CONTRIBUIÇÃO PRÉVIA À MINUTA DO EDITAL Nº 001/2026

Sandbox Regulatório SESP/PR — Fronteira

Audiência Pública nº 7/2026

Prezados(as) Senhores(as),

A Proc Group vem, tempestivamente, apresentar contribuição prévia à minuta do Edital nº 001/2026 (Sandbox Regulatório SESP/PR — Fronteira), no âmbito da Audiência Pública nº 7/2026, com os questionamentos e ponderações a seguir, acompanhados da respectiva fundamentação jurídica e técnica, com o objetivo de colaborar para o aprimoramento do instrumento convocatório e para a segurança jurídica dos futuros participantes.

1. Viabilidade jurídica da abertura de código de hardware de terceiros

O art. 19 da minuta exige que as soluções testadas sejam licenciadas sob padrões de código aberto, assegurando "acesso irrestrito ao código-fonte". Ocorre que soluções de segurança pública frequentemente dependem de hardware e firmware fornecidos por fabricantes terceiros (drones, sensores, câmeras e demais equipamentos), cujo código-fonte não pertence ao participante do Sandbox e, portanto, não pode por ele ser aberto — independentemente da tecnologia ou do fabricante envolvido, já que não se tem notícia, no mercado, de fabricante que disponibilize publicamente o firmware de seus equipamentos.

Solicita-se esclarecimento se a exigência de abertura recai exclusivamente sobre os artefatos desenvolvidos ou adaptados especificamente para o piloto (integrações, modelos, algoritmos próprios), ou se abrange também componentes de hardware/firmware de terceiros — hipótese em que a exigência, tal como redigida, seria de cumprimento materialmente inviável para qualquer participante do certame, em prejuízo do próprio interesse público na ampla competitividade do Sandbox.

Fundamentação

- Impossibilidade jurídica de disposição sobre direito alheio: nos termos da Lei nº 9.609/1998 (Lei do Software) e, subsidiariamente, da Lei nº 9.610/1998 (Lei de Direitos Autorais), a titularidade dos direitos patrimoniais sobre o programa de computador pertence ao fabricante do hardware/firmware. Exigir que o participante do Sandbox disponibilize código-fonte de terceiro equivale a impor obrigação de impossível

cumprimento, o que colide com o princípio geral de direito segundo o qual ninguém pode dispor de direito que não detém (nemo dat quod non habet).

- Vinculação a critérios exequíveis e julgamento objetivo: a Lei nº 14.133/2021 (Nova Lei de Licitações e Contratos Administrativos), em seus arts. 5º e 11, consagra os princípios da razoabilidade, da competitividade, do julgamento objetivo e da vinculação ao instrumento convocatório, os quais pressupõem que as exigências editalícias sejam materialmente cumpríveis pelos licitantes/participantes.
- Restrição indevida à competitividade: exigência de cumprimento impossível a todos os concorrentes, por afetar de igual modo qualquer solução que dependa de hardware de mercado, tende a esvaziar a finalidade competitiva do certame (art. 11, IV, da Lei nº 14.133/2021), recomendando-se a delimitação expressa do alcance do art. 19 aos artefatos de titularidade do próprio participante.

2. Risco à própria eficácia da política de segurança pública

Ainda em relação ao art. 19, chama-se atenção para ponto de ordem estratégica e de interesse público: a exigência de disponibilização pública de modelos, pesos, arquiteturas e documentação (§3º), quando aplicada a soluções de segurança fronteiriça, pode produzir efeito colateral relevante e contraproducente. Tornar público o funcionamento detalhado de tecnologias de detecção, vigilância e repressão a ilícitos transfronteiriços — rotas de monitoramento, lógica de detecção, parâmetros de biometria, arquitetura de sensores — pode fornecer a organizações criminosas informação suficiente para identificar e neutralizar os próprios mecanismos de proteção que a solução busca implementar, comprometendo a efetividade da política pública que o Sandbox pretende fomentar.

Solicita-se que a Comissão de Sandbox esclareça se está prevista alguma exceção ou tratamento diferenciado para informações cuja divulgação pública possa comprometer a efetividade operacional da segurança pública, à luz das "hipóteses legais de proteção" já mencionadas no §3º do art. 19, e se essa hipótese abrange o risco de exposição de metodologias sensíveis de segurança.

Fundamentação

- Hipóteses legais de sigilo previstas na Lei de Acesso à Informação: a Lei nº 12.527/2011 (LAI), em seu art. 23, autoriza a classificação como sigilosa de informação cuja divulgação possa colocar em risco a defesa e a soberania nacional, comprometer atividades de

inteligência ou de investigação em curso, ou prejudicar ou causar risco a planos e operações estratégicos das Forças Armadas e órgãos de segurança pública. Trata-se de fundamento normativo direto para o tratamento diferenciado ora solicitado.

- Regime próprio de dados para segurança pública na LGPD: a Lei nº 13.709/2018 (LGPD), em seu art. 4º, III, e §1º, reconhece regime de tratamento próprio — disciplinado por lei específica ou, na sua ausência, pelos princípios gerais da própria LGPD — para dados tratados com finalidade exclusiva de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, reforçando a necessidade de tratamento diferenciado em relação ao regime geral de transparência.
- Ponderação entre transparência e eficácia da política pública: a própria LAI (art. 23, §2º, e regulamentação correlata) prevê que a classificação de sigilo deve observar o interesse público da informação e ser motivada, admitindo-se, portanto, a convivência entre publicidade como regra geral do Sandbox e sigilo pontual e motivado para elementos cuja exposição comprometa a política de segurança que o próprio programa busca testar e fomentar.

3. Alcance da preservação da propriedade intelectual prevista no §2º do art. 19

O §2º do art. 19 estabelece que "a propriedade intelectual do código-fonte desenvolvido será preservada", ao passo que o caput exige seu licenciamento sob modalidades abertas (open source), com acesso irrestrito ao código-fonte e liberdade de modificação e redistribuição.

Considerando que as licenças abertas usualmente preservam a autoria (atribuição), mas podem restringir ou eliminar a exclusividade econômica de exploração do software, solicita-se esclarecimento acerca do alcance jurídico da expressão "propriedade intelectual será preservada". Em especial, questiona-se se a intenção da Administração é preservar apenas a titularidade autoral do desenvolvedor ou também assegurar mecanismos que mantenham sua capacidade de exploração econômica futura, evitando-se interpretações que possam desestimular a participação de empresas inovadoras no Sandbox.

Fundamentação

- Distinção entre direitos morais e direitos patrimoniais: a Lei nº 9.610/1998, aplicável subsidiariamente ao software por força do art. 2º da Lei nº 9.609/1998, distingue com

clareza os direitos morais do autor (irrenunciáveis e inalienáveis, como o direito de paternidade da obra) dos direitos patrimoniais (disponíveis, cedíveis e licenciáveis). O licenciamento sob padrões abertos regula o exercício de direitos patrimoniais, sem afetar a autoria — daí a relevância de o Edital indicar precisamente a qual desses planos se refere a expressão "preservação da propriedade intelectual".

- Compatibilidade com o Marco Legal das Startups: a Lei Complementar nº 182/2021, ao instituir o ambiente regulatório experimental (sandbox regulatório) como instrumento de fomento à inovação, tem por finalidade estimular a experimentação e a atração de soluções inovadoras — finalidade que pode ser esvaziada caso o regime de propriedade intelectual aplicável não assegure, ao menos, previsibilidade quanto à possibilidade de exploração econômica do ativo desenvolvido.
- Segurança jurídica e regime supletivo em caso de silêncio: sugere-se que o Edital ou seus anexos remetam expressamente ao(s) tipo(s) de licença aberta admitido(s) (ex.: MIT, Apache 2.0, GPL, permissivas versus copyleft), já que cada modalidade produz efeitos distintos sobre a exploração econômica futura, sanando eventual antinomia aparente entre o caput e o §2º do art. 19.

4. Sigilo da proposta técnica e dos dados operacionais, para além do código-fonte

Os questionamentos anteriores tratam da abertura de código e de hardware, mas há camada adicional que extrapola o código-fonte: a própria proposta técnica submetida ao Sandbox — incluindo dados, estratégias de uso dos algoritmos, rotas e geolocalização de operações, e demais elementos do projeto como um todo, do qual o hardware de terceiros é apenas componente periférico.

Solicita-se esclarecimento sobre como a SESP/PR pretende preservar o sigilo dessas informações operacionais e investigativas ao longo do Sandbox: se o tratamento será de sigilo parcial ou completo, quais elementos da proposta técnica ficarão protegidos por padrão, e como se compatibiliza essa proteção com os dispositivos do Edital voltados à transparência e à publicidade dos resultados (a exemplo do §1º do art. 15, quanto à fundamentação do resultado preliminar, e do art. 19, quanto à abertura de modelos e documentação).

Fundamentação

- Sigilo de propostas técnicas na Lei nº 14.133/2021: o art. 25 e correlatos da Lei nº 14.133/2021 admitem tratamento sigiloso de informações sensíveis contidas em

propostas, sem prejuízo do dever geral de publicidade que rege os procedimentos administrativos, cabendo à Administração disciplinar, em regulamento próprio do Sandbox, os limites objetivos desse sigilo.

- Classificação de informações sigilosas por grau e prazo: a LAI (Lei nº 12.527/2011, arts. 23 a 24) estabelece graus de sigilo (reservado, secreto e ultrassecreto) e prazos máximos de restrição de acesso, oferecendo parâmetro normativo objetivo que o Edital pode adotar para classificar, com previsibilidade, os elementos da proposta técnica que permanecerão protegidos.
- Necessidade de disciplina específica e prévia: recomenda-se que o próprio Edital (ou anexo específico) defina, de forma exaustiva e anterior à submissão das propostas, quais informações serão consideradas sigilosas por padrão, evitando-se insegurança jurídica ao participante quanto ao risco de exposição involuntária de dados operacionais e investigativos sensíveis.

5. Restrição de participação a empresas com capital estrangeiro, à luz da soberania tecnológica

O Edital elenca "Soberania Tecnológica e Residência de Dados no Brasil" como critério da Matriz Avaliativa (Anexo V, peso 3), mas trata o tema apenas como pontuação, e não como requisito de elegibilidade. Diante da natureza sensível do escopo — segurança pública em faixa de fronteira internacional —, questiona-se se a SESP/PR pretende adotar como critério eliminatório, e não apenas classificatório, a limitação de participação a empresas de capital nacional, sem aporte de fundos ou controle societário estrangeiro, de forma a assegurar efetiva soberania sobre as tecnologias empregadas na segurança da fronteira.

Fundamentação

- Necessidade de amparo legal expresso para restrição eliminatória: o princípio da isonomia entre licitantes/participantes, previsto no art. 5º da Lei nº 14.133/2021, somente admite restrição à participação de empresas de capital estrangeiro quando amparada em vedação legal expressa ou em interesse público devidamente motivado e proporcional (arts. 5º e 11, Lei nº 14.133/2021), não bastando referência genérica à "soberania tecnológica" sem parâmetro objetivo.
- Faixa de fronteira como área de interesse da segurança nacional: a Lei nº 6.634/1979 e o Decreto nº 85.064/1980, que dispõem sobre a faixa de fronteira, reconhecem esse

território como área de interesse fundamental para a segurança nacional, o que pode servir de fundamento legítimo para eventual tratamento diferenciado — desde que a exigência seja compatível com o objeto do Sandbox e proporcional ao risco que se pretende mitigar.

- Recomendação de definição de critério objetivo e motivado: sugere-se que a Comissão de Sandbox esclareça, de forma expressa, se o requisito será eliminatório ou meramente classificatório e, caso opte pela primeira hipótese, apresente a motivação técnica e jurídica correspondente, de modo a resguardar a legalidade e a proporcionalidade da exigência e a evitar questionamentos futuros quanto à isonomia do certame.

6. Guarda e hospedagem dos dados em infraestrutura local, sob custódia das forças de segurança

Ainda quanto à soberania e à governança de dados, solicita-se esclarecimento se o Edital pretende exigir que os dados coletados e processados pelas soluções — em especial os de natureza operacional e investigativa — permaneçam sob custódia direta das forças de segurança pública, em infraestrutura local, vedando-se o processamento ou armazenamento em ambiente de nuvem, ainda que localizado em território nacional. O Edital, hoje, trata a "residência de dados no Brasil" (Anexo V) como suficiente para fins de soberania, sem distinguir entre nuvem nacional e infraestrutura local sob custódia estatal — distinção que se reputa relevante dado o grau de sensibilidade dos dados envolvidos.

Fundamentação

- Regime diferenciado de dados de segurança pública na LGPD: conforme já mencionado, o art. 4º, III e §1º, da Lei nº 13.709/2018 (LGPD) exclui do regime geral o tratamento de dados para fins de segurança pública e persecução penal, remetendo-o a lei específica ou, na sua falta, aos princípios gerais de proteção de dados — o que reforça a competência (e a conveniência) de a SESP/PR disciplinar, em ato próprio, requisitos adicionais de custódia e armazenamento compatíveis com a sensibilidade da informação.

- Distinção técnico-jurídica entre residência de dados e efetiva custódia: "residência de dados" (data residency) refere-se apenas à localização geográfica do armazenamento, sem necessariamente implicar controle direto do órgão de segurança sobre o ambiente de processamento; já a custódia local sob gestão estatal acrescenta camada de controle operacional e de acesso, relevante notadamente para dados de investigação em curso e de inteligência de fronteira.

- Parâmetro de boas práticas em contratações de tecnologia sensível: recomenda-se que o Edital adote, por analogia às boas práticas já observadas em contratações de tecnologia para órgãos de segurança pública e de inteligência, critérios objetivos que diferenciem nuvem pública nacional, nuvem privada nacional e infraestrutura on-premises sob custódia estatal, de modo a permitir que os participantes dimensionem adequadamente suas propostas técnicas e financeiras.

Considerações finais

Os esclarecimentos ora solicitados têm por objetivo contribuir para a segurança jurídica do certame, a exequibilidade das exigências do Edital e a proteção do interesse público subjacente ao Sandbox — notadamente a efetividade da política de segurança pública na faixa de fronteira —, sem prejuízo da ampla competitividade e do estímulo à inovação que orientam o instrumento.

Permanecemos à disposição para esclarecimentos adicionais.

Atenciosamente,

ProcGroup