementação é consideravelmente mais complexa, pois requerem processamento e interpretação de fluxos de áudio. Por esta mesma razão (isto é, a necessidade de gravar e analisar um período inicial de conversação), introduzem atrasos na chamada e são vulneráveis a problemas como ruídos sonoros, perdas de compressão e afins. Além disso, algumas legislações de privacidade exigem prévio consentimento para a gravação da voz humana, o que pode limitar a implementação de tais técnicas.[9]

A terceira e última categoria, *Caller Compliance* (Conformidade do Originador), abrange um conjunto de técnicas nas quais o originador está submetido ao atendimento de certas regras antes e/ou durante a realização da chamada. Se o originador está aderente às regras ele pode estabelecer comunicação com o destinatário. As regras devem ser de fácil atendimento pelos originadores legítimos, mas difícil (ou custoso) para o *spammer*. Algumas dessas técnicas necessitam de ajustes ao processo de originação da chamada ou aos terminais de comunicação. Outras, requerem que instruções sejam transmitidas ao originador antes da realização da chamada.[10]

Uma breve síntese dessas técnicas, reunidas em suas respectivas categorias, pode ser conferida na Tabela 3, abaixo.

Tabela 3 –Técnicas Básicas de Combate ao *Spam* Telefônico

Call Request Header Analysis	***Caller ID Blacklisting*** – a chamada é rejeitada caso o número originador (obtido do *Caller ID* ou de algum serviço automatizado de identificação) esteja cadastrado na lista de bloqueio. O bloqueio é silencioso (não há qualquer

(Análise do Cabeçalho de Requisição da Chamada)	importuno ao destinatário) e permissivo a todos os demais números, que não estiverem na lista. Como o *Caller ID* já está presente nos sistemas de telefonia, não existem problemas de compatibilidade com essa técnica, que é de fácil implementação e requer poucos recursos computacionais. Sua eficiência é bastante dependente da qualidade da lista, no entanto. Além disso, a técnica pode ser facilmente burlada com o uso de *spoofing*. ***Caller ID Whitelisting*** – somente são aceitas as chamadas de números originadores presentes da lista de permissão, composta por "números confiáveis". As demais ligações são rejeitadas, silenciosamente. Como na técnica anterior, é de fácil implementação e requer poucos recursos computacionais (há aplicativos para *smartphones* que fazem esse tipo de gerenciamento de chamadas, por exemplo). Embora seja fácil popular a lista de números permitidos (por exemplo, a lista de contatos da agenda telefônica), possui o inconveniente de bloquear chamadas legítimas de números fora da lista de permissão. Apesar de também ser vulnerável ao *spoofing*, sua implementação é muito mais difícil, pois requer prévio conhecimento dos números presentes na lista de permissão do destinatário em questão. ***Caller Reputation System*** – essa técnica utiliza um sistema de reputação ou confiança para determinar se um dado número de telefone está sendo utilizado por *spammers*. As notas associadas a cada número são computadas a partir de diferentes informações, tais como listas de bloqueio/permissão, comportamento do originador, reputação do domínio do originador, reputação/perfil do destinatário, conexões sociais e *feedback* dos destinatários. O terminal do usuário pode então ser configurado para bloquear, silenciosamente, as chamadas com baixa reputação, por exemplo. Um sistema como esse requer uma grande quantidade de dados, usualmente obtidos por meio de *crowdsourcing* de muitos usuários. Além disso, esses dados precisam ser processados, curados e mantidos por um terceiro, de modo a assegurar que estejam válidos e atualizados. A coleta de tais informações (pessoais), no entanto, pode representar riscos de privacidade. Ademais, técnicas como essa podem ser vulneráveis a fraudes de identidade ou uso de múltiplas identidades, além de ataques maliciosos e sabotagens de reputação. ***Caller Behavior Analysis*** – técnica que realiza análise do comportamento do originador da chamada para determinar se é um *spammer*. São analisados, por exemplo, a quantidade/velocidade das chamadas, o total/média/variância das ligações, a razão entre ligações rejeitadas e originadas, a contagem de cabeçalhos inválidos, a razão de rediscagem, a razão entre tráfego de saída/entrada, número de ligações simultâneas e determinados comportamentos do domínio do originador. O fornecimento dessas informações usualmente é exigido por força de regulação, pois não existe qualquer interesse das prestadoras de telecomunicações em divulgá-las. As informações precisam ser constantemente atualizadas para que a aplicação da técnica seja efetiva e confiável. A técnica é vulnerável à prática do *spoofing* e ao uso de subterfúgios de mascaramento e distribuição do volume de ligações entre múltiplos números/identidades. ***Device Fingerprinting*** – consiste na coleta de uma variedade de metadados do cabeçalho da requisição de chamada para formar uma "impressão digital" de identificação do terminal originador, conforme propriedade tais como diversidade e estabilidade. Diferentemente das chamadas nas redes TCP/IP, na telefonia comutada tais informações de cabeçalho são bastante escassas, limitando a utilidade da técnica. ***Caller ID Anomaly Detection*** – técnica que procura padrões anômalos no *Caller ID*, tais como números inválidos, formato/marcação incorreta, códigos

	gratuitos e de área utilizados de forma incompleta/inadequada e outras situações inesperadas. É relativamente simples de implementar e requer poucos recursos computacionais, razão pela qual está presente em muitos aplicativos de bloqueio/gerenciamento de ligações telefônicas. Sua eficácia pode ser comprometida por falsos negativos, no entanto, em chamadas legítimas de usuários VoIP ou de originadores que utilizam configurações de privacidade específicas. Além disso, o *spammer* pode escapar da detecção simplesmente ao utilizar um código aderente ao padrão válido de formato/marcação (isto é, não anômalo). ***ANI-CPN Matching*** – técnica que verifica se as informações do *Calling Party Number* (CPN) (identificação do originador, no *Caller ID*) batem com as informações do serviço de *Automatic Number Identification* (ANI). O ANI é um serviço separado, que pode identificar a originação mesmo que as informações do *Caller ID* não estejam presentes, pois foi projetado para possibilitar o faturamento de chamadas de longa distância e/ou com regras especiais (0800, por exemplo). A técnica presume que deve haver coincidência entre as duas fontes de informações. O serviço de ANI geralmente não está disponível aos usuários regulares (*i.e.*, o consumidor comum), de modo que apenas usuários corporativos/especiais poderiam tirar proveito dessa técnica. Outrossim, a técnica nem sempre consegue identificar corretamente o originador da chamada (casos envolvendo PABX, VoIP, terminais públicos etc.). ***ANI-II Filtering*** – técnica que bloqueia certos tipos de origem, com base na identificação do serviço associado ao *switch* originador. Como na técnica anterior, possui vários riscos de falsos positivos nas chamadas em redes TCP/IP. Além disso, tal serviço não costuma estar disponível ao usuários regulares, sendo mais utilizados pelos clientes corporativos que possuem números de ligação gratuita e serviços de emergência, utilidade pública e afins.
Voice Interactive Screening **(Triagem Interativa de Voz)**	***Audio Fingerprinting*** – baseia-se na análise prévia de extratos de voz, ou outras informações do áudio da chamada, em busca de similaridades com perfis típicos das chamadas de *spam*. Em caso positivo, a chamada é classificada como *spam* e rejeitada. A técnica foi proposta para combater as ligações que reproduzem mensagens pré-gravadas (de telemarketing ativo, por exemplo). Sua performance depende da completude e exatidão dos perfis de áudio das chamadas de *spam*, o que usualmente não é conhecido pelos usuários. Assim, faz-se necessário que um terceiro colete e mantenha atualizados esses perfis de chamadas de *spam*. Mesmo assim, a solução anti-*spam* pode ser frustrada por um *spammer* que dinamicamente crie variações na mensagem de áudio (introduzindo artefatos ao sinal de áudio ou personalizando o conteúdo da mensagem, por exemplo) para evitar a detecção. ***Speech Content Analysis*** – nesta técnica, a voz do originador é gravada, convertida em texto e interpretada. O conteúdo de texto é então comparado aos perfis típicos das chamadas de *spam*, para fins de classificação da ligação. A análise de um corpo de texto é usualmente muito mais simples do que a de um *streaming* de voz. Além disso, muitas ligações de *spam* seguem *scripts* simples, com muitas palavras-chave de fácil identificação. A efetividade desses sistemas, como seria de se esperar, é fortemente dependente da precisão do reconhecimento de voz e do modelo de classificação de chamadas. ***Acoustic Pattern Analysis*** – padrões de áudio distintivos (por exemplo, perdas de sinal, uniformidade de pico, atividade de voz e duplicidade de áudio) são extraídos do *streaming* de áudio do originador da chamada e analisados para determinar se se trata de *spam*. Diferentemente das duas técnicas anteriores, esta não requer grandes coleções conhecidas de padrões e perfis de *spam*.

	Assim, como elas, todavia, a técnica é facilmente derrotada por técnicas de manipulação de áudio. ***CAPTCHA/Turing Test*** – técnica na qual o originador da chamada precisa completar um teste de Turing reverso para determinar se é humano ou uma *robocall*. O teste em si é planejado para ser facilmente realizado por um humano, mas difícil para um computador. Por exemplo, o teste pode solicitar que o originador digite um código aleatório apresentado em um clipe de áudio distorcido. É preciso tomar cuidado, todavia, com pessoas com dificuldades com o idioma ou necessidades especiais. Ademais, a aplicação desta técnica pode representar um obstáculo irritante para um chamador legítimo, exigindo alto grau de esforço e atrasando significativamente a concretização da chamada.
***Caller Compliance* (Conformidade do Originador)**	***Do Not Call Registry*** – a lista de Não Perturbe, que relaciona os números de telefone para os quais os *spammers* não podem ligar. Se descumprida, pode implicar no pagamento de multas. Os usuários precisam, todavia, ativamente fornecer um *feedback* de descumprimentos para a atuação governamental. A técnica pode ser uma boa medida de controle para as empresas nacionais de telesserviços que respeitam as regras, mas costuma ser pouco eficiente contra empresas que fazem *spoofing*, bem como os *spammers* internacionais. ***Graylisting*** – nesta técnica, a primeira ligação é automaticamente rejeitada e a segunda tentativa, se realizada num curto espaço de tempo, é aceita. É uma técnica eficiente contra discadores automatizados que apenas seguem a lista de contatos, sem tentativas imediatas de rediscagem. Ela presume que um chamador legítimo, mesmo que desconhecendo a medida, tentará realizar um novo contato para estabelecer a comunicação logo em seguida à primeira tentativa fracassada. É fácil de implementar e não requer ajustes na infraestrutura. O chamador legítimo, no entanto, precisará realizar duas ligações, acrescentando atraso ao processo de chamada e, possivelmente, custos de ligação. A técnica também pode ser facilmente superada por um *spammer* que configure seu discador automático para realizar a rediscagem, muito embora isso reduza sua eficiência e implique em novos custos ao processo. ***Consent-based Communication*** – técnica baseada no prévio consentimento do destinatário da chamada. O consentimento pode ser obtido, por exemplo, com o chamador respondendo seu nome a um sistema de secretária eletrônica, que então repassa o pedido de ligação ao destinatário. Apesar de limitar a exposição do usuário à chamada indesejada, ele continua sendo importunado. Além disso, a solução acrescenta complexidade e atraso a todas as chamadas, indistintamente. ***Call Back Verification*** – a primeira tentativa de contato é rejeitada e o originador é forçado a aguardar que o destinatário retorne a ligação. É uma boa defesa contra o *spoofing*, pois obriga o chamador a fornecer um número genuíno para a realização do retorno. A implementação do mecanismo é simples e, em alguns casos, completamente automatizada. Ela pode restringir alguns originadores legítimos (usuários VoIP ou terminais de extensão telefônica). O atraso de comunicação pode ser grande, pois depende do retorno do destinatário, além de acrescentar os custos da nova ligação. ***Weakly Secret Information*** – o chamador precisa conhecer a “chave da semana” para ser capaz de estabelecer a comunicação. A técnica pode ser implementada de diferentes formas: uma senha, um código de extensão, um número de telefone temporário ou um identificador de mensagem específico. Ela exige que o destinatário previamente distribua a informação necessária aos

	originadores confiáveis, o que pode gerar restrições a comunicações legítimas e causar dificuldades de implementação em larga escala. ***Payment at Risk*** – técnica baseada em custo de microtransação. O originador, antes de realizar a chamada, precisa depositar uma pequena quantia. Se a chamada for denunciada como *spam*, o depósito é confiscado ou fica com o destinatário. Isso limita os volumes maciços de chamadas de *robocall*, pois os custos tornam-se proibitivos, enquanto a repercussão para um chamador legítimo é pequena. A aplicação da técnica, no entanto, requer a implementação de um complexo sistema universal de microtransações, que coleta e distribui pagamentos chamada a chamada. Há também questões relacionadas à legalidade da retenção do depósito (ou confisco) e à possibilidade de abusos nas denúncias de *spam*. ***Proof of Work*** – técnica baseada em custo computacional, que requer que o terminal do originador apresente uma prova de trabalho, como um *hashcash*, moderadamente complexo de calcular, mas de fácil confirmação pelo recebedor. Originadores legítimos teriam baixo custo computacional, pois fazem poucas ligações, enquanto *spammers* sofreriam com custos proibitivos para a distribuição de grandes volumes de chamadas. A técnica possui vantagens em relação às baseadas em microtransações econômicas, mas não é imune a críticas. Por exemplo, ela deve ser permissiva aos terminais telefônicos de baixa complexidade, o que exige processos computacionais mais simples, que podem ser explorados pelos *spammers*. Adicionalmente, a técnica pode ser incompatível com diversos perfis de usuários que fazem/recebem grandes volumes de chamadas legítimas, como bancos e serviços de teleatendimento. ***Proof of Identity*** – nesta técnica, o originador da chamada precisa encaminhar um token verificável, que autentica sua identidade/credencias a cada ligação realizada. É um processo bastante conhecido no domínio IP, onde a utilização de certificados e infraestruturas de verificação de chaves-públicas já estão bem desenvolvidas. A técnica desencoraja o *spamming* pois o realizador da chamada pode ser responsabilizado (e, consequentemente, punido) pela realização das chamadas abusivas e tentativas de fraude. O processo de verificação também previne o uso de múltiplas identidades. É mais simples de implementar que a técnica anterior, pois não há custos computacionais associados; todavia, sua implementação ainda é considerada complexa, pois é preciso estabelecer mecanismos e autoridades de verificação das chamadas, o que pode requerer mudanças no processo/protocolo de requisição e atendimento de chamadas.

FONTE: elaboração própria, a partir de Tu, Doupé e Zhao (2016).

1.4 CRITÉRIOS DE AVALIAÇÃO

Apresentadas as principais técnicas básicas empregadas no combate ao *spam* telefônico, os autores propõem três critérios de avaliação:

1. ***Usability Criteria* (“Usabilidade”)**: avalia a facilidade de uso da técnica, seja da perspectiva do originador, seja do destinatário da chamada, conforme o caso.
2. ***Deployability Criteria* (“Implementabilidade”)**: identifica o quão fácil é a sua implementação (instalação, adoção e operação).
3. ***Robustness Criteria* (“Robustez”)**: avalia o quanto ela é resiliente contra falhas e efetiva contra os *spammers* ativamente procurando evitá-la ou contorná-la.[11]

A Tabela 4, a seguir, resume os critérios de avaliação das técnicas:

Tabela 4 – Critérios de Avaliação das Técnicas de Combate ao *Spam* Telefônico

***Usability Criteria* (Critério de Usabilidade)**	***No-Disturbance-to-Recipient* (Não Perturba o Destinatário)** – quando da chegada de uma chamada sabidamente indesejada/*spam*, a técnica não importuna o destinatário (isto é, não requer dele qualquer ação). ***Scalable-for-Recipient* (Escalável para o Destinatário)** – a técnica não aumenta o trabalho/ônus do destinatário conforme aumenta o volume de chamadas indesejadas. Ou seja, a técnica consegue lidar com uma grande quantidade/variedade de *spam* apenas com interações mínimas com o destinatário. ***Effortless-for-Caller* (Sem Esforço para o Originador)** – ao iniciar a chamada, a técnica exige mínimo ou nenhum esforço do originador. ***Negligible-Changes-to-Call-Setups* (Alterações Não Significativas ao *Setup* de Chamada)** – a técnica não acarreta ajustes significativos ao *setup* ou às configurações dos terminais dos originadores das chamadas. ***Negligible-Delays* (Atrasos Não Significativos)** – o tempo adicionado pela aplicação da técnica, no momento da realização da chamada, não é significativo ou perceptível pelo destinatário, quando considerado o tempo usual. ***Permissive-for-VoIP-Callers* (Permissiva aos Originadores VoIP)** – a técnica não restringe chamadas legítimas realizadas por usuários VoIP. ***Permissive-for-Unknown-Callers* (Permissiva aos Originadores Desconhecidos)** – a técnica não restringe chamadas legítimas de originadores não conhecidos pelo destinatário.
***Deployability Criteria* (Critério de Implementabilidade)**	***Negligible-Changes-to-Infrastructure* (Alterações Não Significativas à Infraestrutura)** – a técnica não requer ou requer mínimas alterações aos padrões, protocolos e/ou infraestrutura da telefonia comutada. ***No-Third-Party-Involvement* (Sem a Necessidade da Participação de Terceiros)** – a técnica não requer a participação de terceiros para sua aplicação. ***Low-Resource-Requirement* (Requer Poucos Recursos)** – a implementação e/ou aplicação da técnica não requer quantidades significativas de recursos, tais como pessoas, equipamentos, engenharia, remuneração etc. **Low-Maintenance (Baixa Manutenção)** – a técnica possui baixo custo de manutenção, sejam custos administrativos, de tempo, recursos etc. ***Negligible-Cost-per-Call* (Custo Por Ligação Não Significativo)** – os custos que a aplicação da técnica adiciona a cada chamada não são significativos. Esse custo também pode ser indireto (como reduções de eficiência ou de capacidade).
***Robustness Criteria* (Critério de Robustez)**	***Effective-Against-Dynamic-Caller-ID-Spoofing* (Efetiva Contra o *Caller ID Spoofing* Dinâmico)** – a técnica é robusta mesmo quando o *spammer* utiliza técnicas de *spoofing* não determinísticas.

	Effective-Against-Targeted-Caller-ID-Spoofing (Efetiva Contra o *Caller ID Spoofing* Direcionado) – a técnica é robusta mesmo quando o *spammer* se apropria de um *Caller ID* que possui a confiança do destinatário. ***Effective-Against-Unavailable-Caller-ID* (Efetiva Contra *Caller ID* Indisponível)** – a técnica é robusta mesmo quando o *spammer* utiliza um *Caller ID* indisponível ou indica um incorreto/incompleto para causar erros. ***Effective-Against-Multiple-Identities* (Efetiva Contra Múltiplas Identidades)** – a técnica é robusta mesmo quando o *spammer* utiliza múltiplas fontes originadoras de chamadas (várias assinaturas ou *botnets*, por exemplo). ***Effective-Against-Answering-Machine-Detection* (Efetiva Contra Detecção de Secretária Eletrônica)** – a técnica é robusta mesmo quando o *spammer* utiliza tecnologias para detecção de secretárias eletrônicas, usualmente presentes nos discadores automatizados para distinguir entre o atendimento humano e do equipamento. Com a técnica, o discador automatizado pode ser configurado para ligar novamente mais tarde se a chamada não foi atendida por um humano, ou deixar uma mensagem de áudio na secretária eletrônica. ***Effective-Against-Dynamic-Audio-Content* (Efetiva Contra Conteúdo de Áudio Dinâmico)** – a técnica é robusta mesmo quando o *spammer* utiliza discador automatizado capaz de personalizar ou alterar a mensagem de áudio entre os diferentes destinatários. Essa é uma capacidade comum dos discadores capazes de sintetizar texto em fala.

FONTE: elaboração própria, a partir de Tu, Doupé e Zhao (2016).

Combinando as informações dessas duas últimas Tabelas, Tu, Doupé e Zhao apresentam uma análise geral das técnicas básicas, isoladamente consideradas, face às categorias e aos critérios de avaliação apresentados.

O Gráfico 2, a seguir, adaptado do mencionado artigo, ilustra essa avaliação. É interessante de se observar no gráfico como a categoria das técnicas com maior Usabilidade (facilidade de uso pelo originador/destinatário) são as mais vulneráveis ao *spoofing*, que somente é eficientemente combatido pelas técnicas com pior Implementabilidade (isto é, as que requerem maiores ajustes de infraestrutura e custos de instalação/operação). Além disso, a Complacência do Originador (submissão a regras específicas para a realização de chamadas) igualmente mostra-se essencial para o combate ao *spoofing*.

Gráfico 2 – Avaliação das Técnicas Básicas, conforme os critérios de Tu, Doupé e Zhao

		Usability						Deployability						Robustness					
		No-Disturbance-to-Recipient	*Scalable-for-Recipient*	*Effortless-for-Caller*	*Negligible-Delays*	*Permissive-for-VoIP-Callers*	*Permissive-for-Unknown-Callers*	*Negligible-Changes-to-Infrastructure*	*Negligible-Changes-to-Call-Setups*	*No-Third-Party-Involvement*	*Low-Maintenance*	*Low-Resource-Requirement*	*Negligible-Cost-per-Call*	*Effective-Against-Dynamic-Caller-ID-Spoofing*	*Effective-Against-Targeted-Caller-ID-Spoofing*	*Effective-Against-Unavailable-Caller-ID*	*Effective-Against-Multiple-Identities*	*Effective-Against-Answering-Machine-Detection*	*Effective-Against-Dynamic-Audio-Content*
Call Request Header Analysis	Caller ID Blacklisting	●	◐	●	●	●	●	●	●	●	◐	●	●	○	○	○	◐	●	●
	Caller ID Whitelisting	●	●	●	●	●	○	●	●	●	◐	●	●	●	○	○	●	●	●
	Caller Reputation System	●	◐	●	●	●	◐	●	●	◐	○	◐	●	◐	○	○	◐	●	●
	Caller Behavior Analysis	●	●	●	●	●	◐	●	●	◐	○	◐	●	◐	○	○	◐	●	●
	Device Fingerprinting	●	●	●	●	●	◐	●	●	◐	○	◐	●	◐	○	◐	◐	●	●
	Caller ID Anomaly Detection	●	●	●	●	●	●	●	●	◐	◐	●	●	◐	○	◐	○	●	●
	ANI-CPN Matching	●	●	●	●	◐	●	●	●	●	●	●	◐	◐	○	◐	○	●	●
	ANI-II Filtering	●	●	●	●	◐	●	●	●	●	●	●	◐	◐	○	◐	○	●	●
Voice Interactive Screening	Audio Fingerprinting	●	●	◐	○	●	●	●	●	◐	○	○	◐	●	●	●	●	◐	◐
	Speech Content Analysis	●	●	◐	○	●	●	●	●	◐	◐	○	◐	●	●	●	●	◐	◐
	Acoustic Pattern Analysis	●	●	◐	○	●	●	●	●	◐	◐	◐	◐	●	●	●	●	◐	◐
	CAPTCHA/Turing Test	●	●	○	○	●	●	●	●	●	◐	◐	◐	●	●	●	●	●	●
Caller Compliance	Do Not Call Registry	◐	◐	◐	●	●	●	●	●	○	◐	◐	●	○	○	○	◐	●	●
	Graylisting	●	●	◐	○	●	◐	●	◐	●	●	●	○	●	●	●	●	●	●
	Consent-based Communication	○	○	◐	○	●	◐	●	◐	●	●	●	◐	●	◐	●	●	●	●
	Call Back Verification	◐	◐	◐	○	◐	◐	●	●	●	●	●	○	●	●	●	●	●	●
	Weakly Secret Information	●	◐	◐	◐	●	○	◐	◐	●	◐	●	●	●	●	●	●	●	●
	Payment at Risk	●	○	◐	●	●	○	○	○	○	○	○	○	●	●	●	●	●	●
	Proof of Work	●	●	●	●	●	○	◐	○	●	●	◐	●	●	●	●	●	●	●
	Proof of Identity	●	●	●	●	●	○	◐	○	◐	●	◐	●	●	●	●	●	●	●

●= satisfy the criteria ◐= may satisfy the criteria ○= does not satisfy the criteria

FONTE: adaptado de Tu, Doupé e Zhao (2016) (p.13).

Feitas tais considerações acerca do *framework* de análise, passa-se ao breve relato das medidas adotadas pelos outros países para coibir o telemarketing abusivo e as chamadas de *robocall*.

2. MEDIDAS ADOTADAS POR OUTROS PAÍSES

As tabelas a seguir sintetizam as principais medidas legais e regulatórias recentemente adotadas pelos outros países para o combate às chamadas indesejadas. Informações complementares podem ser obtidas nos respectivos Anexos deste documento.

2.1 ESTADOS UNIDOS DA AMÉRICA

Estados Unidos da América (vide Anexo A para maiores informações)		
Medida	*Descrição*	*Há similar no Brasil?*
Cessar e Desistir	***Cease-and-Desist Order***. Em 7 de julho de 2022, a *Federal Communications Commission* expediu um *Public Notice*[12] dirigido a todas as prestadoras de telecomunicações sediadas nos EUA, com regras de combate a chamadas de *robocall*. Ela exigiu que dezenas de provedores de serviços que aparentemente facilitaram atividades ilícitas de *robocall* em suas redes imediatamente interrompam e descontinuem essas atividades. Se a prática não for imediatamente interrompida, alertou o órgão regulador estadunidense, o tráfego de rede dos infratores será bloqueado nas demais prestadoras. A FCC está monitorando as atividades das empresas sob suspeita. Em caso de irregularidade/reincidência, poderá autorizar o bloqueio do tráfego de qualquer uma dessas empresas devidamente avisadas.	Parcial
Alterações Legais	***Lei Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Disterrence (TRACED ACT).*** Publicada em dezembro/2019 dá à Comissão Federal de Comunicações (FCC) maior autoridade para processar golpistas de chamadas telefônicas e busca facilitar a identificação de chamadas automáticas para evitá-las. A Lei TRACED exige que os provedores de serviços de telecomunicações, como Verizon, T-Mobile/Sprint e AT&T, implementem um sistema de identificação e autenticação dos números das chamadas, sem custos para os consumidores. Também aumenta as penalidades para empresas que utilizam discadores automatizados (*robocallers*). A partir da publicação da Lei, a FCC pode cobrar multas civis de até US$ 10.000 por chamada em tentativas de telemarketing não solicitadas. Além disso, a prescrição foi estendida para quatro anos.	Parcial

Estados Unidos da América (vide Anexo A para maiores informações)		
Medida	*Descrição*	*Há similar no Brasil?*
Autenticação do Identificador de Chamadas (STIR/SHAKEN)	***Signature-based Handling of Asserted information using toKENs* – SHAKEN**[13]. Os padrões de identificação de chamadas STIR/SHAKEN oferecem um conjunto comum de funcionalidades e ferramentas de compartilhamento de informações de rede e verificação de informações das chamadas. Eles são particularmente úteis para proteger os consumidores de chamadas automatizadas e falsificadas, nas quais há mascaramento das informações das chamadas para dificultar o gerenciamento e o rastreamento das ligações. Com a verificação das informações, é possível realizar bloqueios de chamadas de *robocall* de forma mais eficiente e evitar certas tentativas de fraude e golpe telefônico baseados na falsidade de identidade que acometem comunidades vulneráveis, por exemplo. A implementação do STIR/SHAKEN está em andamento nos EUA. Em 30 de junho de 2021, a FCC afirmou que todos os maiores provedores de serviços de voz haviam implementado esses padrões nas seções IP de suas redes, em conformidade com o prazo estipulado. Interessante mencionar que alguns prestadores de pequeno porte receberam extensão de prazo para a implantação, enquanto para outros o prazo foi reduzido pela metade, pois identificou-se que realizavam grandes volumes de chamadas irregulares.	Em discussão
Banco de Dados de Mitigação de Chamadas de *Robocall*	***Robocall Mitigation Database***. As prestadoras devem registrar o estado de implementação do STIR/SHAKEN nas suas redes IP e certificações, além de informar, em alguns casos, seus esforços para coibir as chamadas de *robocall*. O fornecimento de informações é mandatório e elas devem ser registradas no *Robocall Mitigation Database*[14], mantido pela FCC. Desde setembro de 2021, as prestadoras não certificadas para a implementação dos padrões de autenticação de identificação de chamadas STIR/SHAKEN, ou que não tenham apresentado um plano detalhado de mitigação de *robocall* junto à FCC, podem ter seu tráfego bloqueado pelas outras empresas.	Não

Estados Unidos da América (vide Anexo A para maiores informações)		
Medida	*Descrição*	*Há similar no Brasil?*
Fechamento de *Gateways* Internacionais	**Novas regras para chamadas Internacionais.** Em maio de 2022, a FCC adotou novas regras para combater a entrada de chamadas de *robocall* irregulares, geradas internacionalmente, nas redes telefônicas americanas. Os provedores de *gateway* – as portas de acesso para tráfego de chamadas internacionais – devem agora cumprir protocolos de autenticação de identificação de chamadas STIR/SHAKEN e adotar medidas para validação da identidade do tráfego que eles estão roteando. Além disso, os provedores de *gateway* devem participar e cooperar com os esforços de mitigação e bloqueio dessas chamadas. Eles são responsáveis por elas e devem responder prontamente nas medidas de contenção.	Não
Multas maiores	**Sanções mais severas**. Nos últimos anos, a FCC ampliou e tornou mais agressivas as atividades de fiscalização e sancionamento das empresas de telemarketing e prestadoras de telecomunicações que se utilizam de *spoofing* e realizam grandes volumes de chamadas de *robocall*. A maior multa da história do órgão regulador estadunidense (US$ 225 milhões) foi aplicada a uma operadora de telemarketing de seguros de saúde, pela realização de 1 bilhão de chamadas irregulares. Uma operação de *spoofing* recebeu uma multa de US$ 120 milhões. Há muitos outros exemplos.	Não
Bloqueios de chamadas de voz	***Call Blocking*.** De acordo com as regras da FCC, os provedores de serviços de voz podem bloquear as seguintes de chamadas voz: ▪ Chamadas de números não atribuídos, não alocados ou inválidos. ▪ Chamadas de números na lista Não Originar Chamadas (Do-Not-Originate – DNO). ▪ Chamadas que considere indesejadas com base em padrões razoáveis (o provedor deve permitir que seus clientes desativem esse tipo de bloqueio, caso assim o desejem).	Não
Registro de Não me perturbe	***National Do-Not-Call Registry (DNC).*** As regras do DNC estabelecem que as empresas de telemarketing, com algumas exceções, estão proibidas de iniciar qualquer interação telefônica com os assinantes que tenham se cadastrado no registro nacional de Não Perturbe (DNC), para o não recebimento de comunicações comerciais não solicitadas. Os requisitos se aplicam a chamadas de voz e mensagens de texto.	Sim

Estados Unidos da América (vide Anexo A para maiores informações)		
Medida	*Descrição*	*Há similar no Brasil?*
Conscientização e Aplicativos de Bloqueio de *Robocall*	**Conscientização e Aplicativos**: A FCC tem apoiado os esforços de prestadoras de telefonia e de empresas de soluções de tecnologia para o desenvolvimento e disponibilização, aos consumidores, de ferramentas eficazes de bloqueio de chamadas de *robocall*. As informações provenientes dos padrões STIR/SHAKEN, em processo de implantação nos EUA, são um recurso crítico para tais ferramentas, aliás. Além disso, a FCC elaborou guia sobre como minimizar os impactos das chamadas de *robocall* para ampliar a conscientização dos consumidores sobre o tema[15]. Uma lista de recursos para minimizar os impactos das chamadas indesejadas pode ser consultada em página específica da FCC sobre o tema[16].	Parcial
Exclusão de Prestadoras em não Conformidade com STIR/SHAKEN	**Remoção de prestadoras do RMB.** A FCC iniciou um processo para remover sete provedores de serviços de voz do *Robocall Mitigation Database*, mantida por ela[17]. No combate às comunicações indesejadas, as prestadoras devem executar várias etapas de mitigação das chamadas de *robocall* – incluindo a implementação de STIR/SHAKEN em suas redes IP. Se não demonstrarem que atenderam às regras e requisitos, no prazo de 14 dias, essas prestadoras poderão ser excluídas da base de dados e, por consequência, as outras prestadoras deixarão de transportar seu tráfego.	Não
PROPOSTA – Bloqueio de geradores automatizados de mensagens de texto (*robotext*)	**Bloqueio de mensagem de texto:** Em setembro de 2022, a FCC submeteu para consulta pública proposta de bloqueio de geradores automáticos de mensagens de texto ("*robotext*")[18]. Dentro da proposta estão medidas como: (i) aplicação de padrões de autenticação de identificação de chamadas para mensagens de texto; (ii) bloqueio de mensagens de textos, no nível da rede das prestadoras de telefonia móvel, nas quais se identifiquem números inválidos, não alocados ou não utilizados, e números da lista *Do-Not-Originate* (DNO). Adicionalmente**, a FCC busca comentários sobre a extensão de tais regras para o bloqueio de mensagens indesejadas em aplicativos de comunicação *Over-the-Top* (OTT)**, bem como considerações sobre seu impacto atual nos consumidores. Além disso a FCC também procura informações sobre outras ações que a Comissão possa tomar para lidar com textos ilegais, incluindo uma melhor educação do consumidor.	Não

2.2 REINO UNIDO

Reino Unido (vide Anexo B para maiores informações)		
Medida	*Descrição*	*Há similar no Brasil?*
Plano de Ação para o Combate a Chamadas Indesejadas	*ICO / Ofcom joint action plan 2021/2022*[19]. Em seu plano de trabalho 2021/2022, o regulador das comunicações no Reino Unido (Ofcom) trouxe como uma das metas para o período o combate a chamadas indesejadas e golpes telefônicos. Nesse contexto, o regulador pretende continuar o trabalho junto a provedores de comunicação para interromper e evitar tais comunicações indesejadas, bem como expandir as possíveis ações. Reforça ainda a importância do trabalho conjunto com outras agências de fiscalização, como o *Information Commissioner's Office* (ICO), órgãos de interesse do consumidor e reguladores internacionais, para compartilhar inteligência e melhores práticas no combate a esse problema.	Não
Lista de Não Me perturbe	***Telephone Preference Service (TPS) – Do-not-call list*.** O registro nacional de não perturbe, do tipo *opt-out*, é o único que as organizações são legalmente obrigadas a observar antes de realizar uma ligação de telemarketing ativo. O cadastro é feito gratuitamente por telefone ou pelo sítio eletrônico, sendo que para telefones móveis existe ainda a possibilidade de enviar mensagem de texto para um número específico. Em 28 dias, a solicitação passa a ter efeito. O TPS é voltado a evitar ligações de vendas/telemarketing e se aplica para todas empresas e organizações do Reino Unido, incluindo de caridade, serviço voluntário e partidos políticos. Por outro lado, chamadas de cobrança, ligações gravadas/automatizadas, pesquisas, ligações de empresas no exterior e chamadas fraudulentas, por exemplo, não estão abrangidas pelas ações da plataforma.	Sim

Reino Unido (vide Anexo B para maiores informações)		
Medida	*Descrição*	*Há similar no Brasil?*
Multas[20]	**Sanções mais severas.** Em 15 de março de 2022, o *Information Commissioner's Office* (ICO) anunciou a aplicação de multas, no total de £ 405.000, para cinco empresas que juntas foram responsáveis por mais de 750.000 chamadas indesejadas de marketing especificamente direcionadas para pessoas mais velhas e vulneráveis. A ICO também emitiu para essas empresas notificações executórias que exigem que cessem imediatamente as práticas predatórias. Outras multas aplicadas pelo ICO: ▪ uma empresa de reforma de casas, em £ 200.000, por fazer mais de meio milhão de ligações de marketing não solicitadas, em fevereiro de 2022; ▪ o EB Associates Group Limited, em £ 140.000, por realizar mais de 107.000 ligações ilegais sobre pensões, em dezembro de 2021; ▪ em 2020, uma empresa que fez mais de 193 milhões de chamadas indesejadas com *robocall, em* £ 500.000.	Não
Monitoramento de chamadas incômodas	**Monitoramento Ativo.** As reclamações sobre chamadas indesejadas são relatadas ao Ofcom e ao ICO. As chamadas silenciosas e abandonadas são registradas pelo Ofcom, enquanto as chamadas de marketing ao vivo e gravadas são registradas pelo ICO. Nos últimos anos existia uma tendência de queda das reclamações em ambos os órgãos. Entretanto, em 2021, foi observado aumento nas reclamações. Além disso, percebeu-se uma mudança no perfil das chamadas indesejadas para chamadas fraudulentas, e os textos fraudulentos tornaram-se predominantes[21]. O Ofcom realiza também pesquisa sobre chamadas indesejadas para medir sua frequência junto aos consumidores do Reino Unido. Coletam-se dados sobre estes tipos de chamadas, incluindo a data, hora e duração das chamadas indesejadas, e uma descrição completa da experiência; ou seja, a empresa/pessoa que ligou, sobre o que era a chamada e se o número de telefone do chamador era identificável[22].	Parcial
Oferta de Soluções Anti-*spam* aos Consumidores	O OFCOM e o ICO estimulam às prestadoras para que criem e ofereçam aos seus usuários soluções e funcionalidades para bloquear as chamadas indesejadas.	Não

Reino Unido (vide Anexo B para maiores informações)		
Medida	*Descrição*	*Há similar no Brasil?*
Novas regras para proteger os consumidores	**Novas Regras.** O Ofcom editou novas diretrizes para proteger os consumidores. Abaixo estão resumidas as principais normas e determinações: (i) proibir as prestadoras de telefonia de cobrar dos clientes pela exibição de informações das chamadas, um serviço que ajuda as pessoas a identificar chamadas indesejadas; (ii) os números de telefone exibidos no visor das pessoas que recebem as chamadas devem ser válidos e permitir o retorno das chamadas; (iii) as prestadoras de telefonia devem tomar medidas para identificar e bloquear chamadas com números inválidos – uma característica de muitas chamadas indesejadas – de modo que não cheguem aos consumidores; (iv) o Ofcom agora também pode retomar os blocos de numeração das prestadoras, caso identificado uso sistemático desses recursos de numeração para a prática de chamadas de *robocall* e tentativas de golpe ou fraude.	Parcial
Conscientização do Consumidor	**Guia para o Usuário.** Este guia fornece dicas e indica alternativas para reduzir o número de chamadas indesejadas, além de oferecer conselhos sobre o que fazer ao recebê-las[23].	Parcial
Lista de Não Originar Chamadas	***Do-Not-Originate list* (DNO).** A lista contém os números que não realizam chamadas, indicados como tais ao Ofcom por empresas e entidades do sistema financeiro britânico e órgãos governamentais, por exemplo. A Lista DNO combate a falsificação de números (*spoofing*). Golpistas podem alterar deliberadamente a identificação da origem da chamada, para ocultar sua identidade ou imitar o número de uma empresa real, e assim induzir as pessoas a pensar que a chamada é de uma fonte confiável, como seu banco. Como esses números não fazem ligações e é o consumidor quem inicia a chamada, ele terá certeza de estar falando com o centro de atendimento do seu banco, por exemplo. Em 2020, foram adicionados 361 números a esta lista. A lista agora está sendo adotada por reguladores de outros países, como a Austrália.	Não

Reino Unido (vide Anexo B para maiores informações)		
Medida	*Descrição*	*Há similar no Brasil?*
Formação de Grupo Estratégico em busca de soluções técnicas para o problema	***Strategic Working Group* (SWG).** Em 2015, o Ofcom formou um grupo de trabalho estratégico composto por nove grandes provedores de comunicações, para explorar medidas técnicas para reduzir o impacto das chamadas inoportunas. Tendo identificado características específicas (perfis) das chamadas indesejadas, os membros do SWG medem o tráfego de chamadas que se encaixa nessas características e enviam um relatório sumarizado mensal ao Ofcom. Essas informações são utilizadas pelo regulador para subsidiar seu trabalho de fiscalização. O resumo também é compartilhado com os membros do SWG. A partir do final de 2018, a maioria dos provedores de comunicações deste grupo estão bloqueando rotineiramente chamadas problemáticas dentro da rede e/ou oferecendo aos seus clientes um serviço gratuito para bloquear ou desviar chamadas problemáticas. Esses esforços estão reduzindo o número de chamadas incômodas recebidas.	Parcial
Filtragem de SMS	***SMS Filtering*.** Prestadoras de telefonia móvel introduziram ou estão em processo de introdução de soluções tecnológicas que podem detectar as principais características presentes nos textos fraudulentos trafegando por suas redes, permitindo que bloqueiem mensagens suspeitas. As operadoras de rede móvel também usam detalhes de mensagens e chamadas fraudulentas relatadas ao número específico para denúncias 7726, utilizado para identificar os golpes mais recentes.	Não
Banco de Dados sobre Números Bloqueados	***Blocking List*.** O Ofcom também gerencia um banco de dados que utiliza para compartilhar com o setor os números bloqueados pelo próprio regulador e pelas prestadoras. Estes são números identificados, nos relatórios mensais consolidados pelo Ofcom e de outras fontes, como tendo gerado um grande número de chamadas indesejadas. O Ofcom também compartilha lista de números 'protegidos' e reservados para uso futuro, que podem ser bloqueados sem risco de interferir no tráfego de chamadas legítimas. Nenhum originador de chamada tem o direito de usar esses números e, portanto, quaisquer chamadas que os apresentem são, por definição, ilegais e indesejadas.	Não

Reino Unido (vide Anexo B para maiores informações)		
Medida	*Descrição*	*Há similar no Brasil?*
Estímulo a fabricantes de celular que desenvolvam dispositivos e software de bloqueio	**Estímulo a iniciativas privadas**. O Ofcom busca que cada vez mais telefones celulares também ofereçam filtragem ou bloqueio automatizados de chamadas indesejadas. Eles usam ferramentas de análise de dados, com base em sinalização de rede e informações de *crowdsourcing*, para determinar os números que provavelmente estão associados a chamadas indesejadas e bloquear chamadas originadas desses números.	Não
Iniciativa de Detecção de Fraude pelo setor de Telecomunicações[24]	***The Telecommunications Fraud Sector Charter***[25]**.** Iniciativa liderada pelo setor, que se comprometeu a trabalhar com o governo para reduzir a ameaça crescente de golpes/fraude**.** Tal projeto inclui uma série de ações: ▪ uso de verificação em tempo real para combater fraudes que envolvem a troca de *SIM CARDS*: as prestadoras forneceram às empresas financeiras um procedimento em tempo real que identifica se um telefone celular foi recentemente sujeito a uma troca de SIM CARD. Isso permite que as financeiras verifiquem quaisquer correlações entre atividades financeiras suspeitas e a troca de SIM CARD, o que pode indicar uma tentativa de fraude. ▪ compartilhamento de informações setoriais: as prestadoras devem compartilhar informações para ajudar a detectar e reduzir fraudes. O objetivo é que esse compartilhamento de informações seja estendido às autoridades policiais e às financeiras. ▪ melhor apoio às vítimas: as prestadoras devem trabalhar com grupos de apoio às vítimas para entender as preocupações e identificar as melhores práticas que podem ser adotadas.	Não
Métricas de Chamadas e procedimentos operacionais	**Definição de Métricas e Procedimentos.** Impõe controles sobre o volume de mensagens de texto que pode ser enviado em um período especificado, e limita o número de cartões SIM que podem ser vendidos, por transação, em varejistas on-line. Há ainda o monitoramento do volume de chamadas feitas de números diferentes, bem como outras métricas associadas.	Parcial

Reino Unido (vide Anexo B para maiores informações)		
Medida	*Descrição*	*Há similar no Brasil?*
Troca de Informações Estratégicas	***Unsolicited Communications Enforcement Network* (UCENET)**[26]. O objetivo desta Rede é promover a cooperação internacional no combate a comunicações indesejadas e abordar problemas relacionados a *spam, scam, phishing, smishing* e disseminação de vírus. Os participantes também abrem o Plano de Ação para a participação de outros órgãos públicos e governamentais interessados e de representantes do setor privado, como forma de expandir a rede de entidades engajadas na cooperação contra comunicações indesejadas. Algumas entidades membros: FTC/US, CRTC/Canada, ACMA/Australia, KISA/Coreia, NZDIA/ Nova Zelândia. **Operação Linden:** O ICO lidera a Operação Linden, um grupo que inclui reguladores, grupos de consumidores, associações comerciais e empresas do setor, que trabalham juntos para compartilhar inteligência e identificar oportunidades para lidar com chamadas indesejadas.[27]	Parcial
Proteção da Identificação (IDs) de Remetentes de SMS	***SMS PhishGuard*.** Em 2018, o Ofcom apoiou as prestadoras móveis por meio da *Mobile UK* e do *Mobile Ecosystem Forum* (MEF), em projeto para lidar com SMS fraudulentos, com base na proteção de identificação (IDs) de remetentes (*Sender IDs*). Esta iniciativa desenvolveu um Cadastro de Proteção de Identificação de Remetentes, envolvendo o setor bancário e órgãos governamentais, onde os participantes poderiam registrar e proteger os cabeçalhos das mensagens utilizadas no envio de textos aos consumidores. O registro dificulta que os golpistas enviem comunicação de texto se passando por uma empresa/entidade com sua "marca" registrada na base, pois há verificação do cabeçalho. O MEF informou em 2021 que existem mais de 70 marcas bancárias e governamentais protegidas pelo registro, com mais de 1.500 variantes não autorizadas sendo bloqueadas, incluindo 300 IDs de remetentes relacionados à campanha de coronavírus do governo**.**	Não

Reino Unido (vide Anexo B para maiores informações)		
Medida	*Descrição*	*Há similar no Brasil?*
PROPOSTA[28] – Introdução de padrões técnicos que permitam que a rede de origem da chamada confirme a autenticidade do chamador	***Improving the accuracy of Calling Line Identification (CLI) data***. Ter processos que detectem e bloqueiem números com informações adulteradas ou falsificadas, de forma mais abrangente, é fundamental para lidar com chamadas fraudulentas. *Calling Line Identification* (CLI) é o dado que permite identificar o número de onde uma chamada pode ser feita ou para o qual uma chamada de retorno pode ser feita. As principais ações da proposta: ▪ estabelecer que o formato de uma CLI deve ser um número de 10 ou 11 dígitos; ▪ determinar que o uso de alguns conjuntos de informações que identificam números não devem ser usados como CLI: como informações de alocação de numeração do Ofcom e da lista *Do Not Originate* (DNO); ▪ identificar chamadas originadas no exterior que não possuam CLI válido e bloqueá-las; e ▪ identificar e bloquear chamadas do exterior falsificando a CLI do Reino Unido. O Ofcom planeja emitir uma consulta pública para contribuições no quarto trimestre de 2022, buscando opiniões sobre o papel da autenticação do CLI e o que seria necessário para implementar a tecnologia em todo o setor (inclusive com a possibilidade de adotar protocolos STIR/SHAKEN).	Em avaliação
PROPOSTA[29] – Guia de boas práticas para uso de numeração por provedores de telecomunicações	***Good practice guide to help prevent misuse of sub-allocated and assigned numbers*.** O guia proposto define as etapas que se espera que as prestadoras tomem para ajudar a evitar o uso indevido de números válidos. Principais medidas propostas em Consulta Pública: ▪ realizar um conjunto robusto de verificações de *due diligence* antes de subalocar ou atribuir números; ▪ ter uma abordagem para identificar onde os riscos de uso indevido de números são maiores; ▪ estabelecer controles contratuais que permitam ao provedor cumprir suas obrigações regulatórias; ▪ manter o nível de risco representado por um cliente empresarial sob revisão, monitorando o potencial uso indevido de números; e ▪ ter um processo apropriado para responder a relatos de uso indevido potencial.	Não

2.3 AUSTRÁLIA

Austrália (vide Anexo C para maiores informações)		
Medida	*Descrição*	*Há similar no Brasil?*
Lista de Não Perturbe	***Do-Not-Call Register* (DNCR)[30].** O *Do-Not-Call Register (DNCR)* australiano possui, em outubro de 2022, aproximadamente 12,2 milhões de registros de números de telefone fixo, móvel ou fax. As pessoas podem se registrar por formulário na Internet ou pelo telefone da central de atendimento. O cadastramento é gratuito e, uma vez registrado, o número permanece na lista indefinidamente se titular ou seu representante não solicitarem a exclusão. Além do público em geral, podem ser cadastrados no *Do-Not-Call Register* números das entidades de governo e serviços de emergência. A partir de 30 dias do registro, operadoras de telemarketing não podem mais entrar em contato com números inscritos na lista. Elas têm também a obrigação de comparar suas *mailing lists* ao DNCR. Especificamente para a realização desse procedimento, as empresas de telemarketing devem criar cadastro e assinar o serviço.	Sim
Multas[31]	**Sanções mais severas.** Em maio de 2022, o *Wine Group* pagou US$ 204.240 em multas por violar as leis de *spam* e telemarketing. Em julho de 2022, a empresa *Latitude Finance Australia* foi multada em US$ 1.549.560 por envio de e-mails de marketing e SMS sem consentimento ou sem um recurso funcional de cancelamento de assinatura. Pelo mesmo motivo, a empresa *Sportsbet Pty Ltd* foi multada em US$ 2.508.600.	Não

Austrália (vide Anexo C para maiores informações)		
Medida	*Descrição*	*Há similar no Brasil?*
Plano de Ação para o Enfrentamento do Problema de Ligações Fraudulentas	***Action Plan to Reduce Scam Calls***[32]. O Plano tem três pontos principais: (*i*) Estabelecimento do STAT. (*Scam Telecommunications Task Force*). para promover a coordenação do governo, indústria e operadores na supervisão de estratégias para minimizar as chamadas fraudulentas; (*ii*) Desenvolvimento de obrigações aplicáveis para as prestadoras de telecomunicações para detectar, rastrear, bloquear e interromper chamadas fraudulentas. Há também iniciativas como a publicação do *Reducing Scam Calls Industry Code 2020* e do *Phone Scam Educational Resource,* para aumentar a conscientização do setor, dos consumidores e da sociedade como um todo sobre as fraudes telefônicas e como combatê-las; (*iii*) Testes imediatos de iniciativas de redução de golpes em todo o setor (nesse contexto, as prestadoras de telecomunicações testaram ideias de redução de golpes e bloquearam mais de 30 milhões de chamadas de golpes em 2020).	Parcial
Novas Regras	Foram criadas regras para proteger os consumidores de golpes que visam interações de clientes com sua empresa de telecomunicações. Regras da ACMA sobre verificações de identidade para celulares pré-pagos: as prestadoras de telecomunicações devem verificar a identidade ao ativar um serviço móvel pré-pago. Isso inclui a mudança de SIM Cards para novos dispositivos. Tais regras também valem para a portabilidade numérica[33].	Sim
Alertas	(i) Alertas ao público sobre golpes envolvendo investimentos financeiros e golpes de kits de teste COVID-19; (ii) Alertou-se os consumidores sobre os golpistas que enviavam SMS e mensagens de e-mail de entrega de encomendas com links de aparência incomum ou solicitações para pagar uma taxa para concluir a entrega; (iii) 861 alertas de conformidade enviados a empresas que comercializam produtos de serviços financeiros, notificando-as sobre possíveis problemas de conformidade com leis de *spam* e telemarketing.	Parcial
Bloqueio de chamadas fraudulentas	Desde que as novas regras de combate às chamadas fraudulentas entraram em vigor (em dezembro de 2020), mais de 660 milhões dessas chamadas foram bloqueadas (até junho 2022).	Parcial

Austrália (vide Anexo C para maiores informações)		
Medida	*Descrição*	*Há similar no Brasil?*
Novas frentes relacionadas a comunicações não solicitadas	Para o período 2022-2023, foram estabelecidas duas novas frentes relacionadas a comunicações não solicitadas: (i) Combate a golpes de telefone por SMS e de roubo de identidade, com a aplicação das novas regras de verificação de identidade; (ii) Aplicação de novas regras de cancelamento de assinatura de SMS e e-mail.	Não
Monitoramento ativo	As reclamações dos consumidores são utilizadas como fonte de informação direta para as ações da ACMA e ajudam a identificar problemas e analisar tendências. Também são fornecidos dados sobre as reclamações dos consumidores às empresas de telecomunicações, para ajudá-las a identificar e bloquear chamadas fraudulentas. As reclamações mais comuns envolvem ofertas de varejistas, serviços financeiros e setores de construção/manutenção.	Parcial

Austrália (vide Anexo C para maiores informações)		
Medida	*Descrição*	*Há similar no Brasil?*
Revisão do Código Industrial C661:2022 que tem por objetivo a redução de chamadas fraudulentas e SMS fraudulentos	***CI C662:2022***[34]. Estabelece métricas e padrões de chamadas para identificação de chamadas fraudulentas: De acordo com o Código, tais chamadas têm perfis de comportamento com as seguintes características: (i) alto volume de um número (CLI – *Calling Line Identification*) específico ou intervalo de CLIs; (ii) curta duração; (iii) número de origem não admite retorno da ligação; (iv) número de origem com o CND (*Calling Number Display*) com restrições; (v) número de origem está em um intervalo atribuído a uma prestadora diferente e/ou não foi portado para a responsável pela originação; (vi) número de origem não está em conformidade com a recomendação E.164 da UIT-T; (vii) número de origem de uma chamada internacional usando um número nacional; (viii) nenhum número de origem designado par o chamador de origem de uma chamada internacional; (ix) volumes anormalmente altos de tráfego em um serviço de transporte que geralmente não possui tais características em sua operação normal; (x) números associados ao recebimento de reclamações de consumidores que informam sobre ligações telefônicas que buscam informações utilizadas para fins de fraude, ou relatando que o consumidor sofreu golpe; (xi) reclamações de consumidores informando que seu número telefônico foi sujeito ao *CLI Spoofing*; (xii) reclamações a agências governamentais afetas sobre o uso de uma CLI de origem específica para a realização chamadas fraudulentas; e (xiii) os detalhes do CND são inválidos ou o número apresentado como CLI da origem é válido, mas foi sujeito a falsificação de CLI.	Não
Conscientização do Consumidor	**Informações educacionais sobre chamadas e SMSs fraudulentos.** Prestadoras de telecomunicações precisam disponibilizar material de orientação para clientes (em especial os tipos de fraudes mais comuns, ferramentas que os clientes podem usar para minimizar os riscos, bem como melhores práticas sobre o assunto)[35]. Nesse esforço, é importante deixar claro aos usuários quais são os canais de reclamação que estão disponíveis especificamente para tratar desse problema.	Parcial

Austrália (vide Anexo C para maiores informações)		
Medida	*Descrição*	*Há similar no Brasil?*
Melhorar a precisão do número de origem de chamadas locais	As prestadoras de telecomunicações responsáveis pela originação das chamadas devem impedir o uso de numeração sobre a qual o originador não possui o direito de uso. As prestadoras não devem encaminhar chamadas para operadores internacionais sem o número de origem As prestadoras não devem enviar chamadas para operadoras internacionais com um CLI que não esteja em conformidade com a Recomendação ITU-T E.164, a menos que o CLI esteja associado a um serviço de roaming móvel de entrada internacional ou outro formato seja acordado diretamente com o operador internacional. As prestadoras não devem enviar chamadas para usuários em sua própria rede de telecomunicações, para as prestadoras de transporte ou prestadoras de terminação se os números reservados 13, 1300, 1800 e 1900 estão sendo usados como número de origem.	Parcial
Melhorar a precisão do número de origem de chamadas internacionais	As prestadoras de transporte australianas devem enviar o número de origem internacional de chamadas internacionais conforme recebido do ponto de interconexão entre operadores internacionais. Quando o número de origem não estiver em conformidade com a Recomendação ITU-T E.164, nem com a Recomendação ITU-T E.157 (*International Calling Party Number Delivery*), essas chamadas devem ser avaliadas como potenciais chamadas fraudulentas. As prestadoras não devem encaminhar chamadas internacionais para usuários em sua própria rede de telecomunicações se a identificação de origem da chamada internacional usar um número australiano, salvo casos específicos de exceção previstos na regulamentação. As prestadoras não devem encaminhar chamadas internacionais para usuários em sua própria rede de telecomunicações se a CLI da origem não foi fornecida pelo operador internacional.	Não
Combate à falsificação de Identificação da linha de origem (CLI)	Caso seja identificada a falsificação de numeração de origem, a prestadora de origem deve fornecer informações sobre a falsificação à ACMA, em sistema eletrônico específico. Se uma prestadora identificar indícios de falsificação de CLI em chamadas recebidas de outras prestadoras, ela deve encaminhar a possível suspeita para o prestador de origem, com cópia para o ACMA. O processo deve ser repetido por todas as prestadoras envolvidas no trânsito da ligação, até chegar na prestadora de origem da ligação.	Em avaliação

Austrália (vide Anexo C para maiores informações)		
Medida	*Descrição*	*Há similar no Brasil?*
Monitoramento de chamadas fraudulentas	As prestadoras devem monitorar suas redes para chamadas fraudulentas com base nas características gerais descritas anteriormente, observando que essas características não são exaustivas ou restritivas em termos do monitoramento que possa ocorrer. Quando ocorrer uma notificação de possibilidade de fraude, por outras prestadoras ou por agências governamentais afetas, a prestadora deve apurar o ocorrido.	Parcial
Troca de informações sobre supostas chamadas fraudulentas	Se uma prestadora identificar indícios de chamadas fraudulentas em chamadas provenientes de outras prestadoras, ela deve notificar e fornecer detalhes à prestadora responsável e à ACMA, de modo a permitir que a análise tenha início o mais rápido possível. A notificação deve conter: (a) a data e hora (com deslocamento UTC) do suposto ilícito; (b) a CLI usada para as chamadas fraudulentas; (c) o número de possíveis chamadas fraudulentas identificadas no período; e (d) outras provas e informações, se solicitadas pela prestadora de origem ou de trânsito, para suportar as alegações. Após as investigações, os resultados devem ser compartilhados entre as prestadoras e a ACMA.	Não
Rastreamento de chamadas fraudulentas	Uma prestadora deve implementar processos e soluções que permitam rastrear a origem de possíveis chamadas fraudulentas, se originadas em sua própria rede ou se estiver atuando no transporte ou terminação da chamada. De acordo com as disposições da Lei de Proteção de Comunicações e do Código Penal australiano, as prestadoras devem cooperar entre si na prevenção, investigação e mitigação de chamadas fraudulentas que estão usando seus serviços de transporte.	Parcial
Bloqueio de Chamadas Fraudulentas	Quando as suspeitas de chamadas fraudulentas são confirmadas, as prestadoras de origem devem, o mais rápido possível, tomar medidas para bloquear as chamadas originadas e/ou transportadas em sua rede. Quando uma prestadora tiver uma considerável certeza de que detectou chamadas fraudulentas (com base em certas características e perfis, conforme informações do código CI C662:2022, acima), ela poderá bloquear o número associado a essas chamadas fraudulentas. Quando uma prestadora puder identificar o IMEI do dispositivo que está sendo usado repetidamente para enviar chamadas fraudulentas, mesmo que usando números diferentes ou múltiplas identificações, <u>pode restringir o uso desse dispositivo bloqueando o uso do seu IMEI em todos as operadoras de celular da Austrália, sem aviso prévio.</u>	Parcial

Austrália (vide Anexo C para maiores informações)		
Medida	*Descrição*	*Há similar no Brasil?*
Desbloqueio de Números	Quando um número não estiver mais sendo usado para chamadas fraudulentas nem estiver sujeito a falsificação de CLI, a prestadora deve tomar as medidas para desbloquear esse número o mais rápido possível. Quando um número é bloqueado incorretamente, a prestadora deve tomar medidas para desbloquear esse número o mais rápido possível e notificar a ACMA.	Não
Cooperação internacional	**Colaboração com Operadores Internacionais.** Quando um número significativo de chamadas fraudulentas é identificado como de origem internacional, as prestadoras devem usar dos acordos contratuais disponíveis para garantir a assistência do operador internacional em questão. Com isso, as chamadas fraudulentas direcionadas à Austrália devem ser interrompidas e as autoridades notificadas.	Parcial
Impedir o uso de números australianos para chamadas fraudulentas	Quando uma prestadora identificar que um número está sendo usado para perpetrar (ou tentar perpetrar) um golpe com o objetivo de obter uma resposta por meio de um retorno de chamada de voz ou retorno de SMSs, a prestadora envolvida deve notificar a prestador para a qual o número australiano encontra-se atribuído, tão logo quanto possível. A prestadora detentora do número australiano deve investigar e determinar se o número está sendo usado para perpetrar (ou tentar perpetrar) golpes ou fraudes. Em caso positivo, ela deve: (a) tomar medidas para impedir o uso do número australiano; e (b) informar os detalhes à ACMA sobre o uso do número (incluindo, sempre que possível, a CLI da origem) via sistemas eletrônicos próprios.	Não

2.4 ÍNDIA

Índia (vide Anexo D para maiores informações)		
Medida	*Descrição*	*Há similar no Brasil?*
Registro Nacional de Preferências do Consumidor	***National Customer Preference Register***[36]. As opções de preferência sobre o recebimento de chamadas incluem:(i) categorias de comunicação comercial, (ii) modos de comunicação, (iii) faixas de horários, (iv) dias da semana, incluindo feriados públicos e nacionais. De acordo com a regulamentação indiana, as opções para cadastrar, modificar ou cancelar o registro das preferências do consumidor incluem: (i) envio de SMS para o *short code* 1909; (ii) ligar para 1909; (iii) Sistema Interativo de Resposta de Voz (IVRS); (iv) aplicativo móvel, desenvolvido pelo regulador ou terceiro aprovado por ele; (v) portal *web* com autenticação via OTP; ou (vi) quaisquer outros meios escolhidos pelo regulador. **Código de Conduta para Preferência e Revogação de Consentimento**: estabelece as práticas e procedimentos para a indicação de preferências e revogação de consentimentos (COP-Preferência[37]), desenvolvido pelas próprias prestadoras, com referência ao Anexo II do TCCCPR, de 2018. Toda prestadora é obrigada a cumprir os COPs (autorregulação), contanto que não possuam inconsistências com a regulamentação expedida pela autoridade reguladora.	Sim
Bloco de Numeração Específico para Comunicação Comercial	Os indianos podem facilmente identificar as chamadas de telemarketing, pois todas elas começam com o prefixo “140” e são seguidas por 7 dígitos (formato 140XXXXXXX). Os dígitos também informam a localização de origem. Os seis primeiros números identificam o provedor e a área de atendimento. Por exemplo, a série 140003 pertence ao fornecedor Aircel Ltd. na área de serviço de Delhi. A série 140108 pertence à Loop Telecom Ltd., também na área de serviço de Delhi. É proibido o uso de numeração “comum” de celular para atividades de telemarketing. Caso um desses números seja utilizado para enviar mensagens promocionais, ele será suspenso já na primeira reclamação e poderá ser incluído numa lista negra por até dois anos[38].	Sim

Índia (vide Anexo D para maiores informações)		
Medida	*Descrição*	*Há similar no Brasil?*
Sistema de *Blockchain* para Combate a Comunicações Indesejadas	A Autoridade Reguladora de Telecomunicações da Índia (TRAI) anunciou uma diretiva sob os Regulamentos TCCCP (*Telecom Commercial Communications Customer Preference*) para implementação de uma plataforma habilitada para a tecnologia *Blockchain.* Ela foi parcialmente implementada em 1º de junho de 2020. Ela permite que apenas as empresas autorizadas pelos consumidores possam enviar mensagens. Os processos acordados pelas prestadoras de telecomunicações exigem que cada remetente, incluindo os operadores de telemarketing registrados, sejam verificados pelas prestadoras de telecomunicações antes de ser aceito na plataforma. Mensagens ou chamadas podem ser enviadas apenas por entidades cadastradas na plataforma.	Não
Verificação das Preferências dos Usuários	A prestadora de telecomunicações de envio do texto ou de origem da chamada realiza uma depuração prévia para checar os dados da comunicação comercial frente aos consentimentos e às preferências do usuário de destino. Ela armazena os dados do procedimento de verificação no *blockchain* para que a prestadora de destino da comunicação possa verificar se a depuração aconteceu e o resultado foi favorável. A mensagem só é encaminhada ao destinatário se estiver tudo confirmado.	Não
Reclamações dos Usuários	Os consumidores podem registrar reclamações, que são inseridas no *blockchain*, e a empresa de telecomunicações que enviou a mensagem deve investigar imediatamente e restringir a empresa de telemarketing bem como a empresa de comunicação comercial de origem, se o assinante não forneceu consentimento para a comunicação eletrônica. Se não o fizer ou atrasar, estão previstas multas pesadas para prestadora de telecomunicações e pode-se chegar até a perda da licença.	Não

Índia (vide Anexo D para maiores informações)		
Medida	*Descrição*	*Há similar no Brasil?*
Obrigações para Empresas de Telemarketing e Empresas que Desejam Enviar Mensagens de Comunicação Comercial	Existe um cadastro obrigatório para os operadores de telemarketing e as empresas que desejam enviar comunicações comerciais eletrônicas. Os operadores de telemarketing devem enviar mensagens de comunicação comercial em conformidade com as preferências constantes dos cadastros dos consumidores. Foram criados cabeçalhos separados para mensagens de oferta e promocionais. Também foram criadas séries de númeração separadas para chamadas de voz para atividades de telemarketing. Estão previstas severas sanções financeiras para as empresas de telemarketing e prestadoras de telecomunicações por descumprimento das normas. Além das sanções financeiras, os recursos de telecomunicações podem ser bloqueados e excluídos da rede, e os responsáveis pela realização de atividades de telemarketing que não estão cadastrados na plataforma podem ficar em uma lista negra por até dois anos.	Não

Índia (vide Anexo D para maiores informações)		
Medida	*Descrição*	*Há similar no Brasil?*
Aplicativos de Governo para Bloqueio de Comunicações Indesejadas	A agencia reguladora da India, TRAI, também desenvolveu um aplicativo que permite que usuários de *smartphones* registrem seu número de celular na lista nacional de Não Perturbe (DND). Ela incluiu as comunicações comerciais não solicitadas (UCC), as chamadas de telemarketing ativo e os SMSs. Seu funcionamento é suportado pelo Regulamento de Preferência do Cliente de Comunicação Comercial de Telecomunicações (TCCCP), expedido pela TRAI em 2018[39]. Como principais funções do aplicativo destacam-se: (i) definição das preferências de DND; (ii) reclamações à prestadora sobre recebimento de UCC; (iii) verificação do status e acompanhamento das reclamações apresentadas à prestadora. O aplicativo requer permissão para acessar o catálogo de endereços do smartphone, necessária para distinguir entre chamadas/mensagens provenientes dos contatos cadastrados e aquelas de operadores de telemarketing desconhecidos. A lista de contatos do dispositivo não é compartilhada no *back-end* nem de qualquer outra maneira. A Política de Privacidade do aplicativo pode ser lida na página do regulador indiano[40]. A versão mais recente do aplicativo trouxe os seguintes recursos adicionais: (i) Mecanismo inteligente de detecção de *spam* (somente para SMS) para auxiliar o assinante na geração de denúncias; (ii) *Crowdsourcing* de dados sobre mensagens e chamadas ofensivas para acelerar a detecção de operadores de telemarketing não registrados; (iii) Atualizações sobre ações tomadas em reclamações dentro do App; (iv) Interface e configuração mais fáceis.	Não

2.5 CANADÁ

Canadá (vide Anexo E para maiores informações)		
Medida	*Descrição*	*Há similar no Brasil?*
Lista de Não Perturbe	***National Do-Not-Call List* (DNCL)**[41]. Em operação desde 2008, a DNCL registrou a inclusão de 14.291.077 de números e 56.611 cancelamentos de registro. Somente no último ano fiscal, os canadenses registraram 206.035 números de telefones fixos, celulares e linhas de fax — uma média de mais de 564 números por dia. Os operadores de telemarketing e as empresas clientes delas são obrigados a participar do DNCL de duas maneiras, fazendo cadastramento na plataforma e assinando o serviço. Em 2020-2021, 1.082 novos operadores de telemarketing registaram-se no Operador Nacional DNCL. Já existem mais de 22.766 empresas de telemarketing cadastradas, sendo 829 estrangeiras.	Sim
Autenticação do Identificador de Chamadas (STIR/SHAKEN)	Em decisão de abril de 2021, a Comissão Canadense de Radiotelevisão e Telecomunicações – CCRT, por meio do *Compliance and Enforcement and Telecom Decision CRTC 2021-123*[42], estabeleceu a obrigatoriedade do uso da tecnologia STIR/SHAKEN, em efeito a partir de 30 de novembro de 2021. O objetivo é autenticar e verificar as informações de identificação do chamador (ID), nas chamadas de voz baseadas no protocolo Internet (IP), como condição para oferecer e fornecer serviços de telecomunicações. Além disso, a Comissão determinou que as prestadoras de serviços de telecomunicações apresentem, até 31 de agosto de 2021, relatórios sobre implementação e avaliação da prontidão para os protocolos STIR/SHAKEN.	Em avaliação
Obrigações para os Operadores de Telemarketing	Todos os operadores de telemarketing que realizam atividades em seu próprio nome ou em nome de seus clientes devem aderir às regras. As principais determinações estão consolidadas abaixo: • identificar quem são e, mediante solicitação, fornecer os contatos por meio dos quais seja possível falar sobre as ligações de telemarketing; • exibir o número do telefone originador, ou um número de contato, por meio do qual o consumidor possa falar com o responsável pela ligação; e • ligar ou enviar mensagem apenas entre 9h e 21h30 durante a semana, e das 10h às 18h nos fins de semana.	Não

Canadá (vide Anexo E para maiores informações)		
Medida	*Descrição*	*Há similar no Brasil?*
Mecanismos de Sancionamento	Os principais mecanismos adotados pela CRTC: ▪ cartas de advertência para pequenas violações; ▪ notificações que determinam a adoção de ações corretivas específicas; ▪ autos de infração, que são medidas formais de execução (estabelecidas na seção 72.07 da Lei de Telecomunicações) e podem acarretar multas administrativas pecuniárias; e ▪ acordos negociados de ajustamento de condutas, que são acordos formais entre as entidades que cometem violações e a CRTC. Como parte de um acordo, a entidade deve admitir responsabilidade, comprometer-se a parar de violar as regras, aceitar o auto de infração com uma sanção administrativa e desenvolver um programa de conformidade.	Sim
Multas	As violações podem resultar em multas (por violação) de até US$ 1.500 para indivíduos e até US$ 15.000 para empresas. Desde 2008, um total de US$ 10.716.930 foi aplicado em multas pecuniárias administrativas, pela CRTC, para infrações relacionadas às comunicações indesejadas.	Não
Cooperação Internacional	Até 2021, a CRTC estabeleceu 16 parcerias sobre o tema com organizações em todo o mundo. Esses acordos permitem que as agências envolvidas compartilhem informações e forneçam suporte investigativo, mediante solicitação e de acordo com a lei. Os MOUs estabelecidos também fornecem oportunidades de pesquisa e educação, bem como intercâmbios de pessoal e iniciativas de treinamento conjunto para as partes.	Parcial
Pilotos de Bloqueio de Chamadas com Tecnologia de Inteligência Artificial	Em 2021, a CRTC aprovou um teste de bloqueio de chamadas utilizando tecnologia de inteligência artificial, de modo a permitir que uma grande prestadora de telecomunicações consiga bloquear certas chamadas de voz fraudulentas e importunas. O teste resultou em um número significativo de chamadas fraudulentas bloqueadas com sucesso.	Não
Rastreamento de Chamadas Indesejadas até a Origem	A CRTC continua a apoiar o desenvolvimento de processos para rastrear chamadas indesejadas de volta ao seu ponto de origem, incluindo a aprovação de um projeto de teste de rastreamento, para facilitar os esforços de conformidade e fiscalização.	Parcial

2.6 SINGAPURA

Singapura (vide Anexo F para maiores informações)		
Medida	*Descrição*	*Há similar no Brasil?*
Registro de Não Perturbe	***Do Not Call (DNC) Registry***[43] *O registro foi criado para* disponibilizar aos consumidores de telecomunicações a opção por não receber mensagens de marketing indesejadas ou chamadas para o seu número de telefone. Há três grupos de bloqueio: chamadas de voz, mensagem de texto, mensagem de fax. Não estão incluídas no rol de bloqueio do DNC de Singapura: (i) mensagens de marketing ou chamadas de organizações com as quais você mantém um relacionamento contínuo, se as mensagens forem sobre produtos ou serviços relevantes para você. No entanto, o consumidor pode optar por não recebe-las, caso no qual elas deverão ser bloqueadas em até 21 dias corridos; (ii) mensagens que fazem parte de um estudo ou uma pesquisa de mercado; (iii) mensagens relacionadas a causas beneficentes ou religiosas; (iv) mensagens pessoais enviadas por indivíduos; (v) mensagens públicas enviadas por agências governamentais; (vi) mensagens políticas; e (vii) chamadas ou mensagens de telemarketing enviadas para uma empresa (ou seja, B2B).	Sim
Bloqueios de SMS	Desde 2019, as prestadoras de telecomunicações devem bloquear em suas redes os SMS com mensagens e URLs/sites identificados como maliciosos e fraudulentos. Os *links* nas mensagens SMS são verificados e comparados com um banco de dados de *links* maliciosos conhecidos. Se uma correspondência for detectada, a mensagem SMS é sinalizada e o banco de dados atualizado. Além disso, desde 2021, os agregadores de SMS bloqueiam mensagens fraudulentas com identificadores falsos (*Spoofing*).	Não

Singapura (vide Anexo F para maiores informações)		
Medida	*Descrição*	*Há similar no Brasil?*
Aplicativos de Governo para Bloqueio de Comunicações Indesejadas	O governo de Singapura, encabeçando uma colaboração entre o *National Crime Prevention Council* (NCPC), a *Open Government Products* (OGP) e a *Singapore Police Force* (SPF) desenvolveu um aplicativo chamado *ScamSchield*[44] com o objetivo de reforçar o combate a comunicações indesejadas. O aplicativo filtra as chamadas recebidas e mensagens de texto. Ele as compara com uma lista de números e perfis mantida pela SPF e pela *Comissão de Proteção de Dados Pessoais de Singapura* (PDPC). O aplicativo não filtra mensagens provenientes das pessoas da lista de contatos, ou contatos com os quais já ocorreram conversas. Quando um SMS de um contato desconhecido é recebido, o ScamShield utiliza um algoritmo que roda no próprio dispositivo se avaliar se é uma tentativa de golpe. No iOS, ele filtra as mensagens para uma pasta de lixo eletrônico. No Android, uma notificação é enviada aos usuários para notificá-los de que uma mensagem fraudulenta foi recebida. Os SMSs fraudulentos são copiados ao PDPC e à SPF para análise e atualização das bases.	Não
Bloqueio de Chamadas	Desde 2019, números locais usualmente utilizados em tentativas de golpe e fraude (como de agências governamentais locais e serviços de emergência, por exemplo) devem ser bloqueados quando de fontes ilegítimas. A partir de 2020, chamadas fraudulentas realizadas com o uso de soluções de *robocalls* passaram a ser mitigadas com soluções tecnológicas de reconhecimento de padrões. Além disso, as chamadas provenientes do exterior passaram a ser marcadas com um sinal "+", para alertar o público. Atualmente, está em planejamento a adoção de soluções para bloquear a falsificação de numeração local provinda de origens internacionais.	Parcial
Aplicativos de Terceiros	O regulador de Singapura recomenda a utilização de aplicativos de terceiros com funções semelhantes para bloquear chamadas e mensagens indesejadas: Dentre os principais aplicativos recomendados, destacam-se: (*i*) Truecaller[45], (*ii*) Hiya[46] , (*iii*) Robokiller[47], (*iv*) Nomorobo Robocall Blocking[48], e (*v*) Call Blacklist[49].	Parcial

Singapura (vide Anexo F para maiores informações)		
Medida	*Descrição*	*Há similar no Brasil?*
PROPOSTA[50] – Registro dos Emissores de SMS (*Sender ID*) Obrigatório	Um piloto para a implantação do Registro dos Emissores de SMS (SMS Sender ID Registry – SSIR) foi iniciado em agosto de 2021. No entanto, com o aumento de golpes usando SMS, o IMDA resolveu acelerar a adoção da solução, para março de 2022. Com a plataforma de registros, os SMS usando IDs falsificados ou inválidos já são preventivamente bloqueados, reduzindo-se os riscos de fraudes e golpes. Desde o seu lançamento, mais de 120 organizações do setor público e privado aderiram ao SSIR. Em comparação com os três meses anteriores, o número de casos de fraude por SMS relatados diminuiu três vezes desde o lançamento do SSIR[51]. Embora o SSIR tenha alcançado resultados positivos, ele continua sendo um sistema voluntário. As organizações devem optar por registrar seus IDs de remetente. O público ainda pode receber SMS falsificados, usando IDs de remetentes não registrados. Para criar recursos de prevenção de fraude mais fortes, a IMDA pretende tornar o registro SSIR um requisito obrigatório para organizações que usam IDs de remetente (ou seja, um regime de registro completo). A partir de então, apenas IDs de remetente registrados serão permitidos. Todos os outros IDs de remetente não registrados serão bloqueados por padrão, aumentando a segurança do canal de comunicação.	Não

Singapura (vide Anexo F para maiores informações)		
Medida	*Descrição*	*Há similar no Brasil?*
PROPOSTA[52] – Filtragem de SMS por Machine Learning	Outra proposta em discussão (em consulta pública, no caso) envolve alternativas para identificação e filtragem de mensagens fraudulentas. Essa filtragem seria realizada por meio de varredura automatizada, sem intervenção humana. O sistema, baseado em *machine learning*, procuraria identificar e filtrar mensagens SMS com base em padrões suspeitos presentes nas mensagens SMS, como palavras-chave, frases e formatos de mensagem (perfis) que normalmente são usados em mensagens SMS fraudulentas. Com o *machine learning*, serão avaliados padrões comuns e novos padrões característicos de golpes e mensagens SMS fraudulentas, acompanhando as táticas em evolução dos golpistas. Como parte do processo de aprendizagem, algumas mensagens SMS sinalizadas como suslpeitas podem ser submetidas a uma avaliação mais completa. Antes de serem encaminhadas para avaliação adicional, todavia, essas mensagens SMS suspeitas são anonimizadas pela máquina e, em seguida, encaminhadas para revisão de segundo nível pelo pessoal técnico da prestadora. Com o tempo, isso permitirá que a máquina desenvolva maior precisão e eficácia de filtragem. Esta revisão é exclusivamente para fins de melhoria do processo de aprendizado de máquina, não sendo permitidas outras finalidades. Além disso, as prestadoras de telecomunicações continuam a ter obrigações sob a Lei de Proteção de Dados Pessoais, inclusive para proteger quaisquer dados pessoais e não reter os dados pessoais por mais tempo do que o razoavelmente necessário para facilitar o aprendizado de máquina ou de outra forma que não seja autorizado por lei. Embora essa filtragem adicional de segundo nível não seja infalível, ela ajudará a mitigar ainda mais o risco para os consumidores.	Não
PROPOSTA[53] – Opção de Bloqueio de Chamadas e Textos Internacionais	Criar mecanismos para que os usuários tenham a opção de não receberem chamadas ou mensagem de texto internacionais.	Não

2.7 REGULAÇÃO COMUM EUROPEIA

A situação dos países membros da União Europeia não é diferente dos demais aqui discutidos. Diversos deles adotaram soluções do tipo "Não Me Perturbe" (*Do-Not-Call Registry*), ampliaram a regulamentação contra chamadas indesejadas e a aplicação de sanções contra tais práticas, bem como ativamente buscam, discutem e implementam diversas estratégias para conter o problema.

Na União Europeia, cada Estado-Membro possui seu próprio arranjo regulatório e conjunto de autoridades para regular e fiscalizar o cumprimento as normativas. Nesse quesito, as duas principais normativas são a *Directiva de Privacidade Eletrónica*[54] (*ePrivacy*, ou ePD) e o Regulamento Geral de Proteção de Dados da União Europeia (*European Union General Data Protection Regulation* – GDPR).

A ePD requer que o envio de correio eletrônico de telemarketing atenda a três critérios: (1) consentimento explícito ou implícito do destinatário; (2) inclusão dos contatos do remetente; e (3) inclusão de *link* para o cancelamento/exclusão da lista de contatos.

Ainda nessa linha, a ePD exige que as comunicações comerciais não solicitadas por máquinas automáticas de fax e correio eletrônico (ou seja, e-mail, SMS e MMS) estejam sujeitas ao consentimento prévio de seu destinatário (*opt-in*), se o destinatário for um indivíduo.

> ***Directiva de Privacidade Eletrónica* (ePD)**:
> Artigo 13º
> Comunicações não solicitadas
> 1. A utilização de sistemas de chamada automatizados sem intervenção humana (aparelhos de chamada automáticos), de aparelhos de fax ou de correio electrónico para fins de comercialização direta apenas poderá ser autorizada em relação a assinantes que tenham dado o seu consentimento prévio.

O escopo original de aplicação da ePD, em se tratando de comunicação eletrônica, não abrangia aplicativos de mensagens como o WhatsApp, Telegram, WeChat e outros. No entanto, com a adoção, pelos Estados-Membros, do *Código Europeu de Comunicações Eletrónicas* (*EU Electronic Communications Code* – EECC), os aplicativos passaram a ser obrigados a observar as regras.

Já em relação a comunicações comerciais não solicitadas realizadas por outros meios, como chamadas de voz não iniciadas por uma máquina automática de chamadas, os Estados-Membros são livres para escolher entre um regime de *opt-in* (usuário manifesta o interesse em receber a comunicação) ou *opt-out* (usuário manifesta o interesse em não receber), nos termos do artigo 13º, n.º 3, da mencionada *Directiva*.

> ***Directiva de Privacidade Eletrónica* (ePD)**:
> Artigo 13º
> Comunicações não solicitadas

> 3. Os Estados-Membros tomarão as medidas necessárias para assegurar que, por forma gratuita, não sejam permitidas comunicações não solicitadas para fins de comercialização direta em casos diferentes dos referidos nos n. 1 e 2 sem o consentimento dos assinantes em questão ou que digam respeito a assinantes que não desejam receber essas comunicações, sendo a escolha entre estas opções determinadas pela legislação nacional.

Levantamento realizado pela consultoria Cullen[55] mostra que todos os 15 países europeus pesquisados (Áustria, Bélgica, Bulgária, Rep. Checa, França, Alemanha, Irlanda, Itália, Holanda, Polonia, Romênia, Eslováquia, Espanha, Suíça, Suécia, Reino Unido) escolheram implementar um regime de *opt-in* para comunicações comerciais não solicitadas por máquina automática de chamadas, fax e correio eletrônico. Já o *opt-out* prevalece para chamadas de voz comerciais não automatizadas nos países europeus.

Adicionalmente, o artigo 13º, n.º 4, da *Directiva*, proíbe o marketing direto por correio eletrônico (e-mail, SMS e MMS) que: (1) oculte ou disfarce a identidade do remetente; (2) não inclua um endereço válido para o qual os destinatários possam enviar um pedido para cessar tais mensagens; ou (3) não respeita ou incentiva o destinatário a visitar um site eletrônico que não respeite os requisitos de informação estabelecidos no artigo 6 da *Directiva de Comércio Eletrónico* (*EU Electronic Commerce Directive – eCommerce*), sobre informações a serem fornecidas no contexto de uma comunicação comercial.

Já as comunicações comerciais realizadas no ambiente de aplicativos de comunicação OTT (ex.: WhatsApp, Telegram, Facebook Messenger etc.) são reguladas pela legislação específica de alguns países. É o caso de Bélgica[56], Itália[57], Holanda[58], Espanha[59] e Reino Unido[60]. Eles estabeleceram que as mesmas regras sobre comunicações comerciais não solicitadas também se aplicam aos aplicativos OTT.

No que concerne ao Regulamento Geral de Proteção de Dados (GDPR), é importante inicialmente esclarecer que, ao contrário do que ocorre com as *Directivas*, as regras do GDPR são juridicamente vinculantes para os Estados-Membros da UE.

Ele prevê a obrigatória coleta do consentimento explícito, retroativamente aplicável. Em outras palavras, os indivíduos que no passado deram seu consentimento implícito, mas não explícito, não podem mais ser contatados para receber comunicações de marketing (nas jurisdições onde isso é atualmente permitido). As multas seguem uma abordagem escalonada e as infrações mais graves podem chegar a 4% do faturamento global anual ou € 20 milhões, o que for maior. São responsabilizáveis tanto os controladores quanto os processadores de dados, o que significa que provedores de serviços em nuvem e similares não estão isentos de responsabilidade. Outrossim, a jurisdição se estende para incluir todas as empresas que controlam e processam dados de indivíduos residentes na UE, ainda que sediadas fora da União Europeia (que precisam nomear um representante na União Europeia).

3. CONSIDERAÇÕES SOBRE AS SOLUÇÕES ADOTADAS PELOS OUTROS PAÍSES

Como visto nas seções anteriores, o leque de soluções técnicas e regulatórias para coibir as insistentes ligações de telemarketing abusivo e as irritantes chamadas de *robocall* é extenso e variado. Ademais, o problema ocupa uma posição prioritária na pauta de órgãos reguladores e espaços governamentais do mundo inteiro, que despendem incontáveis horas de planejamento, coordenação e fiscalização buscando combatê-lo, com diferentes graus de sucesso.

As medidas regulatórias variam grandemente em termos de funcionalidades, complexidade, recursos necessários, resiliência e eficiência. Mesmo assim, apesar de possuírem tanta variedade e flexibilidade, há certamente alguns elementos-chave comuns permeando o racional por trás de cada escolha e implementação, que precisam ser reconhecidos e destacados antes de se proceder à discussão das soluções propriamente ditas.

3.1 OS PRINCIPAIS PREJUDICADOS SÃO SEMPRE OS CONSUMIDORES

Este é indubitavelmente um problema que afeta negativamente os consumidores dos serviços de telecomunicações (e suas variantes de comunicação *Over-the-Top*, em alguns casos). Como tal, o principal objetivo perseguido é o de se estabelecer um ambiente de conforto, confiança, segurança e respeito à vontade dos usuários, em particular o indivíduo comum, que possui o direito de não ser perturbado.

Este indivíduo comum, aliás, é a régua e o termômetro regulatório para a escolha e a dosimetria das soluções. Dessa forma, tendem a ser privilegiadas as soluções regulatórias que proporcionem melhor experiência, satisfação e alívio às dores dos usuários.

Adicionalmente, são usualmente buscadas soluções que:

1) provoquem o menor ônus/embaraço aos usuários;
2) sejam silenciosas e/ou transparentes para eles; e
3) não impliquem em atrasos significativos à comunicação, custos adicionais (de ligação, de equipamentos, de serviços, de computação ou outros recursos) ou na aprendizagem de novos processos de marcação e discagem pelos usuários originadores e destinatários de chamadas regulares e legítimas.

Outrossim, por se tratar da proteção dos interesses dos consumidores, são comuns relações e associações com a temática consumerista, seja por meio de vínculos aos arcabouços legais e regulatórios especializados, seja pela gravitação de agentes, órgãos e entidades ligados ao tema.

Outra temática de forte associação e interdependência, em especial mais recentemente, diz respeito à privacidade e à proteção dos dados pessoais dos consumidores, haja vista o valor

transacional das *mailing-lists* que possuem essas informações, bem como a sua imprescindibilidade para o cometimento de muitas das práticas de importuno, golpes e fraudes.

Cabe por fim mencionar um detalhe no mínimo curioso: os perpetradores das chamadas abusivas e tentativas de fraudes também são usuários das redes, serviços e equipamentos de telecomunicações. Por óbvio, eles não podem ser enquadrados na mesma categoria de suas vítimas. Trata-se, usualmente, de "grandes usuários" do ecossistema de telecomunicações, que possuem contratos corporativos e consomem volumes consideravelmente maiores de recursos das redes e sistemas. Ainda assim, continuam sendo usuários e devem, portanto, como todos os demais, respeitar as regras de uso adequado e responsável das redes e serviços.

3.2 A SOCIEDADE ESPERA QUE OS REGULADORES ATUEM PARA SOLUCIONAR O PROBLEMA

O órgão regulador do setor de telecomunicações (ou autoridade equivalente) é invariavelmente chamado a agir. Espera-se deles que se inteirem e dominem o problema, apresentem soluções eficientes e produzam resultados tangíveis de forma célere.

A bem da verdade, o grau de sucesso alcançado tem sido bem variado (vide seções anteriores). De toda sorte, os reguladores estão sempre no centro das discussões e geralmente servem de ponto focal para o tratamento do problema em nível nacional (embora haja exceções), além de serem responsáveis pela atividade fiscalizatória.

Importa mencionar que muitos reguladores também são diretamente ou indiretamente responsáveis pela implementação e manutenção de algumas soluções (como listas de Não Perturbe, coordenação da adoção de padrões STIR/SHAKEN etc.) e possuem canais de relacionamento para o registro de reclamações e denúncias dos usuários, por exemplo.

Há ainda o envolvimento de reguladores em vários casos de colaboração em nível nacional e internacional, com diferentes setores e organizações, bem como aqueles que criam forças tarefa e grupos de trabalho específicos para a adoção de medidas mais drásticas, tais como pronta contenção e bloqueio do tráfego de chamadas de *robocall*.

3.3 NÃO EXISTE BALA DE PRATA

Não existe panaceia, remédio milagroso que cura todas as doenças e alivia todos os sintomas. O elevado número de diferentes técnicas e abordagens empregadas para o combate do *spam* telefônico, bem como o fato de esse ser um problema notoriamente global, sistêmico e ainda sem solução definitiva, dão mostras do quanto seu tratamento é difícil, complexo, multifacetado e multissetorial.

Acrescente-se a isso o fato desse também ser um problema deveras dinâmico. Ele evolui e se alastra, muda de foco e de lugar. À medida que novas soluções técnicas e regulatórias surgem e se aperfeiçoam para miná-lo e contê-lo, novas formas de burlar as ações em prática também são descobertas e implementadas pelos infratores.

Por conta disso, muitas Administrações nacionais, legisladores e reguladores têm sistematicamente adotado múltiplos conjuntos de técnicas e arranjos regulatórios especificamente escolhidos por se complementarem e/ou possuírem sinergias entre si. Eles são então organizados e implementados em iterações sucessivas e faseadas (ou ondas). Mais adiante, neste Estudo, serão apresentados os conjuntos de soluções mais recorrentes e que mais se destacam.

A implementação de conjuntos de ações e soluções em frentes/fases sucessivas, aliás, é a abordagem que tem sido adotada no Brasil, onde são observadas até o momento da publicação desse estudo, a edição de três ondas de medidas regulatórias, por parte da Anatel, para coibir o telemarketing abusivo e as chamadas de *robocall* (vide respectivo Estudo[61] e Relatórios[1] para maiores informações).

Ainda em se tratando da dinamicidade do problema, tem se observado certo movimento dos *spammers* no sentido de busca por espaços menos regulados, principalmente o dos aplicativos de comunicação *Over-the-Top*. Essa já é hoje uma preocupação de diversas autoridades nacionais e supranacionais, e deve representar um desafio para os anos vindouros. A seção anterior, que relata a experiência regulatória europeia, dá mostras de como esse debate tem sido encaminhado.

3.4 A CONSCIENTIZAÇÃO E A EDUCAÇÃO DO CONSUMIDOR SÃO PARTES DA SOLUÇÃO

Diversas Administrações e reguladores têm enfatizado a importância da conscientização e da educação dos consumidores e do público em geral, além de grupos particularmente vulneráveis (como telemarketing abusivo e pernicioso dirigido para crianças, idosos, pessoas endividadas etc.).

Nos Anexos de cada país, acostados ao final deste Estudo, estão indicadas diversas iniciativas e materiais de referência sobre campanhas de informação de direitos e educação para o uso seguro dos serviços de telecomunicações.

3.5 É PRECISO COMBATER O *SPOOFING*

É bem conhecida a associação entre o telemarketing abusivo e as chamadas de *robocall, de um lado,* e a prática do *spoofing* telefônico do outro. Além de dificultar o discernimento do destinatário da chamada de telemarketing abusivo, o *spoofing* também é recorrentemente utilizado para uma série de golpes e fraudes, além da prática de outros crimes ainda mais graves, pois torna difícil e complexo, quando não impossível, o rastreamento da ligação telefônica.

Como se pôde observar na seção alhures que apresentou o artigo de Tu, Doupé e Zhao (2016), a principal preocupação quanto ao critério de robustez das técnicas básicas de combate ao *spam* telefônico está justamente relacionada ao quanto elas são resilientes face ao *Caller ID spoofing*. Ou ainda, face ao *spammer* ativamente utilizando-se de técnicas de *spoofing* e suas variantes para se elidir das técnicas de combate ao *spam*.

Na seção seguinte, restou evidenciado como diversas Administrações e reguladores elegeram o combate ao *spoofing* como essencial e prioritário para o endereçamento da situação e estão adotando uma série de medidas regulatórias para aprimorar os mecanismos de autenticação e verificação das informações das chamadas em suas redes telefônicas. Esse passo pode ser bastante complexo e custoso para o setor, por exigir atualização de padrões e sistemas, além de tratamento adequado às redes legadas. Todavia, a cada dia mais e mais reguladores parecem chegar à conclusão de que esse é um passo imprescindível no combate das chamadas indesejadas e fundamental para o aprimoramento da segurança das redes e serviços.

4. MEDIDAS REGULATÓRIAS MAIS UTILIZADAS

Nos últimos anos, diversos instrumentos têm sido utilizados pelos países que buscam enfrentar o problema de chamadas indesejadas. As cinco mais comumente empregadas são:

1) as listas de Não Perturbe;
2) uso de numeração específica para telemarketing;
3) alterações legais (por exemplo, proibindo as chamadas indesejadas e criminalizando a prática do *spoofing*);
4) adoção de padrões de autenticação e verificação de chamadas (como o STIR/SHAKEN); e
5) uso de aplicativos para bloqueio de chamadas indesejadas.

Logo abaixo, serão explorados alguns casos de aplicação dessas cinco mais utilizadas.

Além delas, também se destacam:

i. aplicação de multas e bloqueio dos usuários que fazem mau uso das redes;
ii. ações de monitoração e controle dos *gateways* internacionais; e
iii. medidas educacionais junto às prestadoras e empresas de telesserviços.

4.1 LISTAS DE NÃO PERTURBE

As listas de Não Perturbe contêm os números de telefone/contatos dos indivíduos que não desejam receber comunicações indesejadas (ligações telefônicas e, em alguns casos, mensagens de texto).

Elas estão presentes em diversos países: África do Sul (*Do not Contact List*[62]), Argentina (*No Llame registro nacional*[63]), Austrália (*Do Not Call Register*[64]), Brasil (*Não Me Perturbe*[65]), Canada (National Do Not Call List – DNCL[66]), Chile (*No Molestar*[67]), Colômbia (*Registro de Números Excluidos*[68]), Estados Unidos (*Do Not Call List*[69]), França (*Bloctel*[70]), Índia (*National Customer Preference Register*[71]), Itália (*Pubblico delle Opposizioni Register*[72]), Nigéria (*Do-Not-Distrub – DND*[73]), Reino Unido (*Telephone Preference Service*[74]), Singapura (*Do Not Call (DNC) Registry*[75]) dentre outros.

Vale destacar que além do cadastro por meio da página eletrônica (a única opção na implementação brasileira), diversos deles oferecem também canais alternativos para os usuários aderirem ou gerenciarem suas inscrições. Por exemplo, pelo envio de mensagens de texto para números específicos, ligações para números de bloqueio integral ou parcial das chamadas indesejadas, uso de Unidade de Resposta Audível (URAs) etc. Em muitos casos, a interação com a URA pode ser feita tanto por meio das teclas do telefone quanto por reconhecimento de voz.

4.2 NUMERAÇÃO ESPECÍFICA PARA ATIVIDADES DE TELEMARKETING

Os "números de telefone" (códigos de acesso) são parte dos Recursos de Numeração, utilizados na prestação de diversos serviços de telecomunicações. De forma assemelhada ao espectro radioelétrico e às posições orbitais, os recursos de numeração constituem um recurso finito, limitado e de uso especial, cuja exploração é organizada e administrada, em regra, pelas agências reguladoras nacionais. Nos seus Planos Nacionais de Numeração, muitos reguladores estabeleceram regras específicas de numeração para as atividades de telemarketing.

Na Itália, o regulador (AGCOM) definiu prefixos únicos (0844+ 6 ou 7 dígitos e 0843+ 6 ou 7 dígitos) para *call centers*, o que distingue as chamadas de publicidade, vendas e comunicação comercial das outras chamadas[76].

A Autoridade Reguladora de Telecomunicações da Índia (TRAI) definiu que as chamadas de telemarketing começam com "140" e são seguidas por um número de 7 dígitos (formato 140XXXXXXX). Além disso, a TRAI proibiu o uso de números "comuns" de celular para a realização de atividades de Telemarketing e quem descumprir pode ficar na lista negra por até dois anos[77].

Um conjunto de medidas bastante interessante está sendo adotado na França. A Autoridade Reguladora para Comunicações Eletrônicas, Correios e Distribuição de Imprensa (*Autorité de régulation des communications électroniques, des postes et de la distribution de la presse* – ARCEP), em decisão de julho de 2019[78], alterou o Plano Nacional de Numeração francês e introduziu a obrigação de apresentar as informações do originador da chamada no dispositivo receptor. Adicionalmente, esse número deve estar de acordo com o Plano de Numeração, ter sido atribuído pela ARCEP, ter sido designado a um usuário específico e deve permitir que o destinatário da chamada retorne a ligação. Mais recentemente, em setembro de 2022, novas regras foram expedidas pela ARCEP, no sentido de reservar as séries numéricas 06 e 07 exclusivamente para comunicações móveis interpessoais, por voz e texto. Jás as comunicações utilizando plataformas informatizadas e automatizadas devem ser realizadas na série 09. Os sistemas automatizados de chamadas também receberam uma série de números geográficos e multifuncionais específicos para esse tipo de comunicação. As empresas que usam esses números devem certificar-se de que o destinatário da chamada aceitou receber a ligação do número exibido[79].

4.3 ALTERAÇÕES LEGAIS

Diversos países reforçaram seu arcabouço jurídico contra as comunicações indesejadas.

Nos Estados Unidos da América, a lei *Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Disterrence* (TRACED ACT), de dezembro de 2019, deu à autoridade reguladora, *Federal Communications Commission* (FCC), maior autoridade para processar os responsáveis pelas chamadas de *scam* (golpes e fraudes por telefone). Além disso, a lei TRACED exige que as

prestadoras de serviços de telecomunicações, como Verizon, T-Mobile/Sprint e AT&T, implementem um sistema de autenticação de número sem custo para os consumidores. Ela também aumenta as penalidades para empresas que utilizam soluções de robocall e aumenta o prazo de prescrição do delito para quatro anos.

Na Alemanha, a Lei contra a Concorrência Desleal (*Gesetz gegen den unlauteren Wettbewerb* ou UWG[80]) proíbe as empresas de fazer chamadas de telemarketing para consumidores que não consentiram em receber essas chamadas (tanto as chamadas feitas por indivíduos quanto por discadores automatizados) e proíbe a ocultação do número originador em chamadas de publicidade. A Agência alemã, BNetzA, publicou orientações sobre a documentação que as empresas precisam manter, por pelo menos cinco anos, para comprovar o consentimento dos consumidores em receber as chamadas de telemarketing[81].

4.4 USO DE PADRÕES DE AUTENTICAÇÃO E VERIFICAÇÃO DE CHAMADAS

A autoridade reguladora estadunidense FCC exigiu[82], em 2018, que o setor de telefonia adotasse um conjunto de protocolos de autenticação de chamadas do tipo SHAKEN/STIR (*Signature-based Handling of Asserted Information Using Tokens* – SHAKEN – e *Secure Telephone Identity Revisited* – STIR). Com isso, as chamadas que trafegam na rede de telefonia recebem uma assinatura que reconhece a legitimidade da identidade na origem, que é validada pelas demais prestadoras até chegar ao destinatário final. O cronograma de implantação foi escalonado de acordo com o porte das empresas, sendo até o final de 2021 o prazo estabelecido para as grandes prestadoras, e até o de 2023, para as demais.

Na Índia, a TRAI expediu uma diretiva sob os regulamentos do *Telecom Commercial Communications Customer Preference* (TCCCP) para implementar uma plataforma, baseada em tecnologia *blockchain*, que permite que apenas empresas autorizadas possam enviar comunicações para os consumidores de serviços de telecomunicações. Ela foi parcialmente implementada e ativada em 1º de junho de 2020[83],

No Canadá, a Comissão Canadense de Radiotelevisão e Telecomunicações (*Conseil de la radiodiffusion et des télécommunications canadiennes* – CRTC) expediu, em abril de 2021, a *Compliance and Enforcement and Telecom Decision CRTC 2021-123*[84]. Nela, o regulador estabeleceu obrigatoriedade do uso dos protocolos STIR/SHAKEN para verificação e autenticação da identidade dos originadores de chamadas de voz, em condições de operar a partir de 30 de novembro de 2021.

4.5 USO DE APLICATIVOS PARA BLOQUEIO DE LIGAÇÕES INDESEJADAS

Outro recurso bastante utilizado são os aplicativos para smartphones que identificam, filtram e bloqueiam as comunicações indesejadas.

Em Singapura, uma colaboração entre o *National Crime Prevention Council* (NCPC), a equipe *Open Government Products* (OGP) e a *Singapura Police Force* (SPF) resultou no desenvolvimento de um aplicativo chamado *ScamSchield*, que filtra as chamadas e mensagens de texto. O aplicativo compara a chamada recebida com uma lista de números bloqueados mantida pela força policial e pela comissão responsável pela proteção de dados pessoais de Singapuara (PDPC). Se uma mensagem de texto de um contato desconhecido é recebido, o *ScamShield* determina se é uma fraude usando um algoritmo de análise no dispositivo. Em caso positivo, a tentativa de fraude é automaticamente remetida para a base de dados, o que ajuda a manter o aplicativo atualizado.

A reguladora indiana, TRAI, desenvolveu um aplicativo para interação com a lista de Não Perturbe. Ele permite que os usuários de *smartphones* registrem seu número e gerenciem suas preferências quanto ao recebimento de comunicações comerciais, além de ser possível acompanhar as reclamações registradas na plataforma. O aplicativo também faz gerenciamento de chamadas, possui mecanismos inteligentes de detecção de *spam* e utiliza de *crowdsourcing* de dados das mensagens de texto e chamadas indesejadas para acelerar a detecção e mitigação de *spammers* desconhecidos.

Além dos aplicativos desenvolvidos por governos – casos de Singapura e Índia –, a iniciativa privada também tratou de desenvolver soluções para minimizar os inconvenientes das comunicações indesejadas. Dentre os mais conhecidos[85] aplicativos destacam-se:

i. Truecaller[86]
ii. Hiya[87]
iii. Robokiller[88]
iv. Nomorobo Robocall Blocking[89]
v. Call Blacklist[90].

Além disso, nos Estados Unidos, algumas prestadoras disponibilizaram seus própiros aplicativos de filtragem e bloqueio, como é o caso da AT&T (AT&T Call Protect[91]) e T-Mobile (T-Mobile Name ID[92]). Existem também iniciativas de alguns fabricantes de celulares e sistemas operacionais. A Apple implementou a partir do iOS 13 um recurso opcional de triagem e bloqueio de chamadas denominado "*Silence Unknown Callers*"[93]. O Google oferece vários aplicativos e ferramentas de bloqueio de chamadas para telefones Android. Os usuários do Google Voice podem usar ferramentas de gerenciamento de chamadas para bloquear chamadas indesejadas e os telefones Google Pixel têm um recurso de triagem e bloqueio de chamadas denominado "*Call Screen*"[94]. A Samsung faz parceria com a Hiya para oferecer uma solução de bloqueio de chamadas chamada "*Smart Call*"[95], para rotular chamadas potencialmente indesejadas.

5. COMPATIBILIDADE E POSSIBILIDADE DE APLICAÇÃO NO CONTEXTO BRASILEIRO

A partir de 2019, a experiência brasileira de combate ao telemarketing abusivo e chamadas de *robocall* foi marcada por três ondas de medidas regulatórias. Na primeira delas, foram desenvolvidos códigos de conduta setoriais e implementada a Plataforma "Não me Perturbe". A etapa seguinte foi concentrada no estabelecimento e implantação de numeração específica para o desenvolvimento de atividades de telemarketing (prefixo 0303). Por fim, a terceira fase foi marcada pela expedição de Medida Cautelar e extinção da regra de não faturamento das chamadas com duração de até três segundos. A Cautelar estabeleceu regras de bloqueio de numeração não atribuída e de usuários que realizam grandes volumes de ligações diárias com características de *robocall*. Como mencionado, um histórico mais completo e informações atualizadas podem ser obtidos no Estudo[1] e Relatórios [96].

Tal contexto é importante para a análise de compatibilidade e possibilidade de aplicação dos achados da pesquisa de *benchmarking* internacional, realizada a seguir. A ordem na qual os tópicos serão abordados aproxima-se da ordem dos critérios de avaliação das técnicas de combate ao *spam* telefônico adotados por Tu, Doupé e Zhao (2016). Isto é, começando pelas técnicas de maior Usabilidade (mais fácil utilização pelos usuários), seguidas por diversos níveis de Implementabilidade (facilidade de implantação e operação) e finalizando nas que procuram endereçar os problemas de Robustez (que são, em geral, as que almejam segurança e resiliência frente ao *spoofing*).

5.1 RECOMENDAÇÃO DE USO DE APLICATIVOS DE BLOQUEIO/GERENCIAMENTO DE LIGAÇÕES E MENSAGENS TELEFÔNICAS

A recomendação de Órgãos Reguladores para que os consumidores adotem e utilizem aplicativos de bloqueio/gerenciamento de comunicações indesejadas está presente entre as medidas adotadas por diversos países. Alguns deles, como a FCC e o Ofcom, apoiam e promovem iniciativas nesse sentido, como parte de suas ações de conscientização e educação para o consumo. Outros, chegam a realizar ações de suporte ao desenvolvimento, para que quaisquer interessados e até as próprias prestadoras desenvolvam seus aplicativos (vide seção anterior).

Não haveria qualquer dificuldade em realizar ações e campanhas informativas desse tipo no Brasil, tomados os devidos cuidados com os aplicativos recomendados.

5.2 APRIMORAMENTO DA PLATAFORMA "NÃO ME PERTURBE"

As listas de Não Perturbe certamente estão entre as técnicas mais empregadas no combate de chamadas indesejadas. A implementação brasileira, Plataforma "Não Me Perturbe", somente possui uma forma de adesão, o acesso e cadastramento pessoal do interessado na página da plataforma na Internet (www.naomeperturbe.com.br).

Até agosto de 2022, haviam se cadastrado na Plataforma "Não Me Perturbe" 5,7 milhões de usuários[97]. Mais de 10 milhões de números telefônicos[98] foram registrados na lista, de um total de 261 milhões de acessos móveis e 32 milhões de acessos fixos existentes no País. A facilitação e ampliação dos meios de ingresso na plataforma podem contribuir para que mais usuários passem a integrar a plataforma e tomem proveito de seus benefícios, bem como revitalizar a sua visibilidade ante o público em geral.

Em linha com o observado na experiência de diversos países, formas alternativas de ingresso poderiam incluir o envio de mensagens e a ligação para números específicos de auto cadastramento, bem como o uso de Unidades de Resposta Audível (URAs) que permitam a inclusão e o gerenciamento de usuários no Cadastro Nacional de Não Perturbe brasileiro.

Além disso, alguns países observaram problemas com a gestão dos dados cadastrais. De posse dessas informações, empresas de telesserviços (e seus funcionários) passaram a utilizá-las para fins opostos aos pretendidos (isto é, como *mailing-list* para a prática de telemarketing abusivo!).

Manter a segurança das informações cadastrais e as preferências de recebimento de ligações dos usuários é essencial nesse contexto. Os indianos, por exemplo, optaram pela utilização da plataforma DLT (baseada em *blockchain*) para distribuir o consentimento e preferências dos usuários entre as prestadoras e empresas de telesserviços, como forma de melhor organizar e dar maior segurança ao processo.

Igualmente, não se vislumbram maiores empecilhos a adoção de desenvolvimentos nesses sentidos, a serem coordenadas junto aos administradores e mantenedores da plataforma.

5.3 LISTA DE CÓDIGOS NÃO ORIGINADORES DE CHAMADAS E LISTA DE NÚMEROS BLOQUEADOS

Essa é uma iniciativa originalmente encabeçada pelo Ofcom, regulador do Reino Unido. Ela consiste na criação de uma base de dados única com o registro dos números que, de acordo as regras do Plano de Numeração britânico, não podem ser utilizados para a geração de chamadas (números bloqueados ou impedidos). Os Estados Unidos também possuem uma lista desse tipo, por meio da qual é possível bloquear a capacidade de geração de chamadas dos números registrados.

O trabalho do Ofcom foi inicialmente realizado em parceria com o setor financeiro. A lista de "Não Originar Chamadas" (*Do-Not-Originate* – DNO) possui um conjunto de números utilizados por essas organizações, mas apenas para receber chamadas, nunca realizá-las. O Ofcom também gerencia um banco de dados próprio, para ser utilizado para se consultar os números bloqueados pelo próprio regulador e pelas prestadoras. Números que realizam grandes volumes de chamadas indesejadas são identificados por um grupo de trabalho (e outras fontes) e consolidados mensalmente em relatórios do Ofcom. Na lista também estão números "protegidos" e reservados para uso futuro, que podem ser bloqueados sem risco de interferir no tráfego de chamadas legítimas.

Esta é, na realidade, uma técnica de combate ao *spoofing*, pois impede que um criminoso roube a identidade da instituição financeira para aplicar golpes nos consumidores. Como é o consumidor quem estabelece a ligação, e o código de numeração possui esse único propósito, o consumidor se conectará ao centro de atendimento do banco, havendo certeza de estar se comunicando com o interlocutor correto. Os critérios e condições de uso da lista de DNO foram recentemente atualizados[99] e ela provavelmente será expandida para incluir números de uma ampla gama de organizações.

Quanto à possibilidade de utilização de uma medida como essa no Brasil, cabe destacar que o processo de bloqueio de códigos de numeração não atribuídos, obrigação presente na Medida Cautelar da terceira onda de ações regulatórias, possui muitas semelhanças operacionais. Quanto às regras pertinentes às centrais de atendimento de consumidores (particularmente a Lei nº 8.078/90 – Código de Defesa do Consumidor e o Decreto nº 11.034/22 – Decreto do Serviço de Atendimento ao Consumidor, SAC), não se vislumbram incompatibilidades. Já no plano normativo de telecomunicações, seriam necessários os respectivos ajustes às regras e procedimentos atinentes à atribuição e designação de códigos de numeração, o que se encontra inteiramente sob a alçada desta Agência. A decisão estaria então mais relacionada ao interesse dos setores econômicos em adotar desse tipo de solução, e à disposição dos consumidores em utilizá-la como canal de relacionamento.

5.4 COMBATE À FRAUDE ENVOLVENDO A TROCA DE SIM CARDS

Outro resultado dos supramencionados esforços de colaboração entre o Ofcom e o setor financeiro britânico: foi desenvolvido um procedimento especial de verificação, chamado "*Fraud Charter*"[100], para o combate às fraudes que se utilizam da troca de SIM Cards.

As prestadoras fornecem ao setor financeiro informações, em tempo real, sobre a troca dos SIM Cards dos telefones celulares. Isso permite que as empresas do setor financeiro possam

perceber tentativas de fraude ao correlacionar, por exemplo, atividades financeiras suspeitas ocorrendo concomitantemente à troca do SIM Card do celular do cliente.

A adoção de uma inciativa como esta dependeria da colaboração e coordenação de diferentes atores e setores, alheios à esfera de atuação regulatória da Anatel, além de demandar certos cuidados especiais em relação ao tratamento de dados e informações pessoais dos consumidores. De toda sorte, parece ser uma iniciativa que merece um estudo aprofundado, pois pode contribuir para o combate de crimes e golpes, além de para melhorar a segurança dos usuários, em complementação a outras técnicas já usualmente utilizadas (verificação por SMS, duplo fator de autenticação, biometria etc.)

5.5 PERFIS DE *SPAMMING*, TÉCNICAS DE *CROWDSOURCING* E INTELIGÊNCIA ARTIFICIAL

Informação é poder. O conhecimento das técnicas e padrões típicos das comunicações indesejadas é um elemento extremamente importante para a gestão do problema. Uma vez definidas suas principais características, podem ser criados filtros e bloqueios automáticos nas redes das prestadoras e *gateways* de tráfego, por exemplo, diminuindo o alastramento e o impacto das chamadas indesejadas.

Muitos países estão se mostrando bastante criativos na busca de informações úteis para complementar os *logs* dos sistemas e as denúncias e reclamações dos usuários. Para além da coleta desses dados e das pesquisas com as técnicas tradicionais, há exemplos de utilização complementar de dados de uso de aplicativos e soluções de *crowdsourcing*.

Singapura tem utilizado técnicas baseadas em *Machine Learning* para ajudar na identificação de perfis e padrões das mensagens indesejadas, possibilitando a criação de filtros mais eficientes. No Canadá, o Regulador CRTC realizou testes em parceria com prestadoras e obteve sucesso na identificação de chamadas indesejadas com o uso de algorítimos de inteligência artificial, o que possibilitou que fossem bloqueadas antes de chegar ao destinatário.

Comunicações indesejadas por mensagens de texto têm crescido bastante, o que, por conseguinte, desencadeou no surgimento de novas soluções de restrição das interações não autorizadas. Foram identificadas algumas iniciativas de utilização de inteligência artificial para reconhecimento de mensagens fraudulentas e realização de bloqueio automático.

Várias dessas experiências podem contribuir para o aperfeiçoamento das medidas adotadas aqui. Por exemplo, foi observado na experiência brasileira de combate às chamadas de *robocall* que essas ligações possuem características mensuráveis específicas, tais como elevada quantidade, curta duração, alta taxa de não completamento, destinatários diversos, dentre outras. Em linha com o que tem sido realizado nos outros países (como Austrália e Singapura), é

argumentável que soluções tecnológicas semelhantes poderiam ser implamentadas nas redes brasileiras para identificar tráfegos irregulares e atuar na mitigação.

Além disso, o bloqueio ou filtragem de mensagens de texto indesejadas/fraudulentas diretamente pelas prestadoras dos serviços tem sido uma estratégia comumente adotada nos outros países (vide EUA, Reino Unido, Singapura e Austrália). Na Índia, esse processo ocorre por meio da verificação do consentimento e preferências registradas na plataforma de DLT, baseada em *blockchain*.

Muito embora tais alternativas demandem a avaliação de custos e eventuais desafios de implementação (estabelecimento de grupos de trabalho, colaboração de equipes, desenvolvimento de sistemas informáticos e cronogramas de implantação, dentre outros), fato é que outros países estão obtendo resultados positivos e descobrindo soluções eficientes e confiáveis de combate ao problema.

5.6 ALTERAÇÕES LEGAIS E REGULAMENTARES E MAIORES SANCIONAMENTOS

Os volumes diários de comunicações indesejadas nas redes e serviços e, por óbvio, o consequente impacto decorrente na qualidade de vida dos consumidores, aumentaram drásticamente nos últimos anos (vide seção correspondente). Em resposta, novas legislações e normativos, mais rígidos e gravosos, surgiram e vieram acompanhados da aplicação de multas consideravelmente mais pronunciadas. Neste quesito, a título exemplificativo, a FCC aplicou a sua maior multa de todos os tempos – US$ 225 milhões – contra uma empresa de telemarketing texana que fez mais de um bilhão de chamadas indesejadas para oferta de planos de saúde durante a pandemia.

Nas seções anteriores foram elencadas diversas alterações legais e regulamentares, realizadas ou ainda em curso. Algumas delas não apenas garantem aos reguladores (ou entidades equivalentes) capacidade fiscalizatória ampliada para o combate do telemarketing abusivo e chamadas de *robocall* dentro do setor de telecomunicações, como reconhecem e estendem a sua competência sobre outros espaços do ecossistema digital. Nessa toada, Bélgica[101], Itália[102], Holanda[103], Espanha[104] e Reino Unido[105], por exemplo, criaram regras similares ou estenderam as regras existentes aplicáveis às telecomunicações para o âmbito dos aplicativos de comunicação *Over-the-Top*.

De toda sorte, o estabelecimento ou a revisão de arcabouços normativos pode ser bastante desejável para trazer estabilidade e segurança jurídica à atuação dos órgãos envolvidos, evidenciando os limites de suas esferas de atuação regulatória.

Ademais, essa pode ser uma das poucas alternativas eficientes para se enfrentar um dos principais desafios do combate às chamadas indesejadas. Como bem destacado por Tu, Doupé e

Zhao (2016), existe um contra incentivo financeiro perverso que torna a batalha muito mais difícil. Diferentemente do que ocorre no *spam* de correio eletrônico, no qual existe incentivo positivo para que os provedores de Internet e de serviços em nuvem envolvidos adotem as medidas de mitigação e contenção do problema, que causa prejuízos a todos, para as prestadoras de telecomunicações, o tráfego de *spam* telefônico representa receitas, pois elas são remuneradas pelas chamadas e pelo uso dos recursos de suas redes. Aqui, somente o usuário é prejudicado.

Isso considerado, ampliar o peso do ônus regulatório que recai sobre as prestadoras e os (grandes) usuários que fazem uso inadequado das redes e serviços parece uma escolha natural. Afinal, o tráfego irregular de chamadas de *robocall* que causa o importuno diário de milhares de consumidores percorre a rede das prestadoras. Elas conhecem e gerenciam o tráfego dessas comunicações indesejadas, que é produzido em volumes massivos, têm origens comuns e concentradas e outras características muito peculiares, fáceis de identificar.

Estabelecer um marco regulatório específico ou revisar as regras de exploração dos serviços pode contribuir para solucionar essa celeuma. Por exemplo, poderiam ser estabelecidas cláusulas contratuais mandatórias ao contrato de adesão dos serviços de telecomunicações, que obriguem às prestadoras o dever de proteção dos seus clientes. Como mencionado, em outros países diversas prestadoras possuem seus próprios aplicativos de bloqueio. Outras alternativas poderiam ser igualmente consideradas, como a previsão do atendimento de metas de qualidade do serviço associadas à eficiência de bloqueio das chamadas indesejadas, por exemplo.

Além disso, os demais participantes da cadeia de valor das chamadas indesejadas devem ser chamados à responsabilidade, tais como as empresas que realizam o transporte nacional e internacional das chamadas, as empresas de telesserviços que realizam os disparos maciços de chamadas com seus discadores automatizados e até mesmo as empresas que delas contratam esses serviços, pois todos são beneficiados pela prática lesiva.

Ainda na linha de responsabilização, considerando-se as recentes vertentes de atuação responsiva e de assimetrias regulatórias adotadas por esta Agência, mostra-se cada vez mais importante estabelecer clara e objetivamente na regulamentação os direitos e obrigações dos grandes usuários dos serviços.

As pirâmides de ônus regulatórios são bem conhecidas e estabelecidas no arcabouço normativo da Anatel. Talvez o exemplo mais notório seja o da exploração do Serviço de Comunicação Multimídia. No nível mais básico da pirâmide, sequer é necessária a obtenção da outorga, basta a mera notificação para o interessado iniciar a prestação do serviço de banda larga fixa. Caso alcance a marca de cinco mil acessos, ou deseje utilizar recurso à prestação que requer autorização do direito de uso (como o espectro radioelétrico), por exemplo, ele obtém a outorga e passa ao patamar de cima, onde os ônus regulatórios e as responsabilidades por sua conduta são maiores. A partir daí ele pode continuar galgando os degraus da pirâmide (como, por exemplo,

obtendo recursos de espectro por meio de procedimento licitatório, submetidos a compromissos específicos) até chegar no topo, onde estão as empresas com PMS e as obrigações regulatórias mais expressivas.

Há outras pirâmides estabelecidas na regulamentação da Anatel que seguem uma lógica parecida. Na certificação e homologação de produtos e equipamentos para telecomunicações, por exemplo, há assimetrias que favorecem os produtos menos complexos e que representem menores riscos para as redes e usuários. O procedimento padrão previsto para eles é meramente declaratório. Já dos produtos e equipamentos que fazem uso ativo do espectro radioelétrico (e, portanto, podem causar interferências prejudiciais) ou podem representar riscos e provocar danos às redes e usuários (como os carregadores e baterias de celular, que, se não atenderem certos critérios e requisitos técnicos, podem dar choques ou até incendiar, em determinadas condições de uso) passam por um processo de avaliação e certificação muito mais minucioso e elaborado.

Ou ainda, um terceiro exemplo de pirâmide de ônus regulatório está estabelecido na regulamentação de segurança cibernética. Nela, os ônus mais exigentes, que incluem maiores medidas de preparação e pronta resposta para incidentes cibernéticos, se aplicam às empresas com redes maiores e mais usuários, nas quais o impacto potencial dos incidentes é consideravelmente maior.

Por outro lado, todos os usuários/consumidores dos serviços sempre foram tratados exatamente da mesma forma, pelo menos até a expedição da Medida Cautelar. Nela, pela primeira vez, foi estabelecida uma assimetria que exigiu que os grandes usuários – neste caso específico, empresas que utilizam soluções tecnológicas para o disparo de grandes volumes de chamadas – adequassem seus discadores à sua efetiva capacidade humana de processamento das chamadas.

Essa é uma iniciativa que precisa continuar seu desenvolvimento e ser incluída na regulamentação da Agência, estendida para incluir não apenas os usuários que utilizam discadores automatizados, mas todos aqueles que consomem grandes volumes das redes e serviços, representam razões significativas do tráfego das redes ou, de qualquer modo, possam impactar, ainda que indiretamente, técnica ou economicamente, na experiência dos demais usuários das redes e serviços. Nesse sentido, regras de conduta ou até cláusulas específicas podem ser exigidas no relacionamento das prestadoras de serviços com esses grandes usuários, por exemplo.

5.7 CRIAÇÃO DE GRUPOS E FORÇAS-TAREFA PARA O BLOQUEIO DE ATIVIDADES IRREGULARES E TRÁFEGO INTERNACIONAL DE CHAMADAS INDESEJADAS

Como mencionado, algumas Administrações nacionais criaram equipes específicas para tratar desse assunto de forma integrada, compostas por diversos órgãos que tem envolvimento direto ou indireto com o tema, com vistas a promover uma melhor coordenação e otimização dos esforços. É o caso, por exemplo, dos EUA e do Reino Unido (vide Anexos correspondentes), que

possuem grupos atuando na gestão do *spam* e *scam* tanto de origem doméstica quanto internacional.

As chamadas indesejadas originadas de outros países, aliás, têm se mostrado um incômodo cada vez maior. Por ser um problema global, ações coordenadas têm sido discutidas em fóruns internacionais, como o *Unsolicited Communications Enforcement Network* (UCENET[106]), do qual participam organizações, entidades e indústria de dezenas de países. Os EUA exigem dos *gateways* internacionais a adoção de uma série de protocolos e a pronta atuação de mitigação, em prazos exíguos de resposta. Já Singapura discute um mecanismo que dá aos usuários a opção de bloqueio de todas as chamadas internacionais, por exemplo.

Voltando à questão das forças-tarefa, independentemente de qualquer distinção da origem do fluxo de chamadas indesejadas, o objetivo comum dessas equipes reside principalmente na busca de soluções rápidas de identificação, análise e contenção. Elas também subsidiam a atuação dos reguladores na tomada de decisões regulatórias gerais e em concreto.

É o caso, por exemplo, do *Robocall Response Team* da estadunidense FCC, que recentemente identificou nominalmente uma série de prestadoras que estavam descumprindo as regras de mitigação das chamadas de *robocall* (vide seção correspondente para maiores detalhes). Caso elas não demonstrem a aderência às regras no prazo de duas semanas, serão excluídas da *Robocall Mitigation Database* e, com isso, seu tráfego não poderá mais ser transportado pelas demais empresas.

Seguindo esses exemplos, algo parecido poderia ser implantado no Brasil. A Anatel já recolheu, via inteligência fiscalizatória e processos especiais de acompanhamento setorial, uma razoável quantidade de informações sobre as maiores responsáveis por gerar e injetar as chamadas com características de *robocall* nas redes de telecomunicações brasileiras. Há processos de apuração e sancionamento específicos em face de algumas delas em curso, aliás.

Além disso, a Agência tem experiência com grupos técnicos e de resposta, alguns inclusive estabelecidos em regulamentação ou previstos em instrumentos convocatórios editalícios. Vejam-se, por exemplo, os grupos para desastres e emergências (RENET), de segurança cibernética (GT-Ciber), de segurança pública e combate a fraudes (GT-Seg), além dos grupos de implantação criados nos Editais de 700 MHz (GIRED) e do 5G (GAISPI e GAPE). A realização dos grandes eventos desportivos de 2013, 2014 e 2016 também contribui para que a Anatel se familiarizasse e incorporasse esse tipo de atuação em equipes técnicas especializadas em sua cultura organizacional.

Do exposto, considerando que no Brasil mais de 90% do fluxo de chamadas com características de *robocall* é dirigido às redes das três maiores prestadoras de telefonia móvel, medidas mais rigorosas de controle desse influxo podem ser estudadas e adotadas nestes e noutros pontos do sistema de telecomunicações. Equipes especiais de acompanhamento, compostas por

membros da Anatel e das empresas envolvidas e suas entidades representativas, poderiam então, por exemplo, recomendar à Agência a adoção de ações de bloqueio e suspensão em concreto, bem como auxiliar na instrução de processos de apuração e de revisão normativa.

5.8 PADRÕES DE AUTENTICAÇÃO E VERIFICAÇÃO DE CHAMADAS E COMBATE AO *SPOOFING*

O combate ao *spoofing* tem se apresentado de modo praticamente unânime como uma das medidas centrais para coibir o telemarketing abusivo e as chamadas de *robocall*. Nessa linha, o principal movimento para aumentar a capacidade de identificação e verificação de chamadas tem sido a implementação de protocolos STIR/SHAKEN nas redes de telefonia.

As preocupações com as limitações técnicas e operacionais (e os custos associados) frente às redes legadas (em particular, das redes TDM que convivem com as soluções IP) estão sendo enfrentadas de diferentes formas nos países que escolheram adotar esse tipo de solução tecnológica, sendo a predominante a escolha de cronogramas faseados para a evolução das redes e a implementação dos protocolos de verificação.

A estratégia que Estados Unidos e Canadá escolheram, por exemplo, utiliza um cronograma de implantação escalonado com diferenciação pelo porte das empresas. Em linha com o observado no item anterior, os EUA reduziram pela metade prazo que algumas prestadoras menores teriam, pois foi identificado pela força-tarefa um elevado volume de *robocall* em suas redes (vide seção correspondente). Outrossim, a opção de escalonamento pelo porte das empresas tem recebido críticas porque as chamadas indesejadas tendem a migrar para as prestadoras que ainda não possuem a solução implantada e, assim, o problema apenas muda de lugar. No momento, o Reino Unido está avaliando adotar a tecnologia até 2025, em todas as prestadoras de telecomunicações.

A estadunidense FCC exige que as prestadoras de telefonia mantenham uma base de informações atualizada, a *Robocall Mitigation Database*. Nela, as empresas indicam e mantêm atualizado o seu estado de adesão ao STIR/SHAKEN e certificações. Em alguns casos, também informam seus esforços concretos de mitigação de comunicações indesejadas de *robocall*.

A adoção dos protocolos STIR/SHAKEN nas redes de telefonia geralmente não vem sozinha. Uma associação bastante comum é com o *Rich Call Data*, solução complementar que mostra no visor do recebedor da chamada uma série de informações adicionais, tais como o nome, empresa, foto/logotipo, endereço, telefone, e-mail, webpage, motivo do contato, etc.[107] Considerando o interesse comercial em motivar o destinatário a atender a ligação, espera-se que soluções como esta ajudem a rentabilizar a atualização tecnológica com um novo modelo comercial de relacionamento com clientes e telemarketing ativo.

Pois bem. A possibilidade de adoção de solução semelhante aqui no Brasil – isto é, a adoção compulsória de protocolos STIR/SHAKEN – já é discutida há algum tempo. Muito embora a Anatel

atualmente prefira abordagens regulatórias mais alinhadas ao princípio de neutralidade tecnológica, em vários momentos a Agência impôs a obrigação de atualização de tecnologias e protocolos das redes e serviços. Ressalte-se ainda que o atendimento de requisitos e a comprovação de conformidade técnica-operacional são as bases do processo de certificação e homologação de produtos e equipamentos para telecomunicações, regularmente realizada pela Anatel.

Se, por um lado, a possibilidade jurídica de atualização compulsória pode ser superada, questões de conveniência e oportunidade posam um desafio maior. Isso porque há várias maneiras de se adotar os protocolos de verificação e autenticação de chamadas, além de diferentes abrangências/profundidades de implementação. As opções mais amplas e generalistas, como a americana, impactam substancialmente nos custos associados e têm sido criticadas por estarem além da capacidade econômica das pequenas prestadoras de soluções VoIP, por exemplo.

Por outro lado, a verificação da legitimidade do originador da chamada é um forte aliado para o combate das chamadas de *robocall* e das tentativas de golpes e fraudes por telefone, ambos muito importantes para os consumidores dos serviços.

6. CONCLUSÃO

Não há solução universal, completa e definitiva para as comunicações indesejadas. O que os demais países têm adotado nos últimos anos, em intensidade crescente, são conjuntos de medidas complementares e sinérgicas que combinam diferentes soluções técnicas e regulatórias. Além disso, o problema é notoriamente complexo e multissetorial, o que demanda soluções coordenadas em diversas camadas e entre múltiplos setores e agentes, incluindo a esfera transnacional.

Uma certa racionalidade permeia a escolha entre as diferentes técnicas de mitigação das ligações de telemarketing abusivo e as chamadas de *robocall*. Primeiro, os consumidores, por serem os maiores prejudicados, servem de régua e termômetro. Nessa linha, são preferidas as soluções que não importunem ou provoquem ônus aos usuários. Segundo, a sociedade espera que os reguladores (ou autoridades equivalentes) atuem na linha de frente para solucionar o problema. Terceiro, esses mesmos reguladores não parecem acreditar que existe uma "bala de prata" que resolva todos os problemas. Pelo contrário, têm-se buscado, em abordagens sucessivas e recorrentes, a aplicação de conjuntos de medidas regulatórias que providenciem alívio às dores dos consumidores e tornem cada vez mais difícil e custosa a realização do *spam* e *scam*. Quarto, os reguladores também veem que a conscientização e a educação do consumidor são partes da solução. Por fim, o combate ao *spoofing* ocupa um lugar de destaque entre essas medidas, não apenas por auxiliar no enfrentamento dos grandes volumes nacionais e internacionais de chamadas com características de *robocall*, mas também ser um instrumento importante para o combate dos golpes e fraudes por telefone, além de outros crimes que se aproveitam da quase impossibilidade de rastreamento da originação da chamada.

De modo geral, não se evidenciaram na pesquisa de *benchmarking internacional* diferenças significativas entre as soluções adotadas nos outros países e aquelas em curso ou sendo discutidas aqui. Como visto, as principais medidas adotadas por eles para coibir o telemarketing abusivo e as chamadas de *robocall* são:

1) as listas de Não Perturbe;
2) o uso de numeração específica para telemarketing;
3) diferentes frentes de alterações legais/normativas (por exemplo, proibindo as chamadas indesejadas e criminalizando a prática do *spoofing*);
4) adoção de padrões de autenticação e verificação de chamadas (como protocolos STIR/SHAKEN);
5) uso de aplicativos para bloqueio de chamadas indesejadas;
6) aplicação de multas e bloqueio dos usuários que fazem mau uso das redes;
7) ações de monitoração e controle dos *gateways* internacionais; e
8) medidas educacionais junto às prestadoras e empresas de telesserviços.

Além disso, várias Administrações nacionais e reguladores mostram-se preocupados com a migração do telemarketing abusivo (*spam*) e das tentativas de golpes e fraudes (*scam*) para espaços menos regulados, como o dos aplicativos de comunicação *Over-the-Top*. A regulação comum europeia, em particular, possui diretivas e regulamentos que tratam do tema, que já foram integrados ao arcabouço jurídico de diversos Estado-Membros.

A atuação da Anatel foi marcada por três ondas de medidas regulatórias a partir de 2019. Na primeira, foram desenvolvidos códigos de conduta setoriais e implementada a Plataforma "Não me Perturbe". A etapa seguinte foi concentrada no estabelecimento e implantação de numeração específica para o desenvolvimento de atividades de telemarketing (prefixo 0303). Por fim, a terceira fase foi marcada pela expedição de Medida Cautelar e extinção da regra de não faturamento das chamadas com duração de até três segundos. A Cautelar estabeleceu regras de bloqueio de numeração não atribuída e de usuários que realizam grandes volumes de ligações diárias com características de *robocall*.

Considerando o contexto brasileiro, este Estudo por fim apresenta algumas considerações e elenca medidas que ainda podem vir a ser adotadas pela Agência. A saber:

(i) Recomendação de uso de aplicativos de bloqueio/gerenciamento de ligações e mensagens telefônicas;

(ii) Aprimoramento da Plataforma “Não Me Perturbe”;

(iii) Lista de Códigos Não Originadores de Chamadas e Lista de números bloqueados;

(iv) Combate à fraude envolvendo a troca de SIM Cards;

(v) Utilização de perfis de *spamming*, técnicas de *crowdsourcing* e inteligência artificial no combate a chamadas indesejadas;

(vi) Alterações legais e regulamentares e maiores sancionamentos;

(vii) Criação de grupos e forças-tarefa para o bloqueio de atividades irregulares e tráfego internacional; e

(viii) Padrões de autenticação e verificação de chamadas e combate ao *spoofing.*

Sem qualquer pretensão de esgotar as possíveis medidas técnicas e regulatórias para o combate das comunicações indesejadas, este Estudo desenvolveu sua pesquisa em âmbito e profundidade viáveis, no intuito de colaborar com todos os esforços que já vem sendo empreendidos pela Anatel para a consecução de sua missão institucional de zelar pela proteção e defesa dos consumidores e pelo desenvolvimento do sistema brasileiro de telecomunicações.

ANEXO A – ESTADOS UNIDOS

Em recente comunicado oficial a presidente da FCC Jessica Rosenworcel afirmou que "Nós não vamos parar até tirarmos *robocallers*, *spoofers* e golpistas da linha."[108] Como pode ser observado em sua página da internet[109], o regulador americano tornou o combate a *robocalls* ilegais e falsificação de identificador de chamadas mal-intencionado uma das principais prioridades de proteção ao consumidor.

Os consumidores dos EUA recebem bilhões de *robocalls* por mês[110]. Infelizmente, os avanços na tecnologia tornam barato e fácil realizar um grande número de chamadas automáticas e "falsificar" as informações do identificador de chamadas para ocultar a verdadeira identidade de um chamador, segundo relato da FCC[111].

O perfil de tais ligações pode ser avaliado conforme dados da última pesquisa realizada pela empresa TRUECALLER[112]. Percebe-se que a maior parte das ligações são do setor de vendas (51,9%), seguido do setor financeiro (30,3%), ligações incomodas (13%) e ligações fraudulentas (4,8%).

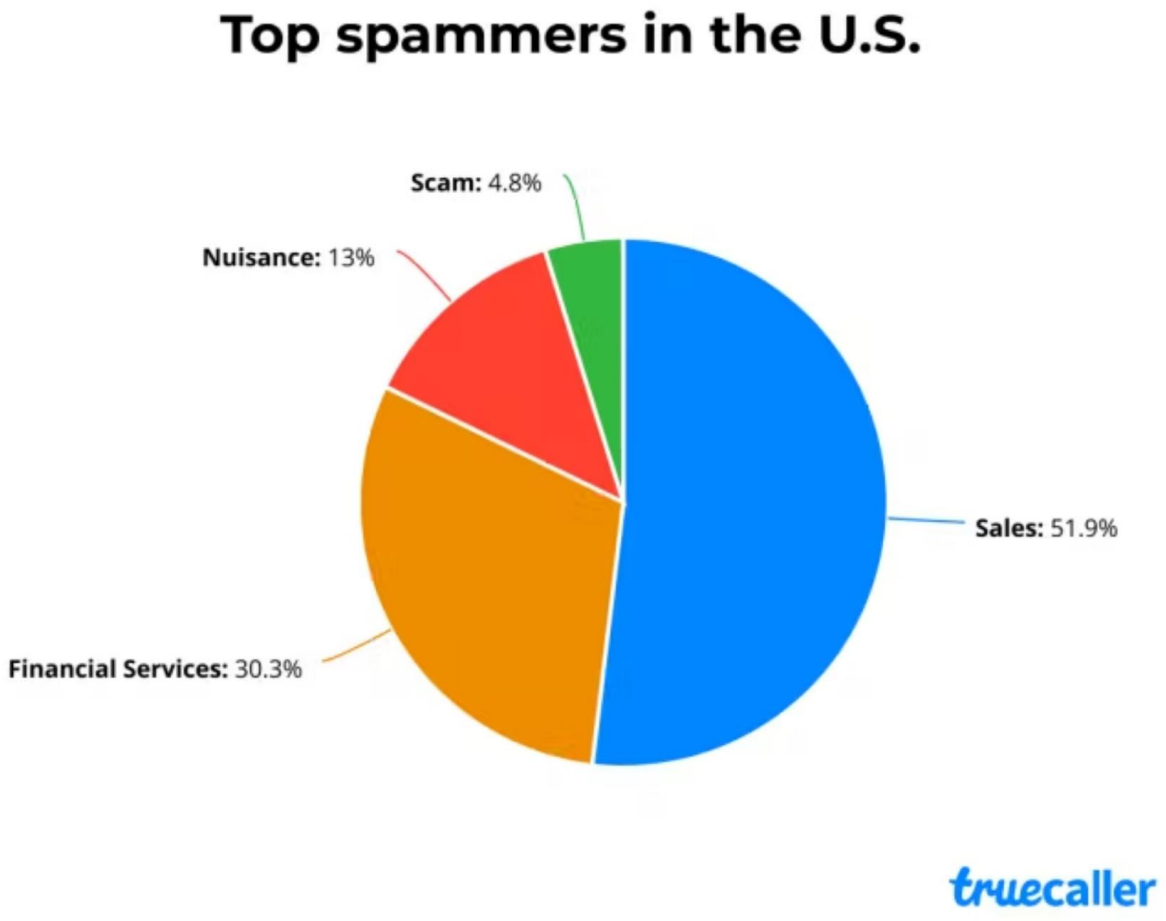


Figura 1 – Principais realizadores de ligações indesejadas nos Estados Unidos 2021.

É importante observar que esse volume de chamadas de spam mencionado aqui não representa todo o volume de spam, mas são dados de usuários do Truecaller nos EUA.[113]

Em outro estudo da mesma empresa TRUECALLER, este focado no contexto americano é possível perceber o crescimento de ligações indesejadas nos últimos anos, bem como o aumento de mensagens de texto indesejadas. Segundo tal estudo os americanos recebiam aproximadamente 31 ligações indesejadas por usuário por mês em 2022[114]

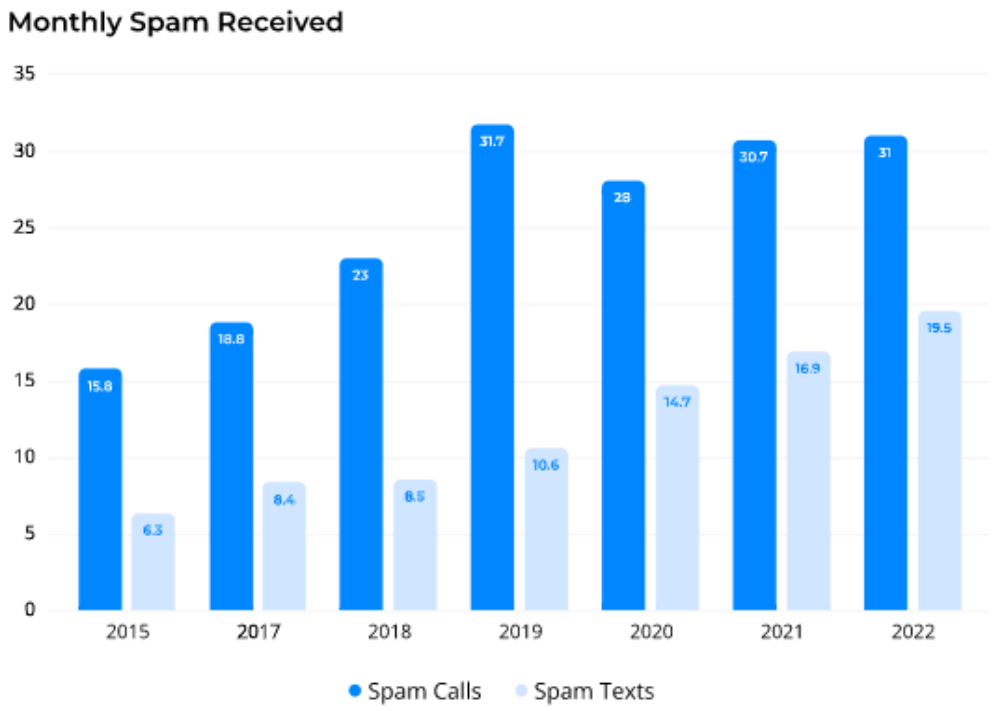


Figura 2 – Evolução das Ligações e Mensagens de Texto indesejadas por usuário, por mês em cada ano

De acordo com Federal Trade Commission (FTC) as reclamações ao longo do tempo têm oscilado entre 600 mil reclamações e pouco mais de 150 mil reclamações por mês[115]. A partir de 2021 apresenta-se uma leve queda muito provavelmente em decorrência das últimas medidas adotadas pela FCC e FTC. As reclamações frente as ligações do tipo *robocall* representam 68% do total.

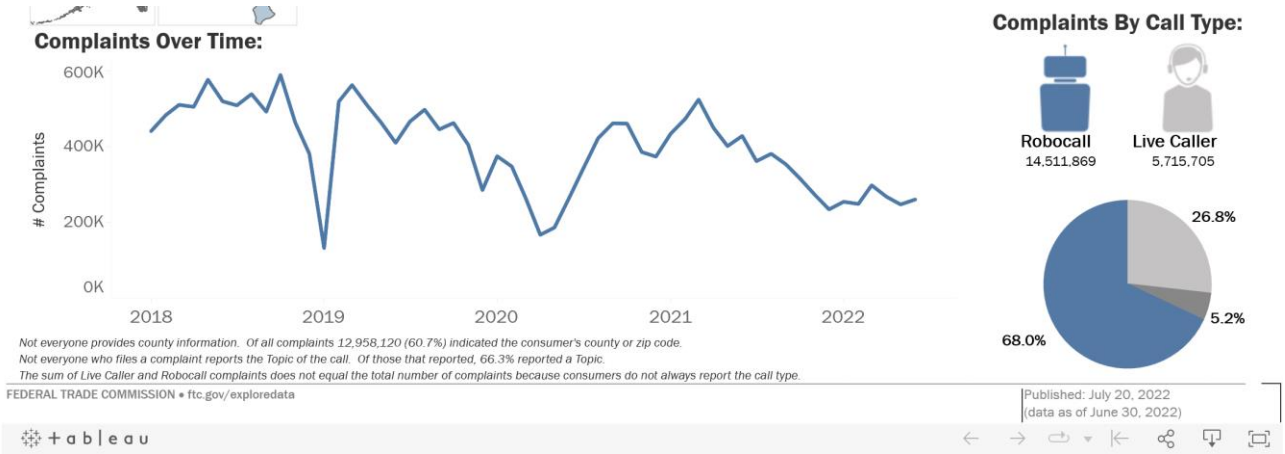


Figura 3 – Evolução das Reclamações junto a FTC e divisão por tipo (Robocall e Chamada ao vivo)

Pelos dados de reclamação da FCC também existe um movimento de queda das reclamações a partir de 2018[116].

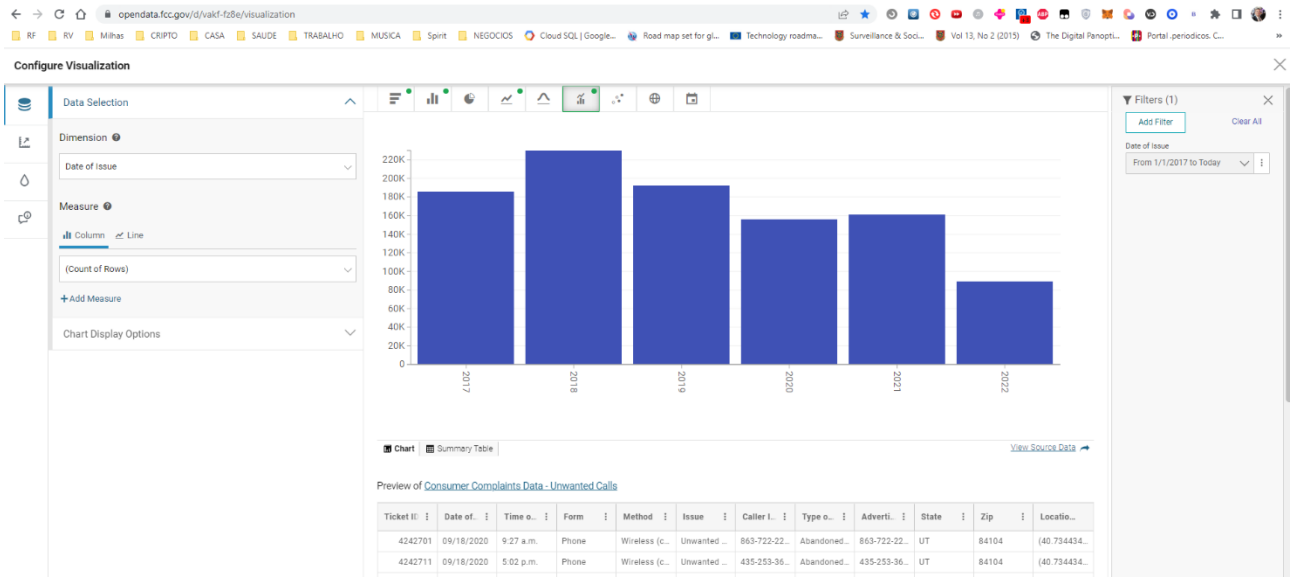


Figura 4 – Evolução das Reclamações junto a FCC sobre chamadas indesejadas.

A FCC implementou uma série de medidas para ajudar a combater as chamadas indesejadas em especial as chamadas automatizadas (*robocalls)* ilegais e falsificação de identificador de chamadas mal-intencionado. Além disso tomou medidas de fiscalização para punir aqueles que desrespeitam as leis de proteção ao consumidor.

Importante destacar também o trabalho de educação realizado pela FCC sobre o tema[117]. Como principais atividades destacam-se: Elaboração de um glossário sobre *Scam* Calls, dicas de como evitar ligações indesejadas fraudulentas (*Scam Calls*) [118], guias sobre tópicos como *Robocalls e Robotexts*, falseamento dos números de chamadas, Bloqueio de ligações e Chamadas de um toque (esperando o retorno da ligação).

Dentre os principais produtos de educação para o consumidor pode-se observar abaixo panfletos e vídeos autoexplicativos.

FCC Consumer Video: Don't Hang On, Hang Up! - To watch this video with captions, click "play," then the "CC" icon.

Figura 5 – Video sobre falsificação de números e chamadas fraudulentas[119]

Figura 6 – Peça publicitária da FCC sobre robocalls e robotexts[1]

As **principais dicas** estão consolidadas[120] na lista abaixo[121]:

Chamadas de números desconhecidos	i. Não atenda chamadas de números desconhecidos. ii. Deixe-os ir para o correio de voz.
Chamadas de números legítimos	i. Se o chamador alegar ser de uma empresa ou organização legítima, desligue e ligue de volta usando um número válido

	encontrado em seu site ou em sua última fatura, se você fizer negócios com ele.
Ao atender uma chamada	ii. Se você atender e o chamador (geralmente uma gravação) pedir para você pressionar um botão para parar de receber chamadas ou pedir para você dizer "sim" em resposta a uma pergunta, basta desligar. iii. Os golpistas costumam usar esses truques para identificar e, em seguida, segmentar respondentes ao vivo ou usar seu "sim" para aplicar cobranças não autorizadas em sua fatura.
Falsificação do número do originador da chamada	i. Esteja ciente: o identificador de chamadas mostrando um número "local" não significa mais que é necessariamente um chamador local.
Chamadas Fraudulentas/Golpe	i. Se você atender e o chamador solicitar o pagamento usando um cartão-presente, provavelmente é um golpe. Organizações legítimas, como a aplicação da lei, não solicitarão pagamento com um cartão-presente. ii. Se você receber uma chamada fraudulenta, registre uma reclamação no Centro de Reclamações do Consumidor da FCC selecionando a opção "telefone" e selecionando "chamadas indesejadas". Os dados que coletamos nos ajudam a rastrear tendências e apoiam nossas investigações de fiscalização iii. Se você perdeu dinheiro devido a uma chamada fraudulenta, entre em contato com a agência de aplicação da lei local para obter assistência.
Serviços das prestadoras de telecomunicações	i. Pergunte à sua companhia telefônica se ela oferece um serviço de bloqueio de robocall. ii. Se não, incentive-os a oferecer um. iii. Você também pode visitar o site da FCC para obter mais informações sobre robocalls ilegais e recursos sobre ferramentas de bloqueio de robocall disponíveis para ajudar a reduzir chamadas indesejadas.
Cadastre-se na lista de não me perturbe	i. Considere registrar seus números de telefone no National Do Not Call Registry. ii. Operadores de telemarketing legais usam essa lista para evitar ligar para os consumidores da lista.

.

Abaixo quadro resumo das principais legislações afetas ao tema bem como os principais atores e sua atuação nos Estados Unidos:

Principais Legislações	a) Telephone Consumer Protection Act (TCPA) e FCC Rules: Restringe determinadas chamadas feitas usando uma voz artificial ou pré-gravada para linhas residenciais; certas chamadas feitas usando voz artificial ou pré-gravada ou um sistema de discagem telefônica automática para números móveis; e certas chamadas de telemarketing. Responsável FCC. b) 2009 Truth in Caller ID Act (TICIDA): Proibição de transmitir a informação enganosa ou imprecisa do ID do chamador “com a intenção de fraudar, causar danos ou erroneamente obter qualquer coisa de valor”. Responsável FCC.

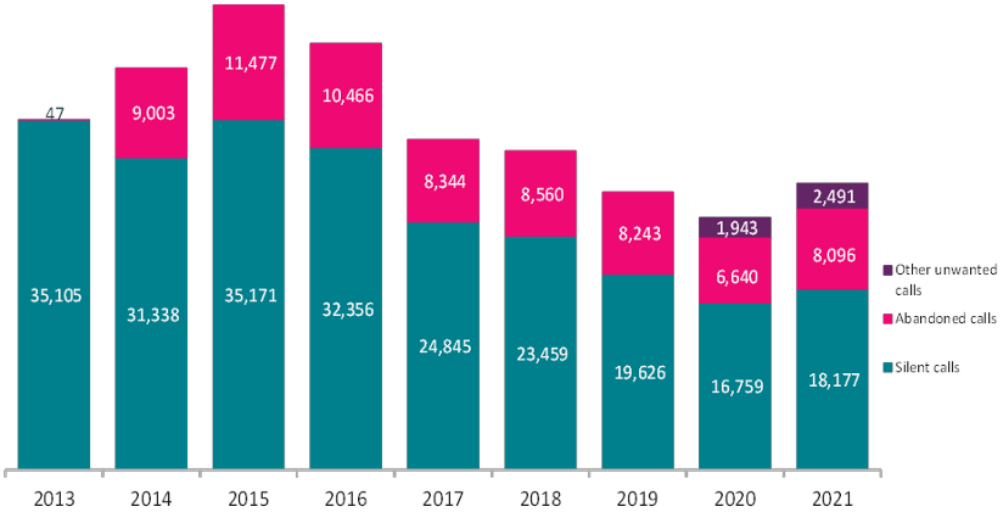
	c) Do Not Call Implementation Act (DNCIA): Autoriza a FTC a cobrar taxas pela implementação e aplicação de um registro Não me Perturbe. Telemarketers devem consultar o National Do Not Call Registry antes de ligar. Requer que a FCC consulte e coordene com a FTC para maximizar a consistência com a regra promulgada pela FTC. d) Telemarketing Consumer Fraud and Abuse Prevention Act (Telemarketing Act): Proíbe atos ou práticas de telemarketing enganosos e abusivos. Responsável FTC. e) **Telemarketing Sales Rule (TSR)**: exige que os operadores de telemarketing façam divulgações específicas de informações relevantes; proíbe declarações falsas; estabelece limites nos horários em que os operadores de telemarketing podem ligar para os consumidores; proíbe chamadas para um consumidor que pediu para não ser chamado novamente; e estabelece restrições de pagamento para a venda de determinados bens e serviços. Responsável FTC.
Atores e Responsabilidades	A responsabilidade pelo gerenciamento de comunicações não solicitadas é dividida entre a Federal Trade Commission (FTC), a Federal Communications Commission (FCC) e cada um dos 50 estados. A FTC promove a concorrência, protege e educa os consumidores sobre seus direitos e responsabilidades, e a FCC implementa e aplica as leis e regulamentos de comunicações dos EUA. Além disso, muitos estados têm seus próprios conjuntos de regulamentos de comunicações não solicitadas, que se sobrepõem às responsabilidades federais. Muitas das operações estaduais são anteriores às operações federais, explicando essa sobreposição. Existem, por exemplo, registros federais e estaduais de Não Me Pertube. As empresas de telemarketing são obrigadas a consultar ambas as listas. A FTC, a FCC e os estados frequentemente colaboram na seleção de alvos e questões de aplicação. Eles também compartilham informações e colaboram em mesas redondas e workshops voltados para o público[122].

ANEXO B – REINO UNIDO

Em seu plano de trabalho 2021/2022[123] o regulador das comunicações no Reino Unido (Ofcom) trouxe como uma das metas para o período o combate a chamadas indesejadas e golpes. Nesse contexto, o regulador pretende continuar o trabalho junto a provedores de comunicação para interromper e evitar tais comunicações indesejadas, bem como expandir as possíveis ações. Reforça ainda a importância do trabalho conjunto com outras agências de fiscalização, como o Information Commissioner's Office (ICO), órgãos de interesse do consumidor e reguladores internacionais, para compartilhar inteligência e melhores práticas no combate a esse problema.

O Reino Unido tem desde 2013 um plano de ação[124] onde o Information Commissioner's Office (ICO) e o Ofcom buscam combater os danos causados por ligações e mensagens indesejadas. Tal plano é revisado periodicamente. O escopo de atuação das duas entidades ficou divido da seguinte forma:(i) chamadas de marketing (ao vivo e gravadas), que são regulamentadas pelo ICO; e (ii)chamadas silenciosas e chamadas abandonadas, que são regulamentadas pelo Ofcom.

Em recente estudo divulgado pela Ofcom[125] percebeu-se um leve aumento de reclamações em 2021 tanto em ligações silenciosas quanto em ligações que são abandonadas.

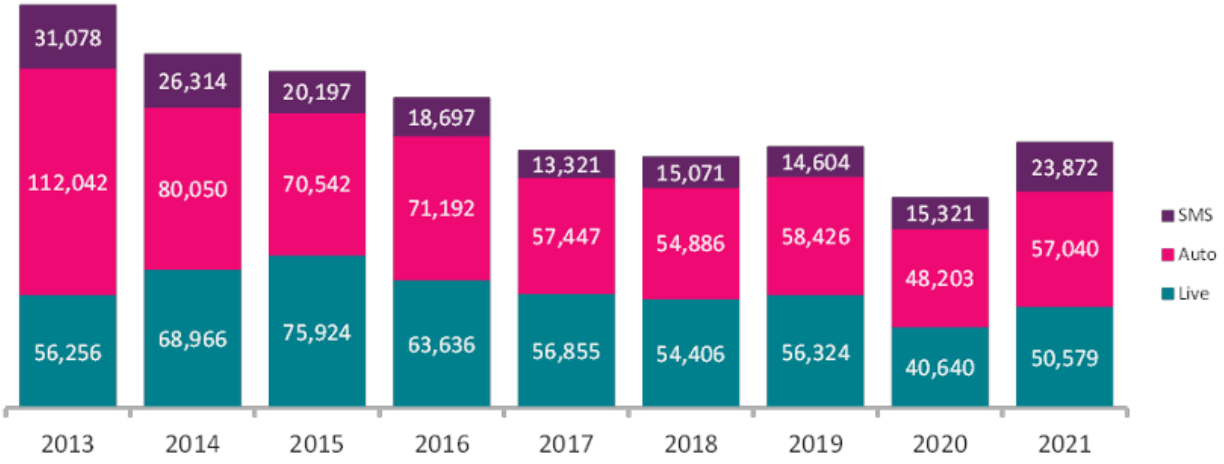


Source: Ofcom consumer complaints data.

Note: A category for 'other' unwanted calls (i.e. defined as all calls other than silent and abandoned calls) was added in 2020).

Figura 7 – Reclamações dos consumidores a Ofcom sobre chamadas abandonadas ou silenciosas (2013 a setembro 2021)

As reclamações na ICO também aumentaram em 2021, seja em ligações ao vivo, ligações automatizadas e por recebimento de SMS, conforme pode ser visto no gráfico abaixo:



Source: ICO, OLRT complaints data.

Figura 8 – Reclamações para a ICO sobre chamadas automatizadas ou ao vivo (2013 a dezembro 2021)

O perfil de tais ligações pode ser avaliado conforme dados da pesquisa realizada pela empresa TRUECALLER[126] em 2020. Percebe-se que a maior parte das ligações são do tipo ligações fraudulentas (36%), seguido do setor de vendas/telemarketing (23%), setor de seguros (22%), setor financeiro e coletores de débito (19%).

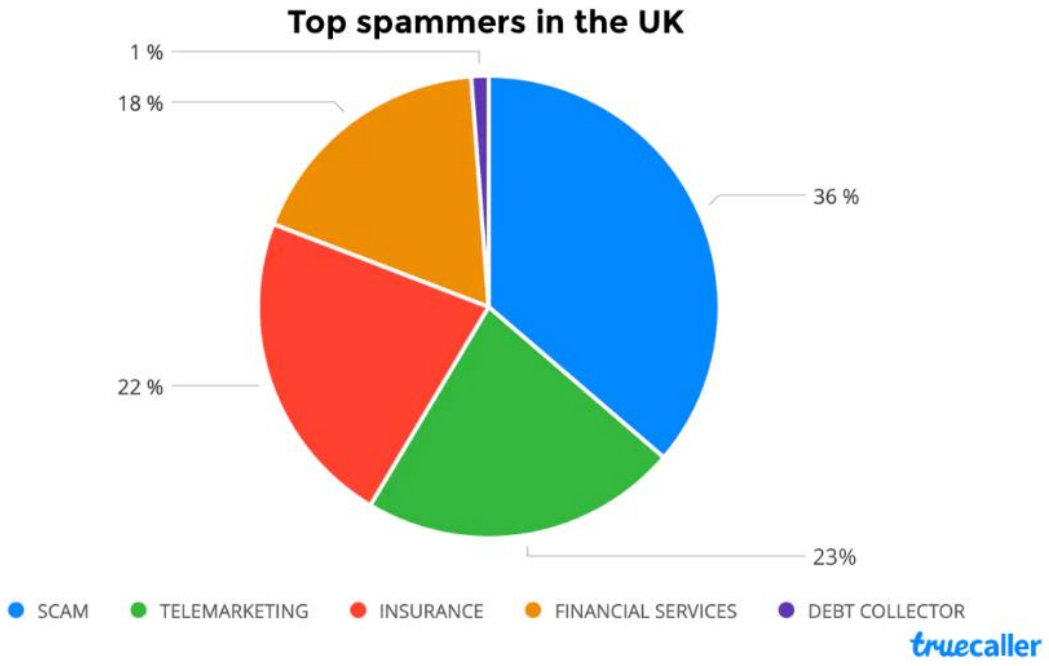


Figura 9 – Distribuição dos tipos de chamadas indesejadas no Reino Unido 2020

Assim como a Espanha, o Reino Unido estava na lista dos 20 países com mais spam em 2018. Em 2020, o Reino Unido viu um aumento de 159% nas chamadas de spam, tornando-se o 4º país com mais spam na Europa e o 7º no mundo. Importante observar que as chamadas fraudulentas representam mais de um terço das principais chamadas indesejadas no Reino Unido (tais chamadas podem trazer impactos financeiros significativos para os usuários).

Em consulta recente (abril/2022[127]) a OFCOM está propondo novas medidas para minimizar os impactos das ligações indesejadas, uma vez que foi identificado que as chamadas indesejadas agora estão mais difíceis de detectar, houve uma mudança de chamadas incômodas para chamadas fraudulentas, os textos fraudulentos tornaram-se predominantes e que é preciso fazer mais que as atuais iniciativas para reduzir chamadas e textos fraudulentos.

Importante observar a complexidade de atores e fluxo de informações que permeiam o tema. Abaixo a figura apresenta um resumo das principais entidades que atuam no tema no Reino Unido:

Source: Ofcom.

A Ofcom também criou diversos encartes e produtos publicitários para ampliar a conscientização dos consumidores do Reino Unido sobre o problema. Alguns exemplos abaixo:

Figura 10 – Produtos de marketing para ampliar a conscientização dos consumidores sobre o tema[128]

Figura 11 – Exemplos de mídia simplificado para ampliar a conscientização dos consumidores sobre o tema[129]

Como principais recomendações aos usuários dos serviços de telecomunicações o regulador do reino unido apresenta as seguintes dicas[130]:

Maneiras de bloquear diferentes tipos de chamadas	i. Fale com sua operadora de telefonia sobre os serviços contenção de comunicações indesejadas que ela oferece. ii. Considere um bloqueador de chamadas. Estes são aplicativos que você pode instalar no seu telefone ou que já podem fazer parte de um telefone. Eles podem ser usados para bloquear diferentes tipos de chamadas. iii. Antes de decidir, ativar ou instalar esses produtos, leia atentamente as instruções para garantir que eles não bloqueiem as chamadas que você deseja receber.
Registre-se gratuitamente no Serviço de Preferências Telefônicas (TPS)	i. O Serviço de Preferência Telefônica (TPS) permite que os consumidores optem por não receber quaisquer chamadas de televendas não solicitadas. ii. É possível registrar o número de telefone - fixo ou móvel - on-line em http://www.tpsonline.org.uk ou pelo telefone 0845 070 0707. iii. O registro é gratuito e leva até 28 dias para entrar em vigor. iv. É uma exigência legal que os operadores de telemarketing não liguem para um número registrado no TPS
Observe atentamente a caixas de opções de “opt-in” ou “opt-out” de marketing das empresas	i. Tenha cuidado para quem você fornece seus detalhes de contato. Quando você precisar fornecê-los, por exemplo, ao comprar algo, entrar em uma competição ou usar um site de comparação de preços, certifique-se de olhar atentamente para as regras das caixas de marketing de “opt-in” ou “opt-out”. Às vezes, essas caixas podem ser projetadas com letras pequenas e geralmente são encontradas perto da parte onde é necessária uma assinatura. ii. Uma caixa “opt-in” geralmente se refere a uma caixa que, se marcada, confirma que você concorda em ser contatado pela empresa ou outras empresas (conhecidas como “terceiros” ou “partes confiáveis”). iii. Com uma caixa "opt-out", você concorda em ser contatado, a menos que marque a caixa. Fique atento a frases como “marque aqui para desativar” ou, se você estiver online, caixas pop-up convidando você a receber o boletim informativo de uma empresa.
O que fazer ao receber chamadas e mensagens incômodas	i. Considere filtrar suas chamadas: pode-se usar um telefone que exibe o número do chamador - conhecido como "ID do chamador" ou "Identidade da linha de chamada" (CLI), ou usando uma secretária eletrônica ou correio de voz. ii. Peça os detalhes do chamador: o nome da organização endereço ou um número de telefone para retorno. Você pode tais informações para notificar a organização de que você não deseja mais receber chamadas de vendas. iii. Não forneça seus dados pessoais. Se alguém ligar para você pedindo informações financeiras pessoais, não as

	forneça. Em vez disso, desligue e ligue para o número de telefone no extrato de sua conta, ou no site da empresa ou do departamento governamental para verificar se a chamada era genuína. Espere pelo menos cinco minutos antes de fazer a ligação – isso garante que a linha foi liberada e que você não está falando com o fraudador ou cúmplice. iv. Ao receber mensagens de texto indesejadas, encaminhe o texto para 7726. Não responda ao texto. Se você responder, a empresa saberá que você leu o texto. Eles podem entrar em contato com você novamente. Não aperte em nenhum link encaminhado.
Reclamações	i. Se você receber uma ligação indesejada, você pode fazer uma reclamação: ii. As informações de reclamações ajudam os reguladores, como ICO e o Ofcom, a tomar medidas direcionadas contra aqueles que fazem ligações ilegalmente. iii. Ao receber uma ligação incômoda, faça uma breve anotação da ligação, se puder, incluindo a data, hora, nome da empresa (se for conhecida) e o número de onde você foi chamado (mesmo que não pareça um número de telefone válido). Em seguida, faça uma reclamação à organização ou regulador relevante

Abaixo quadro resumo das principais legislações afetas ao tema bem como os principais atores e sua atuação no Reino Unido:

Principais Legislações	a) **Privacy and Electronic Communications Regulations (PECR)**: concedem às pessoas direitos específicos de privacidade em relação às comunicações eletrônicas. Existem regras específicas sobre: chamadas de marketing, e-mails, textos e faxes; cookies (e tecnologias semelhantes); manter os serviços de comunicações seguros; e privacidade do cliente em relação a dados de tráfego e localização, faturamento detalhado, identificação de linha e listagens de diretório. b) **Communications Act 2003**: estabelece as competências da Ofcom; sobre a regulamentação da oferta de redes e serviços de comunicações eletrônicas e da utilização do espectro eletromagnético; dentre outros. c) **UK GPDR**: As disposições do GDPR da UE foram incorporadas diretamente à lei do Reino Unido como o UK GDPR. Na prática, há poucas mudanças nos princípios, direitos e obrigações fundamentais da proteção de dados. d) **Código Europeu de Comunicações Eletrônicas (EECC)**:Diretiva da EU que atualizou o marco regulatório dos serviços de comunicações eletrônicas. Embora o Reino Unido tenha saído da UE em 31 de janeiro de 2020, nos termos da o Acordo de Saída, o Reino Unido permaneceu sob a obrigação de implementar o EECC. O governo do Reino Unido fez alterações no Communications Act 2003 para implementar vários requisitos do EECC na legislação nacional. Tais medidas são destinadas a proteger os clientes de serviços de comunicações eletrônicas, incluindo serviços de banda larga, móveis e fixos.
Divisão de Responsabilidades	A responsabilidade pelo gerenciamento de comunicações não solicitadas é dividida entre o *Information Commissioner's Office (ICO)* e o Ofcom. A abordagem do Reino Unido para gerenciar comunicações não solicitadas consiste em:

	• o ICO é responsável pela regulamentação de comunicações de marketing não solicitadas sob o PECR. O conteúdo de marketing é um requisito para o envolvimento da ICO; e • O Ofcom é responsável pela regulamentação de chamadas silenciosas e abandonadas e questões gerais relacionadas à rede, sob a Lei de Comunicações. Além de suas funções de comunicações não solicitadas sob o PECR, o ICO abrange vários outros atos e regulamentos, incluindo a Lei de Proteção de Dados de 1998. É responsável pela comunicação com a indústria sobre a conformidade com o PECR e a UK GDPR, coleta todas as reclamações e coordena ação de execução contra os infratores desses regulamentos. O Ofcom, sob a Lei de Comunicações de 2003, é responsável por grande parte do desenvolvimento da regulamentação relativa à elaboração de regras técnicas – isto é, o que os provedores de telecomunicações podem e não podem fazer – bem como algumas atividades de fiscalização. As responsabilidades do Ofcom em relação ao gerenciamento de comunicações não solicitadas centram-se em trabalhar com provedores de comunicações para fortalecer sistemas e processos para bloquear comunicações de spam antes que elas cheguem aos consumidores (cobrindo chamadas abandonadas e silenciosas). O Ofcom também desempenha um papel fundamental no incentivo e facilitação de soluções técnicas do setor para o spam telefônico. **Lista nacional de não perturbe (Telephone Preference Service - TPS)** – é mantida com recursos da indústria de marketing direto. A gestão do TPS/CTPS recebe reclamações e pode solicitar explicações a quem fez ligação indevida, mas não tem poderes de enforcement. Ao longo de 2017, os sistemas de relatórios de reclamações do TPS/CTPS e da ICO foram integrados, contribuindo para o recebimento mais rápido e para avaliação de inteligência por parte da Comissão. ICO – Tem a responsabilidade estatutária sobre o TPS desde 2017, utilizando-se dos dados do mesmo para realizar enforcement. É a agência responsável por tomar medidas contra as empresas que infringem a *Privacy and Electronic Communication Regulations* de 2003 (PECR) por ligações ilegais de marketing, sejam “ao vivo” ou gravadas, ou envio de mensagens de texto ou e-mails incômodos.

ANEXO C - AUSTRÁLIA

O governo australiano também definiu o combate as práticas de fraudes por telefone, roubo de identidade por SMS e regras de cancelamento de assinatura como prioridades de conformidade para 2022–23[131].

Abaixo um resumo das Principais ações sobre spam e telemarketing realizadas pela ACMA entre abril a junho de 2022:

- Multas: O Wine Group pagou US$ 204.240 em multas por violar as leis de spam e telemarketing.
- Novas Regras: Foram criadas regras para proteger os consumidores de golpes que visam interações de clientes com sua empresa de telecomunicações. Isso inclui a mudança de *SIMs Cards* para novos dispositivos.
- Alertas: Alertamos o público sobre golpes envolvendo investimentos financeiros e golpes de kits de teste COVID-19.
- Bloqueio de chamadas fraudulentas: Mais de 660 milhões de chamadas fraudulentas bloqueadas desde que as novas regras começaram em dezembro de 2020.

Em 2020 o regulador australiano criou um plano de ação para o enfrentamento do problema de ligações fraudulentas conforme síntese abaixo:

Our action plan

Our Combating scams report called for immediate action to tackle common scams.

It featured a three-point action plan to reduce scam calls. Telco industry and government stakeholders worked together to complete action items in 2020.

	Action	Lead	Status
1	Establish a scam telecommunications action taskforce (STAT) to provide government and industry coordination and oversight of telecommunications scam minimisation strategies.	ACMA	✓ STAT met 3 times over 2020 and will continue meeting in 2021.
2	Develop enforceable obligations for telco providers to detect, trace, block and otherwise disrupt scam calls.	Telco industry/ACMA	✓ *Reducing Scam Calls Industry Code* registered 2 December 2020. Published phone scam educational resources to raise awareness about phone scams and how to combat them.
3	Immediate trials of industry-wide scam reduction initiatives.	Telco industry	✓ Telcos trialled scam reduction ideas and blocked over 30 million scam calls in 2020.

Figura 12 – Resumo do plano de ação da ACMA criado em 2020 para combater chamadas fraudulentas

O regulador australiano definiu como prioridades para 2021/22 o marketing ilegal de serviços financeiros e os golpes telefônicos.

Com relação ao Marketing ilegal de serviços financeiros as principais ações e resultados de conformidade e fiscalização desde que eles iniciaram suas atividades incluem: (i) 861 alertas de conformidade enviados a empresas que comercializam produtos de serviços financeiros, informando-as sobre possíveis problemas de conformidade com leis de spam e telemarketing. (ii) 7 investigações concluídas em empresas de serviços financeiros. (iii) Redução de 36,8% nas reclamações de spam e telemarketing em negócios de serviços financeiros.

Com relação ao combate a golpes de telefone, o regulador australiano executou as seguintes atividades: (i) Anunciou que as empresas de telecomunicações relataram o bloqueio de mais de 660 milhões de chamadas fraudulentas sob o “Reducing Scam Calls” (Redução de chamadas fraudulentas) (ii) conforme as novas regras a ACMA compartilha os dados de reclamação desidentificados para ajudar as empresas de telecomunicações a identificar essas chamadas. (iii) Novas regras foram criadas para proteger os consumidores de golpes que visam interações de alto risco de clientes com empresas de telecomunicações. Isso inclui solicitações de troca de SIM e consultas de cobrança. (iv) Notificou formalmente o Symbio Group por violar as regras que exigem

a investigação e o compartilhamento de informações sobre chamadas fraudulentas sob o código Redução de chamadas fraudulentas (v) Alertou os consumidores sobre os golpistas que enviavam SMS e mensagens de e-mail de entrega de encomendas com links de aparência incomum ou solicitações para pagar uma taxa para concluir a entrega. (vi) Trabalhou nos bastidores com empresas de telecomunicações, agências governamentais e outras marcas confiáveis para interromper golpes telefônicos.

Para o exercício financeiro de 2022–23, foram estabelecidas 2 novas frentes relacionadas a comunicações não solicitadas: (i) Combate a golpes de telefone SMS e roubo de identidade. Isso envolve a aplicação de novas regras nas empresas de telecomunicações para usar verificações de identidade mais fortes e estabelecer novas regras para reduzir os golpes de SMS. (ii) Aplicação de regras de cancelamento de assinatura de SMS e e-mail. A ACMA irá concentrar esforços em empresas que não seguem as solicitações de cancelamento de assinatura dos clientes ou dificultam o cancelamento da assinatura.

Abaixo o gráfico resumo das investigações conduzidas e finalizadas pela ACMA entre 2019-2022 sobre o tema.

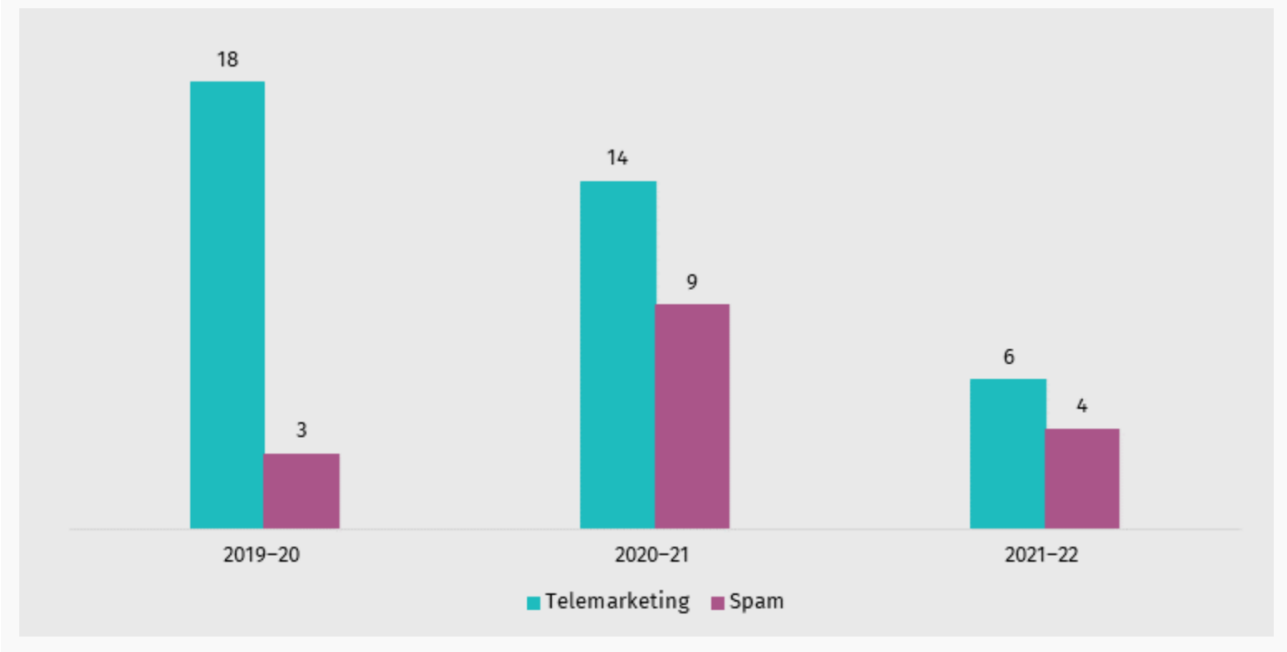


Figura 13 – Investigações sobre o tema finalizadas pela ACMA 2019-2022.

As reclamações dos consumidores são utilizadas como fonte de informação direta para as ações da ACMA e ajudam a identificar problemas e tendências. Também são fornecidos dados de reclamação não identificados às empresas de telecomunicações para ajudá-las a identificar e bloquear chamadas fraudulentas. As reclamações mais comuns foram sobre varejo, serviços financeiros e setores de construção/manutenção.

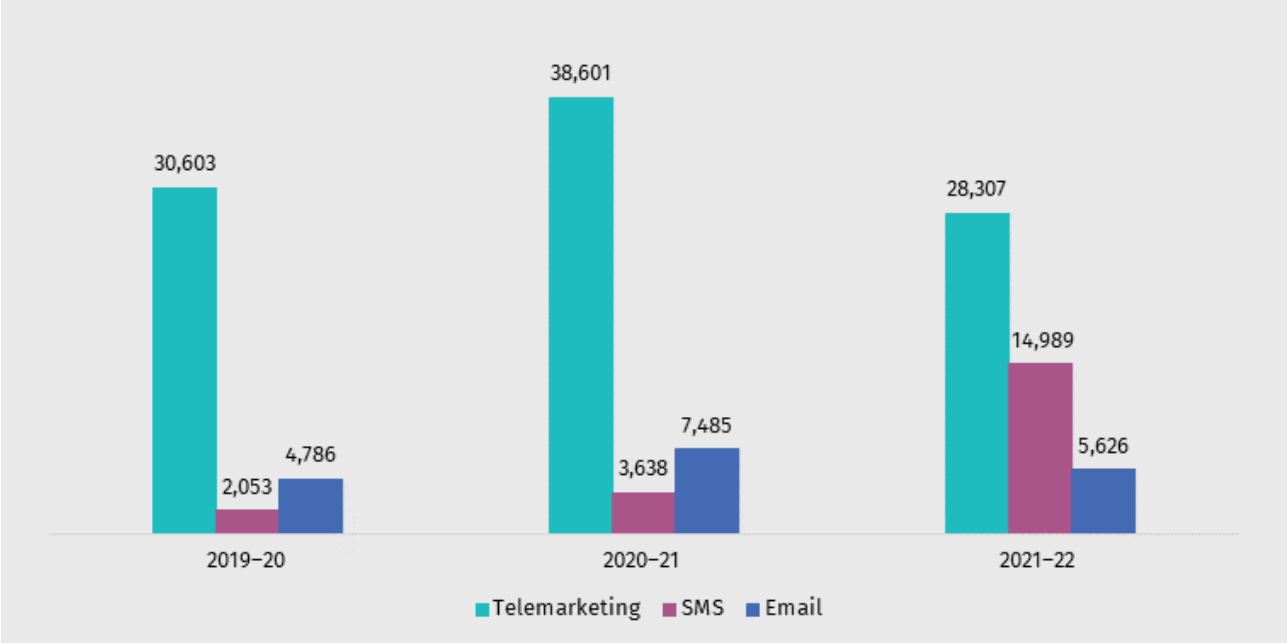


Figura 14 – Tipos de ligações indesejadas nas reclamações recebidas pela ACMA 2019 – 2022. Observação: também foram recebidas 67 reclamações sobre mensagens instantâneas comerciais em 2021–22.

Importante destacar que o Regulador australiano revisou o Código Industrial C661:2022 que tem por objetivo a Redução de chamadas fraudulentas e SMS fraudulentos: Este Código foi concebido para estabelecer processos para identificar, rastrear, bloquear e interromper chamadas fraudulentas e SMS fraudulentos.

A ACMA também criou diversos encartes e produtos publicitários para ampliar a conscientização dos consumidores da Austrália sobre o problema. Alguns exemplos abaixo:

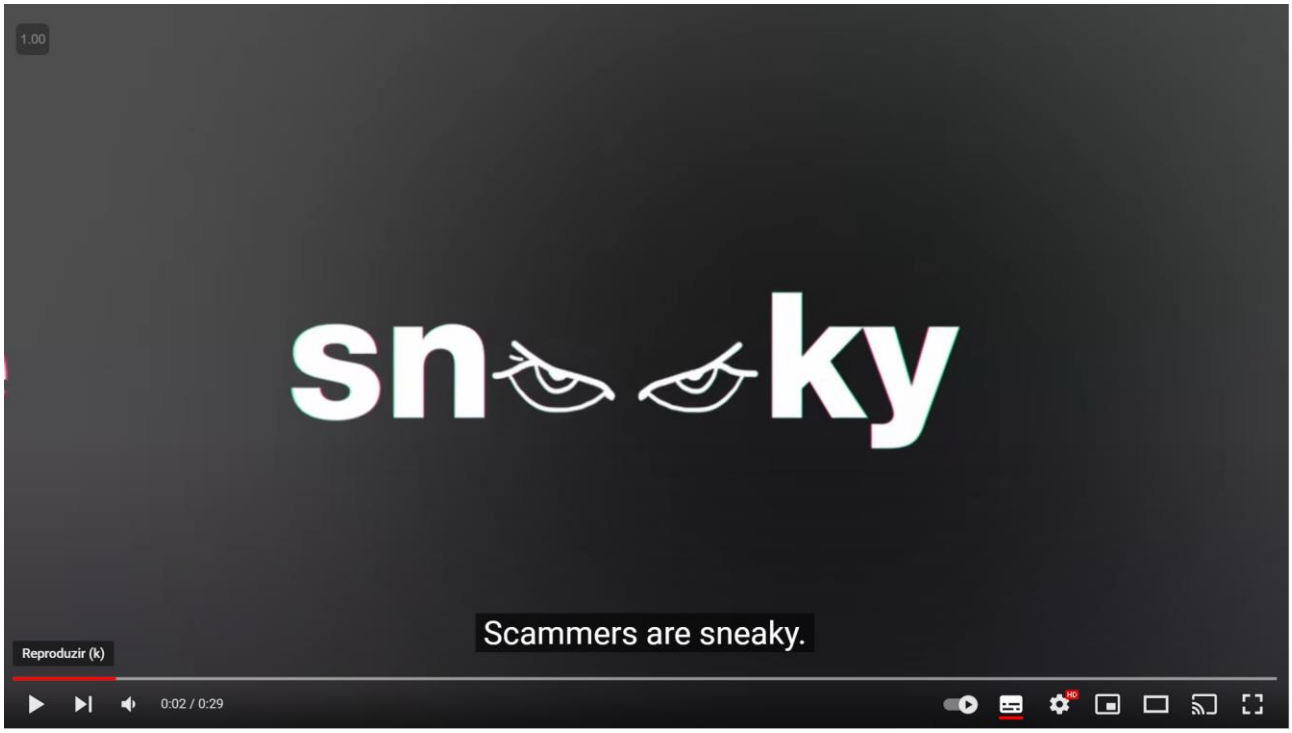


Figura 15 - Vídeo sobre chamadas fraudulentas[132]

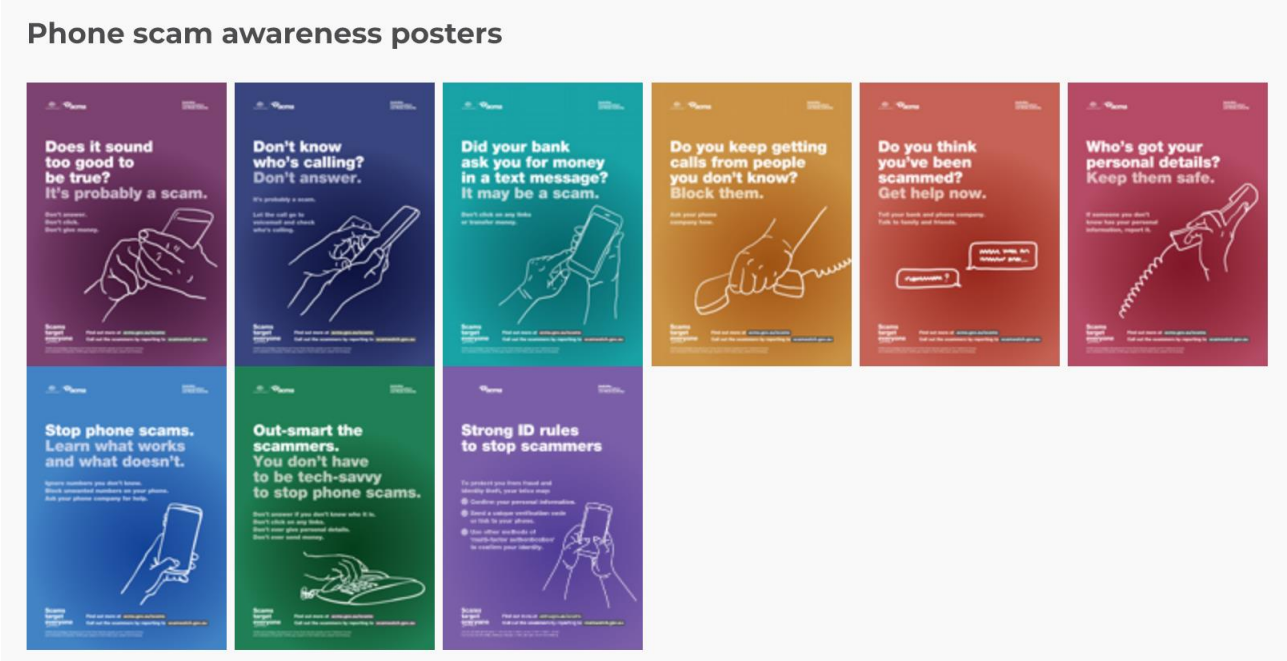


Figura 16 - Esses 9 pôsteres em inglês destacam ações comuns para combater golpes por telefone.

Cada um se concentra em um tópico de fraude diferente. Podem ser usados individualmente ou em conjunto[133].

Como principais recomendações aos usuários dos serviços de telecomunicações o regulador australiano apresenta as seguintes dicas[134]:

Como funciona o registro de não chamar	i. O Do Not Call Register é como um sinal de 'não perturbe' que reduz o telemarketing. É rápido e fácil adicionar o seu: (a) número de telefone residencial, (b) número de celular pessoal e (c) número de fax ii. Você não pode adicionar um número de telefone comercial ao Registro de Não Chamar. iii. Registro online ou ligue para 1300 792 958. Gerenciamos este serviço para o governo australiano iv. Após 30 dias de registro do seu número, o telemarketing só poderá ligar para você: se você deu permissão ou se eles forem isentos v. Mesmo que você dê permissão a uma empresa para ligar para você, você pode dizer a eles a qualquer momento se deseja retirar essa permissão.
O que é telemarketing	Telemarketing é qualquer chamada em que o chamador tem como objetivo vender, anunciar ou promover bens ou serviços.
O que não é telemarketing?	i. Se um chamador não está tentando vender, promover ou anunciar algo para você, não é telemarketing. Por exemplo, eles podem ligar sobre: (a) cobrança de dívida, (b) um lembrete de compromisso, (c) uma falha com um produto ou serviço ii. Chamadas de pesquisa ou pesquisa não são telemarketing. Eles ainda devem seguir as outras regras que protegem você.
Chamadas que você pode receber mesmo com o número na lista de não me perturbe.	i. organizações ou agências governamentais ii. instituições de caridade registradas iii. instituições de ensino onde você é ou foi aluno iv. partidos políticos registrados v. membros do Parlamento vi. candidato em uma eleição
Regras que protegem o usuário	i. Só é permitido ligar em determinados horários do dia. (antes das 9h ou depois das 20h durante a semana, antes das 9h ou depois das 17h aos sábados, a qualquer hora em um domingo ou feriado nacional) ii. O originador deve dizer o nome, o nome do empregador e (se estiverem chamando por outra pessoa), o nome de quem representam. iii. Informar o motivo da ligação iv. Encerrar a chamada se você pedir ou indicar que não deseja continuar v. Possuir um identificador de chamadas exibindo um número de retorno para você usar para obter mais informações

Abaixo quadro resumo das principais legislações afetas ao tema bem como os principais atores e sua atuação na Austrália:

Principais Legislações	(a) the Competition and Consumer Act 2010. (b) the Telecommunications Numbering Plan 2015. (c) the Do Not Call Register Act 2006 [135] : estabelece o registro e descreve as regras para fazer chamadas de telemarketing não solicitadas e enviar faxes de marketing não solicitados para números no registro (d) the Criminal Code Act 1995.

	(e) the Privacy Act 1988. (f) the **Spam Act 2003**[136]. (g) the Telecommunications (Consumer Protection and Service Standards) Act 1999. (h) the Telecommunications (Emergency Call Service) Determination 2019. (i) the Telecommunications (Interception and Access Regulations 2017. (j) Do Not Call Register Regulations 2017: especifica os tipos de chamadas que não são chamadas de telemarketing e as pessoas consideradas indicadas de um titular de conta relevante (l) Telemarketing Industry Standard 2017[137]: define os requisitos mínimos para aqueles que fazem chamadas de telemarketing e pesquisa para números australianos, incluindo quando e como eles podem fazer determinadas chamadas; (k) **Código Industrial C661:2022** Redução de chamadas fraudulentas e SMS fraudulentos: Este Código foi concebido para estabelecer processos para identificar, rastrear, bloquear e interromper chamadas fraudulentas e SMS fraudulentos. (m) **Telecommunications Service Provider Determination (Customer Identity Authentication) 2022**
Divisão de Responsabilidades	A responsabilidade pela gestão das comunicações não solicitadas é da Autoridade de Comunicações e Midia Australiana (ACMA - *Australian Media and Communications Authority*). Ela gerencia o registro de Não me pertube da Australia, inclusive respondendo a violações da legislação. Realizaçao procedimentos de fiscalização, compliance e aplica sanções nos casos pertinentes.

ANEXO D - ÍNDIA

O mercado indiano de telecomunicações conta com mais de 1,2 bilhões de usuários móveis, dos quais mais de 230 milhões estão cadastrados no sistema de não me perturbe local[138].

Conforme último relatório da Truecaller a Índia aparece como quarto país com mais ligações indesejadas em 2021, sendo 93% do setor de vendas. Interessante notar que quando se fala em SMS indesejados a Índia não aparece na lista dos 20 países que mais recebem tais mensagens.

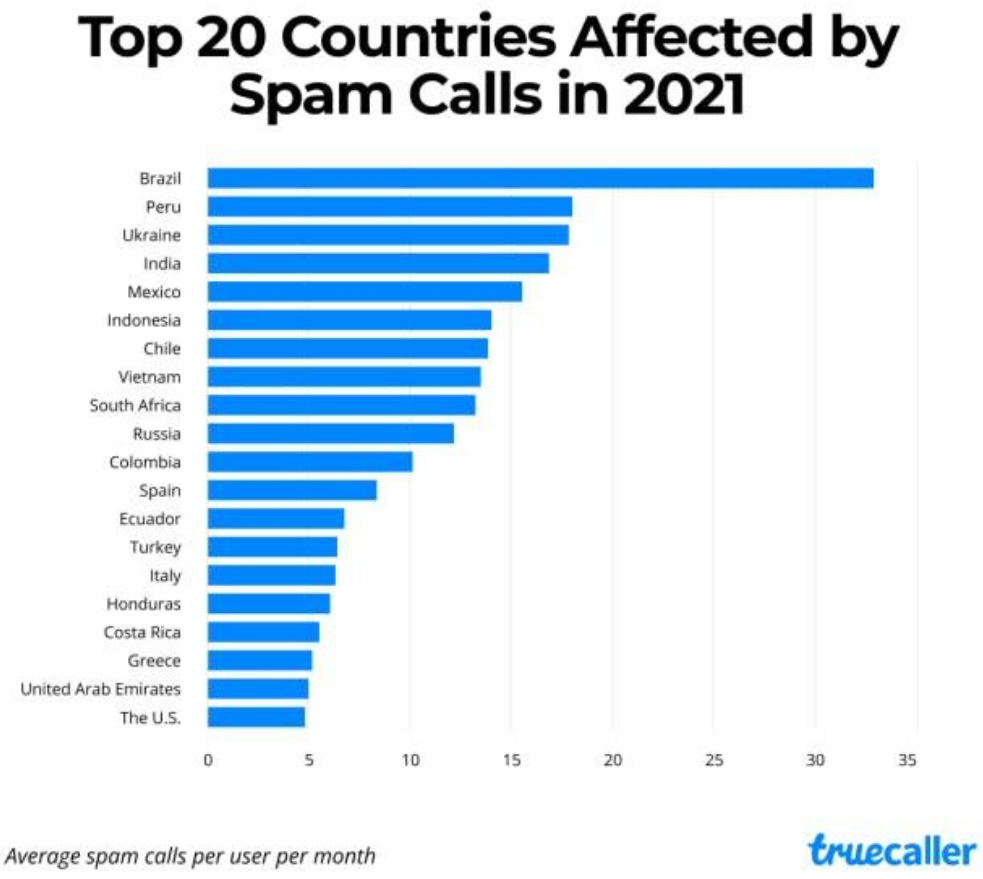


Figura 17 – Top 20 países mais afetados pelas chamadas indesejadas em 2021

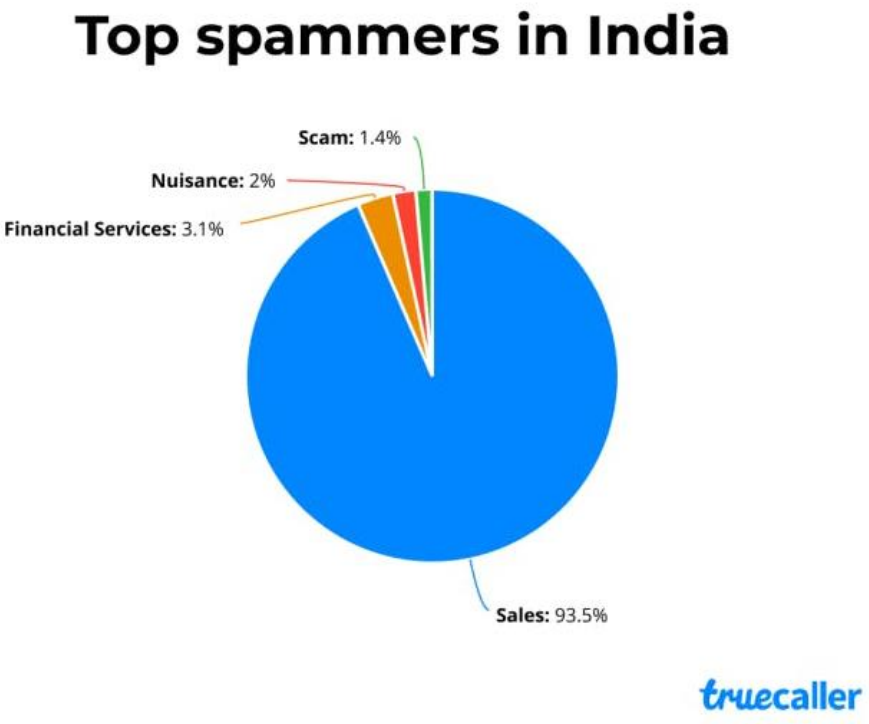


Figura 18 – Principais segmentos de chamadas indesejadas na Índia

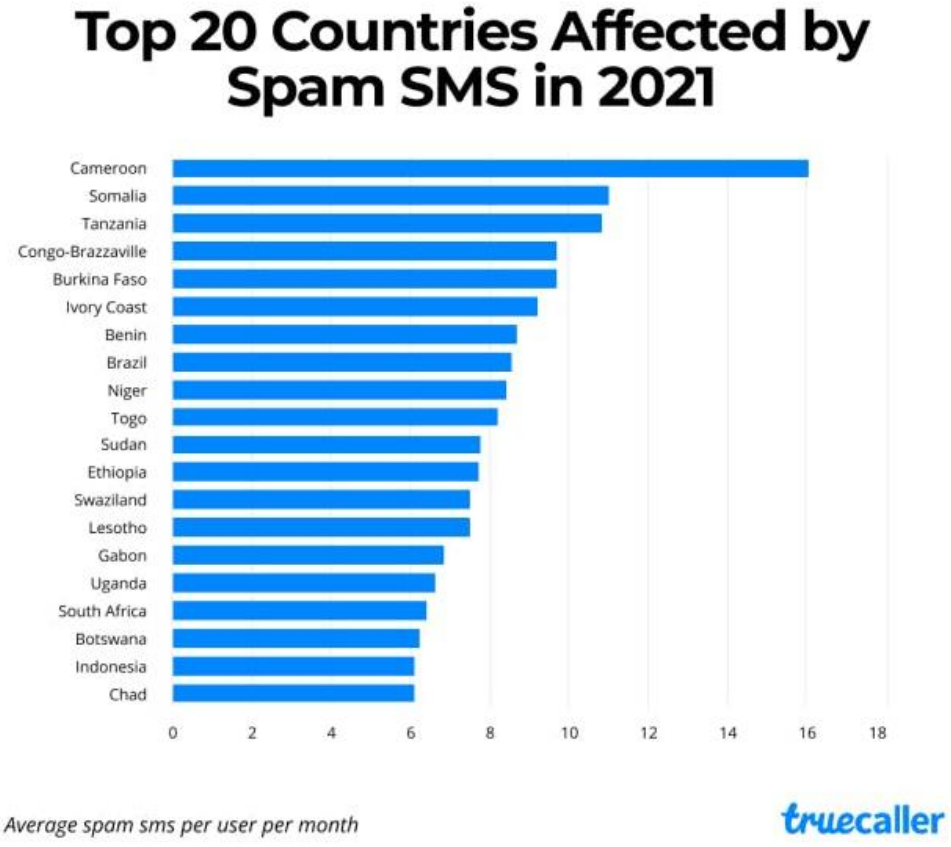


Figura 19 Top 20 países que são mais afetados pelas mensagens de texto (SMS) indesejadas.

A estratégia da Índia contra as mensagens indesejadas parece estar surtindo efeito. Em 2018 o regulador indiano TRAI publicou o Telecom Commercial Communication Customer Preference Regulation (TCCCPR), 2018[139], criado para proteger os clientes das Comunicações Comerciais Não Solicitadas (UCC) e ajudar as Empresas (entidades principais) a enviar comunicações comerciais aos clientes que optaram pelos seus serviços ou definiram as suas preferências e consentimentos. O regulamento TCCCP 2018, estabeleceu um procedimento para facilitar a comunicação comercial (em especial as mensagens de texto) ao destinatário certo e de acordo com a sua preferência, com a utilização de Plataformas DLT (Distributed Ledger Technology)[1] para registro de empresas de Telemarketing (TM), bem como para o registro ou revogação do consentimento do usuário e suas preferências. Aqui vale destacar que essa solução pode ser comparada a um tipo de banco de dados que é "compartilhado e atualizado independentemente por cada participante (ou nó) em uma grande rede."[140]. O sistema é governado usando a tecnologia blockchain (DLT) e todas as entidades do ecossistema são interligadas entre si. O livro distribuído registra todas as transações entre os participantes da rede. Isso cria uma rastreabilidade fim-a-fim das mensagens, bem como do processo de verificação das opções de consentimento dos usuários. As alterações em tal base de dados são feitas somente quando os participantes da rede concordam em fazê-lo por consenso, e cada registro tem um carimbo de data/hora e uma assinatura criptográfica exclusiva que permite uma auditoria precisa[141], trazendo mais transparência para todo o processo.

Dentro desse novo sistema de controle de mensagens de comunicação comercial, a Índia adotou como principais medidas regulatórias as seguintes ações:

- Cadastro obrigatório de operadores de telemarketing e Empresas que desejam enviar comunicações comerciais;
- Os consumidores podem bloquear o recebimento de mensagens promocionais por meio do registro no Cadastro Nacional de Preferências (NCPR);
- Os operadores de telemarketing devem enviar mensagens conforme a preferência cadastrada dos usuários;
- Foram estabelecidas sanções financeiras as empresas de telemarketing registrado e operadores de telecomunicações por descumprimento das normas.
- Foram criados cabeçalhos separados para mensagens de transação e promocionais.
- Foram criados uma série de números separados para chamada de voz de telemarketing.

[1] Distributed Ledger Technologies (DLT) significa um conjunto de soluções tecnológicas que permite que um registro único, sequenciado, padronizado e criptograficamente protegido de atividades seja distribuído com segurança e executado por uma rede de participantes variados e seu banco de dados possa ser distribuído vários sites ou instituições; os registros são armazenados um após o outro (blockchain) em um livro contínuo e só podem ser adicionados quando os participantes chegarem a um consenso.

- Além das sanções financeiras foi estabelecido que se pode realizar a desconexão de todos os recursos de telecomunicações e cadastro em lista negra por dois anos em caso de atividades de telemarketing por entidades não cadastradas.

Importante então entender quais são os atores desse processo e suas principais funções:

Nome	Papel
Entidade Principal (ou agentes autorizados)	É a organização que tem o interesse de realizar a comunicação com seus clientes. Pode ser um indivíduo, empresa de parceria ou qualquer entidade privada e/ou governamental. De acordo com as regras TRAI atualizadas, todas as entidades devem estar registradas nas operadoras de telecomunicações na plataforma DLT.
Executores do Processo	Os prestadores de serviços de telemarketing com auxílio de SMS ou chamadas comerciais são aqueles que fornecem esse serviço para organizações ou empresas. Toda empresa de telemarketing precisa estar registrada na plataforma DLT para enviar mensagens em nome da entidade principal.
Prestadores de serviços de telecomunicações	Esses são os prestadores de serviço de telecomunicações que estariam diretamente ligados à TRAI e auxiliariam no processo de regulação. Exemplo: Vodafone, Airtel, Idea, BSNL etc.
Regulador TRAI	A conformidade regulatória é estabelecida pelo regulador TRAI. Ele audita e rege as operações para proteger os interesses dos clientes e evitar práticas fraudulentas.
Cliente Final	O cliente final é o assinante móvel que receberá o SMS ou chamada. Ele(a) pode fornecer consentimento para receber SMS promocionais de qualquer empresa. O cliente final pode definir preferências, registrar reclamações e cancelar a assinatura a qualquer momento de acordo com as regras da TRAI.

Figura 20 - Principais atores do ecossistema de Proteção contra comunicações indesejadas a Índia.[142]

O procedimento para registro ou alteração de preferência de categorias de conteúdo para Comunicações Comerciais (CC) pode ser feito usando o **aplicativo móvel TRAI DND 3.0**[2], ligando para uma central e escolhendo as opções, uma ligação para um número específico para cada opção ou ainda com envio de SMS conforme está resumido na tabela abaixo:

Categorias de CC para serem bloqueadas (opted out)	IVRS: chamadas para 1909 e pressione o número para bloqueio	SMS: Mande SMS para 1909 com o seguinte texto	USSD: Disque o número XXX seguido de uma opção
Todas as categorias de CC (para serem bloqueadas)	0	FULLY BLOCK	*1909*0#
Bancário/Seguros/Financeiro	1	BLOCK 1	*1909*1#
Imobiliário	2	BLOCK 2	*1909*2#
Educação	3	BLOCK 3	*1909*3#
Saúde	4	BLOCK 4	*1909*4#
Bens de Consumo	5	BLOCK 5	*1909*5#
TICs e Entretenimento	6	BLOCK 6	*1909*6#
Turismo/Lazer	7	BLOCK 7	*1909*7#
Alimentos/Bebidas	8	BLOCK 8	*1909*8#

O procedimento para aderir as categorias é similar alterando apenas os números (Ex: 90 para liberar todas as chamadas, UNBLOCK ALL a mensagem de SMS e *1909*90# para a ligação direta).

Outros números podem ser utilizados para liberar ou bloquear horários específicos, dias da semana, tipos de chamada (Ex: opt-out Chamada de voz 11, SMS 12, Chamada gravada 13, Chamada gravada para atendente 14, *RoboCalls* 15).

A plataforma DLT permite o registro de Operadores de Telemarketing ou Empresas Anunciantes. Para empresas de Telemarketing foram identificados dois tipos: (i) Agregador de Telemarketing: Não possui conexão direta com a operadora de telecomunicações. (ii) Entrega de Telemarketing: Coleta o tráfego de SMS/voz das empresas.

As empresas anunciantes são empresas que lidam com produtos ou serviços que gostariam de se conectar com seus clientes por meio de SMS para aumentar suas vendas. Assim a empresa anunciante precisa ser registrada na plataforma DLT de acordo com as regras TRAI uma vez que

[2] TRAI DND 3.0 (Não Perturbe): O aplicativo tem seguintes recursos: Um mecanismo inteligente de detecção de spam (somente para SMS) para auxiliar o assinante na geração de relatórios; Crowdsourcing de dados sobre mensagens e chamadas ofensivas para acelerar a detecção de operadores de telemarketing não registrados; atualizações sobre ações tomadas em reclamações dentro do App; Interface e configuração mais fáceis.

terá que demonstrar o consentimento de seus clientes bem como suas preferências, os quais receberão as comunicações comerciais.

A plataforma DLT mantém registros de todas as transações realizadas pelos participantes da rede. As mensagens de comunicação como OTP (*one-time password* – senha de uso único), códigos de verificação, notificação etc., enviadas por empresas para seus clientes precisam ser registradas na plataforma TRAI DLT.

Todas as operadoras de telecomunicações implementaram suas plataformas DLT[143]. Dessa forma as empresas de telemarketing e entidades principais podem escolher dentre tais empresas para fazer o registro na plataforma DLT. Um número de registro exclusivo será emitido conforme o cadastramento como operador de telemarketing ou empresa na primeira fase do registro DLT[144].

Os principais benefícios para o cliente dessa solução são: (i) O uso da tecnologia *blockchain* aumenta a segurança e privacidade do processo. (ii) O registro separado para operadores de telemarketing e empresas oferece mais transparência. (iii) O consentimento do cliente é necessário antes de enviar o SMS, até mesmo o horário do slot é selecionado pelos clientes.

Como benefícios para as empresas: (i) Alcance mais direcionado aos clientes. (ii) Todos os cabeçalhos e *templates* são registrados na plataforma. (iii) Melhor comunicação com os clientes que realmente desejam receber suas informações (iv) Práticas de marketing aprimoradas para atingir seu público-alvo.

Apenas a operadora de telefonia dos assinantes tem acesso aos dados originais dos clientes. Para todas as outras empresas, os dados de consentimento estão disponíveis apenas em formato criptografado e com *hash* para dar suporte à depuração. À primeira vista, o DLT parece ser uma solução robusta para lidar com spam.

Assim o registro do consentimento dos clientes é feito na plataforma do provedor principal e pode ser replicado para todas as empresas de telemarketing. Cada empresa de telecomunicações tem um ou mais nós na rede DLT que armazena uma impressão digital ou *hash* dos consentimentos, bem como informações de preferência para todos os assinantes, não apenas para os seus. A solução é semelhante para voz e SMS. Quando uma empresa de marketing deseja enviar uma mensagem em nome de uma marca, ela precisa se registrar e pré-aprovar certos dados de "cabeçalho" com a empresa de telecomunicações remetente, como o número de onde enviará e o título 'mensagem da marca X'. Quando estiver pronto, ele fornece um modelo de conteúdo de mensagem e uma lista de números. Abaixo uma visão dos elementos desse processo[145]

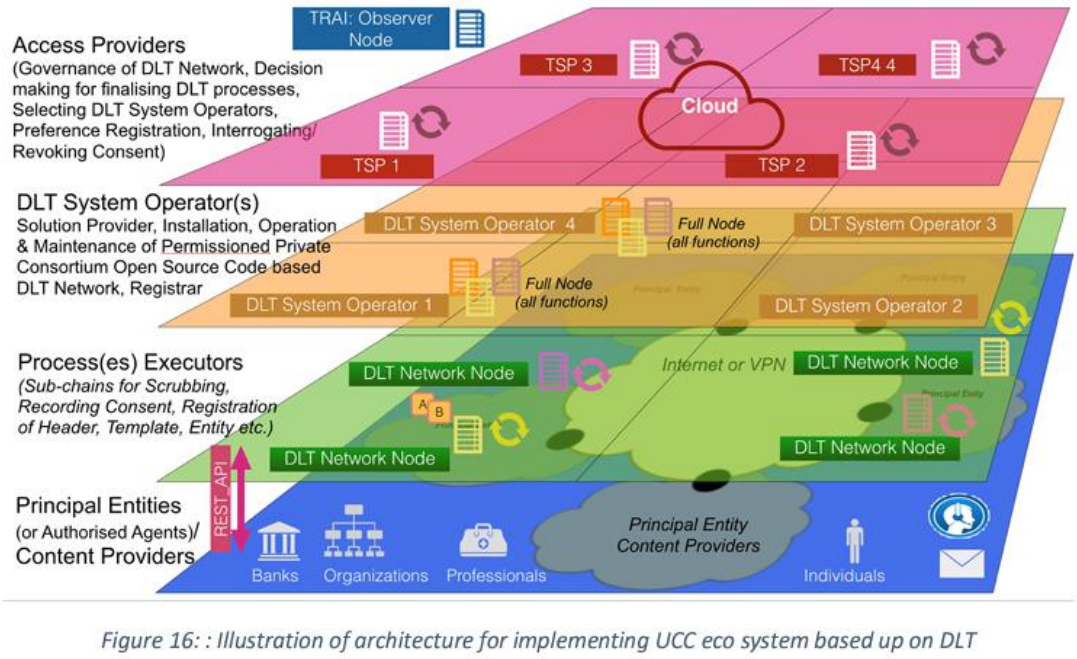


Figure 16: : Illustration of architecture for implementing UCC eco system based up on DLT

Figura 21 – Ilustração da arquitetura para implementar o Sistema UCC baseado em DLT[146]

A operadora de telecomunicações de envio ou de origem realiza a depuração para cruzar os dados com os consentimentos e preferências do assinante. Ele armazena o fato da verificação no *blockchain* para que a operadora de telecomunicações do assinante possa verificar se a depuração aconteceu e a mensagem só é enviada se estiver tudo confirmado.

Os consumidores podem registrar reclamações que são inseridas no *blockchain*, e a empresa de telecomunicações que enviou a mensagem deve investigar imediatamente e restringir a empresa de telemarketing bem como a empresa de comunicação comercial remetente se o assinante não fornecer consentimento. Se não o fizer ou atrasar, há multas pesadas na prestadora de telecomunicações, podendo chegar à perda de sua licença.

Em recente estudo acadêmico[147] foi avaliada a estratégia criada pelo regulador indiano no combate a ligações indesejadas. O gráfico extraído de tal estudo mostra uma linha do tempo do número de reclamações contra operadores de telemarketing registrados (RTM) e não registrados (UTM) ao longo do tempo. A introdução do sistema Blockchain da TRAI mostra uma diminuição do número de reclamações contra empresas de telemarketing cadastrados enquanto o número de reclamações contra UTM continuam aumentando.

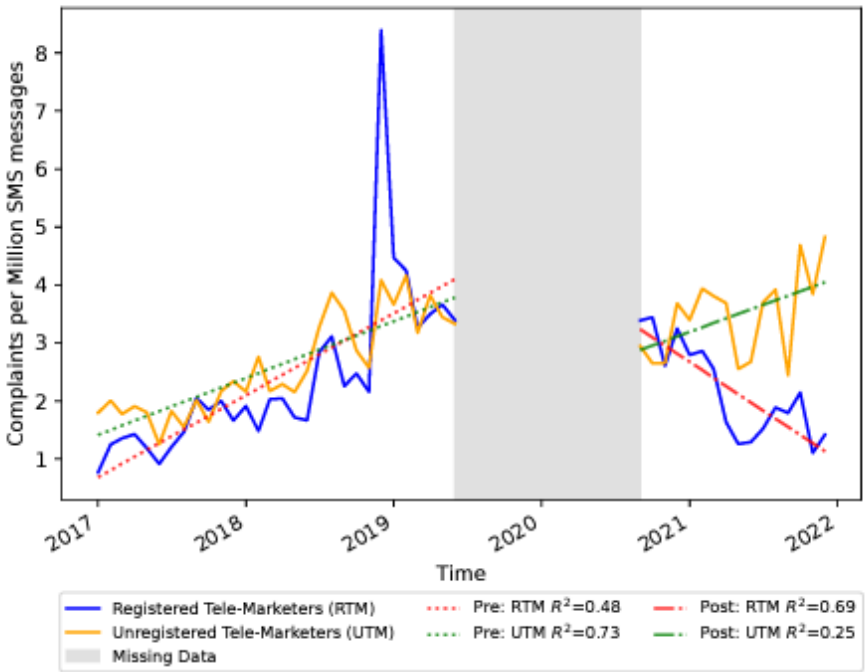


Figura 22 – Evolução das reclamações contra empresas de telemarketing registradas e não registradas (2017 a 2022).

Dessa forma, percebe-se que a solução indiana tem resultados positivos, desde que, as empresas de telemarketing se cadastrem no sistema da TRAI e façam uso das Plataformas DLTs. Viu-se que o sistema da TRAI apesar de estar destinado a chamadas e mensagens indesejadas, hoje as funcionalidades e principais resultados apresentam-se na sua maior parte sobre as mensagens SMS.

A TRAI também criou diversos produtos publicitários para ampliar a conscientização dos consumidores da Índia sobre o problema. Alguns exemplos nas figuras a seguir[148]:

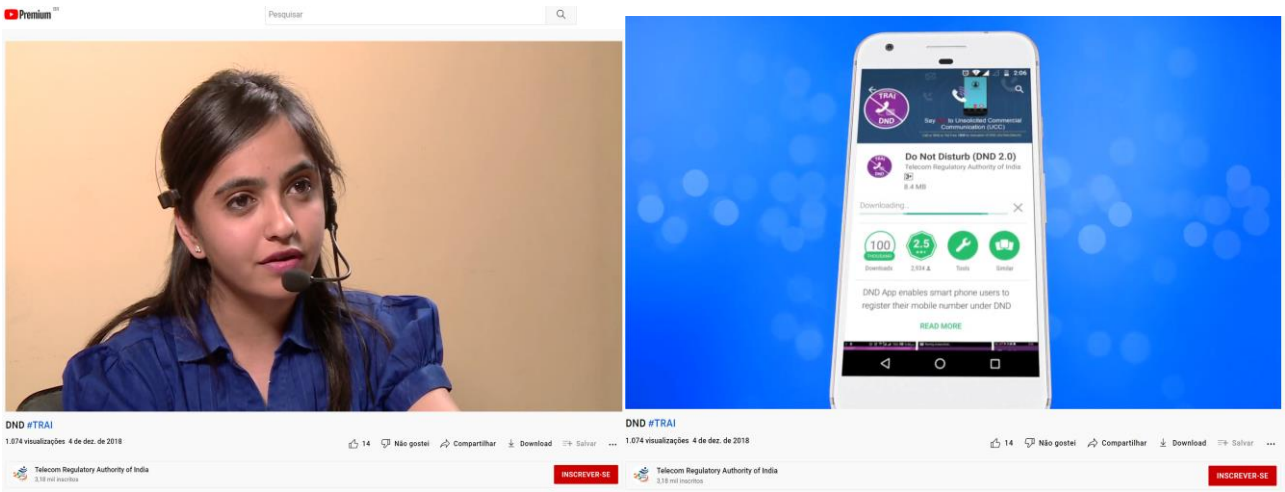


Figura 23 – Video sobre o aplicativo DND da TRAI e formas de combater as chamadas indesejadas.

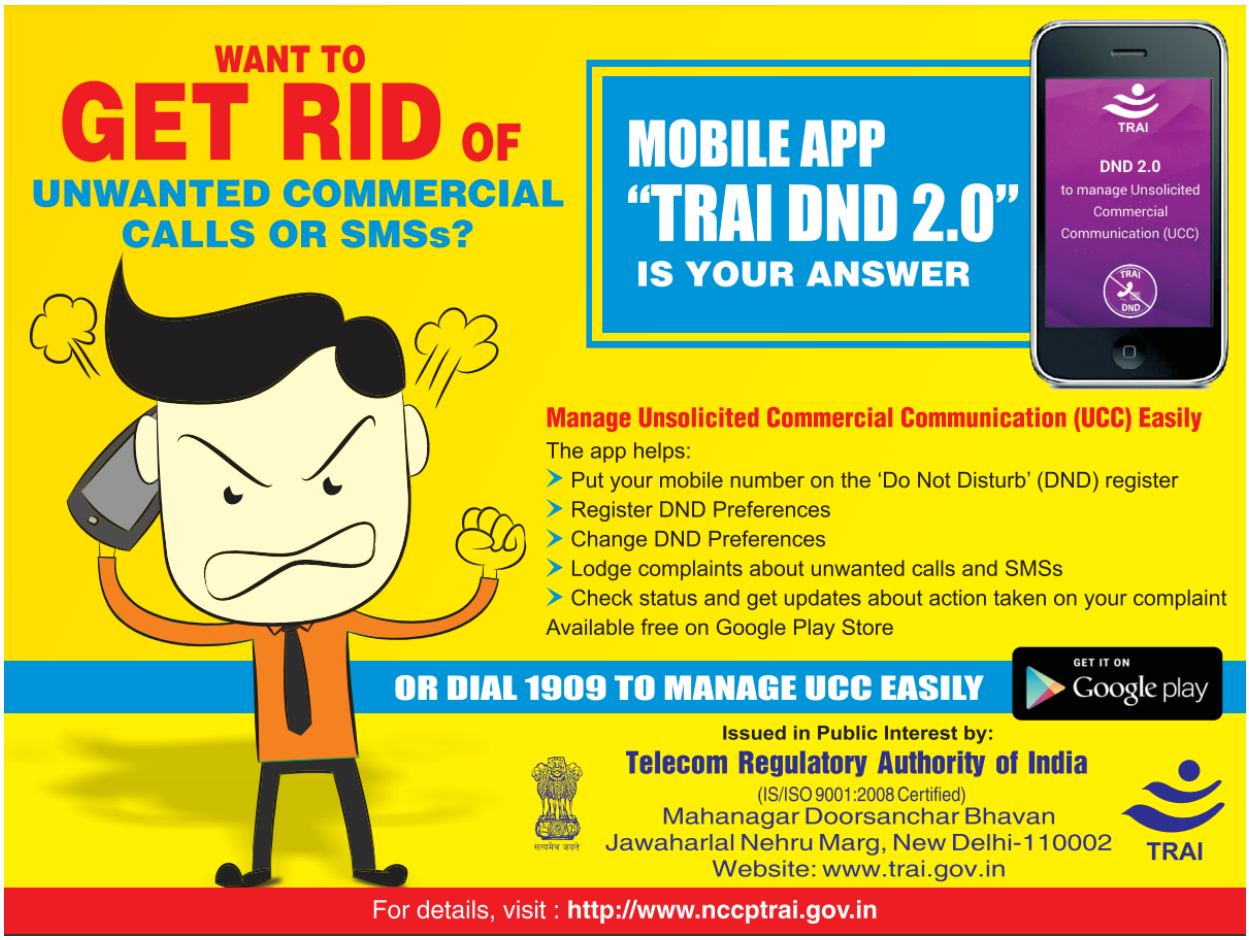


Figura 24 – Banner com instruções sobre gerenciamento de comunicações comerciais não solicitadas.[149]

Recomendações do regulador indiano para proteção do usuário[150]:

Recomendações Gerais	i. Não marque as caixas de inscrição ao preencher formulários on-line

	ii. Não forneça o número do celular a uma possível origem de spam iii. Registre sua preferência para gerenciar quem pode enviar comunicação comercial para você. iv. Gerenciar o consentimento dado às entidades que estão enviando comunicação comercial.
Pense antes de tornar seu número público:	i. Você também pode receber mensagens ou chamadas irrelevantes se tornar seu número de telefone público. ii. Se você não quiser receber essas mensagens, você deve evitar divulgar seu número. iii. Se um remetente violar as regras de UCC ou spam, você pode reclamar ou denunciar: https://trai.gov.in/complain-or-report-against-ucc
Descubra quem lhe enviou o SMS ou fez uma ligação no seu celular:	i. Você pode consultar as informações do remetente digitando os detalhes do cabeçalho. ii. Para obter mais informações, visite o Portal de Informações do Cabeçalho: https://smsheader.trai.gov.in/
SMS/Chamadas que você pode receber:	i. Mensagens/chamadas transacionais ii. Mensagens/chamadas de serviço iii. Mensagens/chamadas de conscientização do governo iv. Alertas/mensagens do provedor de serviços de telecomunicações

Abaixo quadro resumo das principais legislações afetas ao tema bem como os principais atores e sua atuação na Índia:

Principais Legislações	a) **The Telecom Commercial Communication Customer Preference Regulations** (2018)[151]: A fim de regular as chamadas comerciais e proteger o consumidor de chamadas comerciais não solicitadas e mensagens UCC), a TRAI publicou o TCCCPR 2018. As disposições dos regulamentos entraram em vigor a partir de 19 de julho de 2018. b) **The Telecom Regulatory Authority of India (TRAI) Act, 1997:** Estabelece as competências do Regulador Indiano. c) **The Information Technology Act, 2000**: Uma lei que confere reconhecimento legal às transações realizadas por meio de intercâmbio eletrônico de dados e outros meios de comunicação eletrônica, comumente chamados de "comércio eletrônico", que envolvam o uso de métodos alternativos aos métodos de comunicação e armazenamento de informações baseados em papel
Divisão de Responsabilidades	A responsabilidade pela gestão das comunicações não solicitadas é da Autoridade Reguladora de Telecomunicações da Índia (TRAI - Telecom Regulatory Authority of India). Ela gerencia o registro de Não me pertube da India, inclusive respondendo a violações da legislação. Realizaçao procedimentos de fiscalização, compliance e aplica sanções nos casos pertinentes. A TRAI definiu o modelo de Plataforma DLT em 2018 e faz a gestão compartilhada com os operadores de telecomunicações e com os operadores de telemarketing.

ANEXO E - CANADÁ

Relatório Anual[152] 2021 da Canadian Radio-television and Telecommunications Commission (CRTC), entidade que regulamenta as atividades de radiodifusão e de telecomunicações no Canadá, apontou que os custos relacionados a administração do Não me Perturbe (Do Not Call List – DNCL[153]) em 2020/21 foram de aproximadamente 3,3 milhões de dólares (custeado pelas empresas de telemarketings). Desde 2008 o Não me perturbe dos canadenses registrou 14.291.077 números de telecomunicações e 56.611 números cancelaram o registro. Somente no último ano fiscal, os canadenses registraram 206.035 números de telefones fixos, celulares e linhas de fax — uma média de mais de 564 números por dia.

Em 2020/21, os canadenses abriram 45,874 reclamações contra Operador Nacional da DNCL sendo 86% para reclamar que tinham o número na DNCL e mesmo assim recebiam chamadas. Do total de reclamações: (i) 27% eram sobre chamadas ao vivo de operadores de telemarketing suspeitos (ii) 29% eram ligações de operadores de telemarketing suspeitos, mas a ligação não foi atendida (iii) 21% eram sobre ADADs (Automatic Dialing-Announcing Device) (iv) 10% eram sobre suspeitos de telemarketing deixando mensagem de correio de voz (v) 9% eram sobre linhas mortas (ou seja, casos em que um discador preditivo foi usado ou não havia chamador na linha), (vi) 3% eram sobre mensagens pré-gravadas para guardar para um chamador ao vivo, (vii) 1% eram sobre um fax ou som de fax

Empresas de Telemarketing e clientes de telemarketing são obrigados a participar do DNCL Nacional do Canadá de duas maneiras: registrando-se e assinando o serviço. Em 2020/21, 1.082 novos operadores de telemarketing registaram-se no Operador Nacional DNCL. Já existem mais de 22.766 empresas de telemarketing cadastradas (sendo 829 estrangeiras).

Todos os operadores de telemarketing que realizam atividades em seu próprio nome ou em nome de clientes devem aderir às regras. As principais determinações estão consolidadas abaixo:

- identificar quem são e, mediante solicitação, fornecer um número de fax ou telefone onde o chamador possa falar com alguém sobre a ligação de telemarketing;
- exibir o número de telefone de onde eles estão ligando ou para o qual o consumidor pode ligar para alcançá-los; e
- ligar ou enviar fax apenas entre as 9h00 e as 21h30. durante a semana e das 10h00 às 18h00. nos fins de semana.

Com o intuito de garantir a conformidade dos operadores de telemarketing, são reunidas informações para selecionar e investigar casos de supostas violações, usando as ações de fiscalização para responder adequadamente a cada caso específico. Dentre os diversos mecanismos utilizados estão:

- cartas de advertência para pequenas violações;

- citações que estabelecem ações corretivas específicas;
- autos de infração, que são medidas formais de execução (estabelecidas na seção 72.07 da Lei de Telecomunicações), que podem acarretar uma multa administrativa pecuniária; e
- acordos negociados, que são acordos formais entre as entidades que cometem violações e a CRTC. Como parte de um acordo, a entidade deve admitir responsabilidade, parar de violar as Regras, aceitar um auto de infração com uma sanção administrativa e desenvolver um programa de conformidade.

As violações podem resultar em multas de até US$ 1.500 por violação para indivíduos e até US$ 15.000 por violação para empresas. Desde 2008, um total de US$ 10.716.930 foi emitido em multas monetárias administrativas[154].

Até 2021, o CRTC estabeleceu 16 parcerias com organizações em todo o mundo para melhor cumprir seu mandato. Esses acordos permitem que as agências compartilhem informações e forneçam suporte investigativo, mediante solicitação e de acordo com a lei. Esses *MOUs* estabelecidos também fornecem oportunidades de pesquisa e educação, bem como intercâmbios de pessoal e iniciativas de treinamento conjunto para as partes.

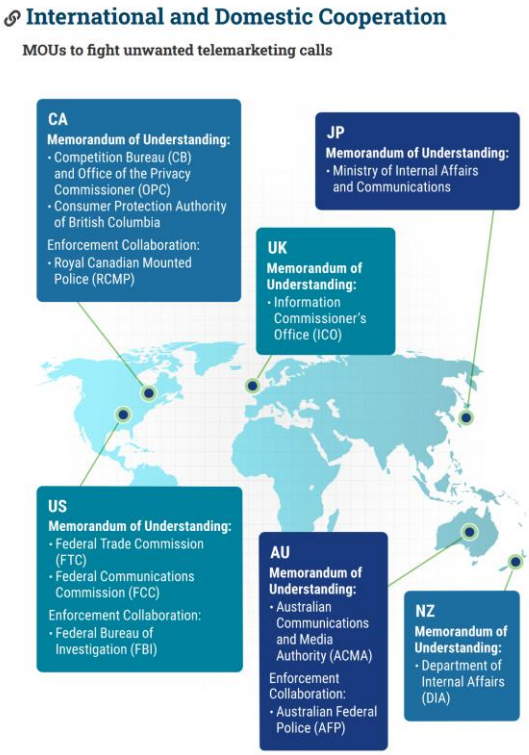


Figura 25 – Mapeamento dos Memorandos de entendimento no combate a chamadas de indesejadas de telemarketing

Em 2021, o CRTC aprovou um teste de bloqueio de chamadas, que utiliza tecnologia de inteligência artificial, para permitir que um grande operador de telecomunicações bloqueie certas chamadas de voz fraudulentas e inoportunas. Este teste resultou em um número significativo de chamadas fraudulentas sendo bloqueadas com sucesso.

Após uma consulta pública, a Comissão determinou que, como condição de oferta e prestação de serviços de telecomunicações, os prestadores de telecomunicações devem implementar STIR/SHAKEN para autenticar e validar chamadas de voz baseadas em IP, a partir de 30 de novembro de 2021. (Compliance and Enforcement and Telecom Decision CRTC 2021-123[155]).

Além disso, o CRTC continuou a apoiar o desenvolvimento do setor de um processo para rastrear chamadas incômodas de volta ao seu ponto de origem, incluindo a aprovação de um projeto de teste de rastreamento, para facilitar os esforços de conformidade e fiscalização.

O CRTC também criou diversos produtos publicitários para ampliar a conscientização dos consumidores da Índia sobre o problema. Alguns exemplos abaixo:

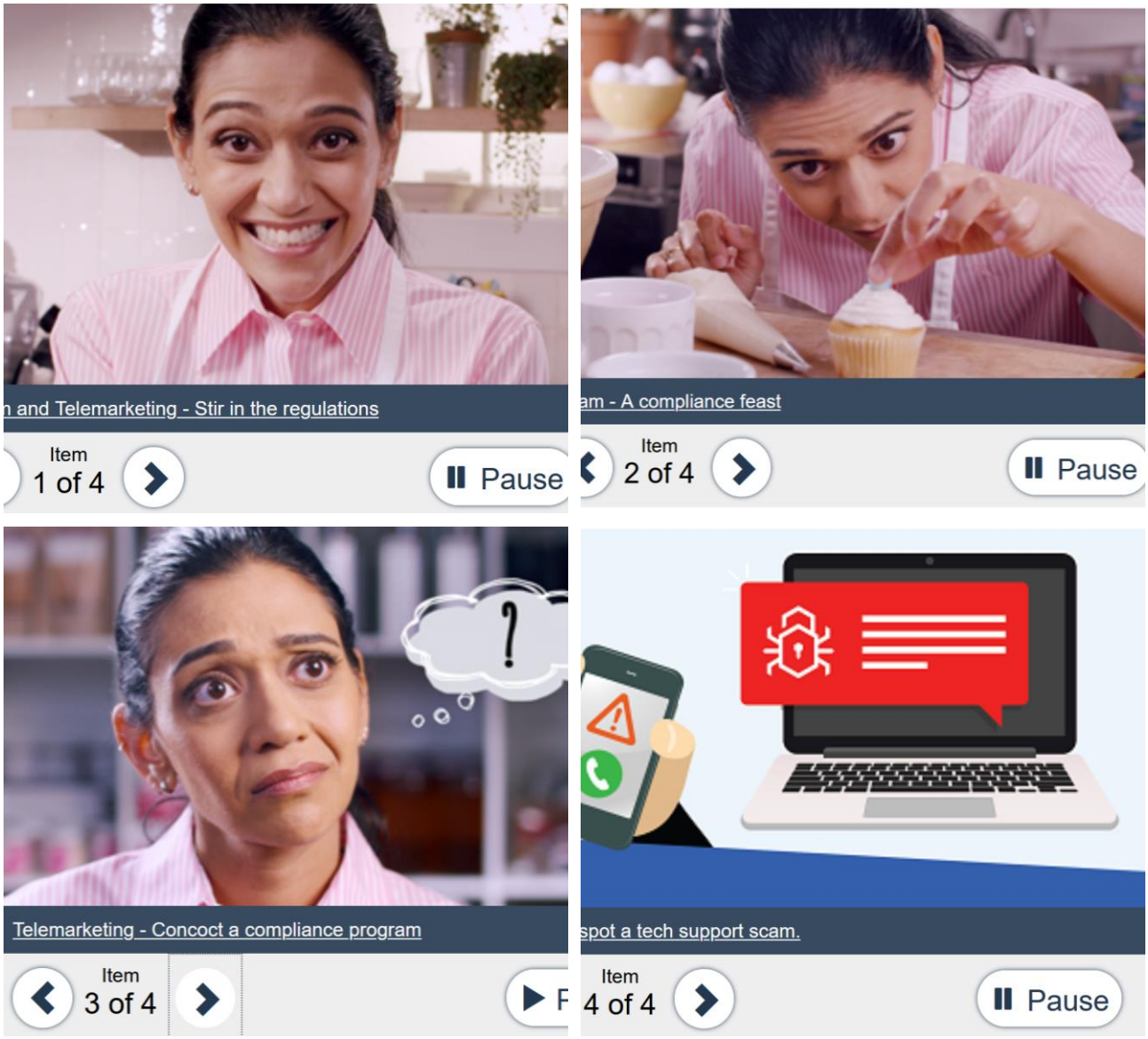


Figura 26 - Exemplos de vídeos criados pelo CRTC para ampliar iniciativas de educação sobreo o tema[156]

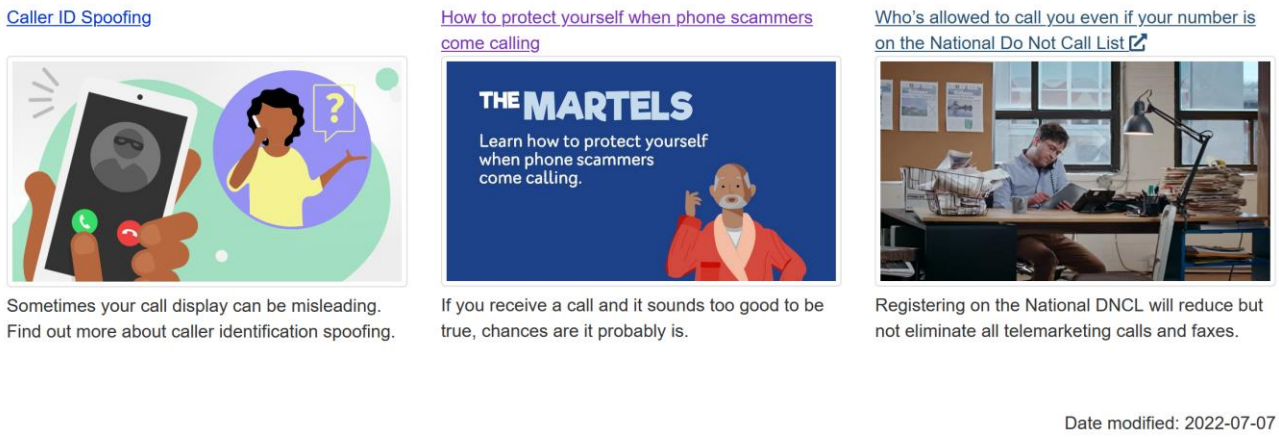


Figura 27 – Campanhas de conscientização sobre o problema de Chamadas Indesejadas[157]

O CRTC também possui uma área específica para educação dos consumidores e consolida as principais dicas sobre o tema[158]. A tabela abaixo é apresentada um breve resumo de tais medidas.

Como evitar chamadas indesejadas	i. Registre seus números de telefone no DNCL Nacional ou ligue para 1-866-580-DNCL (3625). ii. Veja os recursos de gerenciamento de chamadas que seu provedor de serviços telefônicos oferece. iii. Filtre suas chamadas e desligue ou deixe-as ir para o correio de voz. iv. Os operadores de telemarketing raramente deixam mensagens. v. Peça que seu número de telefone seja adicionado à lista interna de não chamadas do operador de telemarketing. vi. Se você suspeitar de uma chamada fraudulenta - NÃO forneça detalhes financeiros pessoais ou conceda acesso ao seu computador. vii. Melhor conselho: DESLIGUE. viii. Se você foi vítima de uma ligação fraudulenta e forneceu informações pessoais, informe seu banco, bem como o Centro Antifraude Canadense em *http://www.antifraudcentre-centreantifraude.ca*. ix. Considere obter um número de telefone não listado: seu número não será publicado e não estará disponível para operadores de telemarketing. x. Tenha cuidado para quem você fornece seu número de telefone - ele pode ser usado para fins de telemarketing.
Como se proteger de ligações fraudulentas /golpes	i. NUNCA dê acesso ao seu computador a um chamador não solicitado. Se você receber um telefonema inesperado sobre o status de segurança ou desempenho do seu sistema de computador e o chamador solicitar acesso remoto ao seu computador, desligue - mesmo que o chamador afirme representar uma empresa ou produto conhecido. ii. Não forneça informações pessoais. Não forneça detalhes do cartão de crédito ou da conta online por telefone, a menos que você tenha feito a ligação e o número para o qual está ligando tenha vindo de uma fonte confiável. iii. Proteja seu computador. Certifique-se de que seu computador esteja protegido com software antivírus e anti-spyware atualizado regularmente e um bom firewall. Mas pesquise primeiro e compre apenas software de uma fonte que você conhece e confia. iv. Leia as políticas de privacidade online. Se você estiver pensando em fornecer dados pessoais a uma empresa, leia primeiro a política de privacidade e os termos e condições dela. Se você não concordar com a forma como eles usarão seus dados, não os forneça.
O que fazer se você acha que foi vítima de Fraude	i. Alerte sua instituição financeira. Se você forneceu os detalhes da sua conta a um golpista, entre em contato com seu banco ou instituição financeira imediatamente e informe-os. ii. Obtenha mais assistência. Entre em contato com o Canadian Identity Theft Support Center.

	iii. Obtenha ajuda de um especialista. Se você tiver problemas com o computador, procure ajuda ou conselho de um técnico de informática qualificado e respeitável. iv. Faça uma reclamação. Você pode relatar chamadas de telemarketing indesejadas no National DNCL. v. Entre em contato com a polícia. Se você acha que a chamada pode fazer parte de um esquema de fraude, entre em contato com as autoridades policiais ou com o Centro Antifraude Canadense.

Abaixo quadro resumo das principais legislações afetas ao tema bem como os principais atores e sua atuação no Canadá:

Principais Legislações	a) **Canada's Anti-Spam Legislation (CASL) 2014**: Legislação Anti-Spam do Canadá foi concebida como de "tecnologia neutra", abrangendo todas as formas do que classifica como comunicação "eletrônica". b) **Unsolicited Telecommunications Rules (UTR/the Rules)**: inclui as regras com relação a Lista de Não me pertube (*the National Do Not Call List* – DNCL), as regras para o Telemarketing, e as regras para dispositivos de discagem/anúncios automatizados (*Automatic Dialing-Announcing Device* – ADAD).
Divisão de Responsabilidades	A responsabilidade de fazer cumprir as obrigações das comunicações não solicitadas recai sobre a Comissão Canadense de Radiotelevisão e Telecomunicações (CRTC). O departamento de Inovação, Ciência e Desenvolvimento Econômico do Canadá (ISED) – o departamento-mãe do CRTC – é responsável pela definição de políticas. Embora o CRTC tenha o papel principal na aplicação da legislação e regulamentação de comunicações não solicitadas, o conteúdo das mensagens pode envolver outras agências, como o *Competition Bureau* (CB), o *Office of the Privacy Commissioner of Canada* (OPC) e o *Royal Canadian Mounted Polícia* (RCMP). O CRTC opera o Centro de Denúncias de Spam, por meio do qual os consumidores podem denunciar violações do CASL para que o CRTC tome medidas. O CRTC também opera um registro nacional Do Not Call (DNC), por meio do qual os consumidores podem denunciar violações do UTR.

ANEXO F - SINGAPURA

Assim como os demais países da Ásia, Singapura também tem sido afetada pelo problema das comunicações indesejadas[159]. Nesse sentido a Infocomm Media Development Authority (IMDA) tem trabalhado em conjunto com a Força Policial de Singapura, agências governamentais e parceiros do setor privado como parte da luta multifacetada contragolpes e comunicações indesejadas.

Foi identificada a necessidade de construir múltiplas camadas de defesa. Dentre as principais medidas adotadas por Singapura destacam-se: (a) um Registro *Do Not Call* (DNC) para disponibilizar aos seus usuários de telecomunicações a opção por não receber mensagens de marketing indesejadas ou chamadas para o seu número de telefone. Decidiu por criar três grupos de bloqueios (chamadas de voz, mensagem de texto, mensagem de fax). Entretanto o Registro DNC não cobre: (i) Mensagens de marketing ou chamadas de organizações com as quais você mantém um relacionamento contínuo, se as mensagens forem sobre produtos ou serviços relevantes para você. No entanto, se pode optar por não receber tais mensagens de telemarketing e a organização deve parar de enviar tais mensagens para seu número de telefone de Cingapura após 21 dias corridos; (ii) Mensagens que fazem parte de uma pesquisa de mercado ou pesquisa; (iii) Mensagens relacionadas a causas beneficentes ou religiosas; (iv) Mensagens pessoais enviadas por indivíduos; (v) Mensagens públicas enviadas por agências governamentais; (vi) Mensagens políticas; ou (vii) Chamadas ou mensagens de telemarketing enviadas para uma empresa (ou seja, B2B). (b) O aplicativo “ScamShield” desenvolvido pelo governo de Singapura tem como objetivo bloquear chamadas fraudulentas conhecidas em uma lista gerenciada pelo Conselho Nacional de Prevenção ao Crime e pela Polícia. Ele também usa um algoritmo no dispositivo com o objetivo de filtrar SMS enviados por pessoas desconhecidas para a pasta de lixo eletrônico. (c) o regulador de Singapura indica ainda a utilização de outros aplicativos de terceiros com funções semelhantes para bloquear chamadas e mensagens indesejadas, como por exemplo, sistema de bloqueio do Google, lista negra de chamadas, Hiya, controle de chamadas[160].

Para aprimorar a proteção contragolpes a Infocomm Media Development Authority (IMDA) está propondo novas ações como o cadastro completo obrigatório do Registro dos emissores de SMS (*Sender ID*). A consulta pública sobre o tema iniciou-se em 15/08/2022[161].

Um piloto de Registro dos Emissores de SMS (*SMS Sender ID Registry* – SSIR) foi iniciado em agosto de 2021. No entanto, com o aumento de golpes usando SMS, o IMDA acelerou a criação do Singapore SMS Sender ID Registry (SSIR) em março de 2022. Os SMS que falsificavam/faziam uso de IDs registrados no SSIR eram, portanto, bloqueados antecipadamente, reduzindo o risco de fraudes.

Desde o seu lançamento, mais de 120 organizações do setor público e privado aderiram ao SSIR. Em comparação com os três meses anteriores, o número de casos de fraude por SMS relatados diminuiu três vezes desde o lançamento do SSIR[162].

Embora o SSIR tenha tido impacto, atualmente continua sendo um sistema voluntário, ou seja, para organizações que optam por registrar e proteger seus IDs de remetente. O público, no entanto, ainda pode estar sujeito a SMS falsificados, usando IDs de remetentes não registrados (por exemplo, de organizações que optam por não se registrar ou IDs que não pertencem a nenhuma organização).

Para criar recursos de prevenção de fraude mais fortes, a IMDA pretende tornar o registro SSIR um requisito obrigatório para organizações que usam IDs de remetente (ou seja, um regime de registro completo). Portanto, apenas IDs de remetente registrados serão permitidos. Todos os outros IDs de remetente não registrados serão bloqueados por padrão. Isso protege ainda mais o SMS como um canal de comunicação.

Em regime de registro completo, a IMDA propõe que: (i) Os comerciantes/organizações que usam IDs de remetente de SMS devem se registrar no SSIR usando seu número de identidade exclusivo (UEN), (ii) Os agregadores que desejam lidar com SMS com IDs de remetente devem participar do SSIR e verificar as inscrições de comerciantes/organizações por meio de seus UENs,

Os requisitos acima permitirão que os comerciantes por trás dos IDs do remetente sejam claramente identificados. Ele fornece uma melhor garantia de que apenas os comerciantes de boa-fé estão usando IDs de remetente.

Como as organizações podem precisar de tempo para se ajustar, é proposto um período de transição a partir de outubro de 2022, antes que o requisito de registro completo do SSIR comece no final de 2022.

Além disso, a tecnologia tornou possível identificar e filtrar possíveis mensagens fraudulentas, dentro da rede de telecomunicações, usando a tecnologia de leitura de máquina. Como primeira fase, as soluções propostas podem detectar links maliciosos dentro do SMS que levam a sites fraudulentos; e os operadores de telecomunicações podem então desenvolver soluções para identificar padrões de mensagens fraudulentas suspeitas e filtrá-las adequadamente.

As medidas propostas fazem parte de uma abordagem contínua em várias camadas para fortalecer a proteção contra fraudes. Isso tem sido feito com as empresas de telecomunicações, para reduzir sistemicamente chamadas fraudulentas e SMS que chegam pelas redes de comunicação.

Desde 2019, empresas de telecomunicações bloqueiam SMS fraudulentos que vinham pelas redes: Bloqueio de SMS fraudulentos e URLs/sites fraudulentos maliciosos uma vez identificados (Fase 1: Os links nas mensagens SMS são verificados e comparados por com um banco de dados de links maliciosos conhecidos. Se uma correspondência for detectada, a mensagem SMS é filtrada;

para isso o banco de dados de links maliciosos deve ser atualizado continuamente para permanecer relevante contra novas ameaças)

Desde 2021, os agregadores de SMS bloqueiam mensagens fraudulentas iniciais usando IDs falsos. Busca-se então tornar obrigatório tal registro ampliando ainda mais o combate contra envio de SMS fraudulentos

Outra proposta que se faz na consulta pública é a de alternativas de filtragem e identificação de mensagens fraudulentas. Semelhante à Fase 1, essa filtragem será realizada por meio de varredura automatizada da máquina sem intervenção humana. A máquina procurará identificar e filtrar mensagens SMS com base em padrões suspeitos nas mensagens SMS. Estes podem incluir palavras-chave, frases e formatos de mensagem que normalmente são usados em mensagens SMS fraudulentas. O aprendizado de máquina será adotado para verificar e identificar padrões comuns e novos que são característicos de golpistas e mensagens SMS fraudulentas, acompanhando as táticas em evolução dos golpistas. Como parte do processo de aprendizado de máquina, pode haver algumas mensagens SMS que são sinalizadas pela máquina como potencialmente suspeitas e uma avaliação mais detalhada será necessária para verificar se realmente são mensagens SMS fraudulentas. Antes de serem encaminhadas para avaliação adicional, essas mensagens SMS suspeitas sinalizadas serão anonimizadas pela máquina e, em seguida, canalizadas para o pessoal técnico da prestadora para uma segunda camada de revisão. Com o tempo, isso permitirá que a máquina desenvolva maior precisão e eficácia de filtragem. Esta revisão é exclusivamente para fins de melhoria do processo de aprendizado de máquina, não sendo permitidas outras finalidades. Além disso, as prestadoras de telecomunicações continuam a ter obrigações sob a Lei de Proteção de Dados Pessoais, inclusive para proteger quaisquer dados pessoais e não reter os dados pessoais por mais tempo do que o razoavelmente necessário para facilitar o aprendizado de máquina ou de outra forma que não seja autorizado por lei escrita. Embora essa filtragem adicional na Fase 2 não seja infalível, ela ajudará a mitigar ainda mais o risco para os consumidores.

Espera-se ainda criar a opção para os consumidores de não receberem SMS internacionais.

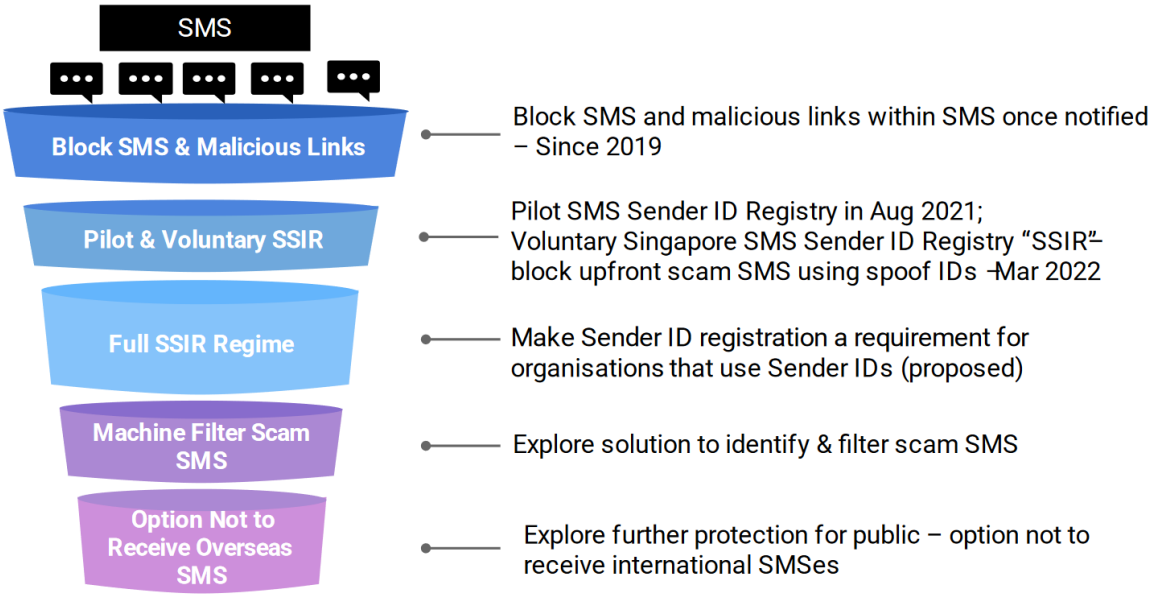


Figura 28 – Resumo da estratégia multicamadas no combate a mensagens fraudulentas

No caso de chamadas fraudulentas, desde 2019, os números locais comumente falsificados (geralmente números que se passam por agências governamentais locais e serviços de emergência, por exemplo, 995) foram bloqueados (bloqueio de números de chamada falsos conhecidos/específicos).

A partir de 2020, *robocalls* (chamadas fraudulentas automatizadas) foram bloqueadas usando tecnologia de reconhecimento de padrões. As chamadas no exterior foram marcadas com um sinal "+" para alertar o público a ficar atento.

Planeja-se o bloqueio de números locais falsificados oriundos de ligações internacionais até o final do ano. Tal procedimento será realizado nas redes das prestadoras como padrão, sem afetar os usuários.

Além disso, busca-se criar mecanismos para que os usuários tenham a opção de não receberem chamadas internacionais

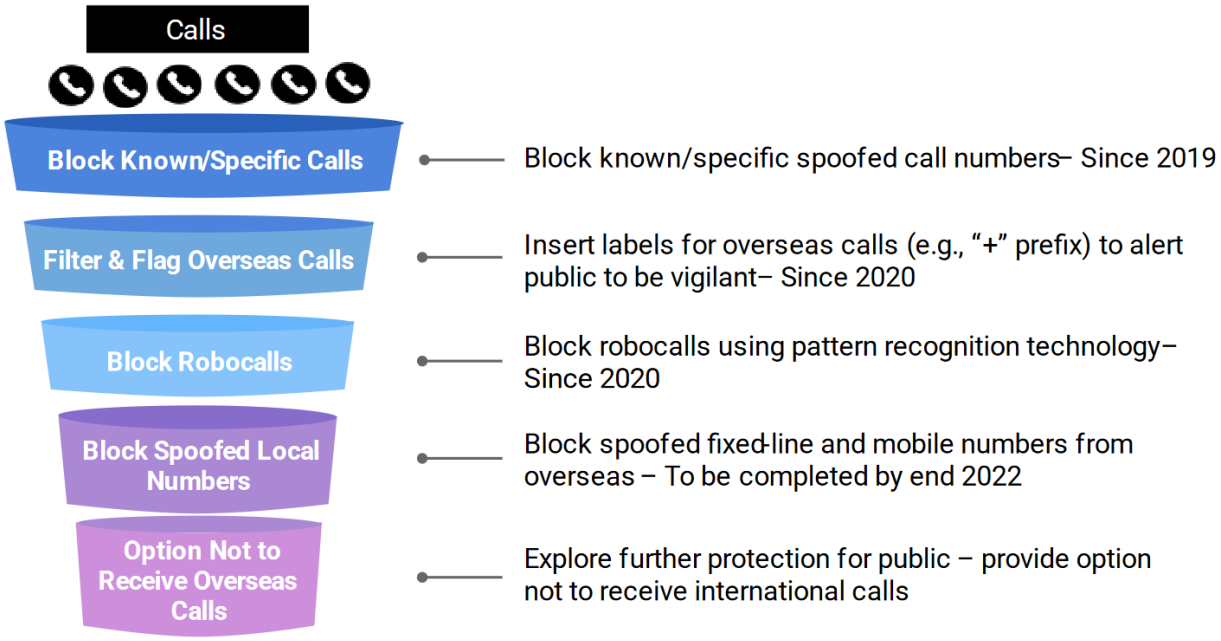


Figura 29 - Resumo da estratégia multicamadas no combate a chamadas fraudulentas

O desenvolvimento de materiais para educação com relação ao tema também é um dos destaques para o governo de Singapura. Abaixo alguns exemplos de encartes produzidos:

Figura 30 – Como identificar uma Chamada fraudulenta[163]

Abaixo quadro resumo das principais legislações afetas ao tema bem como os principais atores e sua atuação em Singapura:

Principais Legislações	**a) Personal Data Protection Act (PDPA) 2012** b) **Spam Control Act of 2007**[164]
Divisão de Responsabilidades	A responsabilidade pelo gerenciamento de comunicações não solicitadas é da Comissão de Proteção de Dados Pessoais (PDPC), que foi criada para implementar o PDPA, e da Autoridade de Desenvolvimento de Mídia e Info-comunicações (IMDA), que tem a responsabilidade de promulgar a Lei de Controle de Spam. O PDPC é uma divisão do IMDA. O PDPC aplica diretamente o PDPA (cobrindo spam de telefone e fax) no que se refere a comunicações não solicitadas. O PDPC também tem a responsabilidade de proteção de dados pessoais, e opera não contatando cadastros por telefone, fax e SMS/MMS. O IMDA tem responsabilidade pela Lei de Controle de Spam, embora a aplicação desta lei aconteça por meio de uma abordagem “multifacetada”, englobando: • o quadro legislativo (ou seja, a Lei); • autorregulamentação do setor – os três principais provedores de serviços de Internet (ISPs), sob a facilitação do IMDA, estabeleceram diretrizes de controle de spam. Essas diretrizes foram adotadas conjuntamente pelos três ISPs para reduzir o spam de e-mail e SMS para seus assinantes. A Associação de Marketing Direto de Cingapura (DMAS) também lançou um Código de Práticas de Marketing por E-mail para seus membros; • cooperação internacional, por meio da participação em várias redes para auxiliar os esforços globais para conter o spam; e • educação pública – fornecendo informações para indivíduos e organizações sobre spam e como combatê-lo, inclusive com a ajuda de parceiros do setor IMDA, conforme apropriado. Os consumidores também podem tomar medidas diretas contra um infrator da Lei de Controle de Spam por meio de ação civil.

NOTAS/REFERÊNCIAS

[1] TRUECALLER. **Report Global Spam & Scam 2021**. Disponível em https://www.truecaller.com/blog/insights/top-20-countries-affected-by-spam-calls-in-2021

[2] TU, Huahong. DOUPÉ, Adam. ZHAO, Ziming. **SoK: Everyone Hates Robocalls: A Survey of Techniques Against Telephone Spam**. Maio, 2016. DOI:10.13140/RG.2.1.2605.6080. Disponível em: https://www.researchgate.net/publication/299794558_SoK_Everyone_Hates_Robocalls_A_Survey_of_Techniques_against_Telephone_Spam

[3] ANATEL**. Ligações indesejadas – Benchmarking Internacional**. Estudo de Tópico Prioritário de Inteligência produzido pela Gerência de Interações Institucionais, Satisfação e Educação para o Consumo – RCIC, da Superintendência de Relações com Consumidores – SRC. Dezembro, 2019. Links: Processo nº 53500.023755/2019-26, SEI nº 4979653.

[4] ANATEL. **Diagnóstico em Qualidade da Informação e Desinformação – Medidas Regulatórias para Coibir Telemarketing Abusivo e Chamadas de Robocall**. Estudo de Tópico Prioritário de Inteligência produzido pela Gerência de Interações Institucionais, Satisfação e Educação para o Consumo – RCIC, da Superintendência de Relações com Consumidores – SRC. Setembro, 2022. Links: Processo nº 53500.313278/2022-93, SEI nº 9191940.

[5] Tu, Doupé e Zhao (2016), p.3.

[6] Tu, Doupé e Zhao (2016), p.4-5.

[7] Tu, Doupé e Zhao (2016), p.5.

[8] Tu, Doupé e Zhao (2016), p.7.

[9] Tu, Doupé e Zhao (2016), p.9.

[10] Tu, Doupé e Zhao (2016), p.10.

[11] Tu, Doupé e Zhao (2016), p.11.

[12] FCC. https://www.fcc.gov/document/fcc-takes-actions-against-auto-warranty-scam-robocall-campaign

[13] FCC, The FCC's Push to Combat Robocalls & Spoofing | Federal Communications Commission

[14] FCC, https://fccprod.servicenowservices.com/rmd?id=rmd_listings

[15] FCC, https://www.fcc.gov/sites/default/files/stop_unwanted_robocalls_and_texts.pdf

[16] FCC, https://www.fcc.gov/call-blocking

[17] FCC, https://www.fcc.gov/document/fcc-remove-companies-robocall-database-non-compliance

[18] FCC, https://www.fcc.gov/document/fcc-start-new-robotext-proceeding

[19] OFCOM, https://www.ofcom.org.uk/__data/assets/pdf_file/0025/216439/nuisance-calls-joint-action-plan-2021.pdf

[20] ICO https://www.tpsonline.org.uk/pages/enforcement

[21] OFCOM, https://www.ofcom.org.uk/__data/assets/pdf_file/0018/232074/statement-tackling-scam-calls-and-texts.pdf

[22] OFCOM, https://www.ofcom.org.uk/research-and-data/telecoms-research/nuisance-calls

[23] OFCOM https://www.ofcom.org.uk/__data/assets/pdf_file/0019/10675/nuisance-calls-and-messages-consumer-guide.pdf

[24] GOV.UK https://www.gov.uk/government/publications/joint-fraud-taskforce-telecommunications-charter/fraud-sector-charter-telecommunications-accessible-version

[25] GOV.UK , https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1028171/Telecommunications_Fraud_Sector_Charter.pdf

[26] UCENET, https://www.ucenet.org/

[27] ICO, https://ico.org.uk/action-weve-taken/nuisance-calls-and-messages/

[28] OFCOM, https://www.ofcom.org.uk/__data/assets/pdf_file/0015/232071/consultation-improving-cli-data-accuracy.pdf

[29] OFCOM, https://www.ofcom.org.uk/__data/assets/pdf_file/0032/232889/consultation-good-practice-guide-on-sub-allocated-assigned-numbers.pdf

[30] ACMA, https://www.donotcall.gov.au/about/about-the-do-not-call-register/

[31] ACMA, https://www.acma.gov.au/investigations-spam-and-telemarketing#outcomes-for-2022

[32] ACMA, https://www.acma.gov.au/sites/default/files/2020-10/Combating-Scams-summary-report.pdf

[33] ACMA, https://www.legislation.gov.au/Details/F2020L00179

[34] ACMA, https://www.commsalliance.com.au/Documents/all/codes/c661

[35] ACMA, https://www.commsalliance.com.au/Documents/all/codes/c661 Exemplos de melhores práticas do Código Australiano: (i) proteger suas informações pessoais e não compartilhá-las com chamadores desconhecidos ou não solicitados; (ii) entrar em contato com sua instituição financeira imediatamente se acreditar que perdeu dinheiro para um golpista; (iii) alteração de PINs e senhas padrão em equipamentos de clientes recém-adquiridos; (iv) selecionar PINs e senhas fortes (por exemplo, não “1234” ou “0000” ou “senha” etc.); (v) dispositivos de travamento com PINs seguros; (vi) garantir que os PINs de correio de voz sejam seguros; (vii) desabilitar portas e recursos PABX que não são usados (por exemplo, encaminhamento remoto de chamadas); (viii) alterar PINs e senhas regularmente; (ix) não responder a chamadas perdidas ou SMs de números internacionais desconhecidos, números australianos desconhecidos ou uma fonte desconhecida; (x) não clicar em URLs ou fazer chamadas de retorno para números de telefone contidos no SMS de números internacionais desconhecidos ou números australianos desconhecidos ou de fonte desconhecida; (xi) Bloqueio de números australianos suspeitos ou desconhecidos ou números internacionais em dispositivos e uso de serviços ou produtos de bloqueio, quando disponíveis, em telefones fixos; e (xii) permitir que chamadas desconhecidas sejam enviadas para o correio de voz e, em seguida, ouvir qualquer mensagem deixada para verificar se esta pode ser uma chamada genuína.

[36] TRAI, Preference Registration | Telecom Regulatory Authority of India (trai.gov.in)

[37] TRAI, https://trai.gov.in/tsps-website#_5z8t0073tf77

[38] TRAI, https://www.trai.gov.in/faqcategory/unsolicited-commercial-communicationsucc

[39] TRAI, http://www.trai.gov.in/telecom/consumer-initiatives/unsolicited-commercial-communication

[40] TRAI, https://trai.gov.in/portals-apps/privacy-policy

[41] CRTC, https://lnnte-dncl.gc.ca/en

[42] CRTC, https://crtc.gc.ca/eng/archive/2021/2021-123.htm

[43] PDPC, https://www.dnc.gov.sg/index.html

[44] Singapura, https://www.scamshield.org.sg/

[45] Truecaller, https://play.google.com/store/apps/details?id=com.truecaller

[46] Hiya, https://pt.hiya.com/products/app

[47] Robokiller, https://apps.apple.com/us/app/robokiller-block-spam-calls/id1022831885?ign-mpt=uo%3D4

[48] Nomorobo, https://apps.apple.com/us/app/nomorobo-robocall-blocking/id1134727588

[49] Call Blacklist, https://play.google.com/store/apps/details?id=com.vladlee.easyblacklist

[50] IMDA, https://www.imda.gov.sg/regulations-and-licensing/Regulations/consultations/Consultation-Papers/2022/Proposals-to-Strengthen-Safeguards-for-SMS-Messages-to-Singapore-Users

[51] IMDA, https://www.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2022/Enhancing-protection-against-scams-IMDA-proposes-full-SMS-Sender-ID-registration-as-part-of-ongoing-measures

[52] IMDA, https://www.imda.gov.sg/regulations-and-licensing/Regulations/consultations/Consultation-Papers/2022/Proposals-to-Strengthen-Safeguards-for-SMS-Messages-to-Singapore-Users

[53] IMDA, https://www.imda.gov.sg/regulations-and-licensing/Regulations/consultations/Consultation-Papers/2022/Proposals-to-Strengthen-Safeguards-for-SMS-Messages-to-Singapore-Users

[54] EU, https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex:32002L0058

[55] Cullen, https://www.cullen-international.com/client/site/documents/CTECEU20220020

[56] Bélgica, https://www.autoriteprotectiondonnees.be/publications/recommandation-n-01-2020.pdf

[57] Itália, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4304228

[58] Holanda, https://www.acm.nl/nl/onderwerpen/telecommunicatie/internet/veelgestelde-vragen-over-spam

[59] Espanha, https://www.aepd.es/es/areas-de-actuacion/publicidad-no-deseada

[60] Reino Unido, https://ico.org.uk/for-organisations/guide-to-pecr/electronic-and-telephone-marketing/electronic-mail-marketing/#texts

[61] Relatório Combate às chamadas abusivas - balanço dos três primeiros meses da cautelar - setembro 2022. https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqazZ0hWdvf35bLAkgb7HEJrqNL5frGp02MyfJlv_HiDWeAmF_HQqOfnU4nYlHxzZRwcyO1ZbMVeZzrbGsGr7cn2

[62] WASPA, https://dnc.org.za/about

[63] AAIP, No llame - registro nacional - https://nollame.aaip.gob.ar/,

[64] FTC https://www.donotcall.gov.au/

[65] Brasil, https://www.naomeperturbe.com.br/

[66] Canadá, https://lnnte-dncl.gc.ca/en

[67] SERNAC https://www.sernac.cl/portal/618/w3-propertyvalue-62998.html

[68] CRC https://tramitescrcom.gov.co/tramites/comun/guia.xhtml?tit=&subt=&tram=ebhrEbS9qKn04bkBEBApXQ==&pr1=3578LkxQ3TO3y3t5FY9/BQ==&onA=S0etv8CCdHqPI8wYF9h5dtdTbijZh1Ii32LohKmsEd6aN1b0ia4DPDtKgFkbFjDn

[69] UIT, https://www.itu.int/dms_pub/itu-d/oth/07/27/D07270000010001PDFE.pdf

[70] BLOCTEL https://www.bloctel.gouv.fr/

[71] TRAI Preference Registration | Telecom Regulatory Authority of India (trai.gov.in)

[72] RPO, https://registrodelleopposizioni.it/en/home/

[73] NCC, https://consumer.ncc.gov.ng/articles/67-understanding-dnd

[74] ICO, Telephone Preference Service - https://www.tpsonline.org.uk/tps/index.html

[75] PDPC, https://www.dnc.gov.sg/index.html

[76] AGCOM, Delibera n. 156/18/CIR. Modifiche ed integrazioni del piano di numerazione, di cui alla delibera n. 8/15/CIR, in attuazione della legge n. 5/2018 - https://www.agcom.it/documentazione/documento?p_p_auth=fLw7zRht&p_p_id=101_INSTANCE_FnOw5lV

OIXoE&p_p_lifecycle=0&p_p_col_id=column-1&p_p_col_count=1&_101_INSTANCE_FnOw5lVOIXoE_struts_action=%2Fasset_publisher%

[77] TRAI, https://www.trai.gov.in/faqcategory/unsolicited-commercial-communicationsucc

[78] ARCEP, ARCEP. Décision n°2019-0954 - https://www.arcep.fr/uploads/tx_gsavis/19-0954.pdf.

[79] ARCEP https://www.telecompaper.com/news/french-regulator-approves-changes-to-numbering-plan--1436335

[80] Gesetz gegen den unlauteren Wettbewerb - https://www.gesetze-im-internet.de/uwg_2004/

[81] BUNDESNETZAGENTUR - Publicidade telefônica

[82] FCC. Combating Spoofed Robocalls with Caller ID Authentication - https://www.fcc.gov/call-authentication.

[83] Document SG1RGQ/174 (India) presents a case study from India regarding Unsolicited Commercial Communications (UCC) and the framework adopted to curb UCC by way of regulation in cooperation with Telecom Service Providers. Document SG1RGQ/358(Rev.1) (India) that highlights the evolution of Regulations in India to curb Unsolicited Commercial Communications and the use of Distributed Ledger Technology.

[84] CRTC, https://crtc.gc.ca/eng/archive/2021/2021-123.htm

[85] Lista com os comparativos de aplicativos destinados a bloqueio/filtragem de comunicações indesejadas: Comparitech, https://www.comparitech.com/identity-theft-protection/best-spam-call-blocker-iphone/ ,Geekflare https://geekflare.com/call-blocker-apps/ , Fossbytes https://fossbytes.com/best-android-call-blocker-app/

[86] Truecaller, https://play.google.com/store/apps/details?id=com.truecaller

[87] Hiya, https://pt.hiya.com/products/app

[88] Robokiller, https://apps.apple.com/us/app/robokiller-block-spam-calls/id1022831885?ign-mpt=uo%3D4

[89] Nomorobo, https://apps.apple.com/us/app/nomorobo-robocall-blocking/id1134727588

[90] Call Blacklist, https://play.google.com/store/apps/details?id=com.vladlee.easyblacklist

[91] AT&T, https://apps.apple.com/us/app/at-t-call-protect/id1181632589

[92] T-Mobile https://apps.apple.com/us/app/t-mobile-name-id/id1367276365?ign-mpt=uo%3D4

[93] Apple, https://support.apple.com/en-us/HT207099

[94] Google, https://support.google.com/phoneapp/answer/9118387?hl=en

[95] Samsung, https://www.samsung.com/br/apps/smart-call/

[96] Relatório Combate às chamadas abusivas - balanço dos três primeiros meses da cautelar - setembro 2022. https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqazZ0hWdvf35bLAkgb7HEJrqNL5frGp02MyfJlv_HiDWeAmF_HQqOfnU4nYlHxzZRwcyO1ZbMVeZzrbGsGr7cn2 e Relatório Combate às chamadas abusivas - balanço parcial de julho de 2022;

[97] Não me perturbe https://www.gov.br/anatel/pt-br/consumidor/telemarketing/nao-me-perturbe

[98] Convergência Digital, https://www.convergenciadigital.com.br/Telecom/Bloqueio-de-telemarketing-Nao-Me-Perturbe-soma-10-milhoes-de-numeros-59968.html?UserActiveTemplate=mobile

[99] Ofcom, https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/policy/tackling-scam-calls-and-texts/do-not-originate

[100] Reino Unido, https://www.gov.uk/government/publications/joint-fraud-taskforce-telecommunications-charter/fraud-sector-charter-telecommunications-accessible-version

[101] Bélgica, https://www.autoriteprotectiondonnees.be/publications/recommandation-n-01-2020.pdf

[102] Itália, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4304228

[103] Holanda, https://www.acm.nl/nl/onderwerpen/telecommunicatie/internet/veelgestelde-vragen-over-spam

[104] Espanha, https://www.aepd.es/es/areas-de-actuacion/publicidad-no-deseada

[105] Reino Unido, https://ico.org.uk/for-organisations/guide-to-pecr/electronic-and-telephone-marketing/electronic-mail-marketing/#texts

[106] UCENET, https://www.ucenet.org/

[107] TRANSNEXUS, https://transnexus.com/whitepapers/rich-call-data/

[108] FCC, https://docs.fcc.gov/public/attachments/DOC-372543A1.txt

[109] FCC, https://www.fcc.gov/spoofed-robocalls

[110] FCC, https://www.fcc.gov/spoofed-robocalls

[111] FCC, https://www.fcc.gov/spoofed-robocalls

[112] TRUECALLER, https://www.truecaller.com/blog/insights/top-20-countries-affected-by-spam-calls-in-2021

[113] TRUECALLER, https://www.truecaller.com/blog/insights/top-20-countries-affected-by-spam-calls-in-2021

[114] TRUECALLER, Truecaller Insights 2022 U.S. Spam & Scam Report - Truecaller Blog

[115] FTC, https://public.tableau.com/app/profile/federal.trade.commission/viz/DoNotCallComplaints/Maps

[116] FCC, https://opendata.fcc.gov/Consumer/Consumer-Complaints-Data-Unwanted-Calls/vakf-fz8e

[117] FCC, https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts

[118] FCC, https://www.fcc.gov/sites/default/files/stop_unwanted_robocalls_and_texts.pdf

[119] FCC, https://youtu.be/PS3llQfRLD8

[120] FCC, https://www.fcc.gov/file/11843/download

[121] FCC, https://www.fcc.gov/spoofed-robocalls

[122] ACMA, https://www.acma.gov.au/publications/2018-10/report/international-best-practice-unsolicited-communications

[123] OFCOM, https://www.ofcom.org.uk/__data/assets/pdf_file/0019/216640/statement-plan-of-work-202122.pdf

[124] OFCOM, https://www.ofcom.org.uk/__data/assets/pdf_file/0025/216439/nuisance-calls-joint-action-plan-2021.pdf

[125] OFCOM, https://www.ofcom.org.uk/__data/assets/pdf_file/0018/232074/statement-tackling-scam-calls-and-texts.pdf

[126] TRUECALLER, https://www.truecaller.com/blog/insights/top-20-countries-affected-by-spam-calls-in-2021

[127] OFCOM, Ofcom, February 2022. Improving the accuracy of Calling Line Identification (CLI) data; Ofcom, February 2022. Good practice guide to help prevent misuse of sub-allocated and assigned numbers.

[128] OFCOM, https://www.ofcom.org.uk/phones-telecoms-and-internet/advice-for-consumers/scams

[129] OFCOM, https://www.ofcom.org.uk/__data/assets/pdf_file/0012/27300/easy-read-nuisance-calls-guide.pdf

[130] OFCOM, https://www.ofcom.org.uk/__data/assets/pdf_file/0019/10675/nuisance-calls-and-messages-consumer-guide.pdf

[131] ACMA, https://www.acma.gov.au/articles/2022-06/acma-target-misinformation-and-sms-scams-2022-23

[132] ACMA, https://www.youtube.com/watch?v=EJLw0CTiRHw&t=23s

[133] ACMA, https://www.acma.gov.au/phone-scam-educational-resources

[134] ACMA, https://www.acma.gov.au/protect-yourself-unwanted-calls-and-faxes

[135] Australia, Do Not Call Register Act 2006

[136] Australia, Spam Act 2003

[137] Australia, Telecommunications (Telemarketing and Research Calls) Industry Standard 2017

[138] TRAI, https://trai.gov.in/sites/default/files/DLT_UCC_28012022.pdf

[139] TRAI, https://trai.gov.in/sites/default/files/RegulationUcc19072018.pdf

[140] Nolan Bauerle, what is a Distributed Ledger?, https://www.coindesk.com/information/what-is-a-distributed-ledger/.

[141] IBM, https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs/index.html

[142] TRAI, https://trai.gov.in/sites/default/files/DLT_UCC_28012022.pdf

[143] Exotel, https://support.exotel.com/support/solutions/articles/3000096504-trai-regulations-on-commercial-communications-dlt-portal-sms-in-india

[144] https://www.corefactors.in/blog/what-is-dlt-registration/

[145] TRAI, https://www.trai.gov.in/sites/default/files/RegulationUcc19072018.pdf

[146] TRAI, https://trai.gov.in/sites/default/files/DLT_UCC_28012022.pdf

[147] https://www.tanla.com/news/bridging_telecom_policy_and_blockchain_practice.pdf

[148] TRAI, https://trai.gov.in/consumer-info/

[149] TRAI, https://trai.gov.in/consumer-info/consumer-outreach-program

[150] TRAI, https://trai.gov.in/measures-be-taken-avoid-ucc

[151] TRAI, https://trai.gov.in/sites/default/files/RegulationUcc19072018.pdf

[152] CRTC, https://crtc.gc.ca/eng/DNCL/rpt210930.htm

[153] DNCL, https://lnnte-dncl.gc.ca/en/About-Us

[154] CRTC, https://crtc.gc.ca/eng/DNCL/rpt210930.htm

[155] CRTC https://crtc.gc.ca/eng/archive/2021/2021-123.htm

[156] CRTC, https://crtc.gc.ca/eng/phone/telemarketing/

[157] CRTC, https://crtc.gc.ca/eng/martel/s01e13.htm

[158] CRTC, https://crtc.gc.ca/eng/phone/telemarketing/fraud.htm#_How_to_protect

[159] IMDA, https://www.imda.gov.sg/-/media/Imda/Files/About/Media-Releases/2020/COS2020/Annex-D-COS-2020---Factsheet---Mitigating-Spoof-Calls.pdf?la=en

[160] PDPC, https://www.pdpc.gov.sg/Help-and-Resources/2021/10/Protecting-Yourself-from-Spam-and-Scam

[161] IMDA, https://www.imda.gov.sg/regulations-and-licensing/Regulations/consultations/Consultation-Papers/2022/Proposals-to-Strengthen-Safeguards-for-SMS-Messages-to-Singapore-Users

[162] IMDA, *https://www.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2022/Enhancing-protection-against-scams-IMDA-proposes-full-SMS-Sender-ID-registration-as-part-of-ongoing-measures*

[163] IMDA, *https://www.imda.gov.sg/seniorsgodigital/-/media/Seniors-Go-Digital/PDF/pdf9/Scam%20Infographic%20-%20English.pdf/*

[164] Singapura, *https://sso.agc.gov.sg/Act-Rev/SCA2007/Published/20211231?DocDate=20080731&ViewType=Pdf&_=20220406224813*