2020 | MAIO

CARTA AO COMITÊ CENTRAL DE GOVERNANÇA DE DADOS

COMENTÁRIOS ÀS REGRAS DE COMPARTILHAMENTO DE DADOS DO CCGD

Ao Sr. Ciro Pitangueira de Avelino,
Presidente do Comitê Central de Governança de Dados (CCGD).

Em primeiro lugar, gostaríamos de agradecer a receptividade durante a conversa que tivemos na semana passada. O diálogo foi essencial para que pudéssemos compreender melhor a estratégia deste Comitê em relação à governança de dados dentro da Administração Pública Federal (APF). Esperamos que futuros contatos como esse aconteçam, de modo que possamos nos apoiar em criar um ambiente seguro para o exercício e a proteção da privacidade e dos dados pessoais dos cidadãos brasileiros.

Conforme nos foi cordialmente solicitado, encaminhamos, junto a esta carta, uma análise dos principais aspectos apresentados no **Guia de Boas Práticas para Implementação da Lei Geral de Proteção de Dados (LGPD) na Administração Pública Federal**.

Aproveitamos também para, no espaço desta carta, apresentar algumas considerações que tivemos a respeito das regras estipuladas para compartilhamento de dados no âmbito da administração pública federal, expostas no documento **Regras para Compartilhamento de Dados - CCGD**. A seguir, seguem alguns dos tópicos que consideramos mais relevantes a serem trabalhados para o que julgamos ser um aprimoramento dos trabalhos deste Comitê.

Análise do Documento *Regras para Compartilhamento de Dados*

Quando da publicação do Decreto n. 10.046/2019, que estabeleceu as regras para governança de dados pessoais na APF, conforme determinado pela LGPD, vários especialistas e organizações da sociedade civil se posicionaram contra as regras ali estabelecidas. As principais críticas feitas à época rondavam em torno de três principais tópicos:

1. A falta de compatibilidade entre os conceitos apresentados no decreto, como dados cadastrais, sigilosos, restritos e amplos, bem como de gestor

de dados, e conceitos da LGPD como dado pessoal, controlador e operador de dados.

2. À luz da norma, foi disseminada a interpretação de que o governo pretendia criar uma base única para armazenar todos os dados pessoais de cidadãos brasileiros. Isso poderia trazer consequências graves à proteção de dados no Brasil, considerando que uma base como essa poderia ser objeto de ataques massivos de *hackers* que pretendessem coletar todos os dados armazenados pelo governo federal.
3. A ausência de representantes da Sociedade Civil na composição do CCGD, ainda que apenas com poder de voz, ferindo a abordagem multissetorial estabelecida em outros modelos de Governança Digital, a exemplo do CGI.br e do processo de elaboração da LGPD.

A conversa que tivemos com este Comitê nos revelou que a real intenção do Decreto n. 10.046/2019 era a de aplicar a LGPD dentro do aparato estatal e compatibilizá-la com as regras atuais de compartilhamento de dados. Além disso, compreendemos, à luz do que nos foi exposto, que o Cadastro Base do Cidadão não se trata de uma base de dados única, mas sim de uma seleção das melhores bases de dados presentes na administração pública federal.

No entanto, as constantes dúvidas em relação ao real intuito do decreto e ao funcionamento do CCGD demonstram que algumas questões devem ser endereçadas com maior clareza à comunidade especializada, à sociedade civil e à população brasileira como um todo.

O primeiro ponto para que chamamos atenção é a **necessidade de se criar uma ponte mais concreta entre os conceitos presentes na LGPD e no Decreto 10.046** e no manual de Regras para Compartilhamento de Dados do CCGD, versão de 04/05/2020 (doravante chamado "Manual"), com especial ênfase em como cada categoria de compartilhamento de dados expressa no Manual se relaciona com o conceito de dados pessoais.

A esse respeito, aproveitamos para sugerir que este Comitê realize uma reunião de apresentação de seu trabalho com especialistas e integrantes da sociedade civil, em especial as entidades-membro da Coalizão Direitos na Rede. O diálogo

entre este órgão, cuja importância no cenário da governança da internet é central, e a maior entidade de direitos digitais brasileira, seria extremamente frutífero para uma melhor compreensão de seu trabalho e para que as dúvidas citadas acima sejam efetivamente endereçadas pelo Comitê.

O conceito de **dados cadastrais** merece destaque. Existe certa confusão no Brasil a respeito de como dados cadastrais se relacionam com a definição de dados pessoais, presente na LGPD. Um exemplo dessa falta de compreensão pode ser extraído de um trecho de carta assinada por ex-presidentes do IBGE a respeito da Medida Provisória n. 954, que determinava o compartilhamento dos dados de nome, telefone e endereço de todos os clientes de telefonia no Brasil ao IBGE para realização de "estatísticas oficiais". Este inclusive foi um dos argumentos de defesa apresentados pelo representante do IBGE no julgamento da Ação Direta de Inconstitucionalidade nº 6.387, que levou a MP para análise do Supremo Tribunal Federal (STF).

Em carta aberta, ex-presidentes do IBGE se manifestaram a respeito dos protestos feitos por especialistas de que a MP não estaria protegendo os dados de brasileiros. De acordo com os redatores da carta, a "preocupação não se justifica, porque os dados não incluem informações pessoais"[1]. A MP foi posteriormente suspensa pelo Plenário do STF, por não garantir o direito à proteção de dados da população brasileira.

No entanto, foi possível perceber que o conceito de dados pessoais não foi bem compreendido pelos citados ex-presidentes do IBGE, e é possível que a mesma dúvida ronde outras áreas da administração pública.

Por isso, achamos **necessário que o Manual especifique melhor de que forma o conceito de dados cadastrais se relaciona com o de dados pessoais.** Conforme se extrai da página 16 do Manual, dados cadastrais incluem "*nome, identificadores (CPF, NIS, título eleitoral, etc), data de nascimento, situação civil, endereço, contatos (telefone, e-mail, etc.), filiação, nome social*".

[1] Simon's Site. **Precisamos das estatísticas do IBGE para ajudar a vencer o COVID-19. 20 abr. 2020**. Disponível em http://www.schwartzman.org.br/sitesimon/?p=6488. Acesso em 23 abr. 2020.

É importante afirmar que tais dados são dados pessoais, e que recaem sobre eles as regras e princípios expressos na LGPD. Isso porque, conforme o art. 5º, I, da LGPD, dado pessoal é qualquer "informação relacionada a pessoa natural identificada ou identificável". O ideal é que este conceito seja descrito com detalhe no Manual de modo a evitar dúvidas, e trazemos a seguinte tabela como sugestão:

<table>
<tr><th colspan="3">Por que informações como CPF e endereço são dados pessoais?</th></tr>
<tr><td colspan="3">Conforme a LGPD, art. 5º, I, dado pessoal é a informação relacionada a pessoa natural identificada ou identificável. Este conceito é composto por quatro elementos:[2]</td></tr>
<tr><td rowspan="3">Elementos do dado pessoal</td><td>Informação</td><td>Pode ter natureza objetiva (ex. idade) ou subjetiva (ex. o devedor X é confiável).</td></tr>
<tr><td>Relacionada a</td><td>Um dado pode ser considerado relacionado a um indivíduo se ele diz respeito a um dos seguintes critérios:
(i) se relaciona a um conteúdo sobre o indivíduo;
(ii) tem a finalidade de avaliar um indivíduo ou seu comportamento; ou
(iii) tem um impacto sobre interesses ou direitos do indivíduo.</td></tr>
<tr><td>Pessoa Natural</td><td>Para ser pessoal, a informação deve estar relacionada a um indivíduo humano.</td></tr>
</table>

[2] Esses elementos são apresentados a partir do conceito legal da LGPD e as referências do Grupo de Trabalho do Artigo 29, Comitê Europeu que regulou matérias de proteção de dados. Para mais informações, checar: Article 29 Working Party, Opinion 4/2007 on the concept of personal data Brussels, 2007. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf. Acesso em: 23 abr. 2020.

	Identificada ou identificável	"Identificada" significa que a ligação ao indivíduo é feita de forma direta, como pelo tratamento de seu nome completo ou sua foto. Como "identificável", a ligação é indireta, e um processo de cruzamento de dados pode ser necessário para a identificação. Isto contudo não elimina a caracterização do dado como dado pessoal. É o caso de identificadores como o RG, CPF, o **endereço** e o **telefone** de uma pessoa natural.

Quando esses elementos da definição de dados pessoais são considerados, pode-se inclusive **questionar se o CNPJ não seria um dado pessoal.** Explicamos: ao se acessar a consulta do CNPJ no site da Receita Federal, a base retorna como um de seus resultados o email de um dos representantes comerciais, além do Quadro de Sócios e Administradores, todos estes pessoas naturais. Logo, o CNPJ é um dado relacionado a uma pessoa natural identificável, e portanto um dado pessoal. Este caso é ainda mais explícito no caso de Microempreendedores Individuais (MEI) que portam seu próprio nome no CNPJ.

Após uma análise da tabela de **subcategorias apresentadas nas páginas 15 a 17** do Manual, verificamos que todas elas **tratam ou têm o potencial de tratar dados pessoais**, inclusive categorias de dados sensíveis, conforme definição do art. 5º, II, da LGPD. Isso exige um maior nível de segurança e de proteção de dados e da privacidade aos seus titulares, o que deve incluir mais controles de acesso e o emprego de métodos de anonimização e pseudonimização mais avançados.

Um exemplo é a subcategoria A06 (p. 15), que se refere a dados de "beneficiários diretos de programa social do governo", o que inclui, no mínimo, seu "nome, CPF mascarado e valor do benefício". Não está claro quais os benefícios sociais aqui incluídos. Caso eles se refiram a benefícios por invalidez trabalhista ou por possuir alguma doença grave, por exemplo, os identificadores apresentados permitirão a

identificação do titular dos dados e o acesso a seus dados de saúde, que são sensíveis.

Caso seja esse o caso, os dados deverão possuir nível de proteção maior do que o garantido pela categoria *Ampla* do Manual, que "[d]ispensa autorização prévia pelo gestor de dados e será realizada pelos canais existentes para dados abertos e transparência ativa (art. 11)" (p. 6). Nesse sentido, é essencial a reconsideração dessa classificação para esse tipo de dado ou a melhor especificação da informação no Manual.

Outra importante informação que não pudemos localizar foi a **comparação entre os conceitos de "controlador" e "operador" de dados, da LGPD, e o de "gestor de dados" e "responsável", do Decreto 10.046.** Isso é essencial para que as partes envolvidas no tratamento de dados, sejam pessoas naturais ou jurídicas, de direito público ou privado, possam compreender quais papéis assumem e quais suas responsabilidade.

Seguindo adiante, notamos que **poucos princípios da LGPD foram devidamente explorados**. Identificamos apenas uma breve menção à transparência como um objetivo do programa de governo digital, mas sem que se trouxesse informações sobre como essa transparência seria garantida; e da segurança, razoavelmente explorada nas páginas 8 a 11. Contudo, princípios fundamentais para garantir o atendimento da LGPD como **finalidade**, **necessidade** e **adequação**, foram deixados de lado.

É importante ressaltar que o próprio Guia de Boas Práticas para Implementação na Administração Pública Federal da LGPD menciona que todos os princípios devem ser observados durante a verificação de conformidade (p. 26), sendo necessários para assegurar a privacidade desde a concepção (p. 46). Assim, é de **extrema importância que o texto do Manual esteja alinhado com o do Guia do governo federal**.

Indo mais além, nos preocupa a **aparente confusão trazida pela definição de dados restritos** apresentados na página 8 do Manual. Conforme o texto, esses dados

> *"podem ser acessados por todos os órgãos e entidades da Administração Pública Federal (APF), sem a necessidade de analisar pedidos e emitir permissões para cada caso. Não emitir permissão não deve ser confundido com não ter controle sobre acessos, como a rastreabilidade destes acessos"*.

Infelizmente, a explicação é uma contradição em si mesma. Conforme a RFC 4949 do Internet Engineering Task Force (IETF), organização internacional de engenheiros que cunhou o termo **controle de acesso,** e o define como a "*proteção dos recursos de um sistema contra acesso não autorizado*", ou ainda, "*um processo pelo qual o uso dos recursos do sistema é regulamentado de acordo com uma política de segurança e é permitido somente por entidades (usuários, programas, processos ou outros sistemas) de acordo com a essa política*."

O controle de acesso não pode se resumir a uma mera rastreabilidade. A **restrição dos dados deve estar atrelada a um controle de acesso,** que inclui um **mecanismo de autorização** para acesso aos dados. Nada impede, contudo, que esse mecanismo seja automatizado pelo uso de hashes criptográficos que autentiquem o acesso a dados quando a necessidade foi comprovada em momento prévio (por exemplo, ao se firmar um convênio entre o órgão requerente e o responsável pela base central).

Outro ponto essencial é **que o funcionamento do Cadastro Base do Cidadão seja descrito com mais detalhamento**. A informação de ele não se tratar de uma base central única de armazenamento de dados deve ser posta em destaque, complementada pelo fato de que é, na realidade, uma catalogação das melhores bases de dados da APF. Isso ajudará especialistas e representantes de organizações da sociedade civil a melhor compreenderem o conteúdo do Decreto n. 10.046.

Além disso, o Manual já poderia trazer informações técnicas e procedimentais relacionadas a **como o titular de dados poderá exercer os direitos previstos na LGPD**, como foco em seu art. 18. Destacam-se os direitos de acesso, retificação, eliminação, oposição, portabilidade, informação das entidades públicas e privadas

com as quais o controlador realizou uso compartilhado de dados, e o de revogação do consentimento.

O Manual também poderia descrever com mais clareza quais técnicas de **anonimização e pseudonimização** deverão ser empregadas de modo a garantir a proteção de dados de cidadãos. Vale ressaltar que a anonimização de dados nunca é perfeita, e que sempre é possível a re-identificação de seu titular. Seu objetivo é, na realidade, fazer com que essa re-identificação seja o mais onerosa e trabalhosa possível.[3]

A esse respeito, chamamos atenção ao trecho em que o Manual afirma que todas "as identificações de pessoas físicas na categoria Ampla serão com nome e CPF mascarado no formato ***.999.999-**" (p. 7). Levantamos a questão de se um processo de pseudonimização como o emprego de *hashes* criptográficos não seria mais efetivo para proteger o cidadão. Recomendamos que, independente da técnica utilizada, seja feita uma validação de que a identidade do indivíduo encontra-se devidamente protegida e não pode ser facilmente identificada pelo mero cruzamento de dados pessoais.

Outro ponto que chama muita atenção é fato de que, com exceção dos dados sigilosos, dados de categoria ampla e restrita poderão ser acessados livremente por outros órgãos, sendo que, no caso de dados restritos, bastará o cumprimento de um formulário descrevendo a razão do tratamento dos dados. Isso poderá representar uma abertura para possíveis violações em massa dos princípios da finalidade, necessidade e adequação. Afinal, **quem exercerá o controle de se os tratamentos de dados estão de fato cumprindo com esses princípios?**

Por isso, de modo a garantir seu cumprimento, é essencial que o Manual preveja que a possibilidade de acesso a determinado dado por outros órgãos seja sempre concedida mediante análise da solicitação, ou seja, o dado não deve ser compartilhado *by default*, sem que haja uma devida autorização.

---

[3] Sobre esse tema, vale a leitura de: FINCK, Michèle; PALLAS, Frank. **They who must not be identified—distinguishing personal from non-personal data under the GDPR**. International Data Privacy Law, Oxford, pp. 1-26, 10 mar. 2020. Disponível em: https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf. Acesso em: 9 abr. 2020.

Consideramos que as medidas apontadas nesta carta serão de grande valia para que a Administração Pública Federal se encaminhe para um grau de cumprimento adequado à LGPD e às boas práticas internacionais de privacidade e proteção de dados. O LAPIN coloca-se à disposição das autoridades brasileiras, em especial deste Comitê Central de Governança de Dados, para futuros diálogos a esse respeito. Por fim, ressaltamos também a conveniência de um encontro deste Comitê com especialistas e representantes da sociedade civil, que o LAPIN se disponibiliza a organizar uma vez dada a anuência do CCGD.

Atenciosamente,

LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET - LAPIN

Pontos de contato:
José Renato Laranjeira de Pereira
Diretor de Relações Públicas e Governamentais
joserenato@lapin.org.br

Thiago Guimarães Moraes
Conselheiro Presidente
thiago@lapin.org.br