CAPÍTULO 7

EMPREGO DO STIR/SHAKEN COMO FERRAMENTA DE PROTEÇÃO DE DADOS & COMPLIANCE PARA PRÁTICAS DE POLITICAS PÚBLICAS

Data de submissão: 01/04/2024 *Data de aceite: 02/05/2024*

Carlos Ricardo Ferreira de Castilho
Auditor Interno de Qualidade
Brasília – DF
http://lattes.cnpq.br/4999094272961100

RESUMO: O presente estudo aborda a importância do emprego do STIR/SHAKEN como instrumento complementar nas políticas públicas voltadas para a proteção de dados, destacando sua relevância no contexto da Lei Geral de Proteção de Dados (LGPD) no Brasil e da Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act nos Estados Unidos. O objetivo central é investigar como a implementação do STIR/SHAKEN pode servir como uma medida eficaz para atender aos requisitos de segurança de dados e, por consequência, fortalecer as políticas públicas nessa área. A metodologia adotada inclui a análise do compliance proporcionada pela LGPD e pela TRACED Act, além da revisão de estatísticas relevantes obtidas de bancos de trabalhos acadêmicos, como o da Capes, para avaliar o estado atual da pesquisa sobre o tema. Os resultados indicam que, embora a tecnologia STIR/SHAKEN seja relativamente nova no Brasil, sua adoção pelas empresas de telecomunicações está avançada em países como Estados Unidos, demonstrando sua eficácia na verificação da autenticidade das chamadas e na prevenção de fraudes. As conclusões reforçam que a implementação do STIR/SHAKEN pode significar um avanço significativo nas práticas de proteção de dados no Brasil, alinhando-se às exigências legais e contribuindo para um ambiente digital mais seguro e confiável.
PALAVRAS-CHAVE: STIR/SHAKEN. Proteção. Segurança. Telecomunicações.

USE OF STIR/SHAKEN AS A DATA PROTECTION & COMPLIANCE TOOL FOR PUBLIC POLICY PRACTICES

ABSTRACT: This study addresses the importance of using STIR/SHAKEN as a complementary instrument in external public policies for data protection, highlighting its relevance in the context of the General Data Protection Law (LGPD) in Brazil and the Telephone Robocall Abuse Criminal Enforcement and United States Deterrence Act (TRACED). The central objective is to investigate how the implementation of STIR/SHAKEN can serve as an effective measure to meet data security requirements and,

consequently, strengthen public policies in this area. The methodology adopted includes compliance analysis provided by the LGPD and the TRACED Act, in addition to the review of statistics obtained from academic work banks, such as Capes, to assess the current state of research on the topic. The results indicate that, although the STIR/SHAKEN technology is relatively new in Brazil, its adoption by telecommunications companies is advanced in countries such as the United States, demonstrating its effectiveness in verifying call transmission and preventing fraud. The guidelines reinforce that the implementation of STIR/SHAKEN can mean a significant advance in data protection practices in Brazil, aligning with legal standards and contributing to a safer and more reliable digital environment.
KEYWORDS: STIR/SHAKEN. Protection. Security. Telecommunications.

INTRODUÇÃO

Na conjuntura atual, marcada pela ubiquidade da tecnologia e pela crescente digitalização de serviços em diversas esferas da vida cotidiana, a questão da proteção de dados pessoais e da segurança da informação ascende à categoria de preocupação primordial para indivíduos, empresas e governos.

A transição para um mundo cada vez mais conectado traz consigo não apenas inúmeras vantagens em termos de acessibilidade e eficiência, mas também expõe usuários e sistemas a uma gama ampliada de riscos e vulnerabilidades. Phishing, fraudes, golpes telefônicos e outras formas de abuso representam ameaças persistentes que comprometem a privacidade, a segurança e a confiança no ecossistema digital.

Nesse cenário, a implementação de soluções tecnológicas inovadoras, aliada à formulação e ao aprimoramento de políticas públicas dedicadas à proteção de dados, emerge como um vetor crítico para o estabelecimento de um ambiente digital seguro e confiável. O protocolo STIR/SHAKEN exemplifica essa categoria de inovações, constituindo-se como uma estratégia tecnológica desenvolvida para autenticar e verificar a origem das chamadas telefônicas em redes de telecomunicações, combatendo assim a falsificação de números e os golpes associados a essa prática.

O protocolo STIR/SHAKEN, acrônimo para Secure Telephone Identity Revisited (STIR) e Signature-based Handling of Asserted Information Using toKENs (SHAKEN), representa uma inovação tecnológica fundamental no combate às chamadas telefônicas fraudulentas e à manipulação de identidades de chamadas. Desenvolvido com o intuito de restaurar a confiança nas comunicações telefônicas, este conjunto de padrões e procedimentos trabalha para verificar a autenticidade da informação de identificação do chamador, empregando tecnologias de certificação digital para assegurar que a origem da chamada seja legítima e verificável.

Ao implementar o STIR/SHAKEN, as operadoras de telecomunicações têm a capacidade de validar e assinar digitalmente as chamadas em sua origem, proporcionando aos destinatários uma garantia robusta de que a identidade apresentada é precisa e não foi alterada ou falsificada durante o trânsito pela rede. Essa abordagem não só facilita a

detecção e a prevenção de práticas maliciosas, como também fortalece a integridade e a segurança das comunicações telefônicas, contribuindo significativamente para a mitigação de riscos associados a fraudes e golpes.

Este estudo visa aprofundar a análise sobre a confluência estratégica entre a implementação do protocolo STIR/SHAKEN e o desenvolvimento de políticas públicas focadas na salvaguarda de dados pessoais e compliance para práticas de políticas públicas.

A investigação se concentra particularmente nas ramificações e nas potencialidades que emergem dessa integração, considerando o contexto regulatório específico da Lei Geral de Proteção de Dados (LGPD) no Brasil e da Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act nos Estados Unidos.

Ambas as legislações representam marcos na evolução das normativas de proteção de dados e segurança da informação, estabelecendo padrões rigorosos para o tratamento de dados pessoais e a condução de práticas comerciais e de comunicação.

Ao explorar como o STIR/SHAKEN pode ser harmonizado com essas leis, o documento busca elucidar as formas pelas quais a tecnologia pode não apenas complementar, mas potencialmente amplificar os esforços regulatórios para proteger os cidadãos de práticas abusivas e fraudulentas, ao mesmo tempo em que se promove a transparência e a confiabilidade nas comunicações telefônicas.

Dessa forma, a análise pretende contribuir para um entendimento mais aprofundado de como as sinergias entre inovações tecnológicas e políticas públicas podem fortalecer o ecossistema digital, assegurando a proteção de dados pessoais e a integridade das comunicações em um ambiente cada vez mais conectado e vulnerável a ameaças.

Adotando uma abordagem multidisciplinar que entrelaça perspectivas legais, tecnológicas e de políticas públicas, este estudo se propõe a desvendar as nuances da integração do STIR/SHAKEN no arcabouço de medidas de proteção de dados. Ao analisar as complexidades jurídicas, as inovações tecnológicas subjacentes ao protocolo e as implicações para a formulação e implementação de políticas públicas, busca-se elucidar o potencial do STIR/SHAKEN em fortalecer e complementar as estruturas existentes de proteção de dados.

DAS POLÍTICAS PÚBLICAS

As políticas públicas para proteção de dados têm se mostrado uma prioridade incontornável em um mundo cada vez mais digitalizado, onde a proteção de informações pessoais e corporativas é fundamental. A definição dessas políticas envolve a criação, implementação e avaliação de medidas governamentais destinadas a garantir a integridade, confidencialidade e disponibilidade de dados. Este processo é vital para prevenir violações de dados, combater fraudes e proteger a privacidade dos cidadãos.

O ciclo de políticas públicas é um processo contínuo que começa pela identificação de problemas, seguido pela formulação de políticas, implementação das medidas propostas e, finalmente, a avaliação de seu impacto. Este ciclo permite ajustes e reformulações constantes para atender às necessidades em evolução da sociedade e às ameaças emergentes à segurança dos dados.

No Brasil, a aprovação de políticas públicas segue um processo democrático que envolve diversas etapas. Inicialmente, a necessidade de uma nova política é identificada, seja por meio da demanda social ou por reconhecimento de lacunas existentes pelas autoridades. A sociedade, cada vez mais consciente da importância da segurança de dados, exige pesquisas de impacto que possam gerar transformações sociais significativas, como apontam Nicli et al. (2020). Essas pesquisas são essenciais para fundamentar a formulação de políticas eficazes.

Uma vez identificada a necessidade, elabora-se uma proposta de política, que deve ser amplamente discutida por stakeholders, incluindo especialistas, sociedade civil e setor privado, contribuindo para reflexões e discussões sobre as dimensões social, ambiental, econômica, cultural, política e as necessárias transformações institucionais, conforme mencionado por Sehnem et al. (2022). Esse diálogo é crucial para garantir que as políticas propostas sejam abrangentes e efetivas.

Após a formulação, a proposta passa pelo crivo do poder legislativo, onde é debatida e, se aprovada, transformada em lei. Este processo é influenciado por decisões políticas que visam ao bem-estar da comunidade, destacando a complexidade da prestação de serviços públicos, como observado por Correia et al. (2020). A implementação das políticas requer uma coordenação eficaz entre diferentes níveis de governo e o setor privado, além de um acompanhamento contínuo para avaliar sua eficácia e fazer os ajustes necessários.

A crescente complexidade e sofisticação das ameaças à segurança de dados têm impulsionado uma revisão contínua e aprimoramento dos métodos e estratégias de proteção. Resende et al. (2022) ressaltam como essa dinâmica impõe uma necessidade imperativa de atualização e flexibilidade nos mecanismos de defesa contra violações de dados e invasões cibernéticas. Neste contexto, as políticas públicas não podem ser estáticas; elas precisam ser concebidas de forma a refletir a natureza fluida do ciberespaço e a adaptabilidade dos cibercriminosos.

A demanda por políticas públicas dinâmicas e responsivas é uma resposta direta à velocidade sem precedentes com que novas tecnologias são desenvolvidas e adotadas, bem como à evolução constante das táticas empregadas por agentes mal-intencionados. Essas políticas devem ser capazes de se antecipar a potenciais vulnerabilidades, incorporando avanços em criptografia, segurança de redes e inteligência artificial para a detecção e prevenção de ameaças.

Além da robustez tecnológica, essas políticas precisam promover uma cultura de segurança entre usuários e organizações, enfatizando a importância de práticas

como a atualização regular de sistemas, a adoção de medidas de autenticação forte e o treinamento contínuo em conscientização sobre segurança de dados. A adaptabilidade das políticas públicas à evolução tecnológica e às ameaças aos dados sensíveis também implica na necessidade de mecanismos de revisão e atualização periódica, garantindo que as regulamentações permaneçam relevantes e eficazes. Este processo contínuo de avaliação e ajuste é crucial para manter a integridade dos dados e a confiança digital numa era caracterizada pela transformação digital acelerada.

Assim, a implementação de políticas públicas para a segurança de dados no Brasil é um processo complexo e multifacetado que requer a colaboração de múltiplos atores, baseando-se em pesquisas sólidas e em uma abordagem holística que considere todas as dimensões da sociedade.

O PROTOCOLO STIR/SHAKEN

O Protocolo STIR/SHAKEN constitui um avanço notável no setor de telecomunicações, marcando uma era de transformações significativas, especialmente nos Estados Unidos. Essa inovação tecnológica, que visa autenticar e verificar a origem das chamadas telefônicas para combater fraudes como o “spoofing”, encontrou um terreno fértil para sua adoção graças à colaboração proativa entre entidades reguladoras e o corpo legislativo americano.

A Federal Communications Commission (FCC, 2018), desempenhou um papel crucial ao formalizar um acordo com as principais operadoras do país. Este acordo não apenas delineou o caminho para a implementação do protocolo STIR/SHAKEN mas também estabeleceu um precedente para uma abordagem colaborativa entre o setor público e privado no que diz respeito à segurança e à integridade das comunicações telefônicas.

O serviço de autenticação proporcionado pela tecnologia STIR/SHAKEN introduz uma abordagem inovadora e estratificada para a validação da origem das chamadas telefônicas, através de um sistema de atestação dividido em três níveis distintos. No primeiro nível, conhecido como Full Attestation (A), a tecnologia fornece a garantia mais robusta sobre a origem da chamada. Neste estágio, o provedor de serviços confirma não apenas que a chamada foi originada dentro de sua rede, mas também que possui um relacionamento direto com o chamador, tendo verificado sua identidade e assegurado o direito legítimo de uso do número de origem. Este nível de atestação representa o mais alto grau de confiança e segurança, indicando que a chamada é autêntica e livre de manipulações maliciosas.

O segundo nível, denominado Partial Attestation (B), oferece um grau intermediário de verificação. Aqui, o provedor atesta que a chamada foi originada em sua rede e reconhece ter um relacionamento com o chamador, permitindo sua identificação. Contudo, diferentemente do nível A, o provedor não pode confirmar de forma definitiva o direito de uso do número de origem pelo chamador. Esse nível de atestação ainda proporciona uma medida significativa de autenticidade, mas com uma garantia ligeiramente menor em comparação ao nível A.

Por fim, o terceiro nível, chamado Gateway Attestation (C), é aplicado em situações onde o provedor de serviços apenas pode confirmar que a chamada entrou em sua rede, sem possuir um relacionamento direto com o originador da chamada. Esse nível indica que, embora a chamada tenha sido aceita pela rede do provedor, a origem exata e a autoridade sobre o número utilizado são incertas. Este nível de atestação é, portanto, o que oferece o menor grau de segurança, sendo utilizado em casos onde as informações sobre a origem da chamada são limitadas.

Essa hierarquia de atestação estabelecida pelo STIR/SHAKEN permite uma avaliação mais nuanciada e detalhada da autenticidade das chamadas, contribuindo significativamente para a redução de chamadas fraudulentas e a melhoria geral da confiança no ecossistema de telecomunicações (ATIS, 2017).

A implementação do protocolo STIR/SHAKEN representa uma medida crucial na batalha contra as chamadas fraudulentas, desempenhando um papel vital na proteção dos consumidores contra práticas enganosas e na preservação da confiabilidade das redes de telecomunicações. Esta tecnologia avançada, ao estabelecer um método padronizado para a autenticação e verificação das identidades de origem das chamadas telefônicas, atua diretamente na raiz do problema das chamadas indesejadas e mal-intencionadas, que frequentemente utilizam técnicas de spoofing para mascarar suas verdadeiras origens.

Ao garantir que cada chamada seja devidamente autenticada e classificada com base nos níveis de atestação, o STIR/SHAKEN oferece aos consumidores uma camada adicional de segurança, permitindo que tenham mais confiança na identificação do chamador exibida em seus dispositivos. Isso não apenas ajuda a reduzir a eficácia das táticas empregadas por fraudadores e spammers, que se aproveitam do anonimato para realizar golpes e propagandas indesejadas, mas também contribui para a criação de um ambiente de comunicação mais transparente e confiável.

Por fim, a implementação bem-sucedida do STIR/SHAKEN tem o potencial de restaurar a confiança dos consumidores nas comunicações telefônicas, um aspecto crucial em uma era dominada por uma crescente desconfiança em relação à segurança e à privacidade das comunicações digitais. Ao tomar medidas proativas para garantir a integridade das chamadas, os reguladores e as operadoras de telecomunicações estão reafirmando seu compromisso com a proteção do consumidor e a melhoria contínua da qualidade e segurança das comunicações telefônicas.

REVISÃO DE ESTATÍSTICAS RELEVANTES OBTIDAS DE BANCOS DE TRABALHOS ACADÊMICOS, PARA AVALIAR O ESTADO ATUAL DA PESQUISA SOBRE O TEMA

A avaliação do estado atual da pesquisa sobre um determinado tema é fundamental para compreender as lacunas existentes, direcionar futuras investigações e identificar as tendências atuais no campo acadêmico. A análise das estatísticas relevantes obtidas de bancos de trabalhos acadêmicos, como o Portal de Periódicos da CAPES, fornece uma visão quantitativa da produção científica e da evolução da pesquisa sobre um tema específico. Este tópico visa apresentar uma revisão dessas estatísticas para entender melhor o cenário atual da pesquisa em questão.

Em pesquisa conduzida através de uma busca sistemática no Portal de Periódicos da CAPES, resultando na identificação de seis trabalhos acadêmicos relevantes para o tema em análise, evidenciando a necessidade de estudos adicionais nesta área (Portal de Periódicos da CAPES, 2024), uma das principais fontes de literatura científica acadêmica, revelou a existência de apenas 6 trabalhos acadêmicos produzidos sobre o tema em questão. Esta quantidade limitada de trabalhos sugere uma área de estudo potencialmente subexplorada ou de nicho dentro do campo acadêmico.

A revisão das estatísticas relevantes evidencia uma necessidade crítica de expansão da abordagem teórica e metodológica no campo de estudo. É fundamental aprofundar a base teórica relacionada ao tema, estabelecendo definições claras, construtos e frameworks que possam guiar futuras pesquisas. Diante dos possíveis desafios metodológicos, é essencial explorar e desenvolver abordagens inovadoras que possam superar as limitações existentes e enriquecer a pesquisa sobre o tema.

Esse panorama revela uma oportunidade significativa para o avanço da pesquisa sobre o tema em questão. A limitada quantidade de trabalhos publicados até o momento sinaliza uma área de potencial crescimento acadêmico e científico, necessitando de uma abordagem teórica e metodológica mais robusta. Incentiva-se a comunidade acadêmica a explorar esse campo, contribuindo para o desenvolvimento de uma base de conhecimento mais ampla e diversificada.

ANÁLISE DO COMPLIANCE DO STIR/SHAKEN EM RELAÇÃO À LGPD E AO TRACED ACT

O cenário global de telecomunicações tem enfrentado desafios significativos com o aumento das chamadas indesejadas e fraudulentas. Nesse contexto, iniciativas como o STIR/SHAKEN nos Estados Unidos surgiram como soluções tecnológicas avançadas para autenticar chamadas e combater fraudes.

A implementação deste padrão foi significativamente impulsionada pela Federal Communications Commission (FCC), que, em acordo com as principais operadoras, estabeleceu a adoção do STIR/SHAKEN, culminando na sua implementação em algumas redes até agosto de 2019 (FCC, 2019).

A FCC também respondeu à aprovação da TRACED Act pelo Congresso Americano, promulgando o FCC 20-42 que mandatava a implementação do STIR/SHAKEN em todas as redes IP até junho de 2021, destacando os benefícios significativos para os usuários e o apoio generalizado para sua rápida implementação (FCC, 2020-a).

Além disso, ao considerar o TRACED Act e seu mandato para a implementação do STIR/SHAKEN, observa-se um esforço legislativo e regulatório para fortalecer a confiança e a segurança no ecossistema de telecomunicações.

Ao analisar o compliance do STIR/SHAKEN em relação à legislação brasileira, especialmente a Lei Geral de Proteção de Dados (LGPD), é importante destacar que, embora a LGPD estabeleça medidas de segurança para proteger os dados pessoais contra acessos não autorizados (LGPD, art. 46), ela não especifica quais ferramentas técnicas seriam adequadas para tal fim.

A LGPD visa proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural, enfatizando a proteção de dados pessoais, inclusive em meios digitais, seja por pessoa natural ou entidade de direito público ou privado (LGPD, art. 1º). Além disso, a lei destaca a importância de proteger dados sensíveis devido ao potencial de uso discriminatório e ao impacto significativo na pessoa humana.

Nesse sentido, a Lei Geral de Proteção de Dados Pessoais (LGPD) do Brasil, em seu Art. 49, estabelece que os sistemas utilizados para o tratamento de dados pessoais devem cumprir requisitos de segurança, seguir padrões de boas práticas e de governança, além de aderir aos princípios gerais definidos na legislação e a outras normas regulamentares. Essa disposição legal ressalta a importância de uma infraestrutura de dados robusta e segura que proteja as informações pessoais contra o acesso indevido, perda ou qualquer forma de tratamento inadequado.

Além disso, a incorporação de padrões de boas práticas e de governança em sistemas de telecomunicações, conforme exigido pelo Art. 49, pode ser complementada pela estrutura regulatória e técnica fornecida pelo STIR/SHAKEN. Isso inclui o desenvolvimento de políticas claras para a gestão de riscos, a implementação de controles técnicos para a autenticação de chamadas e a adoção de uma abordagem de governança que assegure a conformidade contínua com os padrões de segurança.

A integração entre o STIR/SHAKEN e a LGPD revela uma interseção interessante no que diz respeito ao compromisso com a segurança e a privacidade dos usuários. Enquanto o STIR/SHAKEN se concentra especificamente na autenticação de chamadas para prevenir fraudes e proteger os consumidores, a LGPD aborda a proteção de dados pessoais de forma mais ampla, sem detalhar as tecnologias específicas que devem ser empregadas.

No entanto, a implementação de um sistema como o STIR/SHAKEN no Brasil estaria indubitavelmente em conformidade com os princípios da LGPD, pois contribuiria para a segurança dos dados pessoais, protegendo-os contra abusos em comunicações.

Este aspecto alinha-se aos objetivos da LGPD de promover a privacidade e a proteção de dados, sugerindo que iniciativas como o STIR/SHAKEN, se bem adaptadas, poderiam reforçar o compliance com a legislação de proteção de dados no Brasil, garantindo a integridade e a confidencialidade das comunicações e dos dados pessoais envolvidos.

Em conclusão, embora o STIR/SHAKEN e a LGPD se originem de contextos regulatórios distintos e tenham focos específicos, ambos compartilham o objetivo comum de proteger os usuários contra práticas maliciosas e assegurar a confiança nos sistemas de comunicação e no tratamento de dados pessoais. A análise de compliance, portanto, revela uma compatibilidade potencial que, se explorada, poderia beneficiar significativamente a segurança das telecomunicações e a proteção de dados pessoais no Brasil.

CONSIDERAÇÕES FINAIS

O emprego do STIR/SHAKEN como ferramenta de proteção de dados e compliance para práticas de políticas públicas ressalta a intersecção promissora entre inovações tecnológicas e marcos regulatórios na proteção contra fraudes telefônicas e na garantia da segurança de dados pessoais. Embora seja papel da Autoridade Nacional de Proteção de Dados (ANPD) zelar pela proteção de dados pessoais e por regulamentar, implementar e fiscalizar o cumprimento da LGPD, no Brasil a Agência Nacional de Telecomunicações (ANATEL) tomou a iniciativa de coordenar, junto ao mercado, a adoção STIR/SHAKEN como medida essencial nos serviços de telecomunicações.

A implementação do protocolo STIR/SHAKEN, embora originária de um contexto regulatório voltado para o combate a chamadas fraudulentas nos Estados Unidos, apresenta uma compatibilidade significativa com os princípios da Lei Geral de Proteção de Dados (LGPD) no Brasil, a ANATEL exprime esforços para abarcar os conteúdos legais e adequação dos meios existentes no país para uma futura implementação ao protocolo. O que se entende é que, de acordo com Bucco (2024), o protocolo está em fase de homologação que, mediante a cooperação direta da Associação Brasileira de Telecomunicações (ABR Telecom) como autoridade responsável pela oferta do serviço, pretende-se entregar ao cliente usuário em 2024 a operabilidade do sistema com as regras estabelecidas pela ANATEL.

Este protocolo não só atende às exigências de autenticidade e integridade das comunicações, como também contribui para o reforço das políticas públicas voltadas à proteção de dados, alinhando-se aos esforços globais para a criação de um ambiente digital mais seguro e confiável.

A análise demonstrou que a adoção do STIR/SHAKEN pelas empresas de telecomunicações, especialmente em países onde sua implementação está mais avançada, como nos Estados Unidos, tem demonstrado eficácia na mitigação de fraudes e na promoção da confiança nas comunicações telefônicas.

Por outro lado, a escassez de estudos científicos identificada através da pesquisa na plataforma CAPES sobre a implementação e os impactos do STIR/SHAKEN no contexto da proteção de dados e compliance destaca uma lacuna significativa no corpo acadêmico atual. Essa deficiência sugere uma necessidade premente de maior atenção e investimento em pesquisas que explorem as dimensões técnicas, regulatórias e sociais desse protocolo.

A ausência de uma base de conhecimento robusta e diversificada impede uma compreensão plena dos potenciais benefícios, desafios e melhores práticas associadas ao STIR/SHAKEN, limitando a capacidade de formuladores de políticas, reguladores e indústrias de telecomunicações de otimizar sua aplicação e sinergia com as legislações de proteção de dados como a LGPD.

Portanto, é imperativo que a comunidade acadêmica, em colaboração com o setor público e privado, direcione esforços para investigar e disseminar conhecimento sobre este tema, contribuindo assim para a evolução das políticas públicas e estratégias de compliance que abordem as nuances da era digital e suas implicações na segurança de dados e na confiança das comunicações.

No Brasil, a potencial adoção do protocolo STIR/SHAKEN promete marcar uma evolução notável no panorama das práticas de proteção de dados, introduzindo uma barreira adicional contra fraudes telefônicas e abusos de identidade de chamadas. Essa camada adicional de segurança não somente alinha-se com os rigorosos padrões estabelecidos pela Lei Geral de Proteção de Dados (LGPD), mas também reforça o compromisso do país com a segurança cibernética e a privacidade dos cidadãos. Para Bucco (2014) o superintendente de Controle de Obrigações da Anatel, Gustavo Santana Borges alerta que o maior gargalo na implementação do STIR/SHAKEN está na capacidade dos fabricantes de telefonia móvel adequarem seus softweres em contexto tecnológico, como por exemplo a versão do Android, que precisa suportar a capacidade exigida pelo protocolo.

Para os consumidores, essa implementação significa um aumento substancial na confiança nas interações telefônicas, reduzindo significativamente o risco de se tornarem vítimas de golpes e fraudes que se aproveitam de informações pessoais indevidamente obtidas.

Para as operadoras de telecomunicações, representa uma oportunidade de fortalecer a confiabilidade de seus serviços e de se posicionar como vanguardistas no compromisso com a segurança do consumidor. Ademais, a integração deste protocolo pode facilitar a conformidade regulatória das empresas, simplificando a adesão aos complexos requisitos da LGPD e demonstrando uma governança de dados responsável.

É crucial, portanto, que as autoridades reguladoras, empresas de telecomunicações e demais stakeholders relevantes no Brasil estimulem o potencial do STIR/SHAKEN como um complemento eficaz às medidas de proteção de dados já existentes, o que levaria à produção de artigos mais fundamentados em contexto acadêmico.

A integração deste protocolo nas políticas públicas e estratégias corporativas demandará uma abordagem colaborativa e adaptativa, considerando as particularidades do contexto brasileiro e as dinâmicas globais de segurança da informação e proteção de dados.

Em síntese, o estudo reforça a importância de uma sinergia contínua entre inovação tecnológica e regulamentação na era digital, onde a proteção de dados pessoais e a segurança das comunicações se tornam cada vez mais críticas. A implementação bem-sucedida do STIR/SHAKEN no Brasil tem o potencial de estabelecer um marco relevante nesse sentido, contribuindo para a efetividade das políticas públicas de proteção de dados e compliance, e promovendo um ambiente digital mais seguro e confiável para todos os usuários.

REFERÊNCIAS

ATIS. **Signature-based Handling of Asserted information using toKENs (SHAKEN) - ATIS-1000074**. Washington, 2017.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 09 fev. 2024.

BUCCO, R. (2024). **Stir Shaken: adoção esbarra na falta de atualização dos celulares**. Disponível em: https://telesintese.com.br/stir-shaken-adocao-esbarra-na-falta-de-atualizacao-dos-celulares/. Acesso em: 31 mar. 2024.

CORREIA, P. M. A. R., MENDES, I., DIAS, I., & PEREIRA, S. (2020). **A evolução do conceito de serviço público no contexto das mudanças de estado e concessões político-administrativas: uma visão aglutinadora**. Revista da FAE.

EUA. S.151 - **Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act**, Pub. L. N.º 116-105 (2019) - TRACED Act. EUA, 2019.

EUA. S.151 - **Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act**, Pub. L. N.º 116-105 (2019) - TRACED Act. EUA, 2019.

FCC. **Chairman Pai Calls On Industry To Adopt Anti-Spoofing Protocols to Help Consumers Combat Scam Robocalls**. EUA, 2018. Disponível em: https://docs.fcc.gov/public/attachments/DOC-354933A1.pdf. Acesso em: 10 mar. 2024.

FCC**. Chairman Pai Statement on Progress by Major Phone Companies in Implementing Caller Id Authentication**. EUA, 2019. Disponível em: https://docs.fcc.gov/public/attachments/DOC-359087A1.pdf. Acesso em: 10 de mar. 2024.

FCC. **FCC 20-42 - Report and Order and Further Notice of Proposed Rulemaking**. EUA, 2020-a.

FCC. **The FCC's Push to Combat Robocalls & Spoofing**. EUA, 2020-b. Disponível em: https://www.fcc.gov/spoofed-robocalls. Acesso em: 21 fev. 2024.

GEAFT. **Grupo Executivo Antifraude de Telecomunicações** – GEAFT. Brasil, 2005.

NICLI, S.; ELSEN, S. U., & BERNHARD, A. (2020). **Eco-socialagriculture for social transformationandenvironmentalsustainability: A case studyofthe UPAS-Project. Sustainability**, 12(14), 5510. Disponível em: https://doi.org/10.3390/su12145510. Acesso em: 09 fev. 2024.

Portal de Periódicos da CAPES. (2024). **Pesquisa realizada em [data de acesso: 9 de fevereiro de 2024]**, através do buscador Primo, disponível em: https://www-periodicos-capes-gov-br.ezl.periodicos.capes.gov.br/index.php/buscador-primo.html. Acesso em: 09 fev. 2024.

RESENDE, S., CORREIA, P.M.A.R & LUNARDI, F. (2022). **A Modernização da Administração pela Lente do Google Scholar**. European Journal of Applied Business Management.

SEHNEM, S.; QUEIROZ, A. A. F. S. L.; PEREIRA, S. C. F.; CORREIA, G. S., & Kuzma, E. (2022a) **Circular economyandinnovation: A look fromthe perspective** | 285 oforganizationalcapabilities. Business StrategyandtheEnvironment, 31(1), 236- 250. Disponível em: https://doi.org/10.1002/bse.2884. Acesso em: 09 fev. 2024.