A DESCARACTERIZAÇÃO DOS DADOS PESSOAIS EM DOCUMENTOS PÚBLICOS[1]

Rodrigo Pironti[2]

Recentemente, ao debater o tema da descaracterização de dados pessoais em documentos públicos, surgiu a necessidade de ir além dos argumentos já expostos em textos anteriores, principalmente em razão de direcionamentos trazidos no Guia de Transparência Ativa para órgãos e entidades do Poder Executivo Federal, da CGU, em pareceres da Advocacia Geral da União e da Procuradoria da Fazenda Nacional[3], dentre outras tantas orientações neste mesmo sentido em órgãos Estaduais e Municipais, em benefício de uma mais adequada interpretação dos dispositivos da Lei Geral de Proteção de Dados Pessoais, quando o assunto é a descaracterização de dados pessoais.

Antes de adentrar ao tema específico, importante recordar alguns conceitos relevantes da Lei Geral de Proteção de Dados Pessoais, já que uma inadequada interpretação poderia imputar inúmeras dificuldades, custos e incertezas às estruturas dos órgãos e entidades não apenas do Poder Executivo Federal, mas de todas as esferas e Poderes.

Nesse sentido, como já dissemos, vários são os mitos que se colocam decorrentes da falha interpretativa ou do desconhecimento do Regime Jurídico Administrativo. Um dos principais, continua a ser o da descaracterização de dados pessoais em documentos públicos, sejam eles atos, contratos, convênios, outras avenças, documentos públicos de interesse geral ou, ainda, decisões administrativas, arbitrais ou judiciais. Essa descaracterização, como veremos, para além de traduzir – na maioria das vezes – conduta não exigida pela Lei Geral de Proteção de Dados, amplia a ineficiência estatal e burocratiza ainda mais a atividade administrativa, sem garantir necessariamente a proteção devida aos dados pessoais tratados e, como consequência, ao seu titular.

Importante relembrar que estamos em tempos em que a eficiência estatal como princípio deve ser um vetor e a redução de práticas típicas do estamento burocrático[4] devem ser abandonadas em prol da realização do interesse público. É esse inclusive

1 Publicações anteriores em: Blog Zênite e Sollicita

2 Pós-Doutor em Direito Público – Complutense Madrid. Doutor e Mestre em Direito Econômico – PUCPR. Conselheiro do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade – CNPD. Sócio do escritório Pironti Advogados (www.pirontiadvogados.com)

3 Parecer n. 00004/2022/CNMLC/CGU/AGU e Parecer n. 00009/2022/DECOR/CGU/AGU.

4 FAORO, Raymundo. Os donos do poder: formação do patronato político brasileiro. 6a ed. Porto Alegre: Globo, vol. 1: 1984, vol. 2: 1985 [1a ed. 1958].

o contexto trazido no artigo 1º da Lei 13.726/18 (Lei da Desburocratização), quando informa como premissa a necessidade de se racionalizar "atos e procedimentos administrativos dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios mediante a supressão ou a simplificação de formalidades ou exigências desnecessárias ou superpostas, cujo custo econômico ou social, tanto para o erário como para o cidadão, seja superior ao eventual risco de fraude".

Surge, portanto, a necessidade de ampliar a discussão sobre a total desconexão da interpretação da descaracterização dos dados pessoais constantes nos atos e contratos administrativos, com determinação expressa ou fundamento da LGPD, por uma simples avaliação da finalidade dos tratamentos envolvidos e das bases legais que os autorizam.

É dizer, para já antecipar o mínimo, que a LGPD não é uma Lei que propõe sigilo dos dados pessoais ou que seu tratamento deve ser burocratizado em face de uma suposta proteção de tais dados, ao contrário, o que prevê de forma clara é que, os dados pessoais podem ser tratados desde que respeitem os princípios gerais e específicos nela estabelecidos, bem como, tenham uma base legal que autorizem seu tratamento; respeitadas essas balizas, em regra não haveria qualquer motivo para burocratizar a atividade administrativa e exigir-se, por exemplo, a descaracterização dos três primeiros ou últimos dígitos do CPF ou qualquer outro documento pessoal.

A interpretação de que, em razão da vigência da LGPD, deveriam ser descaracterizados os dados pessoais constantes em alguns documentos públicos representa uma excessiva burocratização, quando a própria Lei 13.709/18 já resolveu essas questões em seu texto, sem deixar nenhuma dúvida.

1. ANONIMIZAÇÃO E PSEUDO-ANONIMIZAÇÃO DE DADOS PESSOAIS?

Antes de adentrar na justificativa técnica do porque deve ser afastado o entendimento de descaracterização de dados pessoais em documentos públicos, quando não existe um fundamento específico à justificar o sigilo da informação ou a necessidade da segurança específica do dado pessoal a ser descaracterizado, importante entendermos os conceitos de anonimização e pseudoanonimização trazidos na LGPD.

A lei define em seu artigo 5º, inciso III, que considera-se dado anonimizado, aquele "relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;" e no inciso XI que o processo de anonimização é a "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;" ou seja, anonimizar um dado é, em síntese, retirar-lhe a própria condição de dado pessoal, impossibilitando sua associação direta ou indireta com o titular.

Já o artigo 13, parágrafo 4º, ao trazer o conceito de pseudoanonimização, o faz para circunscrever "o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.", ou seja, diferentemente da anonimização, o dado pseudoanonimizado não perde sua condição de dado pessoal pela impossibilidade de sua associação, mas apenas se lhe retira momentaneamente essa capacidade de identificação, que retorna imediatamente no momento em que este é associado novamente com a informação que lhe dá suporte e segurança.

Veja que a LGPD, quando dispõe sobre as hipóteses de anonimização ou pseudoanonimização, o faz de maneira expressa e sempre com um fundamento relevante vinculado à segurança do dado e aos aspectos justificadores de seu tratamento (finalidade, necessidade e adequação). É assim, por exemplo, nos seguintes artigos:

> "Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> IV - para a realização de estudos por órgão de pesquisa, **garantida, sempre que possível, a anonimização dos dados pessoais;**" (grifo nosso)
> "Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, **conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.**" (grifo nosso)
> "Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
> IV - uso exclusivo do controlador, vedado seu acesso por terceiro, **e desde que anonimizados os dados.**" (grifo nosso)

Ora, qual o motivo então para se descaracterizar o CPF, dado pessoal direto e não sensível, cujo tratamento na grande maioria das vezes é necessário a aspectos comezinhos de controle interno, controle externo e controle social (para dizer o mínimo)? A pergunta é, porquê? A resposta, como veremos, deve passar por alguns rápidos questionamentos trazidos pela própria LGPD, quais sejam: Existe uma base legal que autorize o tratamento do dado pessoal? Se existe tal base, o dado tratado atende à sua finalidade? Da mesma forma, o tratamento é adequado ao que se pretende? E em sendo adequado, é necessário o tratamento daquele dado, naquele contexto específico? Se as respostas para estas perguntas forem, "sim", o que fica é, então porque descaracterizar se é plenamente autorizado e legítimo seu tratamento? E o mais importante: se a resposta para qualquer das perguntas for "não", sequer seria caso de descaracterização do dado, ao contrário, se o dado não satisfaz base

legal ou os princípios básicos para seu tratamento, pela lógica da minimização do tratamento de dados, como vimos, é hipótese de um "não tratamento", mas nunca de descaracterização.

Obviamente que, se houver por legislações específicas a determinação de sigilo, segredo administrativo ou segredo de justiça, a possível descaracterização poderá ser implementada, mas não como fundamento na LGPD, e sim nas legislações processuais ou materiais que determinam tal sigilo, **em razão de uma motivação que, inclusive, pode ser objeto de controle e contraditório.**

2. O SIGILO DOS DADOS PESSOAIS E A INTERFACE ENTRE A LEI DE ACESSO A INFORMAÇÃO E A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Em recente texto escrito em co-autoria com a professora Luanna Ramos[5], alertamos para a igual importância e respeito aos direitos e garantias constitucionais e de que é crucial reconhecer que nenhum direito fundamental deve prevalecer sobre o outro. Portanto, não há nenhuma incompatibilidade entre as práticas de transparência e as normas de proteção de dados pessoais.

Além disso, a eventual confusão entre esses direitos fundamentais surge da falta de observância do fato de que dados pessoais não são necessariamente sigilosos. Pelo contrário, a própria Lei Geral de Proteção de Dados Pessoais reconhece a natureza pública de certos dados pessoais, especialmente os tratados pela Administração, conforme evidenciado nos trechos do artigo 7º, parágrafo 3º[6], e do artigo 26, parágrafo 1º, inciso III[7].

Some-se a isso, o fato de que a **LGPD não classifica qualquer categoria de dados pessoais como sigilosa ou proíbe sua divulgação**. Pelo contrário, o texto da Lei até respalda as operações de tratamento realizadas pela Administração, reforçando o princípio da legalidade ao reconhecer, em seu Capítulo IV, que toda iniciativa do Poder Público deriva exclusivamente da vontade popular expressa por meio de leis e regulamentos. Portanto, é legítimo o tratamento de dados pessoais que protejam os interesses coletivos.

Complementar a isso, a Lei de Acesso à Informação, ao tratar sobre informações pessoais, determina, no artigo 6º, inciso III[8], que o Poder Público observará a

5 FERREIRA. Luanna Ramos; PIRONTI. Rodrigo. A LGPD E A MITIGAÇÃO DE RISCOS ALÉM DO BINÁRIO SIGILO-TRANSPARÊNCIA. No prelo.

6 Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

7 Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.
§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:
III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.

8 Art. 6º Cabe aos órgãos e entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, assegurar a:
III - proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso.

disponibilidade, autenticidade, integridade e eventual restrição de acesso dos dados, tornando-se claro que, uma vez tendo a publicidade como regra na Administração Pública, o sigilo será admitido de forma excepcional e, por isso, será avaliado de forma restritiva ante o caso concreto.

Nesse sentido, versa o artigo 31[9] da Lei nº 12.527/2011 que somente serão admitidas as restrições de acesso às informações que se relacionem à vida privada, intimidade, honra e imagem das pessoas. Ou seja, excepcionados os dados que se insiram na descrição do artigo 31, nem todo dado pessoal deverá receber tratamento sigiloso, fator este que deve ser considerado em todas as situações de aparente conflito entre os interesses individuais e coletivos envolvidos.

Como se pode notar, apesar de alguns ruídos e mal-entendidos a respeito da relação entre LAI e LGPD, as leis funcionam a partir de uma lógica de convergência, já que ambas impulsionam a máxima transparência de informações públicas de interesse público, dentro do contexto e abrangência de cada, de forma a reduzir as assimetrias de informações existentes entre o Estado e seus cidadãos.[10]

Como se não bastasse, no âmbito regulamentar, a própria Controladoria-Geral da União tem se pronunciado através de enunciados[11] acerca da relação da proteção de dados pessoais com as práticas de transparência em diversos contextos e a vedação ao sigilo, vejamos:

> Enunciado CGU n. 5/2023 - Sigilo de licitações, contratos e gastos governamentais Informações sobre licitações, contratos e gastos governamentais, inclusive as que dizem respeito a processos conduzidos pelas Forças Armadas e pelos órgãos de polícia e de inteligência, **são em regra públicas e eventual restrição de acesso somente pode ser imposta quando o objeto a que se referem estritamente se enquadrar em uma das hipóteses legais de sigilo. (grifo nosso)**
> Enunciado CGU n. 7/2023 - Títulos acadêmicos e currículos de agentes públicos. Informações sobre currículos de agentes públicos, como títulos, experiência acadêmica e experiência profissional, **são passíveis de acesso público, uma vez que são utilizadas para a avaliação da capacidade, aptidão e conhecimento técnico para o exercício de cargos e funções públicas. (grifo nosso)**
> Enunciado CGU n. 8/2023 - Provas e concursos públicos. A divulgação de documentos e informações relacionados a candidatos aprovados em seleções para o provimento de cargos públicos, inclusive provas orais, **são passíveis de acesso público, visto que a transparência dos processos seletivos está diretamente relacionada à promoção dos controles administrativo e social da Administração Pública, ressalvadas as informações pessoais sensíveis. (grifo nosso)**
> Enunciado CGU n. 10/2023 – Informações financeiras a respeito de programas e benefícios sociais Informações referentes a valores de

9 Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.

10 BIONI, Bruno Ricardo; SILVA, Paula Guedes F. da; MARTINS, Pedro Bastos L. Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso. Cadernos Técnicos da CGU/ Controladoria-Geral da União. Disponível em: <https://revista.cgu.gov.br/Cadernos_CGU/issue/view/39/46>.

11 Disponível em: https://www.gov.br/acessoainformacao/pt-br/lai-para-sic/transparencia-passiva/guias-e-orientacoes/enunciados-da-lai/@@download/file/NOVOS%20ENUNCIADOS%20LAI%20CGU%203-fev-2023.pdf. Acesso em: 14 jul. 2024.

> benefícios pagos e identificação de beneficiários de programas sociais, ainda quando esses são operados por instituições financeiras, **são de acesso público, não incidindo sobre elas sigilo bancário, tampouco argumentos referentes à proteção de dados pessoais ou à preservação da competitividade de empresas estatais, ressalvados os casos em que a identificação dos beneficiários puder expor informação pessoal sensível. (grifo nosso)**

Da mesma forma, o Tribunal de Contas da União vem adotando entendimentos no sentido de confirmar a prevalência do interesse público na utilização de dados pessoais em sua atividade julgadora, consolidando a convivência do direito à proteção de dados pessoais com os princípios da publicidade e transparência.

Por meio da Resolução nº 354/2023[12], por exemplo, o TCU estabeleceu a obrigatoriedade da identificação dos responsáveis sujeitos à sua jurisdição por meio do CPF, **assim como a vedação aos pedidos de eliminação ou pseudonimização de tais dados, com respaldo no princípio da finalidade, estabelecido no artigo 6º da LGPD, uma vez que o CPF se presta a garantir a identificação inequívoca do titular, evitando inconsistências em razão da homonímia**.

Portanto, a Administração Pública, ao exercer a atividade de tratamento de dados pessoais, deve seguir de forma indistinta os princípios e regras de publicidade das informações e de proteção dos dados pessoais, não podendo utilizar estes para se eximir de cumprir com aqueles, e reciprocamente.

Inexiste, portanto, superioridade entre a Lei Geral de Proteção de Dados Pessoais e a Lei de Acesso a Informação, não servindo a LGPD como justificativa para restringir o acesso aos dados de interesse público, promovendo opacidade e impedindo o exercício do controle.

3. A DESCARACTERIZAÇÃO DOS DADOS PESSOAIS EM DOCUMENTOS PÚBLICOS

O enunciado CGU 12/23, ao tratar sobre informação pessoal alerta que o termo "informações pessoais não pode ser utilizado de forma geral e abstrata para se negar pedidos de acesso a documentos ou processos que contenham dados pessoais, **uma vez que esses podem ser tratados (tarjados, excluídos, omitidos, descaracterizados, etc) para que, devidamente protegidos**, o restante dos documentos ou processos solicitados sejam fornecidos."[13]

A pergunta que fica deste enunciado é: tarjados, excluídos, omitidos,

12 Disponível em: https://pesquisa.apps.tcu.gov.br/documento/norma/*/COPIATIPONORMA:%28Resolu%C3%A7%C3%A3o%29%20COPIAORIGEM:%28TCU%29%20NUMNORMA:354%20ANONORMA:2023/DATANORMAORDENACAO%20desc/0. Acesso em: 14 jul. 2024.

13 Enunciado CGU n. 12/2023 - Informação pessoal. O fundamento "informações pessoais" não pode ser utilizado de forma geral e abstrata para se negar pedidos de acesso a documentos ou processos que contenham dados pessoais, uma vez que esses podem ser tratados (tarjados, excluídos, omitidos, descaracterizados, etc) para que, devidamente protegidos, o restante dos documentos ou processos solicitados sejam fornecidos. Além disso, a proteção de dados pessoais deve ser compatibilizada com a garantia do direito de acesso à informação, podendo aquela ser flexibilizada quando, no caso concreto, a proteção do interesse público geral e preponderante se impuser, nos termos do art. 31, § 3º, inciso V da Lei nº 12.527/2011.

descaracterizados quando? Qual o fundamento para que sejam protegidos? Como veremos, se tais fundamentos de interesse público – que justificam o sigilo em nome da segurança do titular de dados – não estiverem presentes, ou violem princípios comezinhos da Administração Pública, como legalidade, eficiência, controle, dentre outros, não haverá qualquer motivo para que os dados sejam tarjados, excluídos, omitidos ou descaracterizados.

Dito isto, cabe analisarmos então o que traz o Guia de Transparência Ativa para órgãos e entidades do Poder Executivo Federal, que tem por objetivo "auxiliar no correto cumprimento das obrigações de transparência ativa previstas na Lei nº 12.527, de 18 de novembro de 2011 – Lei de Acesso à Informação (LAI), no Decreto nº 7.724, de 16 de maio de 2012, e em demais normas que regem o assunto. A LAI estabelece que as informações de interesse coletivo ou geral devem ser divulgadas, de ofício, pelos órgãos e entidades públicas, espontânea e proativamente, independentemente de solicitações. Além disso, no art. 8º prevê um rol mínimo de informações que devem, obrigatoriamente, ser divulgadas nas páginas oficiais na internet, de órgãos e entidades, no menu principal "Acesso à Informação"."[14]

Ao tratar dos "requisitos para a transparência ativa" o referido guia orienta que:

> A Lei nº 14.129, de 29 de março de 2021, que estabeleceu princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública também elencou os seguintes requisitos que o poder público deverá observar na promoção da transparência ativa de dados:
> VII. Respeito à privacidade dos dados pessoais e dos dados sensíveis, sem prejuízo dos demais requisitos elencados, conforme a Lei Geral de Proteção de Dados Pessoais.

Veja que o próprio Guia reconhece que a divulgação dos dados pessoais é requisito para transparência ativa, desde que esta divulgação respeite os limites trazidos pela LGPD, quais sejam: **o respeito aos seus princípios e autorização por base legal correspondente**. É dizer, cumpre com a transparência ativa a divulgação de dados pessoais, desde que não em prejuízo a LGPD.

Então, reforçamos o questionamento: qual seria o motivo para descaracterização dos dados pessoais de documentos públicos em face da vigência da LGPD? Pela própria fundamentação do Guia, o motivo possível para esta ocultação, seria o desrespeito a LGPD, ou seja e como vimos, o tratamento violar alguns de seus princípios ou não possuir base legal correspondente.

A título de exemplo, vejamos o disposto no item 7.2., do Guia de Transparência Ativa da CGU, que faz referencia aos Contratos:

> "Caso o órgão ou a entidade não utilize o Sistema Integrado de Administração de Serviços Gerais (SIASG), deve disponibilizar a listagem dos contratos realizados no órgão ou na entidade, de maneira estruturada, contendo minimamente as informações abaixo, com link

14 GUIA DE TRANSPARÊNCIA ATIVA PARA ÓRGÃOS E ENTIDADES DO PODER EXECUTIVO FEDERAL • 7ª VERSÃO, SECRETARIA DE TRANSPARÊNCIA E PREVENÇÃO DA CORRUPÇÃO, p. 8.

> para o inteiro teor dos documentos.
> [...] i) CNPJ ou CPF;"

E em nota de rodapé, o próprio Guia enuncia:

> "O CPF deve ser descaracterizado, mediante ocultação dos três primeiros dígitos e dos dois dígitos verificadores. Exceto quando se tratar de Microempreendedor individual (MEI) ou Empresário Individual (EI) que eventualmente utilize seu CPF como dado cadastral em contratos com a Administração Pública, caso em que o CPF poderá ser divulgado sem necessidade de descaracterização."

A pergunta que se coloca é: a divulgação do CPF (dado pessoal direto e não sensível) nos contratos administrativos estaria violando alguns dos princípios do artigo 6º da LGPD ou faltaria base legal para o seu tratamento como dado pessoal? Da leitura atenta da Lei, me parece que a divulgação não viola nenhum dos princípios ali elencados, vejamos aqueles fundamentais a compreensão deste artigo:

> Art. 6. 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;

Da mesma forma, no caso específico dos contratos administrativos, por exemplo, haveria ao menos três bases legais autorizatórias (e veja-se que bastaria uma para o atendimento da LGPD), quais sejam, aquelas estampadas no art. 7, inciso II (Lei 14.133/21, Lei 13.303/16 e o próprio art. 37 da CF); no art. 7, inciso III (interesse público na consecução de uma política ou serviço publico atendido pelo contrato) e uma base legal específica que é a do art. 7, inciso V, (tratamento autorizado em razão dos contratos administrativos ou diligências pré-contratuais. Nestes casos, extensiva a qualquer ajuste ou avença administrativa).O mesmo entendimento se aplicaria aos demais casos em que o Guia sugere a descaracterização de dados pessoais em outros documentos públicos.

É que o controle não poderia, ou ao menos não deveria, traduzir-se em excesso de controle em privilégio a burocratização e em desfavor de uma administração viável, econômica e eficaz. O motivo desta afirmação possui duas vertentes bastante evidentes:

> a. a primeira delas é de ordem normativa. Ora, a vigência da LGPD nunca teve a pretensão de impedir o tratamento de dados ou torná-los técnica ou pragmaticamente inviável, bem como, em se tratando do Setor Público, a proteção de dados pessoais, ainda que um Direito Fundamental, nunca teria o condão de violar o interesse público,

> justamente por isso, foram elencadas as bases legais que autorizam o tratamento em prol do interesse coletivo. Imputar interpretação restritiva a essas bases legais de forma contrária e extensiva a LGPD, sem que a própria LGPD ou qualquer outra legislação determine seu sigilo, é permitir uma negativa do interesse público pretendido pelas demais normas (leis e regulamentos) para burocratizar e muitas vezes limitar o próprio controle, pois como vimos, um dos motivos da não descaracterização dos dados de CPF em contratos administrativos, por exemplo, é o Controle Social, que impõe a bem do interesse público que se conheça quem possui relação com o Poder Público para fins de verificação de conflitos de interesse, práticas nepóticas e a própria legalidade de contratações ou ajustes em face de possíveis limitações legais da pessoa que se relaciona com o órgão público.
>
> b. A segunda é de ordem pragmática: estamos no Brasil, um país de dimensões continentais e com grandes desafios a serem ultrapassados pelo Setor Público na promoção do interesse público. Esses desafios, vinculados ainda a grande escassez de recursos humanos e financeiros na maiorias dos órgãos e entidades da Administração Pública, e somada a uma estrutura administrativa ainda incipiente em tecnologia e inovação (o que prejudica a eficiência do serviço), torna a exigência de descaracterização dos dados pessoais ainda mais questionável, uma vez que imputa ao gestor público uma série de problemas práticos, principalmente em se tratando de órgãos públicos com estruturas administrativas em sua grande maioria mais enxutas e com baixa disponibilidade orçamentária. Veja que se pensarmos em grandes estruturadas da Administração Pública Federal, talvez exista estrutura ou condições técnicas de fazê-lo, mas essa é a exceção em nosso país e, com isso, o ônus a todos os demais – por uma interpretação desconectada das exigências da LGPD – seria por demais oneroso. Os recursos, humanos e financeiros, destinados à essa descaracterização de dados pessoais nos inúmeros municípios brasileiros, poderia ser utilizado, por exemplo, para suas finalidades precípuas, como investimentos em saúde, educação e infraestrutura.

O efeito cascata desse desvio de interpretação já começa a surtir efeitos negativos, em razão da descaracterização dos dados pessoais. Em artigo recente, intitulado "Mau uso da LGPD cria apagão de prestação de contas de convênios"[15], a jornalista Marina Atoji alertou sobre a retirada do ar, pelo Governo Federal, de documentos sobre repasses de recursos via convênios com base na LGPD e que isso já estaria a afetar também os relatórios de gestão fornecidos por Estados e Municípios beneficiados por "emendas PIX":

> "Pois bem. Diante desse parecer, o Ministério da Gestão e Inovação decidiu retirar do ar praticamente todos os documentos relacionados a convênios que estavam disponíveis na plataforma Transferegov.br. Prestações de contas e comprovantes sobre a aplicação dos recursos recebidos, por exemplo, não podem mais ser baixados. A decisão afeta também o acesso a relatórios de gestão fornecidos por Estados e municípios beneficiados por

15 ATOJI, Marina. "Mau uso da LGPD cria apagão de prestação de contas de convênios". https://www.poder360.com.br/opiniao/mau-uso-da-lgpd-cria-apagao-de-prestacoes-de-contas-de-convenios/

> emendas Pix, que não dependem de convênios para serem pagas. Ou seja, reduz drasticamente o impacto de quaisquer medidas implementadas para dar mais transparência a esse tipo de repasse"

Veja-se, ainda a título de argumento, que mesmo que essa exigência não fosse onerosa a maioria dos órgãos em nosso país, a manutenção dessa interpretação violaria o princípio da eficiência e da racionalização de recursos públicos, o que, por si só, impediria essa leitura. Tal interpretação traz excesso de trabalho, aumento de custo e uma reação em cadeia que afeta não apenas os destinatários do Guia de Transparência Ativa para órgãos e entidades do Poder Executivo Federal e de outros pareceres e documentos produzidos com a mesma interpretação em outros órgãos, mas também inúmeras outras estruturas que, ao não possuírem corpo técnico especializado, tem nesses importantes órgãos, como a CGU, um referencial relevante de boas práticas[16].

Também sob o prisma pragmático e, neste caso, apenas em acréscimo ao argumento da ausência de critério jurídico que possa sustentar a exigência, veja-se que o referido Guia, por exemplo, esta a exigir a descaracterização apenas do CPF, contudo, outros dados pessoais diretos tão relevantes quanto o CPF, não são objeto de preocupação em relação a descaracterização, como por exemplo, nome completo e número de identificação funcional, ou seja, o Guia estabelece uma espécie de ranking aos dados pessoais, quando, como dissemos, sequer a LGPD o fez. Como se o CPF fosse um dado pessoal distinto dos demais dados diretos, é dizer, divulgar o CPF não pode, mas identificar de outra forma e por meio de outros dados diretos o titular, é admissível.

No fundo, o que se está a refletir é: o que se está a proteger? O dado pessoal ou o titular do dado? Em linhas gerais, existiria fundamento (motivação congruente) para a determinação de pseudoanonimização apenas do CPF e que essa prática garantiria a não exposição do titular em razão do motivo apontado (muito embora outros dados pessoais diretos expostos)? Se a respota for sim, não haveria problema na pseudoanonimização. Agora, o que não se pode admitir é a determinação de descaracterização sem que haja essa reflexão em relação aos motivos que determinam a descaracterização de alguns dados e não de outros, quando sequer a LGPD os caracterizou de maneira distinta.

É que no âmbito do Regime Jurídico Administrativo, o tratamento de dados pessoais pelas pessoas jurídicas de direito público segue regra adicional à observância de tais princípios, qual seja, aquela elencada em seu artigo 23, que prescreve que, deverá ser observada a *"finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público"*.

16 Frise-se que, em meu entendimento a CGU é um grande referencial de boas práticas e auxilia o pleno desenvolvimento do Controle Interno e todas as suas macrofunções em nosso país, colaborando diretamente para o avanço e, justamente em razão disso, a leitura da descaracterização dos dados pessoais deveria ser repensada no referido Guia.

Diante disso, em se tratando de atos ou contratos administrativos é necessário se avaliar, quando da coleta de dados pessoais, **a pertinência destes dados com as respectivas exigências legais trazidas pelas legislações de regência.** Aí nasce a possível dúvida ou falha interpretativa, pois se é certo que para se relacionar com o Poder Público ou para contratar com a administração, as pessoas e empresas deverão fornecer alguns dados pessoais, também é certo, que os dados pessoais coletados em razão dessa relação, deverão obedecer aos ditames da Lei Geral de Proteção de Dados. Nada mais lógico! **Ora, de onde então deriva essa equivocada interpretação?**

Já dissemos que a Lei Geral de Proteção de Dados, ao estabelecer em seu artigo 7 e incisos, as diversas bases legais autorizatórias do tratamento de dados pessoais, trouxe, dentre outras, a base legal do consentimento, que orienta que o tratamento de dados pessoais, quando fundamentado naquela base, só pode ser realizado com a aquiescência livre, inequívoca e informada do titular dos dados.

> Art. 7. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> Art. 5. Para os fins desta Lei, considera-se:
> XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

Isso induz a uma conclusão lógica: quando a base legal autorizatória do tratamento dos dados for o consentimento eu só poderei fazê-lo com a concordância expressa do particular[17]. E é possível o consentimento no tratamento de dados pela Administração Pública, a própria ANPD deixou evidente[18]:

> Estudante realiza inscrição para participar de um evento organizado por uma universidade pública. O procedimento é realizado online, ocasião em que são solicitadas informações básicas de cadastro, como nome e número de matrícula, este para o fim específico de concessão da gratuidade da inscrição, benefício exclusivo para estudantes. Adicionalmente, o estudante tem a opção de fornecer e-mail, caso queira "receber informações de outros eventos organizados pela universidade". Uma mensagem esclarece que o fornecimento do e-mail é facultativo e a recusa não impede a participação no evento. Ademais, as informações sobre os outros eventos são rotineiramente divulgadas na página da universidade na Internet. Na hipótese, o consentimento é a base legal apropriada para a coleta do e-mail do estudante, podendo ser considerado válido, haja vista a finalidade específica informada ao titular, bem como a existência de condições efetivas para a livre, informada e inequívoca manifestação de vontade.

Ocorre que o consentimento é apenas uma, dentre tantas outras bases legais

17 Isso porque, da leitura do dispositivo legal, que conceitua consentimento como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada", é possível concluir que não existe pela Lei Geral de Proteção de Dados a hipótese de consentimento tácito, já que ao controlador não seria possível comprovar diante do caso concreto, a inequivocidade do consentimento, quando por hipótese, dado de forma tácita.

18 TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO. ANPD. Versão 1.0, ajn. 2022. p 07.

autorizatórias do tratamento de dados pessoais na LGPD e, seguramente, não é a base legal que autoriza o tratamento dos dados pessoais nos atos e contratos administrativos. Para estes, dentre as demais bases legais, há ao menos duas que fundamentam diretamente o tratamento dos dados relativos aos atos e contratos administrativos, quais sejam, as bases legais da obrigação legal e das diligências pré-contratuais ou execução dos contratos[19]. Isto porque, em se tratando de contratos – por exemplo – tanto a Lei 14.133/21, quanto a Lei 13.303/16, ao disporem sobre as formas de contratação na Administração Direta e Indireta tornam evidente o caráter público do procedimento, tanto em sua fase interna, quanto em sua fase externa, dentre outros em privilégio ao controle da atividade administrativa, intrínseco ao Estado Democrático de Direito.

É exatamente esse o entendimento 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**.[20]

Nota-se, que a própria Autoridade Nacional de Proteção de Dados, em seu Guia Orientativo sobre o Tratamento de Dados Pessoais pelo Poder Público[21] destaca a relevância de se perquirir a base legal adequada a cada tipo de tratamento de dados realizado, deixando expresso o entendimento de que "uma das principais providências a serem tomadas antes de realizar o tratamento de dados pessoais é a de identificar a base legal aplicável. O tratamento de dados pessoais pelo Poder Público deve se amparar em uma das hipóteses previstas no art. 7 ou, no caso de dados sensíveis, no art. 11 da LGPD. [...] Esses dispositivos devem ser interpretados em conjunto e de forma sistemática com os critérios adicionais previstos no art. 23, que complementam e auxiliam a interpretação e a aplicação prática das bases legais no âmbito do Poder Público".

Resta claro, da manifestação da ANPD, que a conformidade da adequação com a LGPD deve guardar uma análise sistêmica entre a base legal autorizatória dos dados objeto de tratamento e as legislações incidentes nesta relação. Com isso, no âmbito dos atos administrativos e contratos administrativos, não resta dúvida de que a interpretação sistemática e teleológica da LGPD (e suas bases legais) e das Leis que orientam os processos de contratação pública (com seus princípios e regras), traz

19 Art. 7. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

20 TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO. ANPD. Versão 1.0, jan. 2022. p 06.

21 TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO. ANPD. Versão 1.0, jan. 2022. p 06.

como pressuposto a noção de publicidade e não de sigilo. O sigilo é exceção nestes procedimentos e possui hipóteses bastante específicas para seu reconhecimento.

Esse é o entendimento da própria Lei 14.133/21, quando expressamente manifesta em seu artigo 13, que "os atos praticados no processo licitatório são públicos, ressalvadas as hipóteses de informações cujo sigilo seja imprescindível à segurança da sociedade e do Estado, na forma da lei." A publicidade é, inclusive um dos princípios vetores da Nova Lei de Licitações e Contratos, como também o é, para toda a Administração Pública.

Em se tratando de contratos administrativos a incidência da LGPD é lógica: se os dados coletados em contrato atendem a finalidade e adequação do tratamento estabelecido pela relação contratual e se ajustam aos princípios e regras estabelecidos nas legislações específicas (14133/2021 e 13.303/2016), a base legal será aquela estabelecida no artigo 7, inciso V da LGPD, com incidência do inciso II do mesmo artigo e das regras estabelecidas no artigo 23.

E que não se diga, por exemplo, que dados pessoais constantes dos registros contratuais da pessoa jurídica poderiam afetar os direitos dos titulares de dados, pois inclusive estes dados são públicos e respeitam a uma base legal específica que justifica seu tratamento. É exatamente isso que esclarece a Lei 8.934/94 (Lei de Registro Público de Empresas Mercantis), quando assevera em seu artigo 1, inciso I, que a finalidade da Lei é "dar garantia, publicidade, autenticidade, segurança e eficácia aos atos jurídicos das empresas mercantis"[22] e, quando em seu artigo 29 manifesta que "qualquer pessoa, sem necessidade de provar interesse, **poderá consultar os assentamentos existentes nas juntas comerciais e obter certidões**, mediante pagamento do preço devido".

Não há, portanto, nenhuma justificativa na LGPD para a descaracterização dos dados pessoais constantes de documentos públicos e com previsão expressa em suas legislações de regência. **Entender de forma diversa seria imputar sigilo a dados constantes em documentos públicos quando, sequer sua legislação de regência o fez.**

Exemplificando: a existência de dados pessoais do sócio, em um documento constitutivo da empresa (contrato social), juntado na fase habilitatória do procedimento competitivo (ou ainda que na fase interna), por exemplo, não induz a noção de que os dados pessoais ali constantes devam ser descaracterizados. Se assim o fosse, estaríamos diante de um excesso de formalidade ou exigências

22 Aqueles que exercem profissionalmente atividade econômica organizada para produção ou circulação de bens ou prestação de serviços é considerado empresário nos termos do artigo 966 da Lei 10.406/2002 ("**Código Civil**"). Sobre o empresário, recai a obrigação de registrar os atos societários de sua sociedade na Junta Comercial da unidade da Federação na qual está localizada sua sede, sendo a Junta Comercial, portanto, o órgão responsável pela execução do registro público mercantil, conforme disposto no artigo 967 do Código Civil.
As Juntas Comerciais são responsáveis pela inscrição das sociedades, bem como pelo registro e arquivamento do contrato social e de suas alterações posteriores. O propósito de tais registros é garantir a publicidade, autenticidade e segurança dos atos jurídicos, bem como a atualização cadastral da sociedade e a proteção de seu nome empresarial.
A Lei 8.934/1994, que dispõe sobre o registro público de empresas mercantis, estabelece em seu artigo 36 que os documentos com registro obrigatório na Junta Comercial deverão ser apresentados para arquivamento dentro do prazo de 30 (trinta) dias contados de sua assinatura, cuja data retroagirão os efeitos do arquivamento.

desnecessárias, da violação do caráter público do documento e das informações ali constantes, bem como, da criação de hipóteses de sigilo e de mecanismos direcionados à ineficiência estatal quando sequer existe determinação legal neste sentido.

Em síntese, a interpretação de que as regras da LGPD estariam a determinar a descaracterização de atos ou contratos administrativos ou outros documentos públicos, para além de não encontrar suporte jurídico na legislação vigente, viola princípios constitucionalmente reconhecidos, como o postulado do controle (social, interno e externo) e o princípio da eficiência, cuja consequência se traduz, dentre outros, em uma necessidade de desburocratização do Estado[23].

Qual o motivo para se descaracterizar o CPF ou qualquer outro dado pessoal direto, cujo tratamento na grande maioria das vezes é necessário a aspectos comezinhos de controle interno, controle externo e controle social? Porque descaracterizar?

Se não houver resposta à essa pergunta, a descaracterização é imotivada e, portanto, ilegal. É impossível a descaracterização dos dados sem uma justificativa de fato e de direito que autorizem essa decisão do controlador.

Então alguns questionamentos são necessários:

1. Existe uma base legal que autorize o tratamento do dado pessoal?
2. Se existe tal base, o dado tratado atende à sua finalidade?
3. O tratamento é adequado ao que se pretende?
4. E em sendo adequado, é necessário o tratamento daquele dado, naquele contexto específico?

Se as respostas para estas perguntas forem, "sim", o que fica é, então porque descaracterizar o dado se é plenamente autorizado e legítimo seu tratamento e se não há fundamento que justifique sua anonimização ou pseudoanonimização?

E o mais importante: se a resposta para qualquer das perguntas for "não", como vimos, a questão que resta então é, porque tratar. Ora, neste caso, sequer seria o caso de descaracterização do dado, ao contrário, se o dado não satisfaz base legal ou os princípios básicos para seu tratamento, pela lógica da minimização do tratamento de dados, a hipótese seria de "não tratamento" do dado pessoal, mas nunca de descaracterização, que, como vimos, importaria burocratizar e tornar ineficiente uma gestão pública que já sofre para conseguir entregar o mínimo em nosso país.

Em conclusão: ou a finalidade, a adequação e a necessidade do tratamento do dado pessoal estão presentes, com ao menos uma das respectivas bases legais que autorizem o tratamento (obrigação legal, execução de políticas públicas,

23 Em um exercício pragmático, fico a imaginar que, em se conduzindo a esta interpretação, em breve teríamos que ter, em algumas administrações, áreas específicas para o descaracterização de atos e contratos, dado o volume de contratos e dados coletados para estes fins em algumas estruturas administrativas.

execução de contratos ou diligências pré-contratuais entre outros) e portanto, quando ausente motivação para sua anonimização ou pseudoanonimização, seriam plenamente compatíveis com a LGPD, sem necessidade de qualquer hipótese de descaracterização, ou não haveria autorização para o tratamento do dado, hipótese em que sequer se cogitaria a descaracterização, mas sim, a impossibilidade do próprio tratamento.