Enap Escola Nacional de Administração Pública

Possíveis impactos da LGPD na atividade de inteligência do Cade

Trabalho de Conclusão de Curso apresentado como parte dos requisitos para obtenção do grau de Especialista em Planejamento e Orçamento.

Aluno: Stefano Mozart Pontes Canedo de Souza

Orientadora: Profa. Dra. Maria Abadia da Silva Alves

Brasília, DF
Junho/2020

Enap Escola Nacional de Administração Pública

Possíveis impactos da LGPD na atividade de inteligência do Cade

Stefano Mozart Pontes Canedo de Souza
Conselho Administrativo de Defesa Econômica

Palavras chave: LGPD, inteligência de Estado, riscos

Resumo analítico:

A Lei Geral de Proteção de Dados (LGPD) introduz diversas obrigações e vedações que visam proteger a privacidade das pessoas naturais. Tais disposições sobrecaem, inclusive, sobre a ação do Estado na coleta, processamento e publicação de dados pessoais no decurso da execução de políticas públicas. Este trabalho busca identificar possíveis impactos da LGPD sobre um instrumento específico da ação estatal, a atividade de inteligência, com especial atenção à atuação do Conselho Administrativo de Defesa Econômica.

Abstract:

The General Law for Data Protection (LGPD, in Portuguese) introduces many obligations and prohibitions with the aim to protect the privacy of natural persons. Such provisions apply even to the actions of the State in the collection, processing and publication of personal data used for the carrying out of public policies. This work tries to identify possible impacts of the LGPD over a specific instrument of State endeavor, the intelligence activity, with special attention to the work of the Administrative Council for Economic Defense.

Resumen analítico:

La Ley General de Protección de Datos (LGPD) introduce varias prohibiciones y obligaciones que tienen como objetivo proteger la privacidad de las personas físicas. Tales disposiciones se aplican incluso a la acción del Estado en la recopilación, procesamiento y publicación de datos personales en la ejecución de políticas públicas. Este trabajo tiene como objetivo identificar posibles impactos de la LGPD en un instrumento específico de acción estatal, la actividad de inteligencia, con especial atención a las actividades del Consejo Administrativo de Defensa Económica.

Introdução

A Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados (LGPD), introduz no ordenamento jurídico brasileiro normas gerais de proteção de dados pessoais. A LGPD dispõe, expressamente, que tais normas são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios

O Artigo 9º ordena, por exemplo, que ao titular de dados pessoais seja concedido acesso a informações sobre a forma e duração do tratamento de seus dados, informações detalhadas sobre o compartilhamento de bases de dados, e até mesmo sobre os agentes envolvidos em quaisquer etapas do tratamento de seus dados.

O art. 18, por sua vez, garante que toda pessoa natural tem direito de receber prontamente, da parte do órgão público controlador de dados, confirmação da existência ou não de tratamento de dados de sua titularidade. Caso positivo, também lhe assiste o direito de acesso a seus dados de forma simplificada, garantida a eliminação de dados que julgar desnecessários ou excessivos para o cumprimento das obrigações legais ou regulatórias que justificam o tratamento.

Esses dispositivos estão em linha com o conceito de autodeterminação informativa, apresentado no art. 2º da LGPD como um dos fundamentos da disciplina de proteção de dados. Esse conceito pode ser definido como o poder do indivíduo, no livre exercício do desenvolvimento de sua personalidade, de determinar e controlar a utilização de seus dados pessoais (MENDONÇA, 2014). A garantia da autodeterminação informativa como direito da pessoa natural implica que o sujeito titular de dados pessoais tem poder para interferir em matérias relacionadas ao tratamento de seus dados, e, consequentemente, tem direito de ser informado e optar pela participação em quaisquer processos que resultem na coleta, processamento ou disseminação desses dados.

Por outro lado, bases de dados sobre os administrados são instrumentos cada vez mais relevantes, tanto no desenho quanto na operacionalização de políticas públicas. Não apenas para ganho de escala, mas especialmente como mecanismo de articulação de políticas e de coordenação do arranjo institucional requerido para seu

sucesso (AMORIM; BOULLOSA, 2013). Instrumentos como o CadÚnico (Cadastro Único para Programas Sociais) e a RAIS (Relação Anual de Informações Sociais), de patente relevância para uma extensa gama de políticas públicas no Brasil, poderiam se tornar impraticáveis, do ponto de vista do custo da infraestrutura de computação e telecomunicação, se as centenas de milhões de pessoas físicas listadas nessas bases passassem a exercer seu direito de acesso e revisão dos dados.

A despeito de sua importância no bojo da proteção da privacidade e da liberdade dos cidadãos, tais determinações podem ter um efeito limitador sobre a capacidade dos entes estatais de coletar e tratar dados de pessoas físicas no intuito de executar políticas públicas. Os custos trazidos pelas garantias e obrigações da LGPD devem passar a integrar o desenho e avaliação de políticas, forçando o gestor público a considerar, entre outros fatores, as maneiras e a frequência em que os titulares de dados pessoais e sensíveis podem demandar acesso, alteração ou remoção de seus dados e que incentivos teriam para requerer o exercício desses direitos.

Além disso, os direitos de acesso à informação sobre o uso compartilhado de bases de dados e sobre a identidade dos agentes envolvidos no tratamento dos dados podem limitar, em diversos níveis, a cooperação entre os órgãos de inteligência, investigação e persecução, seja na esfera administrativa ou criminal. Certamente, no âmbito da ação sancionadora do Estado, há diversos incentivos para que o administrado busque a eliminação dos dados de sua titularidade e para que busque conhecer a trilha de processamento e compartilhamento de tais dados.

As questões apontadas até aqui demonstram a necessidade de se levantar e discutir os potenciais riscos impostos pelas disposições da LGPD sobre as atividades de inteligência de Estado no Brasil. Caso se verifique o risco de tais atividades sejam inviabilizadas, em face das novas condições impostas ao tratamento de dados pessoais, limitando a atuação dos entes estatais, é necessário desenhar e desenvolver um novo planejamento da atuação dessas entidades.

Este trabalho busca, portanto, identificar possíveis repercussões das disposições da LGPD nas atividades de inteligência estatal, seja na coleta e tratamento de dados, seja na disseminação de conhecimento, com especial atenção às atividades desenvolvidas no âmbito do Conselho Administrativo de Defesa Econômica (Cade).

A seção 1 traz uma apresentação sucinta da LGPD, dos conceitos introduzidos no próprio texto da Norma e de alguns princípios, garantias, obrigações e vedações relevantes no contexto de inteligência. A seção 2 aborda brevemente a atividade de inteligência de Estado no Brasil e as atividades desenvolvidas no âmbito do Cade que podem ser assim classificadas. O texto se debruça mais detalhadamente, na seção 3, sobre os possíveis impactos da LGPD nas atividades de inteligência e sobre possíveis ações de mitigação dos riscos identificados. A seção 4 discute riscos e estratégias de mitigação específicos para o Cade. A conclusão destaca os achados mais relevantes e aponta questões para aprofundamento futuro.

Esse tipo de mapeamento, por seu caráter exploratório, é útil como insumo para a melhoria da capacidade de planejamento da Administração Pública, bem como no estabelecimento de parâmetros para o desenho de medidas de curto e médio prazo, tais como a substituição de processos, procedimentos e fontes de dados.

Espera-se, ainda, que o conhecimento aqui estruturado, possa instrumentalizar uma discussão mais ampla, que oriente iniciativas como a elaboração e acompanhamento de proposições legislativas para aperfeiçoamento da própria LGPD ou da legislação específica afeta às atividades realizadas pelos diversos órgãos e unidades de inteligência. De sorte que reste garantida, no longo prazo, a efetividade das políticas públicas que, hoje, recebem relevante contribuição dessas atividades, assim como a política de defesa econômica desempenhada pelo Cade.

1 A Lei Geral de Proteção de Dados

Segundo Doneda e Mendes (2019), existem "cinco eixos principais da Lei Geral de Proteção de Dados em torno dos quais a proteção do titular de dados se articula: i) unidade e generalidade da aplicação da Lei; ii) legitimação para o tratamento de dados (hipóteses autorizativas); iii) princípios e direitos do titular; iv) obrigações dos agentes de tratamento de dados; v) responsabilização dos agentes".

De autoria do Deputado Federal Milton Monti (PR SP), o Projeto de Lei 4060 de 2012, trouxe em sua justificativa a seguinte afirmação:

> "Não há dúvida nenhuma que o Estado deve cuidar das questões gerais, mas é também evidente que a sociedade é refratária ao excesso de tutela por parte do

> Estado e que deseja exercer na plenitude seus direitos constitucionais inclusive o de receber se quiser comunicações pelos meios disponíveis no momento." (BRASIL, 2012)

É perceptível que o Projeto, que deu origem à LGPD, baseou-se, desde o princípio, na preocupação de trazer ao ordenamento jurídico pátrio a regulamentação do tratamento de dados pessoais com o intuito de proteger o direito à liberdade individual contra excessos, inclusive da parte do Estado.

O texto final agrega diversas contribuições trazidas durante sua tramitação no Congresso e, posteriormente, pela Medida Provisória nº 869, de 27 de dezembro de 2018, convertida na Lei nº 13.853, de 8 de julho de 2019. Assim, ao passo que teve seu escopo alargado, passando a tratar da criação, organização e competências da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, também se tornou muito mais específico quanto às hipóteses e às condições nas quais o tratamento de dados pessoais passa a ser admitido na forma da lei.

Outro aspecto interessante, que se manteve desde a propositura original, até o texto em sua forma atual, foi a preocupação de especificar no próprio texto da norma os conceitos mais relevantes para a delimitação do objeto jurídico tutelado. Os sete conceitos presentes no texto original foram desdobrados em dezenove no autógrafo. O que indica tanto a necessidade de especificar questões até então não claramente abordadas no regimento pátrio, quanto o ineditismo e a sensibilidade do assunto tratado nos demais dispositivos daquela Lei.

Por fim, destaca-se também o fato de que tanto o texto original quanto sua redação atual trazem a especificação do escopo de aplicação Lei, isto é, das atividades de tratamento de dados sobre as quais a norma se aplica, assim como uma lista de atividades escusadas das obrigações, direitos e vedações por ela introduzidos. Há várias explicações possíveis, inclusive a percepção de que estas últimas se veriam prejudicadas, ou até mesmo inviabilizadas, pelos novos encargos. A proteção ao direito individual é limitada, no contexto dessas atividades, em favor do interesse coletivo.

A última alteração no texto da LGPD se deu por meio da Lei nº 14.010, de 10 de junho de 2020, que acrescentou o inciso I-A ao *caput* do art. 65, modificando a

cláusula de vigência da norma de forma que os dispositivos que tratam das sanções administrativas decorrentes de seus descumprimento (arts. 52, 53 e 54) passarão a ter vigência apenas no dia 1º de agosto de 2021.

O escopo de aplicação da Lei, apresentado brevemente acima, será discutido com mais detalhes na seção 3. Passamos, a seguir, a expor as hipóteses autorizativas, os direitos do titular e as obrigações impostas aos agentes de tratamento.

1.1 Hipóteses legais para o tratamento de dados pessoais e dados pessoais sensíveis

A LGPD traz diferentes graus de restrição para o tratamento de dados pessoais, de acordo com as possíveis motivações e finalidades da atividade desenvolvida. O art. 7º dispõe sobre as hipóteses em que o tratamento de dados pessoais deve ser precedido de expresso consentimento do titular e em que hipóteses, tais como o cumprimento de obrigação legal ou regulatória pelo controlador ou para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas, esse consentimento é dispensado.

O art. 11 traz as hipóteses em que se admite o tratamento de dados pessoais sensíveis. A primeira, é o tratamento sob consentimento específico para finalidades claramente destacadas no termo de consentimento. A segunda hipótese, que dispensa o consentimento, determina que o dado precisa ser indispensável para a consecução de uma das seguintes atividades:

> "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;
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais."
> (BRASIL, 2018)

Várias dessas hipóteses de tratamento de dados pessoais sensíveis estão intimamente relacionadas à atuação da Administração Pública. No entanto, é importante ressaltar que, embora dispensada do dever de receber o consentimento para tratamento de dados pessoais ou dados pessoais sensíveis, a Administração não é dispensada das demais obrigações impostas pela LGPD frente aos titulares, à ANPD, e às demais instâncias jurisdicionais no contexto das normas ali dispostas.

O § 2º do art. 11 determina, por exemplo, que, nas hipóteses de cumprimento de obrigação legal ou regulatória pelo controlador ou de tratamento compartilhado de dados necessários à execução de políticas públicas, fica a Administração sujeita à obrigação de publicizar, em seu sítio eletrônico, a referida dispensa de consentimento, explicitando para quais atividades a informação é indispensável e de que forma é tratada, nos termos do inciso I do *caput* do art. 23.

Além disso, o § 2º do art. 18 garante ao titular o poder de opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto na Lei. Ou seja, se a Administração falhar na observância de quaisquer dos preceitos da LGPD, a despeito da legalidade e da relevância da atividade que envolve o tratamento de dados pessoais, assiste ao titular o direito de opor-se a esse tratamento. O que reforça a importância, no âmbito do planejamento da ação pública, de se conhecer os conceitos, princípios e normas, de caráter geral ou específico, introduzidos pela LGPD, a fim de alinhar o desenho, a execução e a avaliação de políticas políticas públicas, evitando desconformidades com a legislação e danos aos administrados ou ao erário público.

1.2 Conceitos

Há dois conceitos centrais expressos no art. 5º da LGPD: dados pessoais e dados pessoais sensíveis. Dados pessoais são informações acerca de pessoa natural identificada ou identificável (*e.g.* nome, filiação, número de registro civil ou fiscal). Dados pessoais sensíveis são aqueles que, estando vinculados a uma pessoa natural, revelam sua origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, ou informações referentes à saúde ou à vida sexual, ou seus dados genéticos ou biométricos.

Tratamento é “toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração”. A pessoa natural a quem se referem os dados tratados é o titular. O direito ao pleno exercício dessa titularidade fundamenta-se no conceito de autodeterminação informativa (inciso II do art. 2º), abordado anteriormente, e é o centro da relação jurídica entre a pessoa natural e os demais atores atingidos pela norma.

A pessoa, natural ou jurídica, de direito público ou privado, a quem compete as decisões sobre o tratamento de dados pessoais, é chamada de controlador. A pessoa, natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados, é chamada de operador. Uma pessoa pode ser, concomitantemente, controlador e operador. Ambos, controlador e operador, são designados como agentes de tratamento. Por fim, “encarregado” é a pessoa natural indicada por agente de tratamento para, em seu nome, comunicar-se com o titular dos dados, com a ANPD ou com outros agentes de tratamento.

1.3 Garantias, obrigações e vedações

A LGPD reserva o Capítulo III (arts. 17 a 22) para dispor sobre os direitos do titular. Há, no entanto, direitos do titular expressos em diversos outros dispositivos. Alguns direitos, como a privacidade e a autodeterminação informativa, são declarados como fundamentos da disciplina de proteção de dados (art. 2º, incisos I e II). Outros, são expressos na forma de definição de princípios, como é o caso da “garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais”, presente no art. 6º, IV, como descrição do princípio de livre acesso.

O Quadro 1, a seguir, foi elaborado como forma de facilitar ao leitor a identificação dos direitos considerados mais relevantes no contexto da discussão em tela. Com especial atenção àqueles que, para seu exercício, se refletem numa obrigação para os agentes de tratamento.

Quadro 1: Direitos do titular de dados

Descrição	Dispositivos
Liberdade	Art. 1º, *caput*; art. 17
Privacidade	Art. 1º, *caput*; art. 2º, I
Livre desenvolvimento da personalidade	Art. 1º, *caput*; art. 2º, VII
Autodeterminação informativa (titularidade)	Art. 2º, II; art. 17
Liberdade de expressão, de informação, de comunicação e de opinião	Art. 2º, III;
Inviolabilidade da intimidade, da honra e da imagem	Art. 2º, IV
Anonimização	Art 5º, XI; art. 7º, IV; art. 11, II, c); art. 18, IV
Bloqueio	Art 5º, XII; art. 18, IV
Eliminação	Art 5º, XII; art. 18, IV; art. 18, VI
Livre acesso a dados de sua titularidade	Art. 6º, IV; art. 9º; art. 18, II; art. 19, §§ 1º e 2º
Correção de dados de sua titularidade	Art. 18, III
Direito de informação	Art. 6º, I; art 6º II
- Confirmação de existência do tratamento	Art. 9º, I; art. 18, I; art. 19, I, II
- Informações sobre finalidade, forma e duração do tratamento	Art. 9º, II, III, IV; art 9ª,§ 3º; art. 11, § 2º; art. 20, § 1º; art. 23, I
- Informações sobre compartilhamento dos dados	Art. 9º, V; art. 18, VII
Portabilidade de dados	Art. 11, § 4º, I; art 18, IV; art. 40
Peticionar contra o controlador junto à ANPD	Art 18, § 1º
Opor-se a tratamento dispensado de consentimento, em caso de descumprimento da LGPD	Art 18, § 2º
Revisão de decisões tomadas em tratamento automatizado	Art. 20
Exercer a tutela de seus direitos individual ou coletivamente	Art. 22

Fonte: o autor

Quadro 2: Vedações

Vedação	Dispositivo
Tratamento realizado por pessoa de direito privado, em favor de controlador escusado da LGPD	Art. 4º, § 2º
Transferência da totalidade da base de dados de pessoa escusada pela LGPD para pessoa de direito privado	Art 4º, § 4º
Revelar dados pessoais quando da publicação de pesquisas	Art. 13, § 1º
Transferência de dados de instituição de pesquisa para quaisquer terceiros	Art. 13, § 2º
O acesso de terceiros, após o término do tratamento	Art. 16, IV
Utilizar dados fornecidos no regular exercício de direitos contra o titular	Art. 21
Transferência de dados do Poder Público para entidades privadas, exceto nos casos descritos nos incisos I, III, IV e V	Art. 26, § 1º
Transferência internacional, execto nos casos descritos nos incisos I, II, III, IV, V, VI, VII, e IX	Art. 33

Fonte: o autor

As vedações que atingem o Poder Público e que podem gerar repercussões para a atividade de inteligência foram listadas no Quadro 2, acima. As obrigações mais relevantes para o administrador público estão elencadas no Quadro 3.

Quadro 3: Obrigações impostas aos agentes de tratamento

Obrigação	Dispositivos
Utilizar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas	Art. 6, VII
Demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas	Art. 6, X
Manter registro das operações de tratamento	Art. 37
Emitir, sob determinação da ANPD, relatório de impacto à proteção de dados	Art. 32; art. 38
Seguir normas estabelecidas pela ANPD de interoperabilidade, livre acesso e tempo de guarda de registros	Art. 40
Indicar encarregado e publicar sua identidade no sítio eletrônico	Art. 41; art. 41. § 1º
Aceitar reclamações do titular, prestar esclarecimentos e adotar respectivas providências	Art. 41, § 2º, I
Receber comunicações da ANPD	Art. 41, § 2º, II
Seguir normas estabelecidas pela ANPD sobre a definição e atribuições do encarregado	Art. 41, § 3º
Responder solidariamente por danos causados por operador	Art. 42, § 1º, II
O ônus da prova em relação ao "não tratamento" de dados, ou a não violação à legislação ou à culpa de terceiros	Art. 42, § 2º; Art. 43
Responder pelos danos decorrentes da violação da segurança dos dado	Art. 44, Parágrafo ùnico
Adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais	Art. 46
Garantir a segurança da informação prevista na LGPD em relação aos dados pessoais, mesmo após o término do tratamento	Art. 47
Comunicar a ANPD e os titulares acerca de incidentes de segurança	Art. 48
Estruturar todos os sistemas para atender aos requisitos e princípios gerais da LGPD	Art. 49
Implementar programa de governança em privacidade	Art. 50, § 2º, I
Demonstrar a efetividade do programa de governança	Art. 50, § 2º, II
Publicar regularmente regras e padrões de governança	Art. 50, § 3º

Fonte: o autor

2 Atividade de inteligência do Estado

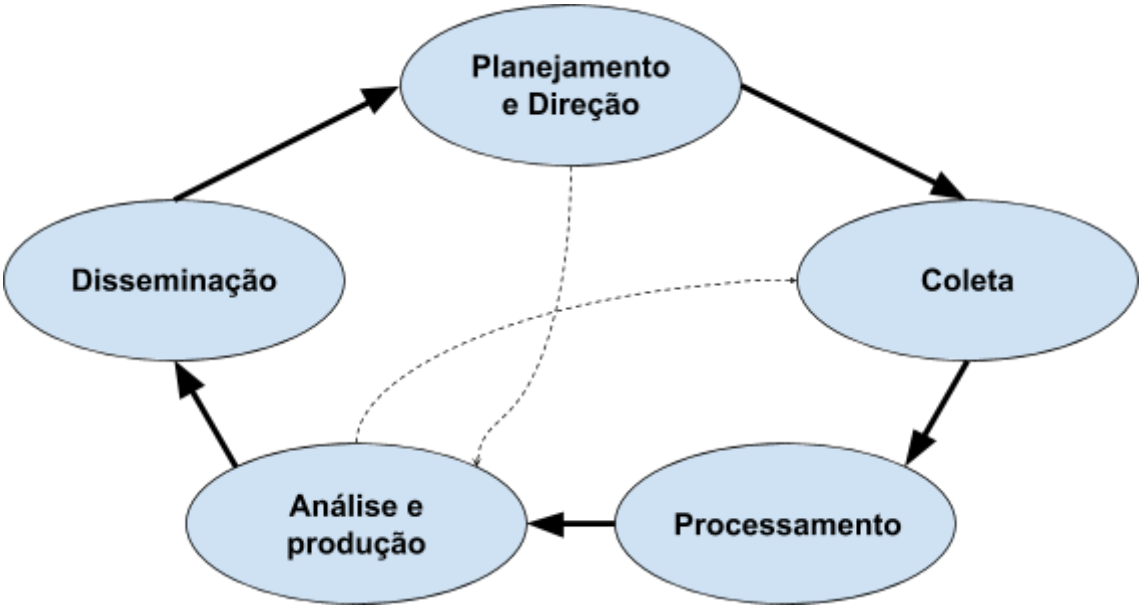
Inteligência Estatal é a atividade sistemática, realizada por agentes do Estado, com o fim de coletar e analisar informações a fim de orientar a ação Estatal (MACIEL; PINHEIRO, 2014). Nos termos da Lei nº 9883, de 7 de dezembro de 1999, que institui o Sistema Brasileiro de Inteligência (Sisbin), entende-se como inteligência a atividade que objetiva a obtenção, análise e disseminação de conhecimentos dentro e fora do território nacional sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado.

Nesta acepção ampla, estão incluídas atividades sobre as quais o sujeito titular de dados pessoais tem incentivos positivos e iniciativa de participação, mas também se incluem atividades sobre as quais o sujeito não pode ser informado, nem pode participar, caso contrário, perderiam seu objeto. Pertencem a este último grupo aquelas atividades relacionadas à persecução penal (como a investigação criminal) e aos procedimentos preliminares em sede de processo administrativo sancionador.

Para essas atividades, há outra definição de inteligência estatal, que está relacionada à "coleta de informações sem o consentimento, a cooperação ou mesmo o conhecimento por parte dos alvos da ação", o que lhe confere o mesmo sentido de segredo ou informação secreta (CEPIK, 2003, p. 27).

Seja na acepção mais ampla, de processamento da informação, seja na visão mais restrita, de tratamento de informação sigilosa, a atividade de inteligência se desdobra em diversos formas de atuação, geralmente coordenadas num arranjo conhecido como o ciclo de inteligência. Este ciclo, de acordo com a definição clássica criada pela Agência Central de Inteligência dos EUA, é o processo de transformar informações brutas em inteligência acabada para os formuladores de políticas usarem na tomada de decisões. Existem cinco etapas que constituem o ciclo da inteligência: 1) Planejamento e direção; 2) Coleta; 3) Processamento; 4) Análise e produção; 5) Disseminação (EUA, 2009).

Figura 1: Ciclo de Inteligência



Fonte: o autor

A relação entre consumidores e produtores de inteligência é expressa como um ciclo fechado, iterativo, pois os tomadores de decisão podem definir requisitos que orientam a coleta e a produção de inteligência, e, de igual sorte, os produtores de informação podem influenciar os tomadores de decisão de modo a orientar a decisão sobre novos alvos de supervisão e coleta de dados. A Figura 1, acima, esboça essa relação.

2.1 Inteligência de Estado para além de segurança pública e defesa nacional

De acordo com Pereira (2009), a atividade de inteligência é um instrumento que possibilita, por meio de métodos e técnicas próprios, a coleta e a busca de dados e informações com vistas à produção de conhecimento que servirá como subsídio à tomada de decisão, permitindo que o Estado possa reduzir os riscos e as incertezas de sua atuação, agindo de forma mais racional e econômica.

A atividade de inteligência é, portanto, para além de suas aplicações nos contextos de segurança pública e defesa nacional, um instrumento de gestão. O Sisbin conta hoje com 42 membros. Alguns, como a Agência Brasileira de Inteligência e as unidades de inteligência das Forças Armadas, representam o contexto clássico da

inteligência. Mas a maior parte dos membros corresponde a unidades do Ministério da Justiça e Segurança Pública e unidades de inteligência de atuação eminentemente administrativa, como a Controladoria-Geral da União e as agências reguladoras.

Também existem diversos órgãos que executam atividades de inteligência de Estado nos âmbitos municipal e estadual, tanto fora do Sisbin quanto no âmbito do Sistema. Note-se, ainda, o fato de haver representação indiretas desses entes, via Secretaria Nacional de Segurança Pública, no Sisbin.

No entanto, considerando a limitação temporal para conclusão deste trabalho e o esforço necessário para levantar e analisar a legislação correlata vigente em todos os entes federativos, o texto se limita à análise dos impactos da LGPD à atividade de inteligência realizada no âmbito administrativo, com especial atenção às suas repercussões para a atuação do Cade.

2.2 A atividade de inteligência no Cade

O Conselho Administrativo de Defesa Econômica é responsável pela execução da política de defesa e promoção da concorrência, em âmbito nacional. Também tem, entre as competências que lhe confere a Lei nº. 12.529, de 30 de outubro de 2011, a responsabilidade de não só investigar, como também decidir, em última instância, sobre a matéria concorrencial.

O Cade também representa o Brasil, como país não membro, em atividades de cooperação econômica junto à Organização para Cooperação e Desenvolvimento Econômico (OCDE), especialmente no âmbito do combate a cartéis e outras infrações à ordem econômica de abrangência internacional que porventura afetem o Brasil. Além de ações de cooperação bilateral, firmadas com autoridades de defesa da concorrência de diversos países.

Na Lei 13.249 de 13 de janeiro de 2016 (PPA 2016-2019), essa atuação era sintetizada pela iniciativa 04WO: “Fortalecimento da política de combate a cartéis, com ênfase na persecução de cartéis em compras públicas, inovando e aprimorando os mecanismos de investigação e de inteligência por meio do uso integrado de informações e da institucionalização de parcerias com órgãos da administração pública e organismos internacionais”. No PPA 2020-2023, a atuação do Cade é orientada, sumariamente, pela

Meta 050X – Alcançar 80% do índice de direitos promovidos aos cidadãos, de acesso ao acervo da memória nacional, da defesa do mercado concorrencial e do consumidor e da aplicação da justiça na gestão de ativos, do Programa 5015 - Justiça.

O Conselho é composto por três órgãos: o Tribunal Administrativo de Defesa Econômica; a Superintendência-Geral (SG); e o Departamento de Estudos Econômicos. O Tribunal Administrativo é o órgão judicante ao qual compete, entre outras coisas, decidir sobre a existência de infração à ordem econômica e aplicar as penalidades previstas em lei.

À Superintendência-Geral, por sua vez, compete, dentre outras responsabilidades, o monitoramento e acompanhamento das práticas de mercado e o dever de promover, em face de indícios de infração da ordem econômica, procedimento preparatório de inquérito administrativo, inquérito administrativo e processo administrativo para apuração de infrações à ordem econômica.

Várias das atividades desenvolvidas no âmbito dessa competência têm o caráter de inteligência de Estado, não apenas as que envolvem busca e apreensão ou aplicação de técnicas forenses para levantamento de provas. O simples monitoramento de práticas de mercado requer a aplicação de técnicas avançadas de análise econômica e inferência estatística, com vistas à identificação de comportamentos anômalos e potenciais riscos à livre concorrência, que são, essencialmente, aplicações da disciplina de análise do ciclo de inteligência.

3 Possíveis impactos da LGPD

Os conceitos de inteligência de Estado apresentados na seção anterior demonstram sua importância e sensibilidade como instrumento de gestão e de orientação da ação do Poder Público.

Se os direitos e obrigações introduzidos pela LGPD se estendessem a todas as atividades dos órgãos de inteligência, os cidadãos poderiam exercer o direito de informação sobre como, quando e em que atividades esses órgãos coletam dados, sobre agentes envolvidos no tratamento de seus dados e sobre as informações trocadas entre os diversos órgãos. Assim, teríamos uma situação *sui generis* no Brasil – tornando

pública praticamente toda a atividade de inteligência do Estado, que, por sua natureza, tem caráter eminentemente sigiloso.

O legislador, no entanto, criou uma lista taxativa, no art. 4º, de atividades para as quais não se aplicam a maior parte das obrigações e vedações. A LGPD não se aplica às atividades realizadas para fins jornalísticos, artísticos e acadêmicos (caso em que se aplica a obrigatoriedade de consentimento expresso). O inciso III do *caput* escusa, ainda, o tratamento de dados realizado para fins exclusivos de segurança pública; defesa nacional; segurança do Estado; ou atividades de investigação e repressão de infrações penais. A essas atividades aplicam-se apenas as vedações impostas nos §§ 1º a 4º.

O texto proposto originalmente, trazia, em seu Artigo 6º, a seguinte redação:

> "Art. 6º. Esta lei não se aplica:
> I – aos bancos de dados utilizados para o exercício regular da atividade jornalística;
> II – aos dados relativos a pessoas físicas, quando se referirem, exclusivamente, a informações relativas às suas atividades profissionais e/ou comerciais;
> III - aos bancos de dados utilizados para a pesquisa histórica, científica ou estatística, de administração pública, investigação criminal ou inteligência;
> IV – ao tratamento de dados pessoais de informações de domínio público."
> (BRASIL, 2012)

Note que o legislador excetuou expressamente, em sua proposta legislativa, os bancos de dados utilizados para a atividade de inteligência. Já o dispositivo análogo na redação final, o Artigo 4º, dispõe o seguinte:

> "Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
> II - realizado para fins exclusivamente:
> a) jornalístico e artísticos; ou
> b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
> III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais; ou
> IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

> § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.
> § 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.
> § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.
> § 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público."
> (BRASIL, 2018)

Especialmente no que toca a ação Estatal, a redação final troca expressões que delimitam a natureza das atividades (i.e. "administração pública", "investigação criminal", "inteligência") por uma abordagem que expressa a finalidade das atividades excetuadas. Dessa forma, nem toda atividade de inteligência está livre dos encargos desta lei.

Como essas exceções tratam da finalidade das atividades, e não da natureza ou missão institucional do órgão que as realiza, várias questões podem surgir: quando uma informação pessoal ganha o caráter de dado essencial à segurança pública, ou à defesa nacional? Quando uma pessoa pode ser alvo de coleta de informações em sede de investigação criminal? Como justificar o tratamento de dados pessoais de uma pessoa sem, primeiramente, levantar dados sobre sua identidade e sobre a materialidade dos fatos sobre determinada conduta que, eventualmente, lhe possa ser atribuída?

Para além dessas questões de cunho jurídico, há uma questão extremamente relevante do ponto de vista administrativo: o fato de que a LGPD não conferiu o mesmo tratamento dado à persecução penal à persecução em âmbito administrativo. Ao tratar das atividades escusadas, a Lei é silente quanto à figura do procedimento administrativo sancionador.

A sanção administrativa é a "penalidade prevista em lei, instrumento editalício ou contrato, aplicada pelo Estado no exercício da função administrativa, como consequência de um fato típico administrativo com a observância dos princípios

constitucionais do contraditório e da ampla defesa, garantidos por meio do devido processo legal" (BRASIL/MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO, 2015).

O procedimento sancionador inclui tanto o processo administrativo quanto os atos administrativos preliminares, necessários ao levantamento e processamento de informações que deverão orientar a própria abertura do processo. As partes têm direito à ampla defesa e, consequentemente, ao pleno conhecimento sobre os fatos nos quais se baseia o processo. Mas sua participação não é requerida, e, na maior parte das vezes, é impeditiva aos procedimentos preliminares, que produzem as informações que motivam a abertura do processo e justificam a ação estatal sancionadora.

De acordo com Abreu e Silva (2018), o processo administrativo sancionador visa demonstrar, num contexto democrático, de um Estado de direito, a ocorrência do ilícito administrativo. Essa demonstração, segundo o autor, "investe o Estado do dever de punir" (ABREU E SILVA, 2018, p. 32). No entanto, a própria abertura do processo deve ser fundamentada pela autoridade competente, recaindo sobre esta o ônus da prova, ou o estabelecimento da verdade material sobre a conduta do administrado, que justifique o peso das obrigações – decorrentes do próprio exercício do direito de ampla defesa – a ele impostas pela simples existência do processo.

Essa necessidade de orientar e fundamentar o gestor no exercício do poder, ou dever, sancionador deu causa à criação de inúmeras unidades de inteligência no âmbito administrativo. Órgãos como as agências reguladoras, a Receita Federal do Brasil e o Cade, cuja missão institucional inclui a tutela de interesses coletivos específicos, se utilizam dessas unidades para identificar, colher e analisar informações, fornecendo insumos para que, através do devido processo legal, se busque efetivamente punir as infrações no âmbito de sua competência administrativa.

Há, ainda, casos singulares como a unidade de inteligência da Agência Nacional de Vigilância Sanitária, cuja atuação é imprescindível para o cumprimento do mandato daquela Agência na vigilância e defesa sanitária e epidemiológica, especialmente no monitoramento e controle de vetores e riscos iminentes à saúde. Outro exemplo é a unidade de inteligência estratégia da Secretaria de Defesa Agropecuária, do

Ministério da Agricultura Pecuária e Abastecimento, responsável pelo monitoramento de riscos fito e zoossanitários, e pelo assessoramento do Secretário em sua participação no âmbito do Sistema Internacional de Vigilância Agropecuária.

A LGPD não ignora a existência dessas unidades, nem mesmo a existência de cooperação internacional no âmbito de suas atividades. Por isso mesmo, no seu art. 33, ao dispor sobre a transferência internacional de dados pessoais, inclui entre os casos permitidos, aqueles "quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional".

Aqui, a LGPD não restringe a atividade de inteligência à persecução penal, à segurança pública ou à defesa nacional. O texto reconhece, portanto, ainda que tacitamente, a existência de órgãos públicos de inteligência em âmbito administrativo. Mesmo assim, houve a opção legislativa de restringir a escusa aos pesados encargos da Lei, como discutido anteriormente, apenas à atividade cuja finalidade seja a segurança pública, a defesa nacional, a segurança do Estado ou a investigação e repressão de infrações penais.

3.1 Desafios identificados

Estabelece-se aí, aparentemente, um conflito: de um lado, a genuína preocupação do legislador em resguardar a privacidade e a dignidade da pessoa natural, vedando inclusive ao Estado a capacidade de limitar sua autodeterminação informativa. De outro, a igualmente genuína necessidade da sociedade de monitoramento e pronta reação do Estado a riscos à saúde, às infrações à ordem econômica e a toda sorte de infrações, no âmbito administrativo, que trazem dano a todo o corpo social.

Sob a égide dos princípios da Legalidade e da Eficiência, não pode o gestor público furtar-se de atender ao mandamento legal. Pelo contrário, cabe-lhe identificar, planejar e implementar as alterações necessárias a fim adequar procedimentos, sistemas, instrumentos e arranjos institucionais ora existentes à norma que passa a viger, garantindo a manutenção e melhoria da eficiência de sua atuação.

3.1.1 O direito de acesso aos dados

O primeiro risco a ser considerado é o de que os custos decorrentes do direito ao acesso inviabilize a infraestrutura requerida pelas ações de inteligência. O Cade faz uso, por exemplo, de diversas bases de dados referentes a compras governamentais públicas da União, bem como de vários Estados e Municípios. Só o sistema pregões eletrônicos da União representa um acervo de cerca de 150 milhões de lances, com mais de 1 milhão de pessoas naturais registradas, como representantes ou sócios das pessoas jurídicas com as quais a União realiza negócios.

Se essas pessoas exercerem o simples direito de acesso simplificado aos dados, a infraestrutura do Cade não seria capaz de suportar a demanda e as bases seriam, forçosamente, abandonadas. Mesmo que o Cade cesse sua atuação como operador do tratamento, e passe a demandar o mesmo tipo de análise que hoje realiza de outro órgão, sua qualidade de controlador (ou seja, demandante do tratamento de dados) ainda o obrigaria a conceder o acesso aos dados.

Há também o risco de que o acesso aos dados diminua a potência ou o alcance da atuação sancionadora. Há incentivos claros para que, com a entrada em vigor da LGPD, empresários e administradores de empresas potencialmente envolvidas em infrações à ordem econômica, passem a buscar saber se há tratamento de seus dados. Esse tipo de conhecimento pode incentivar alterações ou tentativas de camuflagem de condutas, degradando o poder e o alcance do trabalho de inteligência do Cade.

3.1.3 O direito de informação sobre compartilhamento

Há também um risco associado à cooperação entre unidades de inteligência. O direito de acesso a informações detalhadas sobre o compartilhamento de bases de dados e sobre a participação de cada agente na trilha de tratamento de dados pode representar um desincentivo à cooperação.

Além disso, há o risco de que acordos de cooperação técnica firmados antes da vigência da LGPD possam ser considerados nulos, por vício de legalidade, ou precisem ser revistos, de forma que as partes passem a oferecer garantias recíprocas de atendimento às exigências da LGPD, inclusive em relação ao estabelecimento de um encarregado por parte de cada instituição.

3.1.3 O direito de oposição ao tratamento

Outro risco a ser considerado é a possibilidade de que uma falha no cumprimento dos termos da LGPD possa dar causa ao exercício do direito de oposição por parte dos titulares. Conforme discutido anteriormente, o § 2º do art. 18 dá ao titular a capacidade opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento.

Note que a LGPD traz uma lista extensa de mandamentos, tais como a obrigação de seja indicado um encarregado pelo tratamento de dados pessoais (art. 23. II; art. 41); a obrigação de estruturar os sistemas para atender aos requisitos e princípios gerais da LGPD (art. 49); a obrigação de implantar um programa de governança em privacidade (art. 50, § 2º, I); a obrigação de demonstrar a efetividade desse programa (art. 50, § 2º, I); entre outras obrigações para as quais boa parte das organizações públicas ainda não está preparada. E o descumprimento de quaisquer dessas obrigações torna o tratamento de dados desconforme e, portanto, oponível, nos termos da lei.

3.1.4 A possibilidade de ação de tutela coletiva

O risco do exercício do direito de oposição é potencializado pelo fato de que a LGPD admite a tutela coletiva dos direitos individuais homogêneos ali expressos. O art. 22 é claro, ao afirmar que a defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente.

De acordo com Roque (2019), “não é difícil imaginar, nessas circunstâncias, que diversas ações coletivas venham a ser ajuizadas com amparo na LGPD”. Ainda de acordo o autor, ações coletivas em matéria de tutela de dados pessoais podem, em tese, envolver uma grande diversidade de pedidos.

Os legitimados coletivos, em especial o Ministério Público e a Defensoria Pública, podem pleitear, além da remoção de dados, a reparação de dano material e moral e até mesmo a tomada de providências de ordem estrutural, de forma a bloquear toda atividade que envolva o tratamento de dados até que a Administração tenha adequado seus sistemas e procedimentos aos requisitos da LGPD.

3.1.5 A ação da ANPD

Existem, no texto da LGPD, mais de 40 hipóteses de atuação da Autoridade Nacional de Proteção de Dados. A maior parte delas se aplica à Administração Pública e também pode afetar a atuação dos órgãos de inteligência. Além da competência sancionadora, presente nos arts. 52 a 54, a ANPD tem poder normativo, especialmente quanto ao que dispõe o art. 55-J.

À ANPD compete elaborar a Política Nacional de Proteção de Dados e da Privacidade; dispor sobre as formas de publicidade das operações de tratamento de dados; editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade; e deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos.

Isso significa que o gestor deve manter constante vigilância a fim de adequar quaisquer processos e atividades que incluam o tratamento de dados pessoais aos instrumentos normativos emitidos pela ANPD. Como há uma gama muito grande de competências e de hipóteses de iniciativa normativa da ANPD, há um risco acentuado de desconformidade.

Do ponto de vista da disciplina de manutenção dos sistemas de informação que dão suporte à atividade inteligência, o risco de desconformidade com normativos emitidos pela ANPD implica também a necessidade de planejar e executar auditorias e revisões periódicas dos sistemas.

4 Possíveis impactos na atuação do Cade

Os riscos descritos na seção anterior aplicam-se, em maior ou menor medida, a qualquer unidade de inteligência atuando no âmbito administrativo. Há, no entanto, algumas questões que têm maior relevância para a atuação do Cade.

Além de decidir sobre a subsistência dos indícios e provas produzidos em sede de procedimento preparatório, à Superintendência-Geral do Cade também compete a instauração e instrução do processo administrativo para imposição de sanções administrativas por infrações à ordem econômica, procedimento para apuração de ato de concentração, processo administrativo para análise de ato de concentração econômica e

processo administrativo para imposição de sanções processuais incidentais instaurados para prevenção, apuração ou repressão de infrações à ordem econômica.

Para cumprir esse mandato legal, no interesse da instrução dos diversos tipos processuais, a Lei 12.529/2011 também confere à SG a capacidade de requerer documentos e informações; realizar diligências; requisitar vista e cópia de documentos e objetos constantes de inquéritos e processos administrativos instaurados por órgãos ou entidades da Administração Pública Federal e requerer vista e cópia de inquéritos policiais, ações judiciais de quaisquer natureza, bem como de inquéritos e processos administrativos instaurados por outros entes da federação, devendo o Cade observar as mesmas restrições de sigilo eventualmente estabelecidas nos procedimentos de origem.

4.1 Possível conflito entre normas

Dessa forma, no âmbito do Cade, se amplifica o impacto associado ao direito de acesso e de informação, que assiste ao titular, acerca do compartilhamento de seus dados pessoais. Evidentemente, como autoridade de abrangência nacional em matéria concorrencial, o Cade se comunica e interage com Ministérios Públicos e Polícias, tanto no âmbito Federal, quanto dos Estados.

Além do acesso a inquéritos policiais, ações judiciais de quaisquer natureza, bem como de inquéritos e processos administrativos instaurados pela União e por outros entes da federação, o Cade também firma acordos de cooperação técnica, que incluem tanto o compartilhamento de esforços e expertise de inteligência, análise e investigação, quanto de bases de dados compartilhadas no âmbito de operações conjuntas.

A Lei 12.529/2011 é clara ao determinar que, nestes casos, o Cade deve conferir às informações compartilhadas o mesmo nível de sigilo empregado na origem. Ora, os Ministérios Públicos e Polícias estão livres, como discutido anteriormente, da obrigação de informar o titular de dados pessoais acerca da existência de tratamento ou mesmo do compartilhamento desses dados. O Cade, por não atuar no escopo de atividades escusadas pela LGPD, em princípio, seria, por um lado, obrigado pela LGPD a prestar essas informações e, por outro, proibido pela Lei 12.529/2011 de fazê-lo.

A solução jurídica ainda não é clara, mas esse pode ser um caso em que o disposto em matéria de procedimento de persecução penal seja aplicado, por extensão ou analogia, à persecução no âmbito administrativo.

4.3 Práticas de cooperação internacional

Além de representar o Brasil no âmbito de organizações internacionais e acordos bilaterais de cooperação, o Cade também mantém uma participação em fóruns internacionais de proteção concorrencial como o Comitê de Concorrência da OCDE e a International Competition Network. Essas organizações são exemplos de *soft law* internacional. Ou seja, são mecanismos multilaterais que não possuem jurisdição ou caráter vinculativo, e cuja efetividade depende da articulação entre seus membros.

Além do trabalho institucional, produzindo estudos e *guidelines*, esses fóruns promovem uma cooperação, de certo modo, informal, onde representantes das autoridades de defesa da concorrência passam a conhecer formas de atuação, casos de sucesso e desafios enfrentados em outras jurisdições. Esse tipo de comunicação dá origem, em muitas ocasiões, à troca de experiências e opiniões acerca de casos e investigações específicos. No Processo Administrativo 08012.000820/2009-11 (conhecido na literatura como “Caso dos Compressores”), por exemplo, houve troca de informações que levou a uma ação de busca e apreensão coordenada em diversos países.

O risco que se vislumbra é o de que, sabendo da obrigação da autoridade brasileira de revelar o tratamento ou troca de dados, os parceiros internacionais passem a evitar o envolvimento do Brasil em ações coordenadas dessa natureza.

4.2 Possíveis estratégias de mitigação dos riscos

Os riscos associados à presença de potencial conflito entre normas podem ser mitigados por meio de consultas específicas à Advocacia Pública, não afastado, evidentemente, possível controle jurisdicional. No entanto, independente da solução aplicada ao caso concreto, a autoridade pública deve resguardar-se, tomando todas as medidas à disposição no intuito de garantir a segurança e a proteção da privacidade dos dados pessoais sob sua custódia.

Quanto aos riscos associados à provável alteração de comportamento dos administrados, uma vez amparados pelos dispositivos da LGPD, é preciso realizar uma análise minuciosa para identificar medidas mais precisas de probabilidade e volume de requisições de acesso aos dados. De toda sorte, é importante planejar e preparar os sistemas e as configurações de infraestrutura de telecomunicações, de acordo com os padrões mais recentes de provisionamento sob demanda e monitoramento da capacidade de serviços, para garantir sua robustez frente a elevações repentinas ou sazonais nos níveis de demanda.

O § 4º do art. 17 admite a negativa a pedidos de acesso, revisão ou eliminação de dados, desde que o controlador emita resposta indicando as razões de fato e de direito que impedem a adoção da providência requerida. Uma medida válida de contingência é o levantamento, sob orientação de consultoria jurídica competente, de impedimentos de ordem técnica, orçamentária e legal, inclusive de tratados e acordos internacionais, que justifiquem a negativa de atendimento às possíveis requisições. Esse levantamento pode dar base à redação de respostas que possam ser apresentadas de maneira homogênea para o não atendimento aos diversos tipos de requisição. Esse tipo de medida é especialmente relevante no contexto de ações de cooperação internacional.

Quanto aos riscos de desconformidade, o gestor deve prevenir-se, garantindo sempre disponibilidade orçamentária e de pessoal qualificado para a execução de ações de auditoria de conformidade e revisão evolutiva ou corretiva das ferramentas e processos.

Conclusão

A Lei Geral de Proteção de Dados introduziu importante disciplina no ordenamento jurídico, regulando o tratamento de dados pessoais e resguardando os direitos da pessoa natural à liberdade e ao livre desenvolvimento de sua personalidade, num contexto de crescentes complexidades introduzidas por novas tecnologias e novas modalidades de exploração econômica e política da informação.

Os direitos e obrigações introduzidos pela LGPD, como demonstrado acima, repercutem na atividades de inteligência de Estado, trazendo riscos à

continuidade e à viabilidade daquelas atividades que dependem do tratamento de pessoas físicas. Por isso, o gestor público deve reagir às novas condições impostas pelas vigência desta Lei, alterando o planejamento, o desenho e a execução das ações sob sua responsabilidade a fim de garantir sua conformidade e continuidade.

O Cade, em especial, desenvolve atividades de inteligência que dependem do uso de bancos de dados compartilhados com outros órgãos de inteligência e com órgãos de persecução penal. Há riscos, discutidos na seção anterior, de ordem jurídica e de ordem operacional, que podem acarretar a interrupção de tais atividades. Por isso, recomenda-se a auditoria dos processos e ferramentas empregados nessas atividades para garantir, em tempo, e no que for possível, sua conformidade com os preceitos da LGPD.

Por fim, destaca-se a necessidade de investigações mais profundas acerca do amparo jurídico, à luz das obrigações introduzidas pela LGPD, da interação e compartilhamento de dados entre órgãos escusados por aquela Lei e órgãos atingidos por tais obrigações, e da cooperação internacional entre autoridades de defesa da concorrência.

Referências

ABREU E SILVA, M. L. **O ônus da prova no processo administrativo sancionador**. 201p. 2018. Dissertação (Mestrado em Direito). Pontifícia Universidade Católica de São Paulo (PUC-SP), São Paulo, 2018.

AMORIM, S.; BOULLOSA, R. F. O estudo dos instrumentos de políticas públicas: uma agenda em aberto para experiências de migração de escala. **Amazônia, Organizações e Sustentabilidade**, v. 2, n. 1, p. 59-69, 2013.

BRASIL. Câmara dos Deputados. **Projeto de Lei 4060/2012**. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em: https://camara.leg.br/pplen/destaque.html?codProposicao=548066. Acesso em: 22 jun. 2020. Texto Original.

BRASIL. **Lei nª. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados. Brasília, DF: Presidência da República, [2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 21 jun. 2020.

CENTRAL INTELLIGENCE AGENCY (Estados Unidos da América). The Center Of Intelligence. **The Work of a Nation**. Washington DC: 2009.

CEPIK, M. A. C. **Espionagem e democracia**. Rio de Janeiro: FGV, 2003.

DONEDA, D. & MENDES, L. S. Um perfil da nova Lei Geral de Proteção de Dados brasileira. *In:* BELLI, L. & CAVALLI, O. **Governança e regulações da internet na América Latina**. Rio de Janeiro: FGV, 2019. p. 325-343.

MACIEL, R. & PINHEIRO, M. K. (2014). O conhecimento na Inteligência de Estado. **Datagramazero - Revista de Ciência da Informação**, São Paulo, v. 9, n. 2, 2014.

MENDONÇA, F. G. O direito à autodeterminação informativa: a (des)necessidade de criação de um novo direito fundamental para a proteção de dados pessoais no Brasil. *In* SEMINÁRIO INTERNACIONAL DE DEMANDAS SOCIAIS E POLÍTICAS PÚBLICAS NA SOCIEDADE CONTEMPOR NEA, IX, Santa Cruz do Sul, 2014. **Anais...** Universidade de Santa Cruz do Sul, Santa Cruz do Sul, 2014.

MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO. Secretaria de Logística e Tecnologia da Informação. **Sanções Administrativas: Diretrizes para formulação de procedimento administrativo específico**. Brasília, 2015.

PEREIRA, C. V. **A atividade de Inteligência como instrumento de eficiência no exercício do controle externo pelo Tribunal de Contas da União**. 2009. 91 f. Monografia (Especialização) Inteligência de Estado e Inteligência de Segurança Pública com Inteligência Competitiva - Centro Universitário Newton Paiva / Escola Superior do Ministério Público de Minas Gerais, Belo Horizonte, 2009.

QUINTIERE, V. M. Questões controversas envolvendo a tutela jurisdicional penal e as novas tecnologias à luz da Lei Geral de Proteção de Dados (LGPD) brasileira: dataveillance. **Revista ESMAT**, v. 11, n. 17, p. 175-188, 17 set. 2019.

ROQUE, A. A tutela coletiva dos dados pessoais na Lei Geral de Proteção de Dados Pessoais (LGPD). **Revista Eletrônica de Direito Processual - REDP**. 20(2), 1-19. Disponível em https://www.e-publicacoes.uerj.br/index.php/redp/article/view/42138. Acesso em: 25 jun. 2020.

TEFFÉ, C. S. de; VIOLA, M. (2020). Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **civilistica.Com**, 9(1), 1-38. Disponível em: http ://ebooks.pucrs.br/edipucrs/projetosdeflosofa.pdf. Acesso em: 21 jun. 2020.

Bacharel em Ciência da Computação (UnB, 2008), Especialista em Inteligência Estratégica (Faculdade AVM, 2015) e Mestre em Engenharia Elétrica (UnB, 2016). Tem mais de vinte anos de experiência no serviço público, tendo atuado como analista de sistemas, com foco em segurança da informação, no Tribunal Regional Federal da 1ª Região e no Superior Tribunal Militar, e como Analista de Planejamento e Orçamento na Secretaria de Orçamento Federal. Como parte de sua pesquisa de mestrado, desenvolveu, em cooperação com a Diretoria de Atenção Básica à Saúde do Ministério da Saúde, um protótipo de Registro Eletrônico em Saúde baseado em criptografia homomórfica e com preservação de ordem para permitir a extração de medidas estatísticas do Registro Eletrônico em Saúde Nacional sem a quebra da privacidade dos pacientes. Atualmente, como candidato ao título de Doutor em Engenharia Elétrica, no Departamento de Engenharia Elétrica da Universidade de Brasília, desenvolve pesquisas relacionadas à utilização de protocolos de criptografia homomórfica e de computação segura de múltiplas partes para a criação de modelos de aprendizado de máquina com garantias formais de privacidade.

Stefano Mozart Pontes Canedo de Souza

Mestre em Engenharia Elétrica (2016). Analista de Planejamento e Orçamento.
stefano.souza@cade.gov.br.