• • •

PARECER DO MINISTÉRIO PÚBLICO

CONSULTORIA JURÍDICA DA PROCURADORIA-GERAL DE JUSTIÇA DO MINISTÉRIO PÚBLICO DO ESTADO DO RIO DE JANEIRO

PROCESSO ADMINISTRATIVO

MPRJ nº 2020.00315512

Exmo. Sr. Procurador-Geral de Justiça,

I

Trata-se de processo administrativo instaurado a partir do Ofício OMP nº 104/2020, da Ouvidora-Geral do Ministério Público, no qual solicita orientação acerca de como proceder quanto ao compartilhamento de dados dos usuários da Ouvidoria, por meio da rede de Ouvidorias Públicas, tendo em vista que "*não existe, no formulário de acesso ao sistema da Ouvidoria do Ministério Público, nenhum alerta ou opção de consentimento quanto ao compartilhamento de dados do titular quando este é identificado*".

Segundo a solicitante, o fluxo regular do trabalho em rede com outras Ouvidorias, em que os dados dos comunicantes transitam livremente entre os órgãos que integram a rede, requer um posicionamento acerca da possibilidade de disponibilizar a identidade e os dados dos comunicantes, de modo que não haja ofensa ao dever de sigilo. Esclarece, ainda, que, diante do cuidado no trato desses dados junto à Ouvidoria, só tem compartilhado em rede as comunicações anônimas e aquelas em que é possível omitir os dados pessoais do comunicante. Para a douta requerente, tanto a identificação como a proteção dos dados devem ser motivo de preocupação institucional, tendo em vista a confiança do sigilo depositado na Ouvidoria no momento da comunicação.

Considerando a natureza do objeto a ser analisado, os autos vieram a esta Consultoria Jurídica.

II

A questão posta à Chefia Institucional é relevante na medida em que a boa-fé e a confiança devem reger as relações entre o cidadão e as Ouvidorias, especialmente em se tratando de uma Ouvidoria do Ministério Público. A confiança depositada pelo usuário

na Ouvidoria não comporta relativização, sendo imprescindível que a coletividade tenha conhecimento da forma como as informações ofertadas serão trabalhadas.

Especificamente quanto à questão apresentada pela douta Ouvidora, "*como preservar a identidade e o sigilo de dados do denunciante, num contexto de Ouvidorias em rede*", a questão será analisada a partir de duas vertentes, (i) a boa-fé e a confiança como princípios básicos que regem a relação da Ouvidoria com a sociedade e (ii) o contexto legal que estabeleceu inovações em relação às Ouvidorias e delineou, no âmbito nacional, a Rede de Ouvidorias Públicas.

Permeando essas duas vertentes, é importante fixar a distinção entre a "informação sigilosa" e "informação pessoal", o que não exigirá maiores esforços, considerando terem sido devidamente distinguidas e conceituadas pela Lei nº 12.527/2011, a Lei de Acesso à Informação. Esse diploma normativo, contudo, estatuiu que, quer estejamos perante informação pessoal, quer perante informação sigilosa, o acesso a ambas é restrito.

De acordo com a Lei de Acesso à Informação, são consideradas informações sigilosas aquelas submetidas temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado. A proteção das informações sigilosas é tratada no art. 25 da Lei nº 12.527/2011, segundo o qual *é dever do Estado controlar o acesso e a divulgação de informações sigilosas produzidas por seus órgãos e entidades, assegurando sua proteção*. O acesso às informações sigilosas é restrito àqueles que tenham a necessidade de conhecer o seu teor. O Decreto nº 7.845/2012 regulamentou procedimentos para credenciamento de segurança e tratamento da informação classificada em qualquer grau de sigilo.

Dados pessoais, por sua vez, são as informações relacionadas à pessoa natural, identificada ou identificável. O seu tratamento 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. As informações pessoais não são públicas e estão sujeitas a acesso restrito, independentemente de classificação de sigilo.

Assim, devidamente diferenciadas as espécies, deve-se observar que a Ouvidoria direciona suas atenções à proteção dos dados pessoais do usuário do serviço, já que questões relacionadas à avaliação do sigilo das respectivas informações serão da alçada do órgão destinatário.

Portanto, quando nos referimos à sistemática objeto do presente expediente, estamos diante de informações afetas às pessoas que utilizam o sistema. A proteção das informações pessoais está prevista no art. 31 da Lei nº 12.527/2011. De acordo com este diploma normativo, as informações pessoais podem ser divulgadas ou acessadas por terceiros somente nos casos de previsão legal ou quando houver o consentimento expresso da pessoa do noticiante.

In casu, especificamente em relação à pessoa do usuário da Ouvidoria, dois aspectos de ordem jurídica envolvem a restrição de acesso.

O primeiro aspecto está assentado nos princípios da boa-fé e da confiança. Afinal, quando a pessoa busca a Ouvidoria Pública, o faz com a expectativa de que sua identidade estará preservada e protegida contra o noticiado. Esse aspecto, aliás, influi diretamente na esfera jurídica alheia, sendo, portanto, a nosso ver, direito subjetivo a ser protegido. Não é por outra razão que o princípio da proteção ao noticiante tem sido previsto em atos de direito internacional, a exemplo da Convenção das Nações Unidades contra a Corrupção.[1]

De acordo com o princípio da proteção ao noticiante, o dever de sigilo deve estar tão intrinsecamente enraizado no trabalho desenvolvido pelas Ouvidorias que, tratando-se de notícia tida como sigilosa em relação à identificação do denunciante, não é possível que a Ouvidoria informe tais dados nem mesmo ao membro do Ministério Público, sem o consentimento expresso do denunciante. A esse respeito, a própria Ouvidoria Nacional do Ministério Público, analisando solicitação realizada por Promotores de Justiça do Estado do Maranhão, que buscavam identificar os noticiantes em determinado caso, sendo invocada a supremacia do interesse público sobre o privado e a relatividade dos direitos ligados à privacidade e à intimidade, decidiu pelo seu indeferimento.[2]

Portanto, sob o ponto de vista dos princípios que regem a atuação das Ouvidorias, sem a anuência do comunicante, não se deve compartilhar, em rede, informações e dados pessoais ali tratados. Primeiro, porque não se pode admitir que o cidadão, na confiança de que sua identidade não será revelada, posteriormente veja seus dados manipulados e sua identidade revelada por Ouvidorias outras. Segundo, porque, sob o ponto de vista dos princípios, caso haja quebra da confiança na relação entre usuário e Ouvidoria, a exemplo do que pode ocorrer com a transferência e a divulgação em rede dos dados sigilosos tratados no âmbito de uma Ouvidoria específica, estar-se-á desvirtuando a própria *ratio essendi* do órgão. Terceiro, porque a Ouvidoria Nacional entendeu pela completa impossibilidade de quebra administrativa do sigilo conferido aos dados pessoais, sem a anuência do comunicante.

---

[1] O art. 33 da Convenção das Nações Unidas contra a Corrupção expressamente dispõe sobre a proteção aos denunciantes: "Cada Estado Parte considerará a possibilidade de incorporar em seu ordenamento jurídico interno medidas apropriadas para proporcionar proteção contra todo trato injusto às pessoas que denunciem ante as autoridades competentes, de boa-fé e com motivos razoáveis, quaisquer feitos relacionados com os delitos qualificados de acordo com a presente Convenção."

[2] Ofício nº 30/2016/OUVIDORIA/LC-CNMP: *"Esclareço que a Ouvidoria Nacional não é órgão correicional, tampouco punitivo e, aqueles que aportam à Ouvidoria, assim o fazem, na certeza de que aqui é uma instância de solução concertada e pacífica de eventuais conflitos. O cidadão, quando requer o sigilo de sua identidade, tem esse pedido deferido de pronto, se o contrário ocorresse, correríamos o risco de macular a relação de confiança depositada na Ouvidoria Nacional. Assim, o direito de recorrer a nós não pode ser convertido em um ônus, por isso, esse direito deve ser preservado. Se eventuais ações futuras de quem se socorre à Ouvidoria Nacional venham a causar danos, essa sim deve ser sancionada e corrigida, mas nunca o seu contato com esse setor, que nada mais é do que um canal aberto de comunicação da sociedade com o Conselho Nacional do Ministério Público e com o próprio Ministério Público brasileiro. Por tais razões, a Ouvidoria Nacional mantém o sigilo pleiteado e espera que sua atuação tenha sido satisfatória, a ponto de não ter que agir de forma a causar danos a ninguém."*

A partir dessas considerações, ao abordar o segundo aspecto citado, o da legislação, veremos, também, que a restrição de compartilhamento é a regra, como bem já adiantou a douta Ouvidora em seu pedido inicial.

No caso de informações pessoais, a Lei de Acesso à Informação (Lei nº 12.527/2011), em seu art. 31, impõe o tratamento de modo transparente e com respeito à intimidade e à vida privada. Devem, ainda, ser protegidas por no máximo 100 anos, a contar da data de produção, independentemente de serem informações classificadas, ou não, como sigilosas. O acesso por terceiros, por sua vez, dependerá de previsão legal ou consentimento expresso da pessoa a que se referirem (art. 31, § 1º, II).

A Lei nº 13.608/2018 dispôs sobre a figura do *whistleblower* (soprador de apito)[3]. De acordo com o seu art. 4º, "*a União, os Estados, o Distrito Federal e os Municípios, no âmbito de suas competências, poderão estabelecer formas de recompensa pelo oferecimento de informações que sejam úteis para a prevenção, a repressão ou a apuração de crimes ou ilícitos administrativos*". Também aqui foi encampado o princípio da proteção ao noticiante, assegurando ao usuário uma margem de proteção contra ações ou omissões passíveis de serem praticadas em retaliação ao exercício do seu direito de relatar (art. 4º-C). A mesma sistemática foi introduzida no art. 4º, VI e VII, da Lei nº 10.201/2001, sendo prevista, além da garantia de sigilo, a premiação em dinheiro para a resolução de crimes. Este último diploma legal foi revogado pela MP nº 841/2018, que dispôs sobre o Fundo Nacional de Segurança e encampou o mecanismo no art. 5º, IX e X, mas teve a sua vigência encerrada no prazo constitucional. Vale lembrar que há uma nítida inversão de valores no ambiente social, que vê de modo negativo aquele que fornece informações, às autoridades competentes, sobre os autores de ilícitos, o que reforça sobremaneira a necessidade de seus dados pessoais não serem fornecidos a terceiros.

A Lei nº 13.460/2017, que trata da participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública, dispõe que a proteção das informações pessoais é um direito básico do usuário de serviços públicos e deve ser protegido com restrição de acesso, nos termos da Lei nº 12.527/2011.

O Decreto nº 9.492/2018, que regulamentou a Lei nº 13.460/2017 no plano federal, além de estabelecer os mecanismos de proteção e defesa do usuário de serviços públicos, criou a Rede Nacional de Ouvidorias, que tem por finalidade integrar

[3] No direito norte-americano, o *Sarbanes-Oxley Act* (SOX) de 2002 exigiu das corporações públicas com ações em bolsa a adoção de um programa de *compliance*, também impondo, em sua seção 406, que fosse divulgado se os oficiais financeiros seniores tinham adotado um Código de Ética. A seção 806 dispõe sobre medidas de proteção para os *whistleblowers* (noticiantes do bem) e a seção 1.107 cominou sanções criminais para aqueles que adotassem medidas de retaliação contra esses noticiantes. O *Dodd-Frank Wall Street Reform and Consumer Protection Act* de 2010, que também reformou o *Securities Exchange Act* de 1934, estimulou as corporações a estabelecerem uma autorregulação, desenvolvendo canais formais para a comunicação de ilícitos, e estatuiu que as recompensas para os *whistleblowers* elegíveis seriam fixadas entre 10% e 30% das penalidades financeiras pagas em processos conduzidos pela *Securities and Exchange Comission* (SEC), órgão que já exigira, em momento anterior, por meio do *Investment Advisers Act* [*Rule* 206(4)-7], que as corporações implementassem o programa de *compliance* e contassem com um *chief compliance officer*. Nitish Sing e Thomas J. Bussen (2015: 5) observam que a SEC recebeu 6.573 comunicações de *whistleblowers* entre 2011 e 2013, pagando 14,8 milhões de dólares em recompensas apenas em 2013.

as ações de simplificação desenvolvidas pelas unidades de ouvidoria da União, dos Estados, do Distrito Federal e dos Municípios, sob a coordenação da Ouvidoria-Geral da União (art. 24).

A adesão à Rede é voluntária e garante aos órgãos e entidades participantes o uso gratuito do Sistema Nacional Informatizado de Ouvidorias (e-Ouv), bem como a promoção de ações de capacitação para agentes públicos em matéria de ouvidoria e simplificação de serviços.

Em linhas gerais, a Rede Nacional de Ouvidorias, da qual o Ministério Público do Estado do Rio de Janeiro é participante, é um fórum que integra as unidades de ouvidoria, com o objetivo de buscar a consolidação de uma agenda nacional de ouvidoria pública, com a devida participação social, visando à garantia dos direitos dos usuários dos serviços públicos.

As medidas de salvaguarda da identidade de noticiantes, no âmbito da Rede Nacional de Ouvidorias, são estabelecidas pela Resolução nº 03/2019. Esse ato normativo, em seu art. 5º, tratou especificamente da proteção dos dados pessoais, *verbis*:

> *Resolução nº 03/2019 – Rede Nacional de Ouvidorias*
>
> *Art. 5º Nos termos do art. 10, § 7º da Lei nº 13.460, de 26 de junho de 2017, desde o recebimento da denúncia, todo denunciante terá sua identidade preservada, que deverá ser mantida com restrição de acesso pelo prazo de que trata o art. 31, §1º, I, da Lei nº 12.527, de 18 de novembro de 2011.*
>
> *§1º A preservação da identidade dar-se-á com a proteção do nome, endereço e quaisquer elementos de identificação do denunciante, que ficarão com acesso restrito e sob a guarda exclusiva da unidade de ouvidoria responsável pelo tratamento.*
>
> *(...)*
>
> *§3º Observado o disposto no § 1º, a unidade de ouvidoria responsável pelo tratamento deverá providenciar a pseudonimização da denúncia recebida para envio às unidades de apuração competentes para realizar a análise.*
>
> *§4º Os elementos de identificação do denunciante poderão ser solicitados pelo agente público responsável pela apuração da denúncia, demonstrada a necessidade de conhecê-la.*
>
> *§5º O encaminhamento de denúncias com elementos de identificação entre unidades de ouvidoria deverá ser precedido do consentimento do denunciante.*
>
> *§6º O compartilhamento da informação com outros órgãos não implica a perda de sua natureza restrita, sobretudo com relação à identidade do denunciante, nos termos da legislação em vigor.*

Como se constata do ato normativo acima, é dever da Ouvidoria que aderiu à Rede zelar e resguardar o sigilo da identidade e dos dados pessoais do denunciante no seu âmbito interno, praticando ações como a pseudonimização[4] e a anonimização[5].

Como o trabalho em Rede possibilita que uma Ouvidoria encaminhe, para outra, fato noticiado em sua esfera de atuação, o encaminhamento da notícia com os elementos de identificação do noticiante, para outra Ouvidoria ou para a Rede, somente poderá ser feito com o consentimento expresso do respectivo noticiante. Esse consentimento, aliás, caso se entenda conveniente, pode ser objeto de questionamento imediato ao usuário no momento do próprio registro de sua manifestação.

Nessa linha, o posicionamento do Ministério Público do Estado do Rio de Janeiro não pode caminhar em sentido contrário ao que preconiza o princípio da proteção integral dos dados do noticiante. Desta forma, o entendimento não pode ser outro senão o de que a identidade e os dados pessoais dos usuários da Ouvidoria do Ministério Público só podem ser compartilhados com expressa autorização desses interessados, independentemente da existência, ou não, de pedido de sigilo.

III

Considerando o exposto, esta Consultoria Jurídica se manifesta no sentido de que a identidade e os dados dos noticiantes da Ouvidoria do Ministério Público devem ser protegidos, somente sendo acessíveis a terceiros, incluindo no âmbito de outras redes de ouvidorias, com a expressa autorização do referido noticiante.

Rio de Janeiro, 11 de maio de 2020.

EMERSON GARCIA

Consultor Jurídico

[4] Pseudonimização é 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.

[5] 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.