

Opinião: Comentários à Portaria nº 34 da Receita Federal

A secretaria da Receita Federal do Brasil (RFB) publicou no dia 18 de maio a Portaria nº 34, que dispõe sobre o compartilhamento de dados não protegidos por sigilo fiscal com órgãos e entidades da Administração Pública federal. Assim, por mera solicitação à Receita Federal, tais órgãos e entidades passam a poder obter dados (como nome, filiação, data de nascimento, sexo, endereço, ocupação, telefone e e-mail de contato, dados do cônjuge) de diversas bases da Receita, como Cadastro de Pessoas Físicas (CPF), Cadastro Nacional da Pessoa Jurídica (CNPJ), Cadastro de Imóveis Rurais (Cafir), cadastro do Simples Nacional, Declaração de Operações Imobiliárias (DOI) e Nota Fiscal Eletrônica



A iniciativa deu início a uma discussão sobre seu escopo e

gerou preocupações em relação à privacidade dos dados dos cidadãos brasileiros. Neste artigo, gostaríamos de situar a Portaria nº 34 da RFB em meio a uma série de iniciativas adotadas pelo governo federal à luz da legislação constitucional e infraconstitucional de privacidade e proteção de dados (incluindo a Lei Geral de Proteção de Dados Pessoais, Lei 13.709/2018), bem como à luz de recentes decisões do STF.

É primeiro necessário dizer que o compartilhamento de dados (incluindo os chamados dados pessoais) entre órgãos e entidades da Administração Pública não é, em si, um mal ou algo a ser combatido. Pelo contrário, o compartilhamento e uso do gigantesco volume de dados controlados por diversos órgãos da Administração Pública pode levar a uma gestão de políticas públicas mais inteligente e eficiente, pautada em dados e evidências. Nesse sentido, a Secretaria da Receita Federal informou que a portaria *"otimiza o fluxo de disponibilização de dados não protegidos por sigilo fiscal, tornando mais céleres as análises e decisões referentes às solicitações de disponibilização de dados das bases do CPF e do CNPJ"*.

No entanto, é ingênuo não reconhecer que o compartilhamento de dados também pode levar a um cerceamento de direitos fundamentais, incluindo os direitos a privacidade, intimidade, sigilo dos dados e proteção de dados pessoais. Desse modo, o amplo compartilhamento de dados teoricamente autorizado pela Portaria nº 34 — sem que o cidadão seja informado disso — deve ser visto com muito cuidado.

Apesar de a portaria falar que apenas dados não protegidos pelo manto do sigilo fiscal serão compartilhados, na prática algumas informações elencadas na portaria deveriam estar cobertas por tal proteção, como, por exemplo, informações detalhadas sobre parcelamentos, isto é, saldo devedor, quantidade de parcelas, valor consolidado da dívida em cobrança, global e por tributo, valor da dívida com exigibilidade suspensa por processo judicial.

Ademais, embora a portaria diga que será necessária uma solicitação formal à Receita com demonstração da necessidade do compartilhamento e das finalidades de uso dos dados solicitados, nos parece preocupante a quebra de sigilo e confidencialidade de tais informações, sobretudo sobre a segurança na uniformidade de tratamento de tais informações por todos os órgãos públicos.

Privacidade sob ataque

Esse cuidado é ainda maior quando se considera o contexto no qual se insere a Portaria nº 34. Ela tem como base o Decreto 10.046/2019, que dispõe sobre a governança no compartilhamento de dados no âmbito da Administração Pública federal e que criou o Cadastro Base do Cidadão (o chamado Cadastrão). Atualmente, tal decreto é questionado no Supremo Tribunal Federal em duas ações: a Ação de Descumprimento de Preceito Fundamental nº 695/DF, ajuizada pelo Partido Socialista Brasileiro (PSB) em junho de 2020, e a Ação Direta de Inconstitucionalidade nº 6.649/DF, ajuizada pelo Conselho Federal da Ordem dos Advogados do Brasil (OAB).

Em sua ação, o Conselho Federal da OAB argumenta que o Decreto nº 10.046/2019 ostenta inconstitucionalidades formais (no caso, a invasão de matérias de competência privativa de lei, em afronta ao artigo 84, incisos IV e VI, "a") e materiais, quais sejam, a violação dos direitos fundamentais à privacidade, à proteção de dados pessoais e à autodeterminação informativa. E arremata: *"O Decreto nº 10.046/2019 cria um poderoso instrumento estatal para elaboração de profilings, confecção de dossiês de espionagem contra opositores políticos e atividades de vigilância totalitária. Desta forma, 'coloca em risco a própria democracia liberal, no contexto da sociedade da informação, ao ignorar a divisão informacional de poderes, pavimentando, com isso, o caminho para a criação de um indomável Leviathan 4.0'"*, citando artigo publicado por Juliano Maranhão e Ricardo Campos.

STF reconheceu direito à proteção de dados pessoais

Em sua argumentação, a petição cita ainda recente decisão do Plenário do Supremo Tribunal Federal na Ação Direta de Inconstitucionalidade 6.387/DF — igualmente proposta pelo Conselho Federal da OAB — e nas ADIs 6.388/DF, 6.389/DF, 6.390/DF e 6.391/DF. A decisão já é considerada paradigma pelos especialistas porque consagrou o reconhecimento de um direito autônomo à proteção de dados pessoais.

Para contextualizar, o presidente da República havia publicado a Medida Provisória nº 954/2020, que determinava que as empresas de telecomunicação deveriam disponibilizar à Fundação Instituto Brasileiro de Geografia e Estatística (IBGE) a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas. Tais dados deveriam ser utilizados exclusivamente para a produção estatística oficial durante a pandemia do novo coronavírus. Na decisão da ADI nº 6.387/DF, o STF deferiu medida cautelar para suspender a eficácia da MP nº 954/2020 *"a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel"*.

Em seu voto, a ministra relatora Rosa Weber apontou que a Constituição Federal confere especial proteção à intimidade, à vida privada, à honra e à imagem das pessoas e prevê, no artigo 5º, XII, a inviolabilidade do sigilo dos dados. Além disso, o respeito à privacidade e à autodeterminação informativa foram positivados pela LGPD em uma disciplina específica da proteção de dados pessoais. Assim, tal uso e tratamento de dados pessoais requer, necessariamente, observar os limites delineados pela legislação nacional, bem como a necessidade, a adequação e a proporcionalidade da medida.

Não era o que acontecia, segue a ministra, com a MP 954 por: a) não oferecer condições para avaliação da sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades; e b) não apresentar mecanismo técnico ou administrativo apto a proteger os dados pessoais de acessos não autorizados, vazamentos acidentais ou utilização indevida. A ministra afirmou que *"exigir que normas que envolvam direitos fundamentais e da personalidade observem requisitos mínimos de adequação constitucional tampouco pode ser lido como embaraço à atividade estatal"* e alertou que situações de crise e de adoção de medidas excepcionais tendem a favorecer o enfraquecimento de direitos e a criação de narrativas que o justifiquem.

O ministro Luiz Fux, que acompanhou o voto da ministra relatora, arrematou: as leis que tratam da coleta e tratamento de dados devem atender a propósitos legítimos, específicos, explícitos e informados; limitar a coleta ao mínimo necessário para a realização das finalidades normativas; prever medidas técnicas e administrativas de segurança aptas a proteger os dados pessoais de acessos não autorizados e prevenir a ocorrência de danos, consoante os parâmetros desenhados no direito comparado e na Lei Geral de Proteção de Dados Pessoais (LGPD).

Desse modo, é forçoso reconhecer que malgrado eventuais pontos benéficos que sejam alegados pela Receita Federal, a Portaria nº 34 surge em meio a outras tentativas do governo federal que não são adequadas aos padrões exigidos de respeito a privacidade, intimidade e proteção a dados pessoais exigidos tanto pela legislação mais recente – como a própria LGPD — como pela própria Constituição Federal. Em artigo recente, a advogada e professora Ana Frazão destacou que o governo federal não só demonstra pouco entusiasmo pelo tema da proteção de dados pessoais (pelos sucessivos vazamentos de dados por órgãos públicos e a falta de transparência sobre o que é feito para remediá-los, os adiamentos da entrada em vigor da própria LGPD, a demora em criar a Autoridade Nacional de Proteção de Dados (ANPD) e o fato de a autoridade ter sido criada vinculada à presidência da República, e não mais como autarquia) como também adota iniciativas diametralmente opostas aos direitos dos titulares de dados.

E não é possível simplesmente afirmar que a LGPD não se aplica quando o tratamento dos dados ocorrer para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais, quando a própria LGPD prevê que o tratamento de dados pessoais para cumprimento a estas hipóteses será regido por legislação específica que *"deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular"* previstos na LGPD.

O valor do uso de dados pessoais para uma administração mais eficiente e baseada em fatos e evidências é claro. O que não é possível é que sob o argumento de buscar uma maior eficiência governamental seja criada uma estrutura de vigilância e amplo compartilhamento de dados pessoais e outras informações dos cidadãos de modo a ferir os direitos fundamentais à privacidade, à intimidade e à proteção de dados. Como escreveu a advogada, professora e atual diretora da ANPD Miriam Wimmer, *"ainda que se possa, em determinadas circunstâncias, admitir o compartilhamento de dados pessoais no âmbito do poder público com mudança das finalidades que justificaram sua coleta, não basta simplesmente conferir um verniz de legalidade para formalmente justificar tal uso secundário. É necessário, ao invés, o estabelecimento de salvaguardas materiais e procedimentais e a observância de todo o conjunto de direitos e princípios associados à proteção de dados pessoais, justificando-se, claramente, o interesse público específico a ser atingido, tendo em vista os parâmetros protetivos conferidos pelos princípios constitucionais que asseguram a liberdade individual, a privacidade e o livre desenvolvimento da personalidade"*.

Date Created

30/06/2021