

PROJETO DE LEI Nº , DE 2025

(Do Sr. ALEX SANTANA)

Institui a Identificação Digital Segura de Agentes Públicos (ID-Agente), no âmbito da Estratégia Nacional de Governo Digital, de que trata a Lei nº 14.129, de 29 de março de 2021.

O Congresso Nacional decreta:

Art. 1º A Lei nº 14.129, de 29 de março de 2021, passa a vigorar acrescida dos seguintes dispositivos:

“Art. 16-A Fica instituída a **Identificação Digital Segura de Agentes Públicos (ID-Agente)**, no âmbito da Estratégia Nacional de Governo Digital, com o objetivo de aumentar a segurança e a transparência na interação entre agentes públicos e cidadãos durante atividades externas, como visitas domiciliares, fiscalizações e diligências.

Art. 16-B A **Identificação Digital Segura de Agentes Públicos (ID-Agente)** consiste na disponibilização de uma plataforma tecnológica centralizada, integrada à plataforma de que trata o art. 15 desta Lei, que permita a verificação, pelo cidadão, da identidade funcional e da legitimidade da ação de servidores e agentes públicos.

§ 1º A verificação de que trata o *caput* será realizada por meio de código de resposta rápida (*QR Code*) ou tecnologia similar, a ser exibido em local visível no uniforme ou vestimenta do agente, em seu material de identificação portátil e, quando aplicável, no veículo utilizado para a realização do serviço ou diligência.

§ 2º O código de que trata o § 1º deste artigo deverá conter assinatura digital em padrão compatível com a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), de modo a garantir sua autenticidade, integridade e a possibilidade de validação *offline*.



Art. 16-C A adesão dos Estados, do Distrito Federal e dos Municípios a **Identificação Digital Segura de Agentes Públicos (ID-Agente)** será voluntária e formalizada por meio de termo de adesão, na forma prevista em regulamento.

Parágrafo único. O termo de adesão estabelecerá as obrigações e responsabilidades da União e do ente federativo aderente, incluindo o compromisso de observância aos padrões técnicos e de segurança da informação.

Art. 16-D Caberá ao Poder Executivo federal:

I - desenvolver, manter e disponibilizar a plataforma tecnológica da **Identificação Digital Segura de Agentes Públicos (ID-Agente)**;

II - regulamentar os padrões técnicos, de segurança e de interoperabilidade da **Identificação Digital Segura de Agentes Públicos (ID-Agente)**, observadas as disposições da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais);

III - prestar apoio técnico aos entes federativos aderentes para a implementação da **Identificação Digital Segura de Agentes Públicos (ID-Agente)**; e

IV - promover a cooperação federativa, podendo, para tanto, celebrar convênios, acordos de cooperação técnica ou outros instrumentos congêneres para o fomento à implementação da **Identificação Digital Segura de Agentes Públicos (ID-Agente)**." (NR)

Art. 2º Esta Lei entra em vigor na data de sua publicação.

JUSTIFICAÇÃO

Nossa proposição legislativa tem como objetivo central a criação da **Identificação Digital Segura de Agentes Públicos (ID-Agente)**, um mecanismo de fácil acesso, destinado a conferir transparência, legitimidade e segurança à atuação dos servidores públicos e demais agentes do Estado que realizam visitas domiciliares e atividades externas.

A interação entre o cidadão e o agente público em atividades externas, como fiscalizações, visitas domiciliares e diligências, constitui um ponto



crítico de vulnerabilidade no tecido social. A ausência de um método de verificação de identidade que seja padronizado, criptograficamente seguro e universalmente acessível cria um vácuo de confiança que é sistematicamente explorado, por exemplo, por criminosos. As consequências podem ser devastadoras, abrangendo desde perdas patrimoniais e roubo de dados sensíveis até crimes violentos, minando a percepção de segurança e a credibilidade das instituições.

A fraude por usurpação da identidade de agentes públicos corrói a segurança patrimonial, a privacidade dos dados e, de forma mais profunda, a confiança do cidadão nas instituições que deveriam protegê-lo. A análise dos fatos revela um padrão de sofisticação e diversidade nas abordagens criminosas, que exploram a credibilidade associada à função pública para enganar, extorquir e cometer crimes graves.

A atuação de falsos agentes públicos abrange um vasto espectro de categorias funcionais, cada qual com um *modus operandi* adaptado para explorar vulnerabilidades específicas da população.

Criminosos se passam por agentes comunitários de saúde para aplicar golpes em idosos, prometendo falsas facilidades em consultas e medicamentos. Utilizam uniformes e blusas do Sistema Único de Saúde (SUS) para ganhar acesso a residências, onde praticam furtos e roubos. Em outras abordagens, coletam dados pessoais para a aplicação de fraudes financeiras ou ameaçam os moradores com a "retirada do cadastro" para forçar a entrada no domicílio. A ousadia dos golpistas chega ao ponto de criar sites falsos em nome do Ministério da Saúde para vender cursos fraudulentos, lesando profissionais da área.

No âmbito fiscalizatório, os exemplos também estão na mídia, com frequência. Utilizando técnicas de *spoofing*¹ para simular endereços de e-mail oficiais, criminosos enviam comunicações alarmistas sobre supostas "pendências fiscais graves". Essas mensagens, que imitam a identidade visual da Receita Federal e citam legislação tributária, induzem a vítima ao pânico e a clicar em *links* que instalam *malware* ou roubam dados bancários. O padrão se repete com falsos fiscais da vigilância sanitária, que enviam cobranças fraudulentas de "débitos sanitários" ou alvarás de funcionamento, visando principalmente comerciantes e empresários.

Nesse contexto, a **Identificação Digital Segura de Agentes Públicos (ID-Agente)** é apresentada como uma solução que se apropria de

¹ *Spoofing* é a prática de falsificar informações ou identidades, geralmente com intenções fraudulentas, enganosas ou maliciosas. Isso pode envolver a falsificação de números de telefone, endereços de e-mail, endereços IP ou outros dados para enganar pessoas, sistemas de segurança ou sistemas de autenticação. Vide: <https://www.aurum.com.br/blog/spoofing/>. Acesso em 14/10/2025.



tecnologias já consolidadas e validadas no setor público brasileiro para criar um padrão nacional de segurança. A proposta é uma evolução e a unificação das melhores práticas de identificação digital, elevadas a um patamar de segurança criptográfica e interoperabilidade federativa.

O cerne da **ID-Agente** consiste em oferecer ao cidadão um método de verificação instantâneo, universal e intuitivo. Conforme previsto na minuta, a verificação se dará por meio da leitura de um código de resposta rápida (*QR Code*) exibido no uniforme, crachá ou no veículo oficial usado pelo agente público. Essa tecnologia é universal, exigindo apenas a câmera de um smartphone comum para sua utilização, o que garante máxima acessibilidade e uma baixíssima barreira de adoção pelo público.

A escolha pelo *QR Code* segue tendência já consolidada na administração pública. Por exemplo, a nova Carteira de Identidade Nacional (CIN) utiliza essa tecnologia para verificação de autenticidade. Diversas iniciativas de sucesso em diferentes esferas de governo já empregam o mesmo mecanismo, como a Prefeitura de São Paulo em sua identidade funcional digital, o Governo Federal para servidores do executivo por meio do aplicativo *SouGov.br*, e até mesmo órgãos do judiciário, como o Tribunal de Justiça do Distrito Federal e dos Territórios (TJDFT) e o Tribunal Regional do Trabalho da 4ª Região (TRT-4), que já preveem a validação de suas carteiras funcionais digitais por *QR Code*.

O diferencial do nosso projeto, que eleva a segurança a um patamar superior, é uma outra exigência contida na minuta: o *QR Code* deverá conter uma assinatura digital em padrão compatível com a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

A ICP-Brasil, instituída pela Medida Provisória nº 2.200-2, de 2001, é a espinha dorsal da segurança e da validade jurídica em documentos e transações eletrônicas no País. Uma assinatura digital qualificada, emitida sob essa infraestrutura, utiliza criptografia assimétrica para garantir a autenticidade (prova da identidade do emissor), a integridade (garantia de que a informação não foi alterada desde sua emissão) e o não-repúdio (o emissor não pode negar a autoria).

Ao embutir essa assinatura criptográfica no *QR Code*, nosso projeto de lei assegura que a verificação da identidade do agente seja virtualmente imune a fraudes e falsificações. E mais: a assinatura digital permite a validação *offline*. Isso significa que, mesmo em localidades remotas sem acesso à internet, a autenticidade do código poderá ser verificada com base na criptografia contida nele, utilizando



aplicativos validadores como os já disponibilizados pelo Governo. Esta característica é fundamental para garantir a universalidade do programa em um País com as dimensões e a diversidade de conectividade do Brasil.

Como oportuno, registro meu reconhecimento e agradecimento ao senhor Jó Carneiro da Rocha Menezes, advogado, Especialista em Orçamento Público e graduando do curso de Gestão de Políticas Públicas, pela Universidade de Brasília, por ter indicado a apresentação deste projeto, pela contribuição que deu na revisão e elaboração do texto final e pelas tratativas e encaminhamentos que realizou junto a Consultoria Legislativa desta Casa.

Assim, contamos com o apoio e sensibilidade dos nobres Pares, no sentido do debate, aprimoramento e aprovação deste importante projeto de lei.

Sala das Sessões, em de de 2025.

Deputado ALEX SANTANA

