DIÁRIO OFICIAL DA UNIÃO

Publicado em: 30/06/2025 | Edição: 120 | Seção: 1 | Página: 104

Órgão: Ministério da Justiça e Segurança Pública/Gabinete do Ministro

PORTARIA MJSP Nº 961, DE 24 DE JUNHO DE 2025

Estabelece diretrizes sobre uso de soluções de tecnologia da informação aplicadas às atividades de investigação criminal e inteligência de segurança pública.

O MINISTRO DE ESTADO DA JUSTIÇA E SEGURANÇA PÚBLICA, no uso das atribuições que lhe são conferidas pelo art. 87, parágrafo único, incisos I e II, da Constituição, e tendo em vista os arts. 3º e 10 da Lei nº 13.675, de 11 de junho de 2018, o art. 35, incisos XXI e XXIII, da Lei nº 14.600, de 19 de junho de 2023, e o que consta no Processo Administrativo nº 08250.000028/2025-73, resolve:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Portaria estabelece diretrizes sobre o uso de soluções de tecnologia da informação aplicadas às atividades de investigação criminal e inteligência pelos órgãos de segurança pública.

§ 1º As diretrizes estabelecidas nesta Portaria se aplicam aos seguintes órgãos:

I - Polícia Federal;

II - Polícia Rodoviária Federal;

III - Polícia Penal Federal;

IV - Força Nacional de Segurança Pública;

V - Força Penal Nacional;

VI - Secretaria Nacional de Segurança Pública; e

VII - Secretaria Nacional de Políticas Penais.

§ 2º O disposto nesta Portaria será observado pelos órgãos de segurança pública estaduais, distritais e municipais nas iniciativas que envolvam recursos oriundos do Fundo Nacional de Segurança Pública e do Fundo Penitenciário Nacional para projetos, ações e objetos relacionados à compra de soluções de tecnologia da informação, incluindo repasses e doações.

Art. 2º As diretrizes estabelecidas nesta Portaria são norteadas pelos seguintes valores:

I - o respeito aos direitos e às garantias fundamentais;

II - a inviolabilidade da intimidade, da vida privada, da honra, da imagem e do sigilo das comunicações telefônicas, de dados e das correspondências;

III - o direito à proteção de dados pessoais;

IV - o devido processo legal;

V - a legitimidade dos fins e a adequação, a necessidade e a proporcionalidade das medidas que afetem direitos fundamentais;

VI - a integridade e a confiabilidade dos sistemas informacionais;

VII - a prevenção à fraude e outros crimes patrimoniais; e

VIII - a transparência, a responsabilização e a prestação de contas.

Art. 3º Esta Portaria tem por objetivo assegurar:

I - a legalidade, a adequação, a necessidade e a proporcionalidade como condições do uso de sistemas de tecnologia da informação nas atividades de investigação criminal e inteligência de segurança pública que possam gerar riscos à privacidade e a outros direitos fundamentais;

II - a padronização dos procedimentos para o uso de soluções de tecnologia da informação pelos órgãos de segurança pública;

III - o estabelecimento de padrões de segurança da informação para impedir acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, difusão ou vazamentos de dados;

IV - a incorporação de medidas técnicas e administrativas de preservação e verificação da cadeia de custódia da prova para manter a integridade de elementos informativos e assegurar sua autenticidade;

V - a instituição de mecanismos de avaliação e mitigação de riscos; e

VI - a adoção de mecanismos de transparência, auditabilidade, responsabilização e prestação de contas.

Art. 4º Para os fins desta Portaria, considera-se:

I - dado pessoal: informação relacionada a uma pessoa natural identificada ou identificável;

II - dado pessoal sensível: informação pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - dado sigiloso: informação protegida por sigilo constitucional ou legal;

IV - inteligência de segurança pública: exercício permanente e sistemático de ações especializadas para a identificação, acompanhamento e avaliação de ameaças reais ou potenciais na esfera de Segurança Pública, orientadas para produção e salvaguarda de conhecimentos necessários à decisão, ao planejamento e à execução de uma política de Segurança Pública e das ações para prever, prevenir e reprimir atos criminosos de qualquer natureza ou atentatórios à ordem pública;

V - investigação criminal: atividade estatal, fundada em justa causa, desempenhada pelos órgãos com competência para o exercício das funções de polícia judiciária, que têm por objetivos a apuração de fatos supostamente criminosos e a preservação das fontes, dos meios e da cadeia de custódia da prova;

VI - soluções de tecnologia da informação aplicadas às atividades de investigação criminal: conjunto de bens e serviços digitais empregados para fins de investigação criminal, que incluem, entre outros, programas de computadores, equipamentos digitais, plataformas de interoperabilidade, infraestruturas de tecnologia da informação, ferramentas de monitoramento remoto, equipamentos de extração de dados, soluções de inteligência artificial, armazenamento e tratamento de dados;

VII - soluções de tecnologia da informação adotadas em atividades de inteligência de segurança pública: conjunto de bens e serviços digitais destinados às atividades de inteligência, incluindo programas de computadores, equipamentos digitais, plataformas de interoperabilidade, infraestruturas de tecnologia da informação, ferramentas de monitoramento remoto não intrusivas, soluções de inteligência artificial e tratamento de dados;

VIII - tratamento de dados pessoais: toda operação realizada com informações pessoais ou sensíveis, como a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, tratamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

IX - órgãos gestores: unidades responsáveis pelas decisões referentes às soluções de tecnologia da informação aplicadas às atividades de investigação criminal e de inteligência de segurança pública; e

X - log: registro informacional cronológico de todos os eventos ou atividades que ocorrem em um sistema, aplicativo ou ambiente específico.

CAPÍTULO II

DA UTILIZAÇÃO DE SOLUÇÕES DE TECNOLOGIA DA INFORMAÇÃO

Art. 5º A utilização de soluções de tecnologia aplicadas às atividades de investigação criminal e inteligência de segurança pública deve respeitar direitos fundamentais e ser limitada ao estritamente necessário para alcançar finalidades compatíveis e circunscritas às competências e atribuições dos órgãos de segurança pública.

Parágrafo único. É vedado o uso indiscriminado, sem objetivo certo ou declarado, das soluções de tecnologia da informação referidas no caput deste artigo.

Art. 6º Na atividade de segurança de estabelecimentos prisionais, poderão ser utilizadas soluções de tecnologia da informação para:

I - detectar, identificar e localizar dispositivos móveis emissores de radiofrequência, com o objetivo exclusivo de efetuar o bloqueio da emissão de sinais e de apreender os dispositivos no interior de unidades prisionais; e

II - obter acesso aos dados armazenados em dispositivos móveis ou dispositivos eletrônicos apreendidos no interior de unidades prisionais, assegurado o controle posterior pela autoridade judicial competente.

Parágrafo único. O acesso aos dados de que trata o inciso II do caput deverá:

I - obedecer ao disposto nos §§ 2º e 3º do art. 7º, no que couber; e

II - ser objeto de comunicação ao Juízo competente.

Seção I

Da obtenção de dados sigilosos

Art. 7º Os órgãos de segurança pública utilizarão soluções de tecnologia da informação para a obtenção de dados sigilosos somente quando houver decisão judicial específica que autorize a medida para fins de investigação criminal e instrução processual penal, conforme previsto em lei.

§ 1º O uso das soluções a que se refere o caput deste artigo é condicionado à indicação do procedimento investigativo ou judicial correspondente e, sempre que tecnicamente viável, à apresentação da cópia da decisão judicial que autorizou a quebra de sigilo ou do mandado judicial específico, expedido em sua decorrência.

§ 2º A obtenção de dados sigilosos será reduzida a termo juntado aos autos do respectivo procedimento e do qual devem constar:

I - número do inquérito;

II - número do processo e dados do juízo;

III - descrição e alcance da medida deferida;

IV - data da decisão judicial;

V - período de execução;

VI - solução empregada e forma de execução; e

VII - resultados obtidos.

§ 3º Sempre que tecnicamente viável e compatível com as obrigações de preservação de elementos informativos relevantes para a produção de prova, serão descartados os dados sigilosos:

I - de terceiros não relacionados à investigação criminal, tão logo haja conhecimento do seu tratamento;

II - de investigados, assim que considerados irrelevantes no âmbito da investigação criminal; e

III - obtidos fora do período de duração autorizado judicialmente.

§ 4º Informações encontradas de forma fortuita, que possam constituir crime e extrapolem a autorização inicial, deverão ser comunicadas ao juízo competente para eventual continuidade das investigações.

Art. 8º São vedados o compartilhamento, a transferência ou a remessa não autorizados judicialmente de dados sigilosos obtidos por meio das soluções de tecnologia da informação de que trata este Capítulo.

Art. 9º O uso das soluções de tecnologia da informação de que trata este Capítulo deve observar a regulamentação do setor de telecomunicações, preservando as infraestruturas críticas nacionais.

Seção II

Das soluções de inteligência artificial

Art. 10 A utilização de soluções de inteligência artificial nas atividades de investigação criminal e inteligência de segurança pública deverá ser proporcional, observar o dever de prevenção de riscos e as leis aplicáveis à espécie.

Parágrafo único. Na hipótese de haver risco de lesão a direitos fundamentais, os agentes de segurança pública responsáveis pela aplicação das soluções referidas no caput revisarão o resultado da inferência algorítmica.

Art. 11. Os órgãos de segurança pública poderão utilizar soluções de inteligência artificial, desde que de seu funcionamento e de suas capacidades não possa resultar lesão à vida e à integridade física das pessoas.

§ 1º É vedado aos órgãos referidos no caput utilizar soluções de inteligência artificial que permitam a identificação biométrica à distância, em tempo real, em espaços acessíveis ao público, exceto nos seguintes casos:

a) instrução de inquérito ou processo criminal, mediante autorização judicial prévia e motivada, quando houver indícios razoáveis da autoria ou participação em infração penal, a prova não puder ser feita por outros meios disponíveis e o fato investigado não constituir infração penal de menor potencial ofensivo;

b) busca de vítimas de crimes, de pessoas desaparecidas ou em circunstâncias que envolvam ameaça grave e iminente à vida ou à integridade física de pessoas naturais;

c) flagrante delito de crimes punidos com pena privativa de liberdade máxima superior a dois anos, com imediata comunicação à autoridade judicial;

d) recaptura de réus ou detentos evadidos; ou

e) cumprimento de mandados de prisão ordenados pelo Poder Judiciário e das medidas e penas previstas no inciso II do art. 319 do Código de Processo Penal e no inciso IV do art. 47 do Código Penal.

§ 2º A utilização de soluções de inteligência artificial que não se enquadre nas hipóteses listadas no § 1º deste artigo deverá ser formalmente justificada e precedida de estudos que considerem os impactos negativos da inferência algorítmica.

CAPÍTULO III

DAS OBRIGAÇÕES DOS ÓRGÃOS GESTORES

Art. 12. Os órgãos de segurança pública adotarão medidas técnicas, administrativas e organizacionais de segurança, em relação às soluções de tecnologia da informação sob sua gestão, a fim de garantir:

I - o controle de acesso, assegurando que apenas agentes no pleno exercício de suas funções e previamente autorizados possam ingressar nas respectivas instalações e utilizar as soluções, por meio da adoção de certificados digitais, biometria ou autenticação multifator;

II - a adoção e a revisão periódica de perfis, que definam papéis, privilégios e direitos de acesso às funcionalidades e às informações, assim como regras para a sua concessão e revogação;

III - a limitação do uso de perfis habilitados para atividades de inteligência a agentes com prerrogativas correspondentes e lotados em órgãos com tal atribuição;

IV - a elaboração de planos de contingência de segurança da informação e de recuperação de desastres, para que as soluções de tecnologia da informação possam ser restauradas à condição imediatamente anterior ao incidente;

V - a transparência das contratações e a disponibilização de informações relevantes, atualizadas e íntegras sobre os processos licitatórios;

VI - o uso correto, ético e responsável das soluções de tecnologia da informação, promovendo capacitação aos usuários e adotando medidas para coibir o uso indevido das soluções sob sua responsabilidade pessoais;

VII - a continuidade das soluções de tecnologia da informação, promovendo sua evolução e manutenção adequada e avaliando periodicamente seus benefícios, necessidade, utilidade e uso;

VIII - a identificação e a investigação de casos de acessos indevidos, mediante a adoção de políticas de alerta contra usos maliciosos e atípicos das soluções de que trata esta Portaria; e

IX - a realização periódica de auditorias e do monitoramento de eficácia das medidas de segurança referidas neste artigo.

Parágrafo único. Os órgãos gestores assegurarão que a utilização das soluções de tecnologia da informação previstas nesta Portaria por outras entidades públicas será condicionada à adoção das medidas referidas neste artigo mediante assinatura de termos de responsabilidade.

CAPÍTULO IV

DOS REGISTROS DA UTILIZAÇÃO DAS SOLUÇÕES

Art. 13. Os órgãos de segurança pública devem registrar todos os acessos em log, contendo:

I - o nome e o CPF do usuário;

II - o endereço IP;

III - a data e a hora; e

IV - a natureza da operação, inclusive o histórico das consultas, sempre que tecnicamente viável.

Art. 14. Terão acesso aos registros de log as autoridades com competência legal para realizar o controle e assegurar o bom funcionamento das soluções de tecnologia da informação aplicadas às atividades de investigação criminal e inteligência de segurança pública, assim como para verificar a legalidade de seu uso e a integridade e segurança dos dados.

CAPÍTULO V

DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 15. O uso indevido das soluções de tecnologia da informação referidas nesta Portaria ficará sujeito à responsabilização administrativa, civil e criminal.

Art. 16. Os órgãos de segurança pública deverão revisar e atualizar os atos normativos e instrumentos contratuais relacionados às soluções de tecnologia da informação aplicadas às atividades de investigação criminal e inteligência de segurança pública, submetendo-os à análise e aprovação do Ministro responsável pela Pasta em até noventa dias da publicação desta Portaria.

Parágrafo único. No mesmo prazo do caput serão apresentados planos de conformidade para a implementação das medidas técnicas e organizacionais de adequação.

Art. 17. Aplica-se o disposto nesta Portaria às soluções de tecnologia da informação utilizadas em investigações no âmbito do Conselho Administrativo de Defesa Econômica - Cade e da Autoridade Nacional de Proteção de Dados - ANPD.

Art. 18. Casos omissos referentes às disposições desta Portaria serão resolvidos pelo Ministro de Estado da Justiça e Segurança Pública.

Art. 19. Esta Portaria entra em vigor na data de sua publicação.

RICARDO LEWANDOWSKI