

Seria o CPF um dado pessoal “especial”? A “novela” da descaracterização de dados pessoais em documentos públicos.

Por Rodrigo Pironti¹⁻²

Recentemente, ao debater novamente o tema da descaracterização de dados pessoais em documentos públicos, escutei de um dos debatedores que o CPF precisava ser descaracterizado/tarjado porque é um dado especialmente relevante e não poderia ser divulgado. Daí surgiu novamente a necessidade de discutir o tema sob esse prisma: seria o CPF um dado pessoal especial? O que teria de diferente o CPF, se comparado a outros dados pessoais? Seria o CPF mais importante que o nome, RG, número da carteira de habilitação ou outros dados também diretos e não sensíveis? Se sim, qual o motivo? Sob outra ótica: é razoável o que ocorre hoje na maioria dos documentos públicos, em que o CPF é descaracterizado, mas inúmeros outros dados diretos são disponibilizados no mesmo documento?

Importante recordar que vários são os mitos decorrentes da falha interpretativa ou do desconhecimento do Regime Jurídico Administrativo e da Lei Geral de Proteção de Dados, mas um dos principais, sem dúvida, continua a ser o da descaracterização de dados pessoais em documentos públicos, que, para além de traduzir – na maioria das vezes – conduta não exigida pela LGPD, 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.

A LGPD não propõe sigilo dos dados pessoais em face de uma suposta proteção, ao contrário, o que prevê de forma clara é que, os dados pessoais podem e devem ser tratados desde que respeitem os princípios nela estabelecidos, bem como, tenham uma base legal que autorize seu tratamento. Respeitadas essas balizas, em regra, não haveria qualquer motivo para a descaracterização 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.

Sem “fulanizar” neste artigo as condutas já verificadas neste sentido, tenho lido inúmeros pareceres e orientações de órgãos de segunda linha, principalmente decorrentes das Controladorias e da Advocacia Pública, informando sobre a necessidade de se descaracterizar o CPF de documentos públicos em razão da Lei Geral de Proteção de Dados, como se isso estivesse previsto expressamente na Lei e sem qualquer outra fundamentação razoável, quase que

¹Pós-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.pirontiadogados.com)

² Os argumentos expostos no artigo são opiniões baseadas no entendimento do autor e não se confundem com manifestações ou posicionamentos coletivos de nenhuma das entidades que integra ou participa.

decorrência maior do argumento de autoridade. Ora, se existe um fundamento para o sigilo dos dados pessoais ele deve estar na Lei e, ao estar na Lei, o nexo de causalidade no caso concreto se impõe, sob pena violação do princípio da motivação administrativa.

O sigilo é exceção aos documentos públicos e sua determinação deve partir de uma motivação razoável que permita afirmar que, no caso concreto, a descaracterização de um dado pessoal é realmente necessária a garantir a condição de proteção ao direito fundamental do titular para sepultar a necessária transparência que fundamenta, inclusive, os controles típicos de um Estado Democrático de Direito.

É dizer: afirmar que a descaracterização do CPF deve ocorrer para garantir o cumprimento ou a boa aplicação da Lei não basta e, para além de ser uma falácia, pois nestes casos a LGPD não determina expressamente a anonimização ou a pseudoanonimização, também viola a motivação administrativa necessária para a determinação da ocultação ou sigilo aos documentos públicos.

Para além disso, o parecer que motivar a necessidade de descaracterização do CPF, deve também motivar o porquê da manutenção de outros dados diretos, como nome e RG, por exemplo, caso contrário, estaríamos criando uma escala de prioridade entre dados diretos, onde seria possível afirmar que o CPF é mais relevante do que o RG, ou de que o RG é mais relevante que os dados constantes e derivados da carteira de habilitação e assim por diante. É dizer, se eu devo tarjar o CPF, também devo tarjar todos os demais dados diretos presentes no documento público e, neste caso, na maioria das vezes, inviabilizado estaria o controle social e, em alguma medida, o controle interno e externo de tais documentos.

Neste contexto, O TCU fez auditoria operacional, objeto do Acórdão 506/2025 – Plenário, para avaliar aspectos sobre a garantia à transparência das informações que devem ser publicadas e a proteção de dados pessoais, à luz da Lei Geral de Proteção de Dados Pessoais (LGPD) e da Lei de Acesso à Informação (LAI). Entre as constatações da auditoria, estão: i) Normas e orientações possuem maior ênfase em proteção de dados do que em transparência das informações e não tratam dos temas de forma integrada; ii) Necessidade de maior padronização quanto ao uso de técnicas de anonimização, pseudonimização e tarjamento de dados pessoais; e iii) Falta de equilíbrio das ações de capacitação na abordagem dos temas da transparência pública e da proteção de dados pessoais.³

O excesso interpretativo em razão da LGPD é tamanho, que o próprio Ministro do Tribunal de Contas da União, Bruno Dantas, publicou artigo intitulado “Transparência ou opacidade? Como a má aplicação da LGPD ameaça a democracia”⁴, em que comenta:

A resposta, como demonstra o relatório do Tribunal de Contas da União (TCU) julgado no último dia 12 de março, está na primazia da Lei de Acesso à Informação

³ <https://portal.tcu.gov.br/imprensa/noticias/falta-de-publicidade-pelos-orgaos-publicos-diminui-transparencia-e-dificulta-controle-social>.

⁴ DANTAS, Bruno. Transparência ou opacidade? Como a má aplicação da LGPD ameaça a democracia. Folha de São Paulo, 18 de março de 2025.

(LAI) sobre a Lei Geral de Proteção de Dados (LGPD) quando se trata de interesse coletivo. O acórdão 506/2025 revelou que, dos 580.236 pedidos analisados entre 2019 e 2023, 30,8% foram indevidamente classificados como “restritos”.

Em muitos casos, utilizou-se o pretexto genérico da “proteção de dados” para negar informações públicas essenciais. **Isso evidencia um desvirtuamento da finalidade da LGPD, que não pode ser usada para encobrir atos administrativos que devem ser acessíveis à sociedade.** A relação entre privacidade e transparência exige um equilíbrio delicado. De um lado, a proteção de dados pessoais assegura direitos fundamentais do indivíduo. De outro, a publicidade dos atos governamentais é indispensável para evitar abusos.

[...]

O Tribunal de Contas da União não tem se omitido e permanecerá vigilante sobre a observância da LAI, **garantindo que a proteção de dados não seja instrumentalizada para restringir indevidamente o acesso à informação.**

Rousseau afirmava, em “O Contrato Social”, que a vontade geral só se manifesta em um ambiente de clareza. Essa ideia foi bem sintetizada pelo juiz da Suprema Corte dos Estados Unidos Louis Brandeis, um dos mais influentes defensores da transparência e do direito à informação. Brandeis foi pioneiro na formulação do direito à privacidade.

Sua célebre frase, “a luz do sol é o melhor desinfetante”, reflete uma verdade inegável: governos opacos minam a confiança da sociedade e abrem espaço para abusos. **Permitir que a LGPD sirva de escudo para a opacidade não fere apenas a LAI, mas o próprio pacto democrático.** Afinal, sem transparência, não há democracia. (grifo nosso)

Vamos evoluir ainda mais no tema. Veja que, ao tratar dos dados pessoais a Lei 13.709/18, assim os define:

Art. 5º Para os fins desta Lei, considera-se:

- I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
- II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
- III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

Do conceito trazido pela Lei, não há nenhuma dúvida de que o CPF é um dado pessoal direto, por meio do qual é possível que a pessoa natural seja identificada, mas passa ao largo e não se confunde com o conceito de dado pessoal sensível, cujas características denotam,

para além da capacidade de identificação do titular, informações diretamente vinculadas à condição humana e de dignidade do titular dos dados.

Ainda que se quisesse estender ao CPF, a proteção conferida ao tratamento de dados sensíveis, muito em razão de uma possível falha interpretativa do parágrafo primeiro, do artigo 11 da LGPD, o uso do CPF estaria autorizado em documentos públicos em razão de ao menos três hipóteses legais previstas nos incisos deste mesmo artigo, quais sejam: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral.

E porque então recairia sobre o CPF, e na maioria das vezes, só sobre ele, a tão anunciada descaracterização dos três últimos ou três primeiros dígitos do documento? Fui buscar no sítio eletrônico da Receita Federal do Brasil a resposta e encontrei o óbvio: a busca pelo CPF permite identificar o seu detentor, ou seja, o meu número de CPF, quando pesquisado no sítio da RFB, permite a minha identificação, e apenas isso, nada mais. É dizer, não haveria qualquer fundamento para que a exigência de descaracterização recaísse sobre o CPF e não sobre o nome, por exemplo, se por meio de um, logicamente, só se pode chegar ao outro.

Mas há que se ter um fundamento para tantas orientações de importantes órgãos nacionais e regionais neste sentido. Seria então porque a LGPD traz em seu texto as noções de anonimização e pseudoanonimização, não estaria aí o fundamento para a descaracterização?

A Lei Geral de Proteção de Dados, quando dispõe sobre as hipóteses de anonimização ou pseudoanonimização, o faz de maneira expressa e sempre com uma motivação relevante vinculada 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)

As hipóteses da LGPD em relação a anonimização e pseudoanonimização, de per si, não determinam e sequer se aproximam de uma determinação normativa para descaracterização do dado direto CPF.

Mas porque então o CPF seria diferente? Porque teria relevância destacada aos demais? Onde estaria motivada essa tal relevância? Se não pelos critérios de anonimização ou pseudoanonimização, qual seria o interesse público a justificar o sigilo do CPF em contraposição aos parâmetros legais de transparência e controle, por exemplo?

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

Voltamos a “estaca zero”. 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 valorização da transparência e do interesse público para atividades administrativas de controle interno, controle externo e controle social? A pergunta é, porque o CPF é tão “especial” e precisaria ser descaracterizado?

A resposta, como veremos, deve passar por alguns rápidos questionamentos trazidos pela própria LGPD para se permitir o tratamento de um dado pessoal, quais sejam: Existe uma base legal que autorize o tratamento do dado pessoal? Se existe tal base, o dado tratado atende à sua finalidade? 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 positivas e não houver legislação ou ato normativo determinando ou orientando sua ocultação ou sigilo, o dado pessoal, seja qual for, pode ser tratado.⁵

Então por que descaracterizar o CPF se é plenamente autorizado e legítimo seu tratamento? Vamos avaliar agora pelo prisma da Lei de Acesso a Informação.

⁵ Ao contrário, se a resposta para qualquer das perguntas realizadas for negativa, poderia se questionar que, talvez, sequer fosse 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 poderia ser uma hipótese de “não tratamento” e não de descaracterização.

Em recente texto escrito em co-autoria com a professora Luanna Ramos⁶, 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 3º⁷, e do artigo 26, parágrafo 1º, inciso III⁸.

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 proteja os interesses coletivos.

Como se não bastasse, a Lei de Acesso à Informação, ao tratar sobre informações pessoais, determina, no artigo 6º, inciso III⁹, que o Poder Público observará a 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 31¹⁰ 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, que para tal deverão ter motivação suficiente e congruente, nem todo dado pessoal deverá

⁶ FERREIRA. Luanna Ramos; PIRONTI. Rodrigo. A LGPD E A MITIGAÇÃO DE RISCOS ALÉM DO BINÁRIO SIGILO-TRANSPARÊNCIA. No prelo.

⁷ 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.

⁸ 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.

⁹ 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.

¹⁰ 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.

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 uma, de forma a reduzir as assimetrias de informações existentes entre o Estado e seus cidadãos.¹¹

Como já manifestado em outros textos, no âmbito regulamentar, a própria Controladoria-Geral da União tem se pronunciado através de enunciados¹² 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)**

¹¹ 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>.

¹² 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.

Enunciado CGU n. 10/2023 – Informações financeiras a respeito de programas e benefícios sociais. Informações referentes a valores de 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 354/2023¹³, 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.**

Especificamente em razão do CPF, a própria ANPD, ao tratar de questão exemplificativa em seu guia orientativo para o Tratamento de dados pessoais pelo Poder Público¹⁴, assim expõe:

Exemplo 9 - Dados coletados para elaboração de contrato administrativo

A Secretaria de Educação de um Município contrata, por licitação, uma empresa para fornecer merenda nas escolas. Para firmar o contrato com a Secretaria, tanto o representante da empresa quanto o servidor público que assinará o contrato fornecem os seus dados, como nome, profissão, **cpf**, rg, estado civil e endereço residencial. Para atender a outros dispositivos legais e dar publicidade à contratação da empresa, o contrato é divulgado no sítio eletrônico da Secretaria de Educação.

No fundo, o que se está a refletir é: o que realmente se está a proteger? O dado pessoal ou o titular do dado? Em linhas gerais, existiria fundamento (motivação congruente) para a determinação da descaracterização apenas do CPF? Essa prática garantiria a não exposição do

¹³ 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: 28 mar. 2025.

¹⁴ Disponível em:

<https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 28 mar. 2025.

titular em razão do motivo apontado (muito embora outros dados pessoais diretos expostos)? 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.

Se há risco ao tratamento do dado pessoal CPF e sua relevância pode ser evidenciada em detrimento de outros dados pessoais diretos, que seja elaborado então, uma vez previstos os seus requisitos gerais e específicos, o devido Relatório de Impacto a Proteção de Dados (RIPD) que justifique a medida mitigatória da descaracterização, por exemplo. É isso que orienta a LGPD e a própria ANPD em seu referido guia orientativo:

Em outras situações, nas quais a coleta seja necessária e não seja cabível a eliminação dos dados, podem ser adotadas medidas de mitigação de risco, que fortalecem e tornam mais segura a possibilidade de divulgação dos dados pessoais, haja vista a diminuição de seu potencial lesivo aos direitos dos titulares. Eventualmente, essas medidas podem ser descritas em relatório de impacto à proteção de dados pessoais, documento do controlador que “contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco” (art. 5o, xvii; 38, parágrafo único).

O que não se pode permitir é que sem produzir motivação suficiente ao sigilo e sem que haja a elaboração dos documentos técnicos correspondentes, como quando necessário o RIPD, seja orientada a descaracterização do CPF em razão de uma suposta adequação à LGPD.

Para concluir: seria o CPF um dado pessoal “especial”? Vimos que não há qualquer fundamento para que o CPF seja alçado a condição de um dado especial perante a LGPD, ao contrário, como dado direto e não sensível, guarda relação de paridade com outros dados de mesma natureza e qualquer orientação diversa deve estar suficientemente motivada a alçá-lo à condição de ocultação.

Não há, portanto, nenhuma justificativa na LGPD para a descaracterização do CPF em documentos públicos. Entender de forma diversa seria imputar sigilo a dados constantes em documentos públicos quando, sequer sua legislação de regência o fez. **É dizer, em sendo o CPF um dado direto, não sensível e necessário a identificação pessoal daqueles que se relacionam com o Poder Público, bem como, não havendo determinação legal ou normativa para sua ocultação ou sigilo, qualquer orientação de descaracterização é desarrazoada, burocratizante e viola não apenas princípios comezinhos da LGPD e da LAI, mas principalmente, aqueles fundamentais a manutenção do Estado Democrático de Direito.**