**DISPAROS DE AVISOS E ALERTAS DE RISCO PELA DEFESA CIVIL EM CONFORMIDADE COM A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS**

**Porto Alegre/RS**

**2023**

**DISPAROS DE AVISOS E ALERTAS DE RISCO PELA DEFESA CIVIL EM CONFORMIDADE COM A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS**

**RESUMO**

Analisa-se a possibilidade jurídica de disparos de avisos e alertas de risco por órgãos de proteção e defesa civil para a população residente em áreas sob risco de desastres, independentemente da exigência de prévia solicitação específica ou consentimento do titular dos dados pessoais. Além do que, indicam-se alternativas ao gestor público para implementação de um serviço de difusão de alertas mais efetivo e eficiente, seja mediante o compartilhamento de dados pessoais com a entidade responsável pelas soluções em tecnologia da informação e comunicação para o ente público, seja mediante a contratação de prestadores especializados em serviços de mensageria.

**Palavras-chave:** Proteção de dados. Defesa Civil. Política Pública. Consentimento.

**INTRODUÇÃO**

A cada ano, consolida-se a percepção de que os desastres naturais ocorrem com uma recorrência maior. Não é por acaso que a imprensa internacional se refere ao atual estado de coisas, permeado por furacões, inundações, ondas de calor, ciclones, como o “novo normal” decorrente das mudanças climáticas[[1]](#footnote-1). No Estado do Rio Grande do Sul, por exemplo, ocorreram três ciclones apenas no mês de julho de 2023[[2]](#footnote-2). Essa realidade impõe ao Poder Público a adoção de novas medidas administrativas e técnicas com vistas à prevenção ou mitigação de danos nas áreas que serão atingidas por intempéries climáticas, no que se destaca a busca por uma comunicação mais efetiva dos órgãos de defesa civil com a população residente nas áreas de risco.

Os procedimentos para envio de alertas à população sobre a possibilidade de ocorrência de desastres encontram-se regulados na Portaria nº 2.216, de 4 de julho de 2023, do Ministério da Integração e do Desenvolvimento Regional, na qual se confere aos órgãos de proteção e defesa civil dos municípios a competência para envio dos alertas, sempre acompanhados de recomendações ou ações emergenciais para a população em risco de desastre, com vistas ao salvamento ou melhor atendimento dos prováveis atingidos.

Residualmente, dispõe-se que os órgãos estaduais exercerão essa atribuição em caso de incapacidade dos municipais em razão da falta de estrutura operacional para operação do serviço adrede citado. Ademais, nas situações de impossibilidade de envio por parte dos órgãos estaduais e municipais, ou em caso de desastres excepcionais, o Centro Nacional de Gerenciamento de Riscos e Desastres poderá endereçar mensagens à população. Em todo caso, como instrumento para operacionalização desse serviço, a Secretaria Nacional de Proteção e Defesa Civil disponibiliza o sistema Interface de Divulgação de Alertas Públicos (IDAP), uma plataforma que pode ser utilizada para envios de alertas de desastres em todos os meios disponíveis, tais como SMS, WhatsApp[[3]](#footnote-3), Telegram, plataforma Avisos Públicos do Google e televisão por assinatura.

No entanto, a plataforma de difusão de alertas públicos tem tido baixo alcance, conforme conclusão da equipe técnica do Tribunal de Contas da União, que apontou entre as causas o pequeno percentual da população previamente cadastrada na plataforma, sendo tal circunstância um obstáculo para a adoção de medidas preparativas para o resguardo dos mais vulneráveis.

Nesse contexto, mostra-se de significativa relevância, como problema de pesquisa, a discussão sobre a possibilidade jurídica de órgãos de proteção e defesa civil diligenciarem para que haja disparos de alertas em massa para a população em risco, independentemente de prévio cadastramento voluntário para esse serviço, tendo em conta a necessidade premente de redução dos danos humanos ocasionados por desastres naturais cada vez mais intensos e recorrentes.

Atualmente, aponta-se a Lei Geral de Proteção de Dados Pessoais (LGPD) como um dos principais óbices para a difusão de alertas de desastres a partir de bancos de dados geridos ou contratados pelo Estado, dado o imprescindível tratamento de dados pessoais como local de residência, número de celular e e-mail, abrindo espaço para o direito fundamental autônomo à proteção dos dados pessoais[[4]](#footnote-4), que foi expressamente incluído no texto constitucional por força da Emenda Constitucional nº 115, de 10 de fevereiro de 2022.

Por conseguinte, para enfrentamento do tema ora proposto, o artigo será estruturado da seguinte forma: no primeiro capítulo, serão abordadas as bases legais para o tratamento de dados pessoais pelo Poder Público, em especial a inadequação da utilização preferencial do consentimento; no segundo, será identificada a base legal legitimadora do tratamento de dados pessoais para o disparo de alertas de desastres e serão oferecidas alternativas aos gestores responsáveis pela prevenção e defesa civil com vistas à implementação de um serviço de difusão de alertas mais efetivo e eficiente, seja mediante o compartilhamento de dados pessoais com a entidade responsável pelas soluções em tecnologia da informação e comunicação para o ente público, seja mediante a contratação de prestadores de serviços de mensageria; no terceiro capítulo, será estudada a conformidade das propostas com os princípios do art. 6º da LGPD.

**I – INADEQUAÇÃO DA UTILIZAÇÃO PREFERENCIAL DO CONSENTIMENTO COMO BASE LEGAL PARA O TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO**

Inicialmente, deve ser assentado que a Lei Geral de Proteção de Dados, expressão brasileira da tendência global de proteção jurídica do direito fundamental à autodeterminação informativa no contexto do *Big Data* no qual “os dados são o novo petróleo” (na consagrada versão original: “*data is the new oil*”), não foi concebida para proibir o tratamento de dados pessoais, seja nas relações privadas, seja nas atividades administrativas do Estado.

Na perspectiva contemporânea, o Poder Público não somente pode, como deve, realizar inúmeras operações de tratamento de dados pessoais a fim de prestar serviços públicos eficientes, personalizados e capazes de concretizar os objetivos sociais plasmados no texto constitucional. Afinal, o paradigma das “políticas públicas baseadas em evidências”, iniciado ainda no final dos anos 1990 no Reino Unido, propugna que os governos devem agir embasados nas melhores evidências existentes, enfrentando, com uma ampla gama de dados, estatísticas e recursos informacionais cientificamente apurados, os desafios que se apresentam nas tarefas de formulação e implementação de políticas públicas.

O disparo de avisos e alertas de risco para residentes em áreas a serem atingidas por desastres climáticos, que terão seus direitos fundamentais à vida e à integridade física colocados à prova por situação de força maior, invoca a necessidade de utilização dos recursos informacionais existentes, que envolvem, no mínimo, dados pessoais como número de celular e e-mail, para envio das mensagens, e local de residência, para filtragem dos potenciais destinatários dos alertas de desastres. Em suma, o ente público fará uso de evidências que possui para salvar vidas e minorar impactos das intempéries naturais, viabilizando que os cidadãos se preparem adequadamente para o evento climático.

Descabe a cogitação jurídica de que o desenrolar do agir administrativo acima narrado estaria condicionado à prévia solicitação específica de cada interessado em receber tais avisos e alertas de risco aos órgãos de proteção e defesa civil. Primeiro, porque a disciplina civilista preconiza que os direitos da personalidade, no qual se inclui o direito à vida, são irrenunciáveis, conforme o art. 11 do Código Civil; segundo, porque a omissão do Estado na formulação e implementação de medidas de proteção e defesa civil seria inconstitucional; terceiro, porque a LGPD não exige o consentimento em tais ações administrativas, sendo essa uma difundida incompreensão que precisa ser fulminada, como se demonstrará abaixo.

O tratamento de dados pessoais somente pode ser realizado quando se enquadrar em uma das hipóteses legais elencadas no art. 7º da LGPD ou, para dados pessoais sensíveis, no seu art. 11. Em ambos os casos, o consentimento é uma das hipóteses de tratamento (art. 11, I ou art. 7º, I, respectivamente), mas não constitui a única nem guarda qualquer relação de superioridade hierárquica perante as demais bases legais.

No âmbito do Poder Público, o tratamento de dados pessoais usualmente se configura para o cumprimento de obrigação legal ou regulatória pelo controlador (art. 7º, II, da LGPD) ou para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei (art. 7º, III).

No que toca ao tratamento dos dados pessoais sensíveis no setor público, o cenário se apresenta deveras semelhante, sendo comumente admitido, sem fornecimento de consentimento do titular, quando for indispensável para o cumprimento de obrigação legal ou regulatória pelo controlador (art. 11, II, “a”) ou para o tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos (art. 11, II, “b”).

Sendo assim, para o deslinde da análise jurídica sobre a necessidade de prévia solicitação específica ou consentimento do titular com vistas ao disparo de alertas de desastres, cabe consignar que o enquadramento do tratamento de dados pelo Poder Público na hipótese legal de consentimento, na maioria das vezes, sequer seria adequado, uma vez que a utilização compulsória de dados pessoais para o exercício de prerrogativas estatais típicas não poderia ficar condicionada à concordância do titular em manifestação livre, informada e inequívoca[[5]](#footnote-5). Nesse sentido, a Autoridade Nacional de Proteção de Dados – ANPD, no seu “Guia Orientativo: tratamento de dados pessoais pelo Poder Público”, esclarece didaticamente o caráter residual do consentimento no contexto do setor público[[6]](#footnote-6).

Além disso, diferentemente da opção adotada pelo legislador comum europeu no GDPR, ao não estabelecer regras diferenciadas para o tratamento de dados pessoais por parte da administração pública, a LGPD veicula um capítulo específico para o Poder Público, com dispositivos que devem ser interpretados e aplicados sistematicamente em diálogo com as hipóteses legais para o tratamento dos artigos adrede citados.

Nesse sentido, o tratamento de dados pessoais pelos órgãos de proteção e defesa civil municipais ou estaduais, além de ser lastreado em alguma das bases legais dos arts. 7º ou 11 da LGPD, deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, consoante a dicção do art. 23 da LGPD.

Feitas tais considerações, apresenta-se a seguinte sistematização sobre as bases legais da LGPD a serem usadas no setor público. Em suma, o tratamento de dados pessoais pelo Poder Público ocorrerá, em regra, para o cumprimento de obrigação legal ou regulatória; e para a execução de políticas públicas previstas em leis ou regulamentos (nos casos de dados pessoais não sensíveis, com a possibilidade de serem respaldadas em contratos, convênios ou instrumentos congêneres).

Quanto à base legal radicada no consentimento (art. 7º, I ou art. 11, I, da LGPD), seu emprego deverá ocorrer, em caráter subsidiário, nos casos em que a utilização dos dados não seja compulsória e não haja o exercício de prerrogativas estatais típicas decorrentes de obrigações e atribuições legais, desde que da manifestação de vontade do titular dos dados pessoais não resultem restrições significativas à sua condição jurídica ou ao exercício de direitos fundamentais.

De igual modo, admite-se o tratamento de dados pessoais não sensíveis com fulcro no atendimento aos interesses legítimos do controlador ou de terceiro (art. 7º, IX, da LGPD), nos casos em que a utilização dos dados não seja compulsória e não haja o exercício de prerrogativas estatais típicas decorrentes de obrigações e atribuições legais, desde que seja precedido de uma ponderação entre as expectativas dos titulares e os supostos interesses estatais.

**II – BASE LEGAL LEGITIMADORA DO TRATAMENTO DE DADOS PESSOAIS PARA O DISPARO DE ALERTAS DE DESASTRES E ALTERNATIVAS AOS GESTORES RESPONSÁVEIS PELA OPERACIONALIZAÇÃO DO SERVIÇO**

Considerando que o disparo de avisos e alertas de risco pelos órgãos de proteção e defesa civil municipais ou estaduais, envolve, necessariamente, o tratamento de dados pessoais não sensíveis, constata-se a necessidade de realização de tais operações em conformidade com a Lei Geral de Proteção de Dados Pessoais. Nessas situações, entende-se mais adequado o enquadramento na base legal que versa sobre a execução de políticas públicas previstas em leis ou regulamentos (art. 7º, III)[[7]](#footnote-7), observando-se, ainda, os critérios adicionais do art. 23 da LGPD.

Para fins de interpretação da expressão “políticas públicas”, recorre-se ao esclarecimento da própria Autoridade Nacional de Proteção de Dados – ANPD, no retromencionado “Guia Orientativo: tratamento de dados pessoais pelo Poder Público”[[8]](#footnote-8), do qual se depreende que tal conceito da LGPD deve receber uma interpretação ampla, de modo a abarcar programa ou ação governamental definido em lei, regulamento ou ajuste contratual, nos quais se instituirá, em regra, seus objetivos, metas, prazos e meios de execução.

Exemplificativamente, a ANPD menciona a política pública de controle do tabagismo e prevenção e tratamento do câncer de pulmão, estabelecida em norma infralegal com objetivos, competências e meios de financiamento, que ensejará o tratamento, pela Secretaria de Saúde, de dados pessoais de fumantes atendidos na rede hospitalar pública e seu compartilhamento com a autarquia responsável pela execução do programa de orientação e auxílio das pessoas que desejam parar de fumar.

Com o intuito de conferir uma aplicação prática imediata às teses ora expostas, pode ser utilizado como ilustração a situação no Estado do Rio Grande do Sul, onde a Casa Militar é órgão legalmente responsável pela coordenação, planejamento e execução das ações de defesa civil, nos termos da Lei Estadual nº 15.934/23. Por sua vez, sua Subchefia de Proteção e Defesa Civil detém competência específica de “coordenar as ações de atendimento a situações de emergência ou calamidade pública, articulando a atuação dos órgãos envolvidos e realizando seu controle operacional”; e “prestar assessoramento técnico às Comissões Municipais de Defesa Civil, e realizar a análise de riscos de qualquer natureza com a colaboração de técnicos e demais órgãos competentes”, nos termos do Decreto Estadual nº 48.108/11, atualizado pelos Decretos Estaduais nºs 51.546/14 e 54.865/19.

Ademais, a Lei Estadual nº 15.326/19 (Plano Plurianual 2020-2023 do Estado do Rio Grande do Sul), prevê, no Eixo Sociedade com Qualidade de Vida, o programa “Evolução Sustentável”, com a ação programática “Gestão em Proteção e Defesa Civil”, coordenada pela Casa Militar, tendo como resultado esperado “proteção e defesa civil efetiva, com redução de eventuais danos, por meio do gerenciamento sistêmico de ações voltadas a prevenir ou mitigar a ocorrência de desastres naturais e tecnológicos, ampliando a capacidade de resposta a eventos não evitados”. Uma de suas iniciativas é “desenvolvimento, manutenção e expansão do Sistema de Gerenciamento de Risco e Desastre”, disponibilizando como produto uma plataforma digital para gestão de proteção e defesa civil, com transparência e controle mais efetivo a nível governamental, além de acessível à comunidade gaúcha. Aliás, estimou-se a aplicação de R$ 800.000,00 para tal finalidade na Lei Estadual nº 15.900/22 (Orçamento Anual do Estado 2023), na “Unidade Orçamentária 08.40. Fundo Estadual de Defesa Civil do Estado do Rio Grande do Sul”.

Além do que, no programa RS SEGURO, encontra-se a ação programática “Cidadão Mais Seguro”, coordenada pela Secretaria da Segurança Pública, que abriga a iniciativa de “qualificação da prevenção e combate a sinistros e das ações de busca e salvamento e defesa civil” por parte do Corpo de Bombeiros, tendo como um dos seus produtos o mapeamento de áreas de risco para ampliação das atividades de prevenção e combate a sinistros, bem como de proteção e defesa civil, que, além dos recursos disponíveis, poderão contar com a celebração de “parcerias com a sociedade civil, buscando fornecer ao cidadão pronta resposta diante de eventos que possam colocar em risco a vida”, o que corrobora a preocupação do governo e do legislador estaduais com medidas preventivas baseadas no envolvimento da comunidade.

Diante das informações lançadas acima a título de ilustração, que pode ser objeto de espelhamento para outros entes da Federação, não restam dúvidas de que a Casa Militar do Estado, por meio da Subchefia de Proteção e Defesa Civil, possui competência legal para implementar a política pública de proteção e defesa civil, consoante assinalado em leis, atos infralegais e na sua própria denominação.

Adicionalmente, com o disparo de mensagens sobre avisos e alertas de risco, o Estado atuará na persecução do interesse público, afinal a finalidade pública consubstanciada na adoção de medidas preparatórias em áreas sob risco de catástrofes climáticas almeja, ao fim e ao cabo, salvar vidas e minorar danos nas comunidades atingidas.

Com efeito, restam preenchidos os requisitos para tratamento de dados pessoais do art. 23 combinado com o art. 7º, III, da LGPD (e, na hipótese de dados pessoais sensíveis, com o art. 11, II, “b”), inclusive sendo desnecessária, e até mesmo inadequada, a exigência de prévia solicitação específica ou consentimento do titular dos dados pessoais, o qual poderá ser destinatário dos avisos e alertas de risco dos órgãos de proteção e defesa civil, uma vez que o tratamento para execução de políticas públicas independe de prévio consentimento.

Por sua vez, para operacionalização do projeto de disparo de alertas de desastres para residentes em áreas a serem atingidas por intempéries climáticas, os órgãos de defesa civil poderão ter a necessidade de contratação de terceiros especializados na prestação de serviços de mensageria.

Afora o desenvolvimento de técnicas e rotinas para melhor aproveitamento do sistema Interface de Divulgação de Alertas Públicos (IDAP), disponibilizado pela Secretaria Nacional de Proteção e Defesa Civil, conforme mencionado na introdução deste artigo; projetam-se três possibilidades legais para exame por parte do gestor público: a) abertura de procedimento licitatório para registro de preços de serviços de mensageria a fim de se obter um vencedor que poderá ser contratado por diferentes órgãos e entidades do ente público, a depender da sua necessidade futura; b) dispensa de licitação em razão do pequeno valor para contratação de prestadores especializados em serviços de mensageria, caso a pesquisa de preços indique valor estimado inferior a R$ 57.208,33, previsto no art. 75, II, da Lei Federal nº 14.133/21, atualizado pelo Decreto Federal nº 11.317/22; c) dispensa de licitação para contratação de serviços prestados por órgão ou entidade integrante da Administração Pública e que tenha sido criado para esse fim específico, com base no art. 75, IX, da Lei Federal nº 14.133/21.

Nas três hipóteses, ocorrerá compartilhamento de dados pessoais com terceiros, no mínimo, de números de celular, para envio das mensagens, e endereço residencial ou comercial, para filtragem dos potenciais destinatários dos avisos e alertas de risco. Por corolário, devem ser aplicadas as regras dos arts. 26 e 27 da LGPD, dispositivos que disciplinam o compartilhamento de dados no âmbito do Poder Público.

Ademais, devem ser observadas as conclusões do julgamento conjunto da Ação Direta de Inconstitucionalidade - ADI nº 6649 e da Arguição de Descumprimento de Preceito Fundamental - ADPF nº 695 pelo Supremo Tribunal Federal – STF, bem como as orientações do “Guia Orientativo Tratamento de Dados pelo Poder Público” da ANPD.

A partir dessas balizas legais, jurisprudenciais e regulatórias, cabe apresentar a seguinte sistematização dos requisitos para o compartilhamento de dados pessoais por parte de órgãos e entidades da Administração Pública: a) eleição de propósitos legítimos, específicos e explícitos para o tratamento de dados; b) compatibilidade do tratamento com as finalidades informadas; c) limitação do compartilhamento ao mínimo necessário para o atendimento da finalidade informada; d) formalização e registro das operações de tratamento; e) indicação objetiva e detalhada dos dados; f) enquadramento na base legal mais adequada; g) estabelecimento do período de duração do uso compartilhado dos dados, bem como definição acerca da possibilidade de conservação ou eliminação dos dados após o término do tratamento; h) atendimento ao princípio da transparência, com informações claras, atualizadas e facilmente acessíveis; i) previsão de medidas de segurança, técnicas e administrativas, que serão adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas.

Com efeito, independentemente da via eleita pelo gestor para operacionalização dos serviços de difusão de alertas, o cumprimento de tais requisitos deverá ser perfectibilizado tanto nas etapas preparatórias da contratação, após a identificação da base de dados que será utilizada e a limitação dos seus elementos integrantes que serão objeto de compartilhamento, quanto na detalhada formalização das finalidades específicas e das medidas de segurança, técnicas e administrativas que serão adotadas durante a execução contratual.

**III – OBSERVÂNCIA DOS PRINCÍPIOS DO ART. 6º DA LGPD**

Por derradeiro, cumpre destacar que as operações de tratamento de dados pessoais realizadas pelo Poder Público e por operadores por ele contratados deverão observar os princípios insculpidos no art. 6º da LGPD[[9]](#footnote-9). No que tange à principiologia de proteção de dados que deve nortear as operações de tratamento para fins de disparos de alertas de desastres por parte de órgãos de proteção e defesa civil, deve ser destacada a tríade finalidade, adequação e necessidade.

Por conseguinte, cumpre se proceder à identificação da base de dados que será utilizada e à limitação do compartilhamento aos dados pessoais imprescindíveis para a operacionalização dos disparos dos avisos e alertas de risco, a fim de que, durante a execução do vindouro contrato, não haja o tratamento excessivo ou desproporcional, desbordante da finalidade específica do projeto, qual seja, informar previamente a comunidade sobre as intempéries climáticas que a atingirão, salvando vidas e minorando danos.

De igual modo, recomenda-se que seja dada transparência aos cidadãos sobre o uso e o compartilhamento dos seus dados pessoais para fins de prevenção e defesa civil, inclusive sobre o disparo em massa dos citados avisos e alertas de risco, providência que poderá ser adotada por meio da inserção de informações claras, atualizadas e facilmente acessíveis, preferencialmente nos sítios eletrônicos dos órgãos de proteção e defesa civil, observando-se, assim, a exigência legal do art. 23, I, da LGPD.

Calha sugerir, ainda, que seja ofertada aos destinatários das mensagens uma opção de comunicação, preferencialmente pelo mesmo meio utilizado pelos órgãos de proteção e defesa civil (SMS, WhatsApp ou congêneres), apta a viabilizar a solicitação de correção ou atualização dos seus dados pessoais, face ao direito do titular de requisição da “correção de dados incompletos, inexatos ou desatualizados”, estampado no art. 18, III, da LGPD. Mais ainda, deve lhe ser facultada a opção de solicitar a exclusão do seu número de celular da listagem utilizada para o serviço público em comento (*opt-out*).

O mecanismo de *opt-out* encontra guarida no direito que o titular dos dados pessoais detém de se opor a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto na LGPD, consoante seu art. 18, § 2º. Segundo o Grupo de Trabalho do Artigo 29 (*Article 29 Working Party*), o *opt-out* configura não somente um direito do titular, mas também uma possível salvaguarda a ser aplicada por iniciativa do controlador[[10]](#footnote-10). Por corolário, constitui uma boa prática sua adoção pelo Poder Público mediante a oferta ao destinatário dos disparos da opção de solicitar a exclusão do seu contato do serviço de difusão dos alertas de desastres.

**IV – CONCLUSÕES PROPOSITIVAS**

Diante do exposto, alinham-se as seguintes conclusões propositivas:

a) O consentimento é uma das hipóteses de tratamento de dados pessoais (art. 7º, I ou art. 11, I), mas não constitui a única nem guarda qualquer relação de superioridade hierárquica perante as demais bases legais. O enquadramento do tratamento de dados pelo Poder Público na hipótese legal de consentimento, na maioria das vezes, sequer seria adequado, uma vez que a utilização compulsória de dados pessoais para o exercício de prerrogativas estatais típicas não poderia ficar condicionada à concordância do titular em manifestação livre, informada e inequívoca;

b) Os órgãos de proteção e defesa civil possuem competência, lastreada em leis e atos infralegais, para a implementação de políticas públicas relacionada à proteção da população vulnerável a iminentes desastres decorrentes de intempéries climáticas, inclusive mediante disparos de mensagens sobre avisos e alertas de risco, que envolverão, necessariamente, o tratamento de dados pessoais. Nesse campo, o Estado atuará na persecução do interesse público, afinal a finalidade pública consubstanciada na adoção de medidas preparatórias em áreas sob risco de catástrofes climáticas almeja, ao fim e ao cabo, salvar vidas e minorar danos nas comunidades atingidas. Preenchidos, pois, os requisitos para tratamento de dados pessoais do art. 23 combinado com o art. 7º, III, da LGPD (e, na hipótese de dados pessoais sensíveis, com o art. 11, II, “b”), inclusive sendo desnecessária, e até mesmo inadequada, a exigência de prévia solicitação específica ou consentimento do titular dos dados pessoais, o qual poderá ser destinatário dos avisos e alertas de risco dos órgãos de proteção e defesa civil, uma vez que o tratamento para execução de políticas públicas independe de prévio consentimento;

c) Para operacionalização do projeto de disparo de avisos e alertas de risco para residentes em áreas a serem atingidas por intempéries climáticas, os órgãos de proteção e defesa civil poderão ter a necessidade de contratação de terceiros especializados na prestação de serviços de mensageria. Independentemente da via eleita pelo gestor, o cumprimento dos requisitos legais para o compartilhamento de dados pessoais por parte de órgãos e entidades da Administração Pública deverá ser perfectibilizado tanto nas etapas preparatórias da contratação, após a identificação da base de dados que será utilizada e a limitação dos seus elementos integrantes que serão objeto de compartilhamento, quanto na detalhada formalização das finalidades específicas e das medidas de segurança, técnicas e administrativas que serão adotadas durante a execução contratual; e

d) As operações de tratamento de dados pessoais realizadas pelos órgãos de proteção e defesa civil e por operadores por ele contratados deverão observar os princípios insculpidos no art. 6º da LGPD, especialmente as recomendações para: identificação da base de dados que será utilizada; limitação do compartilhamento aos dados pessoais imprescindíveis para a operacionalização dos disparos dos avisos e alertas de risco; divulgação de informações claras, atualizadas e facilmente acessíveis sobre o uso e o compartilhamento de dados pessoais, preferencialmente nos sítios eletrônicos dos citados órgãos; e disponibilização ao titular de mecanismos aptos a viabilizar a correção de dados incompletos, inexatos ou desatualizados, bem como a exclusão do seu número de celular da listagem utilizada para o serviço público em comento (*opt-out*).

**REFERÊNCIAS BIBLIOGRÁFICAS**

ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC**. 2014.

BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BRASIL. Ministério da Integração e do Desenvolvimento Regional. **Brasil é o primeiro país do mundo a enviar alertas de desastres da Defesa Civil pelo WhatsApp**.

CAMPOS, Ricardo. **Metamorfoses do direito global**: sobre a interação entre Direito, tempo e tecnologia.São Paulo: Editora Contracorrente, 2022.

CORDEIRO, António Menezes. **Tratado de direito civil, I**: Introdução, fontes do direito, interpretação da lei, aplicação das leis no tempo, doutrina geral. Coimbra: Edições Almedina, 2017.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. p. 99-130.

FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. **Curso de proteção de dados pessoais**: fundamentos da LGPD. Rio de Janeiro: Forense, 2022.

GELLES, David. Climate Disasters Daily? Welcome to the ‘New Normal.’ **The New York Times**, Nova Iorque, 10 jul. 2023. Disponível em: https://www.nytimes.com/2023/07/10/climate/climate-change-extreme-weather.html. Acesso em: 19 de jul. de 2023.

MIRAGEM, Bruno. **Teoria Geral do Direito Civil**. Rio de Janeiro: Forense, 2021.

PEREIRA, Manuel das Neves. **Introdução ao direito e às obrigações**. Coimbra: Edições Almedina, S.A., 2019.

RIO GRANDE DO SUL. Governo do Estado. **Meteorologistas explicam recorrência de ciclones e previsões para o inverno e para a primavera no Estado**. 18 ago. 2023. Disponível em: https://estado.rs.gov.br/meteorologistas-explicam-recorrencia-de-ciclones-e-previsoes-para-o-inverno-e-para-a-primavera-no-estado. Acesso em: 19 de jul. de 2023.

RODOTÀ, Stefano. **A vida na sociedade da vigilância** – A privacidade hoje. Coordenação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SILVA, Jorge Cesa Ferreira da. **Antidiscriminação e contrato: a integração entre proteção e autonomia**. São Paulo: Thomson Reuters Brasil, 2020.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. 30 ed. São Paulo: Malheiros Editores, 2008.

SOMBRA, Thiago. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019.

TAVARES, José. **Os princípios fundamentais do direito civil**, vol. I, primeira parte: Teoria geral do Direito Civil. 2 ed. Coimbra: Coimbra Editora, Lim., 1929.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com**, Rio de Janeiro, ano 9, n. 1, 2020. Disponível em: http://civilistica.com/ tratamento-de-dados-pessoais-na-lgpd/. Acesso em: 8 jul. 2023.

VOIGT, Paul; BUSSCHE, Axel von dem. **The EU General Data Protection Regulation (GDPR)**. A practical guide. [s.l.]: Springer, 2017.

1. GELLES, David. Climate Disasters Daily? Welcome to the ‘New Normal.’ **The New York Times**, Nova Iorque, 10 jul. 2023. Disponível em: https://www.nytimes.com/2023/07/10/climate/climate-change-extreme-weather.html. Acesso em: 19 de jul. de 2023. [↑](#footnote-ref-1)
2. RIO GRANDE DO SUL. Governo do Estado. **Meteorologistas explicam recorrência de ciclones e previsões para o inverno e para a primavera no Estado**. 18 ago. 2023. Disponível em: https://estado.rs.gov.br/meteorologistas-explicam-recorrencia-de-ciclones-e-previsoes-para-o-inverno-e-para-a-primavera-no-estado. Acesso em: 19 de jul. de 2023. [↑](#footnote-ref-2)
3. BRASIL. Ministério da Integração e do Desenvolvimento Regional. Brasil é o primeiro país do mundo a enviar alertas de desastres da Defesa Civil pelo WhatsApp. [↑](#footnote-ref-3)
4. Segundo Ana Frazão: “seja em razão do amplo alcance da LGPD, seja em razão da sua preocupação com a tutela das situações existenciais dos titulares de dados, pode-se dizer que foi acolhida concepção convergente com a daqueles que, a exemplo de Rodotà, sustentam que a proteção de dados corresponde a verdadeiro direito fundamental autônomo, expressão da liberdade e da dignidade humana, que está intrinsecamente relacionada à impossibilidade de transformar os indivíduos em objeto de vigilância constante” (FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. p. 99-130, p. 103). [↑](#footnote-ref-4)
5. Sobre o consentimento voluntário e livre: “*In order to ensure its voluntariness, consent may not serve as legal basis for data processing where there is a clear imbalance between the data subject and the controller in a specific case. Imbalance is likely in a specific situation where the controller is a public authority. However, the legislator does not explicitly mention other cases of a clear imbalance. Thus, the notion will have to be specified in the future. The legislator deleted the reference to a clear imbalance in the context of an employment relationship as statutory example, which had been included in an earlier draft of the GDPR. Nevertheless, a clear imbalance might still be identified in this context. This will have to be identified on a case-by-case basis*” (VOIGT, Paul; BUSSCHE, Axel von dem. **The EU General Data Protection Regulation (GDPR)**. A practical guide. [s.l.]: Springer, 2017, p. 95). [↑](#footnote-ref-5)
6. Oportuno transcrever trecho do mencionado guia orientativo da ANPD: “Diante dessas características, em muitas ocasiões, o consentimento não será a base legal mais apropriada para o tratamento de dados pessoais pelo Poder Público, notadamente quando o tratamento for necessário para o cumprimento de obrigações e atribuições legais. Nesses casos, o órgão ou a entidade exerce prerrogativas estatais típicas, que se impõem sobre os titulares em uma relação de desbalanceamento de forças, na qual o cidadão não possui condições efetivas de se manifestar livremente sobre o uso de seus dados pessoais. Não obstante, **o consentimento poderá eventualmente ser admitido como base legal para o tratamento de dados pessoais pelo Poder Público. Para tanto, a utilização dos dados não deve ser compulsória e a atuação estatal não deve, em regra, basear-se no exercício de prerrogativas estatais típicas, que decorrem do cumprimento de obrigações e atribuições legais.**Assim, a utilização da base legal do consentimento no âmbito do tratamento de dados pessoais pelo Poder Público pressupõe assegurar ao titular a efetiva possibilidade de autorizar ou não o tratamento de seus dados, sem que de sua manifestação de vontade resultem restrições significativas à sua condição jurídica ou ao exercício de direitos fundamentais.” *(grifado)* [↑](#footnote-ref-6)
7. As bases legais do art. 7º, VII (para a proteção da vida ou da incolumidade física do titular ou de terceiro) e IX (quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais), em tese, poderiam ser utilizadas em alguns casos para disparos de alertas de desastres, no entanto não se apresentam como as mais adequadas por serem de emprego mais limitado e se submeterem a mais condicionantes legais do que o art. 7º, III, adrede citado. [↑](#footnote-ref-7)
8. Vale registrar a orientação da ANPD sobre o conteúdo da expressão “políticas públicas” no bojo da LGPD: “Nesse sentido, devem ser considerados, ao menos, dois aspectos. O primeiro é a existência de ato formal que institui a política pública, o que pode ocorrer mediante ato normativo (lei ou regulamento) ou por ajustes contratuais (contratos, convênios e instrumentos congêneres). Ressalte-se que o art. 11, I, b, da LGPD, não fez referência às políticas públicas instituídas em ajustes contratuais. Por isso, no caso de tratamento de dados sensíveis pelo Poder Público, a base legal é mais restrita, uma vez que limitada a políticas públicas previstas em ‘leis e regulamentos’. Quanto ao aspecto material, uma política pública envolve, em geral, a definição de um programa ou ação governamental específico, a ser executado por uma entidade ou por um órgão público. Nessa linha, Maria Paula Dallari Bucci destaca que, ‘como tipo ideal, a política pública deve visar a realização de objetivos definidos, expressando a seleção de prioridades, a reserva de meios necessários à sua consecução e o intervalo de tempo em que se espera o atingimento dos resultados’.” (grifado) [↑](#footnote-ref-8)
9. Considerando que o art. 6º irradia sua principiologia em toda a LGPD e que seu descumprimento tem o potencial de configurar graves violações ao direito fundamental à proteção de dados pessoais, considera-se oportuno transcrevê-lo: “Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. [↑](#footnote-ref-9)
10. ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC**. 2014, p. 45. [↑](#footnote-ref-10)