Instituto Rui Barbosa
www.irbcontas.org.br
A Casa do Conhecimento dos Tribunais de Contas

ANEXO

O presente documento é parte integrante da Nota Técnica nº 01/2019.

O Instituto Rui Barbosa criou, em setembro de 2019, um Grupo de Estudos sobre a Lei Geral de Proteção de Dados Pessoais – LGPD –, composto de forma multidisciplinar[1], com representantes e colaboradores de diversos Tribunais de Contas do País.

Como resultado dos trabalhos realizados, foram apresentadas premissas e diretrizes na Nota Técnica nº 01/2019, cujos fundamentos legais e doutrinários estão expostos neste documento.

Registra-se que este trabalho não tem o objetivo de esgotar o tema ou de substituir a necessária análise que os Tribunais de Contas deverão realizar com relação aos tratamentos de dados pessoais e às distintas bases sob sua gestão. No entanto, pretende servir como um ponto de partida para esse exercício e como um instrumento de conscientização quanto à necessidade de realizar, efetivamente, a gestão e a governança dos dados pessoais.

[1] Foram designados membros do Comitê Técnico de Processo, Súmula e Jurisprudência (Rede JurisTCs), do Comitê Técnico de Gestão da Informação (Rede BIBLIOCONTAS) e da Rede INFOCONTAS (ATRICON).

1 CONSIDERAÇÕES INICIAIS

Em 14 de agosto de 2018, foi sancionada a Lei nº 13.709, Lei Geral de Proteção de Dados Pessoais – LGPD –, visando à regulação "do tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, determinando que suas normas gerais são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios" (artigo 1º, parágrafo único).

A referida normativa apresenta os princípios da boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas (artigo 6º).

O tema proteção de dados pessoais não é novo no ordenamento jurídico brasileiro; mesmo antes da publicação da LGPD, várias legislações já faziam referência à necessidade de garantir a proteção de dados pessoais, com abordagens tanto de forma direta quanto indireta.

O texto da Constituição Federal de 1988 trata, no Título II, dos "Direitos e Garantias Fundamentais", dentre os quais se encontram os direitos à intimidade, à vida, à privacidade, à igualdade, à liberdade e ao acesso à informação.

Em que pese a Constituição Federal de 1988 não disciplinar de forma específica a matéria de proteção de dados eletrônicos, em virtude de ser anterior à expansão da Internet como meio de disseminação de informação, o texto constitucional apresenta os fundamentos que objetivam a proteção de dados

pessoais, e trata de um instituto que se aproxima da concepção atual referente à guarda de informações pessoais, qual seja, o *Habeas Data*[2].

No entanto, consoante a explicação de Limberger (2007, p. 81), a aplicabilidade do *Habeas Data* limita-se à proteção de dados pessoais na esfera pública, "pois ele permite apenas que o indivíduo tenha acesso a informações em bancos de dados governamentais ou de caráter público, sendo prejudicada qualquer pretensão quanto o acesso a bancos de dados privados".

Em consonância com a Carta Magna, foi sancionada a Lei nº 8.070, em 11 de setembro de 1990 (Código de Defesa do Consumidor – CDC), que dispõe sobre a proteção do consumidor, disciplinando questões relacionadas aos bancos de dados. Especificamente em seu artigo 43[3], garante ao consumidor o direito de obter informações próprias contidas nos cadastros, fichas, registros e dados pessoais e de consumo arquivados, bem como sobre as suas respectivas fontes.

Em 2002, foi aprovado o Código Civil Brasileiro pela Lei nº 10.406, o qual contém um capítulo específico para tratar dos direitos à personalidade dos indivíduos, além de outros dispositivos que tratam da proteção ao direito à privacidade e à intimidade. Dentre as disposições, destacam-se o artigo 11[4], o qual prevê que os direitos da personalidade são intransmissíveis e irrenunciáveis, e o artigo 21, que consagra que a vida privada da pessoa natural é inviolável[5].

---

[2] Art. 5 º, inciso LXXII - conceder-se-á habeas data: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;

[3] Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

[4] Art. 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.

[5] Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

Por seu turno, transparência na atuação da administração pública constitui elemento fundamental para que os cidadãos possam, além de fiscalizar a aplicação dos recursos públicos, participar da gestão, por meio do controle social.

Por determinação da Constituição Federal de 1988, todo cidadão tem o direito ao livre acesso à informação e a receber dos órgãos públicos informações de interesse particular, coletivo ou geral, conforme previsto pelos artigos 5º, incisos XIV[6] e XXXIII[7], 37, §3º, inciso II[8], e 216, §2[9].

Objetivando regulamentar tais direitos, foi sancionada a Lei nº 12.527, de 18 de novembro de 2011, denominada Lei de Acesso à Informação – LAI –, à qual estão subordinados, entre outros, todos os órgãos públicos integrantes da administração direta dos Poderes Judiciário, Executivo e Legislativo, incluindo as Cortes de Contas e o Ministério Público. Segundo Fortes (2016, p. 56), foi a primeira norma jurídica contemporânea recepcionada no contexto da Internet, tendo sido editada com o objetivo de "garantir o direito fundamental de acesso à informação, aliado a princípios da administração pública, como observância da publicidade para divulgação de informações de interesse público através de meios proporcionados pela Internet". Tal direito à informação tem a finalidade de fortalecer a democracia e a participação do povo na política.

A LAI representa um avanço normativo quanto à regulamentação de dados pessoais e ao direito digital no Brasil, trazendo em seu bojo conceitos para interpretação da lei, dentre elas a definição de "informação", "informação sigilosa", "informação pessoal" e "tratamento da informação". Além disso, obriga a

---

[6] Art. 5º XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;

[7] Art. 5º XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado;

[8] Art. 37 § 3º A lei disciplinará as formas de participação do usuário na administração pública direta e indireta, regulando especialmente: [...] II - o acesso dos usuários a registros administrativos e a informações sobre atos de governo, observado o disposto no art. 5º, X e XXXIII;

[9] Art. 216 § 2º Cabem à administração pública, na forma da lei, a gestão da documentação governamental e as providências para franquear sua consulta a quantos dela necessitem.

administração pública a tratar os dados pessoais de forma transparente, respeitando os direitos fundamentais de intimidade, vida privada, honra e imagem dos indivíduos.

Objetivando tipificar os delitos praticados no âmbito da Internet, foi aprovada a Lei nº 12.737, em 30 de novembro de 2012, conhecida popularmente como Lei de Crimes Cibernéticos, alterando o Código Penal Brasileiro. Segundo VIANA *apud*, FORTES (2018, p.39) o "legislador passou a dar maior proteção aos dados pessoais, caracterizando como crime a invasão de dispositivos informáticos para obter, adulterar ou destruir dados sem autorização do titular".

Em 23 de abril de 2014, foi sancionada a Lei nº 12.965 – Marco Civil da Internet –, consagrando os princípios, as garantias, os direitos e os deveres para fins de utilização da Internet; garantindo a liberdade de expressão, comunicação e manifestação de pensamento, a proteção da privacidade e dos dados pessoais, a preservação da estabilidade, segurança e funcionalidade da rede e a responsabilização dos agentes de acordo com suas atividades; e estabelecendo regras típicas de proteção de dados pessoais.

Igualmente, em decorrência desse cenário de evolução tecnológica e digital, adveio a aprovação, em 2018, da LGPD, a qual, além de dispor sobre o tratamento de dados pessoais, também alterou dispositivos do Marco Civil da Internet.

Após, foi publicada a Medida Provisória nº 869, de 27 de dezembro de 2018, promovendo alterações na redação de alguns artigos da LGPD; modificando pontos considerados incompletos, com o objetivo de promover melhorias no texto, dentre as quais se destacam aquelas referentes às hipóteses de dados sensíveis relacionados à saúde, à regulação da Autoridade Nacional de Proteção de Dados – ANPD – e ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade – CNPDP.

Ao final, adveio a Lei nº 13.853, de 08 de julho de 2019, que introduziu mudanças significativas na LGPD, e que foi originada nas discussões sobre a aprovação da MP nº 869/2018. Entre as principais alterações destacam-se a criação

da ANPD e a exclusão da obrigatoriedade de informar o titular de dados nos casos de tratamento de dados pessoais para cumprimento de obrigação legal ou regulatória ou quando efetuado pela administração pública, para execução de políticas públicas previstas em normas ou contratos.

No que diz respeito à abrangência, a aplicação da LGPD se estende a qualquer pessoa jurídica de direito público ou privado que tenha estabelecimento no Brasil ou que ofereça produtos ou serviços no mercado de consumo brasileiro (artigo 3º). Além disso, ao dispor em capítulo específico sobre sua aplicação no setor público, menciona os Tribunais de Contas ao referenciar as disposições previstas no artigo 1º da LAI[10].

Diante disso, tem-se que a aplicação da LGPD trará reflexos para os Tribunais de Contas tanto na execução de seus processos internos (administrativos) quanto no desempenho de suas atividades finalísticas. Não obstante, sua interpretação e aplicação deverão ser feitas em consonância com o aparato jurídico e constitucional já existente, sem retroceder em termos de publicidade, transparência e acesso à informação.

[10] Art. 1. Parágrafo único. Subordinam-se ao regime desta Lei: I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, **incluindo as Cortes de Contas**, e Judiciário e do Ministério Público.

2 CONCEITOS E PRÉ-REQUISITOS ESTRUTURANTES PARA O ATENDIMENTO DA LGPD

Realizada a contextualização geral do tema, passa-se a abordar, neste tópico, alguns conceitos e pré-requisitos estruturantes, os quais necessitarão ser compreendidos e trabalhados pelos Tribunais de Contas de forma preliminar à aplicação da LGPD.

2.1 CONCEITOS

Conforme previsto no artigo 5º da LGPD, para sua interpretação e aplicação devem ser considerados os conceitos abaixo, transcritos em razão da sua relevância, contudo, sem o objetivo de esgotar seu detalhamento ou explicação:

> 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;
>
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
>
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
>
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
>
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
>
> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
>
> IX - agentes de tratamento: o controlador e o operador;

X - tratamento: 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;

XI - anonimização: 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;

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XVII - relatório de impacto à proteção de dados pessoais: documentação 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;

XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e

XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

2.2 PRÉ-REQUISITOS ESTRUTURANTES

O uso da tecnologia da informação e das técnicas de tratamento de dados tem sido cada vez mais explorado pelos Tribunais de Contas como instrumento para o exercício de suas funções legais e constitucionais de forma mais efetiva e eficiente.

Nesse contexto, os deveres de transparência e de acesso à informação proativa, associado ao regime jurídico existente sobre direito à privacidade, já exigiam dos órgãos públicos uma série de medidas de controle e de auto-organização.

Frente a isso, investir em temas relacionados à gestão de processos, gestão de riscos, segurança da informação e classificação da informação mostra-se ainda mais relevante com o advento da LGPD.

2.2.1 Gestão de Processos

A Gestão de Processos engloba o estudo do trabalho, que é o processo de observação e levantamento de informações de um fenômeno, objetivando detalhar sua lógica de funcionamento. A partir disso, busca-se o entendimento do trabalho para compreender suas particularidades e entender sua lógica de existência.

Partindo da premissa de que as necessidades são muitas e os recursos são escassos, as organizações públicas, entre as quais os Tribunais de Contas, devem priorizar ações e otimizar recursos para alcançar melhores resultados. A readequação da estrutura administrativa e a redução do gasto público são desafios importantes à manutenção dos serviços públicos. (SANTA CATARINA, 2018)

Para enfrentar esses desafios, é necessário valer-se de modelos de governança corporativa mais eficientes. Nesse sentido, as constantes inovações tecnológicas, somadas à intensificação do uso de Big Data nas organizações do mundo todo, trouxeram uma nova roupagem ao gerenciamento dos negócios,

marcando a transformação dos modelos de governança corporativa[11].

Ainda nessa mesma esteira, adveio a Lei Federal nº 13.726/2018, a qual disciplina a racionalização dos atos e procedimentos administrativos dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios[12].

Com o objetivo de aumentar a capacidade do Governo em prestar melhores serviços à sociedade e, baseado na ideia de que um Estado eficiente busca o gerenciamento consciente dos processos e dos recursos, tem-se discutido sobre modelos de governança. Esses conceitos podem ser aplicados, também, no âmbito dos Tribunais de Contas, especialmente neste momento, em que se está a tratar da implantação da LGPD.

Com essa iniciativa, o poder público pretende enxergar amplamente seu negócio a partir da visão da sociedade, ou seja, da expectativa dos cidadãos em relação aos serviços públicos prestados. Nessa perspectiva, as instituições públicas poderão identificar ações ligadas à desburocratização e à melhoria de processos a partir de uma cultura organizacional baseada no princípio de que o serviço público existe para servir, ser útil e ser um facilitador da sociedade. (SANTA CATARINA, 2018)

A modelagem de processos de negócio (BPM – Business Processes Management) corresponde a um sistema integrado de gestão de desempenho de negócios voltado para a Gestão de Processos de negócio ponta a ponta. (PEREIRA, Mariléa, 2017)

---

[11] Seguindo essa tendência, foi editado o artigo 5º, inciso XIII, da Lei Federal nº 13.460/2017.
Art. 5º O usuário de serviço público tem direito à adequada prestação dos serviços, devendo os agentes públicos e prestadores de serviços públicos observar as seguintes diretrizes:
[...] XIII - aplicação de soluções tecnológicas que visem a simplificar processos e procedimentos de atendimento ao usuário e a propiciar melhores condições para o compartilhamento das informações.

[12] Art. 7º É instituído o Selo de Desburocratização e Simplificação, destinado a reconhecer e a estimular projetos, programas e práticas que simplifiquem o funcionamento da administração pública e melhorem o atendimento aos usuários dos serviços públicos. Parágrafo único. O Selo será concedido na forma de regulamento por comissão formada por representantes da Administração Pública e da sociedade civil, observados os seguintes critérios: I - a racionalização de processos e procedimentos administrativos.

Ao falar em resultados, deve-se ter em mente que esses são produtos diretos de processos de negócios, os quais correspondem ao sequenciamento de atividades que ocorrem em conjunto. Quando uma dessas atividades não ocorre como o esperado ou não funciona muito bem, o processo de negócio como um todo acaba falhando. Cada atividade pode ser tratada e analisada individualmente, sem detrimento das demais. Analisando-se resultados, adaptando-se situações e corrigindo pequenas atividades, as melhorias no processo como um todo podem ser sempre aperfeiçoadas. (BROCKE, 2013)

Os Tribunais de Contas diariamente realizam atividades finalísticas e administrativas (processos internos), e ambas devem ser mapeadas e avaliadas na busca de uma administração mais célere e preditiva. (PEREIRA, Wallace, 2017)

Dentre os objetivos da implantação da Gestão de Processos nos Tribunais de Contas, tanto para a área administrativa quanto para a área finalística, tem-se: (SANTA CATARINA, 2013)

- A criação de Fluxos Processuais distintos a partir da estratificação dos processos de negócio;
- Para cada Atividade mapeada, identificar a qual Fluxo de Processo pertence, quais são os possíveis estados comportamentais que podem ser a ela atribuído e, quais os tipos de documentos que por ela são entregues a outras Atividades subsequentes;
- Criar regramentos a partir das tarefas a serem realizadas, por cada Atividade encontrada, a fim de que haja o correto sequenciamento entre as mesmas, fazendo com que os Fluxos de Processos não colidam ou não se sobreponham;
- Possibilitar a pró-atividade nas tarefas que demandam mais esforços para que haja diminuição no tempo de resposta para com o seu jurisdicionado ou público interno;

- A partir do mapeamento prévio dos Fluxos de Processos, identificar, utilizando notação de raia, do BPM (BPM – Business Processes Management), qual o efeito em detrimento da celeridade na execução dos processos de negócio, em cascata, de uma tarefa não realizada;

- Com o regramento das Atividades, documenta-se as regras de negócio inerentes a cada Fluxo de Processo, mantendo a transparência da Gestão do Conhecimento (tácito e explícito);

- Identificar quais os gargalos que impedem a celeridade na integração das diversas ferramentas que norteiam a atuação, dos Tribunais de Contas, em suas Atividades diárias, possibilitando de forma prévia, a mitigar riscos;

- Conhecendo os Fluxos de Processos inerentes às áreas administrativas e finalísticas, e esses perpassando de forma holística pela instituição, levará a cada Tribunal de Contas o engajamento do trabalho colaborativo a seus servidores e jurisdicionados.

2.2.2 Gestão de Riscos

Para atender ao disposto na LGPD, é necessário que os Tribunais de Contas, enquanto controladores de dados, tenham conhecimento dos riscos que podem ser gerados às liberdades civis e aos direitos fundamentais quando realizarem processos de tratamento de dados pessoais.

Conforme preconizado pelo Decreto nº 9.203, de 22 de novembro de 2017, o qual estabelece princípios, diretrizes e mecanismo de governança na administração pública federal, considera-se gestão de risco:

> o processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos.

João Batista Ribas de Moura (2018, p. 42) define:

> O entendimento do conceito de risco, embora pareça trivial, não raras vezes, leva a estratégias errôneas e a retrabalhos quando mal interpretado. A palavra “risco” deriva do italiano antigo risicare e significava ousar no sentido de o risco ser uma opção e não um destino cujos acontecimentos dependerem de sorte ou azar sem possibilidade de ações preventivas.

Segundo o Manual de Gestão de Riscos do TCU (BRASIL, 2018, p.18), a Gestão de Riscos tem como um dos seus princípios a aplicação de forma contínua e integrada aos processos de trabalho de uma instituição. Esses processos de trabalho, quando devidamente mapeados, geram as informações necessárias para subsidiar as seguintes etapas:

- Estabelecimento do contexto;
- Identificação dos riscos;
- Análise dos riscos;
- Avaliação dos riscos;
- Tratamento dos riscos;
- Comunicação e consulta com partes interessadas;
- Monitoramento;
- Melhoria contínua.

A construção de um processo de avaliação de riscos depende da obtenção de informações de qualidade na etapa de “identificação de riscos”, para produção de resultados verdadeiramente úteis aos gestores públicos. Preconiza-se a criação dos Fluxos de Processo com objetivo de servir como base para a produção de relatórios de reconhecimento de riscos mais completos e com credibilidade. (MOURA, 2018, p.42)

Os dois elementos constituintes das fontes de risco são: a ameaça e a vulnerabilidade. Ambos potencializam as chances de um evento afetar, negativamente, o alcance dos objetivos estratégicos de uma organização.

Num outro aspecto, a Gestão de Riscos revela a necessidade de identificar os níveis de risco: impacto e probabilidade que uma determinada atividade ou um conjunto de atividades (processo) podem afetar, negativamente, o alcance dos objetivos estratégicos da instituição. Aqui, mais uma vez, cabe lembrar que o mapeamento prévio dos Fluxos de Processo possibilita uma gestão proativa na mitigação de riscos.

Quando implementada e mantida segundo a ISO 31000:2009, a gestão dos riscos possibilita a uma organização:

- Melhorar a efetividade operacional;
- Aumentar a probabilidade de atingir os objetivos;
- Encorajar uma gestão proativa;
- Melhorar a identificação de oportunidades e ameaças;
- Melhorar a governança;
- Melhorar os controles.

Nesse contexto, a implantação adequada da LGPD exigirá que os Tribunais de Contas atentem para a gestão eficaz dos riscos relacionados à proteção dos dados pessoais, não apenas nas atividades do controle externo, mas na instituição como um todo.

2.2.3 Segurança da Informação

A LGPD exige que os organizações implementem medidas técnicas e administrativas apropriadas para garantir que os dados pessoais sejam processados de forma segura.

Dentre os princípios da Segurança da Informação, destacam-se 4 (quatro), que formam a base para os demais: Disponibilidade, Integridade, Confidencialidade e Autenticidade (ISO 27001:2013).

O processo organizacional de Segurança da Informação pode ser distribuído em 5 (cinco) pilares que sustentarão a prática dessa política pela instituição:

1º - Segregação de permissões e acesso:

- Limitar os usuários a acesso às informações da instituição, a fim de que tenham acesso somente àquilo que lhe é de interesse e de sua competência.
- Bloquear as ferramentas que possibilitam a saída das informações da instituição. Da mesma forma que é importante limitar o acesso a determinados arquivos, também é necessário que haja bloqueio de aplicativos, programas e sistemas que permitam a saída de informações da organização. O aumento exponencial de Nuvens Públicas disponíveis possibilita que os usuários consigam carregar milhares de arquivos em diferentes formatos. O envio e/ou recebimento externo de arquivos, muitas vezes, dificulta o correto tratamento das informações.

2º - Penetração e vulnerabilidade:

- Utilizar a automatização para atuar em tarefas de segurança, diminuindo os erros manuais. Criação de perfis e concessão de permissões a usuários são exemplos que podem ser automatizados;
- Criação de testes automatizados para penetração e vulnerabilidade;
- Separar os arquivos da rede que possuem dados mais relevantes e estratégicos da organização e, sobre eles, criar uma barreira diferenciada de proteção (criptografia, senhas ou mesmo firewalls, que limitem o tráfego nessa parte da rede);
- Reduzir a disseminação de sistemas de informação que tratam do mesmo objeto, dificultando o tratamento seguro dos dados dentro das instituições;
- Criptografar todas as informações em arquivos e banco de dados. Assim, caso haja um vazamento, o receptor da informação terá uma dificuldade

maior para o acesso aos dados originais.

3º - Monitoramento de acessos aos sistemas:

- Manter sempre os sistemas operacionais atualizados;
- Monitorar sistematicamente é imprescindível para que o colaborador que coordena a rede da instituição tenha uma visão geral sobre o que está acontecendo em todo sistema. O administrador da rede tem que ter a certeza de que está realizando uma varredura completa por toda área e que mantém um monitoramento constante e sistemático;
- Alinhar os Fluxos de Processos da instituição, administrativos e finalísticos, com as operações diárias em que as equipes de segurança atuam. Todos devem ter a ciência de que existem regras, que essas regras são para a segurança do negócio e que devem ser cumpridas. Dentre as vantagens desse alinhamento estão as possibilidades de melhorias a partir de feedbacks que podem surgir de outras áreas que não tenham relação com a área de Tecnologia da Informação;
- O próprio mapeamento das atividades inerentes a Segurança da Informação produzirá, ao longo do tempo, métricas e dados capazes de avaliar, gradativamente, o respectivo trabalho. Com os recursos financeiros escassos, esses indicadores são excelentes norteadores para as instituições canalizarem, da melhor forma, os seus orçamentos. A demonstração desses indicadores para alta gestão é muito importante para manter constante a política de Segurança da Informação;
- Caso a instituição já possua computação na nuvem, independentemente do fornecedor, deverá sempre habilitar todas as trilhas de auditoria e monitoramento para verificar possíveis ataques;
- Identificar sempre o direito de uso dos dados de terceiros. Além de manter a credibilidade com que cedeu as informações, a utilização dentro da instituição de um dado comprometido computacionalmente poderá gerar danos à rede corporativa.

4º - Instrumentalização jurídica:

● Criar normas de segurança dentro da instituição. Uma política de segurança da informação corporativa consistente permitirá que administradores de rede, pessoal de segurança em Tecnologia da Informação e outros técnicos possam entender as regras e aplicá-las na rede, colaborando também para a divulgação das mesmas entre os usuários.

5º - Capacitação continuada:

● Capacitar servidores e colaboradores. Muitas vezes os dados são roubados ou perdidos por pura inocência e falta de conhecimento de um usuário. As regras estabelecidas na política de segurança definem o que é ou não permitido no âmbito da instituição e, por isso, devem ser disseminadas e conhecidas pelos usuários.

Portanto, como boa prática de governança, é essencial que os Tribunais de Contas estabeleçam uma Política de Segurança da Informação. No que toca ao adequado cumprimento da LGPD, tal política deverá conter, ainda, regras claras relacionadas a incidentes de segurança[13] (artigo 46), bem como prever como se dará a comunicação à Autoridade Nacional de Proteção de Dados – ANPD – e aos titulares nos casos em que a sua ocorrência puder acarretar risco ou dano relevante (artigo 48).

2.2.4 Classificação da Informação

A classificação da informação, nas suas várias abordagens, pode ser considerada uma das boas práticas para governança de dados. Conforme a NBR

[13] Conforme consta no Guia da Lei nº 13.709/2018 voltado para o setor público elaborado pelo Instituto de Tecnologia e Sociedade (ITS Rio), "a LGPD não define incidente de segurança. O CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), mantido pelo Comitê Gestor da Internet no Brasil (CGI.br), grupo responsável por receber, analisar e responder a incidentes de segurança em computadores, envolvendo redes conectadas à Internet brasileira, define incidente de segurança como "qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores".

ISO 27001[14], a classificação da informação tem por objetivo “assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização”, sendo, além da gestão de riscos, um dos controles necessários para a implementação de um Sistema de Gestão da Segurança da Informação (SGSI)[15].

Os Tribunais de Contas produzem e recebem dados e informações que são essenciais ao exercício de suas competências constitucionais, legais e regulamentares. Tais dados e informações são considerados um dos principais ativos da instituição, devendo permanecer íntegros, disponíveis e, quando for o caso, com o sigilo resguardado ou o acesso restrito.

De acordo com a cartilha sobre classificação da informação editada pelo Tribunal de Contas da União (BRASIL, 2010), as informações são classificadas conforme a:

> **confidencialidade**: garantia de que somente pessoas autorizadas tenham acesso às informações armazenadas em algum local ou transmitidas por meio de redes de comunicação;
>
> **disponibilidade**: garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, durante o período definido pelos gestores da informação;
>
> **integridade**: garantir a não-violação das informações com intuito de protegê-las contra alteração, gravação ou exclusão acidental ou proposital. Evitar que a informação seja apagada ou alterada de qualquer forma sem a permissão do gestor.

[14] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013a, p. 15.
[15] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013b, p. 2.

No diz que respeito à classificação quanto à confidencialidade, deve-se ter presente que a maior parte dos dados e informações existentes nas Cortes de Contas reveste-se de natureza pública, em conformidade com o inciso I do artigo 3º da Lei nº 12.527/2011[16]. Por essa razão, investir na adoção de uma política de classificação permitirá que tais instituições atuem com mais eficiência quando iniciarem a implantação da LGPD.

Ademais, atentar para a classificação das informações é de fundamental importância para outras ações associadas à preservação da memória organizacional. É possível, por exemplo, associar a adoção de uma política de classificação da informação à implantação de uma política de gestão documental (com a definição da tabela de temporalidade e do código de classificação dos documentos), tendo como resultado prático o gerenciamento completo do ciclo de vida dos documentos, desde a produção até a eliminação ou guarda permanente, aplicando-a tanto aos documentos físicos quanto aos digitais.

Para facilitar as atividades de classificação, é recomendável que as instituições realizem inventário dos dados e das informações, bem como regulamentem, por meio de normativo interno, as suas classificações, caso ainda não os tenham.

Cabe referir que a classificação da informação é tratada, de modo geral, pela Lei Federal nº 12.527/2011 – LAI. Em seus artigos 23 e 24, são apresentadas regras quanto à restrição de acesso, bem como quanto à possibilidade de classificação da informação em graus de sigilo. Na sequência, o artigo 31[17] aborda o tratamento das informações pessoais, trazendo importantes disposições que se coadunam com a LGPD[18].

---

[16] Art. 3º Os procedimentos previstos nesta Lei destinam-se a assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com os princípios básicos da administração pública e com as seguintes diretrizes: I - observância da publicidade como preceito geral e do sigilo como exceção.

[17] 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.

[18] Recomenda-se a leitura do artigo 31, §1º ao 5º da Lei Federal nº 12.527/2011.

Uma vez realizada essa classificação, os Tribunais de Contas terão condições de envidar esforços adequados, necessários e proporcionais aos níveis de proteção exigidos, resultando, assim, no uso racional dos recursos (controles) utilizados.

3 A LGPD E SEU IMPACTO NA EXECUÇÃO DOS PROCESSOS INTERNOS DOS TRIBUNAIS DE CONTAS

3.1 Do tratamento de dados pessoais nas atividades administrativas

Para além dos pré-requisitos estruturantes abordados anteriormente, a LGPD exigirá que as Cortes de Contas organizem-se e atentem para alguns impactos específicos que a sua vigência terá sobre as atividades administrativas. Isso porque, a par de suas atividades fiscalizatórias, existem diversos dados pessoais sendo diariamente coletados e trafegados em âmbito interno.

Com a evolução tecnológica, os Tribunais de Contas, assim como o setor público em geral, têm adotado gradativamente o uso de aplicações de *internet* como estratégia para se aproximar de cidadãos, facilitar o acesso à informação e prestar determinados serviços.

Neste sentido, a Lei Federal nº 13.460/2017 – que dispõe sobre a participação, proteção e defesa dos direitos do usuário dos serviços públicos na administração pública – previu como diretriz a necessidade de aplicação de soluções tecnológicas que visem a simplificar processos e procedimentos de atendimento ao usuário e a propiciar melhores condições para o compartilhamento das informações (artigo 5º, inciso XIII).

São exemplos disso o uso de redes sociais, os portais de transparência, os cursos ministrados pelas Escolas de Contas, os Serviços de Informação ao Cidadão (SIC), os canais de comunicação do tipo “Fale Conosco” e “Ouvidoria”, a emissão de certidões, entre outros. Nesses casos, é bastante provável que ocorra a coleta e o armazenamento de informações pessoais de usuários.

Ademais, no desempenho de suas funções administrativas, as Cortes de Contas recebem, arquivam e compartilham diversos dados pessoais, como na contratação de terceirizados e de serviços autônomos, no cadastro de visitantes, na realização de um concurso público (dados dos candidatos inscritos), nos registros de

servidores (informações como telefone pessoal, endereço residencial, existência de pagamento de pensão, crédito consignado), etc.

É importante esclarecer que, independentemente da natureza da atividade realizada (seja administrativa, seja finalística), a atuação das Cortes de Contas é sempre pautada em lei, em observância ao princípio da legalidade.

Hely Lopes Meirelles (2018, p. 91) define:

> A legalidade, como princípio de administração (CF, art. 37, caput), significa que o administrador público está, em toda a sua atividade funcional, sujeito aos mandamentos da lei e às exigências do bem comum, e deles não se pode afastar ou desviar, sob pena de praticar ato inválido e expor-se a responsabilidade disciplinar, civil e criminal, conforme o caso.

O referido doutrinador lembra que, enquanto no campo das relações entre particulares é lícito fazer tudo o que a lei não proíbe (princípio da autonomia da vontade), na administração pública só é permitido fazer o que a lei autoriza.

Isso significa que, no caso de haver tratamento de dados pessoais, mesmo quando os Tribunais de Contas estiverem desempenhando atividades de natureza administrativa, o regime jurídico aplicável será igualmente o previsto no artigo 7º, III[19], combinado com o artigo 23[20] da LGPD.

Nessa perspectiva, e geralmente servindo como modelo de boas práticas para seus jurisdicionados, os Tribunais de Contas precisarão adotar medidas necessárias à sua adequação, até mesmo para evitar a imposição de eventuais sanções.

---

[19] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

[20] Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público [...]

É recomendável, diante disso, a criação de uma comissão ou grupo de trabalho multidisciplinar, com abordagem holística, para fazer o diagnóstico dos impactos, bem como o inventário e o mapeamento dos dados pessoais que trafegam na instituição, identificando os processos de trabalho nos quais são coletados e os documentos em que são inseridos.

Nesse aspecto, cabe referir que a Autoridade Nacional de Proteção de Dados (ANPD) poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais (artigo 32), o que já justificaria a adoção de tais ações.

Não obstante, esse diagnóstico será uma importante fonte de informação para subsidiar a tomada de decisão, podendo ser utilizado como um balizador para as ações que deverão ser implementadas. Assim, as seguintes providências podem ser utilizadas como ponto de partida:

- implantar ou melhorar a governança de dados;
- definir um encarregado;
- instituir a gestão de riscos e incidentes de segurança;
- fortalecer a segurança corporativa da informação;
- institucionalizar um programa ou uma política de governança em privacidade;
- revisar os contratos e convênios, inserindo cláusulas de observância à LGPD;
- promover capacitação, sensibilização e campanhas para servidores, contratados, jurisdicionados e parceiros sobre os cuidados necessários com o tratamento dos dados pessoais.

Não obstante a necessidade da adoção de medidas de segurança da informação e de proteção de dados pessoais, é importante esclarecer que o

princípio da publicidade dos atos administrativos e o dever de transparência institucional[21] devem continuar sendo observados pelas Cortes de Contas, tal como recomendado na Resolução nº 09/2018 da ATRICON[22].

Portanto, não há alteração quanto à obrigatoriedade de divulgação de informações relacionadas aos atos de gestão e de administração dos Tribunais de Contas[23].

Aliás, alinhada às diretrizes de acesso à informação e de transparência, a LGPD assegurou expressamente direitos aos titulares de dados (artigos 17 e 18), razão pela qual é recomendável que as Corte de Contas se organizem para:

- responder às demandas do cidadão com agilidade;
- receber e analisar o pedido do cidadão quando se opõem ao tratamento dos seus dados, mesmo quando há interesse público;
- responder quanto à existência de tratamento de dados do titular;
- dar acesso aos dados que lhe digam respeito;
- corrigir dados pessoais incompletos, inexatos ou desatualizados.

3.2 Da estrutura funcional dos Tribunais de Contas para atender à LGPD

A LGPD prevê, para a gestão do tratamento de dados pessoais, três importantes figuras:

---

[21] Lei Federal nº 12.527/2011. Art. 3º Os procedimentos previstos nesta Lei destinam-se a assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com os princípios básicos da administração pública e com as seguintes diretrizes: I - observância da publicidade como preceito geral e do sigilo como exceção; II - divulgação de informações de interesse público, independentemente de solicitações; III - utilização de meios de comunicação viabilizados pela tecnologia da informação; IV - fomento ao desenvolvimento da cultura de transparência na administração pública; V - desenvolvimento do controle social da administração pública.

[22] Resolução nº 09/2018 da ATRICON - Aprova as Diretrizes de Controle Externo Atricon 3218/2018 relacionadas à temática “Transparência dos Tribunais de Contas e dos jurisdicionados”.

[23] Lei Federal nº 12.527/2011. Art. 8º É dever dos órgãos e entidades públicas promover, independentemente de requerimentos, a divulgação em local de fácil acesso, no âmbito de suas competências, de informações de interesse coletivo ou geral por eles produzidas ou custodiadas.

> Art. 5º Para os fins desta Lei, considera-se:
>
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
>
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
>
> VIII - encarregado: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados; (Redação dada pela Medida Provisória nº 869, de 2018)
>
> IX - agentes de tratamento: o controlador e o operador.

Nos artigos 37 a 41 da LGPD, são detalhadas as competências e as responsabilidades do controlador, do encarregado e do operador.

Diante disso, os Tribunais de Contas terão que definir o seu papel como **controlador**, pessoa jurídica de direito público, respondendo diretamente pelo tratamento dos dados pessoais sob sua guarda no cumprimento de obrigação legal ou regulatória. Nesse contexto, a competência para as atribuições da figura do controlador (entre elas a de indicar o encarregado e a de tomar decisões referentes ao tratamento de dados pessoais) deverá ser regulamentada internamente por cada Corte.

Não obstante, algumas responsabilidades do controlador já estão previstas na LGPD, como a de comunicar à ANPD e aos titulares de dados pessoais a ocorrência de incidente de segurança que “possa acarretar risco ou dano relevante aos titulares”.

Quanto ao **operador,** tem-se que cada Corte de Contas necessita definir internamente se essa figura pertencerá a sua estrutura organizacional ou se será desempenhada por terceiros que farão o tratamento de dados em nome da instituição. Sendo este o caso, será necessário criar acordos controlador-operador; atualizar os acordos do controlador-operador (uso intencional e requisitos de segurança); atualizar outros acordos existentes, quando aplicável; atualizar o

processo de aquisição (critérios de seleção para novos serviços); novas aquisições (novos requisitos incluídos em novos contratos).

Faz-se necessário observar todos os critérios da relação controlador-operador, uma vez estabelecida, pois existe uma responsabilidade solidária e subjetiva entre ambos, por dano patrimonial, moral, individual ou coletivo, quando descumprir as obrigações da legislação e não tiver seguido as instruções permitidas pelo controlador.

Depreende-se, assim, que os Tribunais de Contas, tanto na atividade de controlador quanto na de operador, terão que criar e manter um registro das operações de tratamento de dados pessoais.

Por fim, haverá a necessidade de indicação de um **encarregado**. Antes da MP 869/2018, o encarregado deveria ser uma pessoa natural. Contudo, o termo "natural" foi revogado, o que possibilitou que tanto pessoas naturais quanto pessoas jurídicas possam ser designadas para essa função.

A indicação do encarregado é feita pelo controlador, que no caso em comento é o próprio Tribunal de Contas. O encarregado será responsável por atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD. Portanto, é importante que, ao encarregado, seja assegurado acesso direto à alta administração, autonomia, estabilidade e navegabilidade em toda a instituição.

O encarregado responderá pelo tratamento dos dados pessoais segundo as informações fornecidas pelo controlador, estando entre suas atribuições a de receber e responder às solicitações, interagir com a ANDP, orientar servidores e contratados das práticas de tratamento de dados, coordenar políticas e práticas de privacidade, realizar treinamento, entre outras.

Dito isso, tem-se que os Tribunais de Contas necessitarão adequar sua estrutura para atender ao que prevê a LGPD no que tange às atribuições das figuras do controlador, do operador e do encarregado (artigos 37 a 41).

Poderão, ainda, se valer das estruturas de comunicação já existentes em suas organizações (a exemplo da Ouvidoria, dos Serviços de Informação ao Cidadão e do Protocolo), desde que permitam aos titulares de dados exercerem seus direitos (artigos 17 e 18 da LGPD) de forma facilitada e gratuita (artigo 6º, inciso IV).

Nesse contexto, ganha sentido a previsão da LGPD, ao sugerir, aos controladores e operadores, “formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais” (artigo 50 da LGPD).

4 DO TRATAMENTO DE DADOS PESSOAIS PELOS TRIBUNAIS DE CONTAS QUANDO NO EXERCÍCIO DO CONTROLE EXTERNO

A fiscalização contábil, financeira, orçamentária, operacional e patrimonial é dever estatal, devendo ser realizada pelos entes federativos e pelas entidades da administração direta e indireta, quanto à legalidade, legitimidade, economicidade, aplicação das subvenções e renúncias de receitas, nos termos do artigo 70 da Constituição Federal.

Nesse contexto, e em consonância com o artigo 71 da Constituição Federal, inserem-se os Tribunais de Contas, órgãos autônomos de estatura constitucional, com competências constitucionais e legais, dentre as quais o exercício do controle externo, exercido prioritariamente por meio de atividades fiscalizatórias previstas em suas leis orgânicas, regimentos internos e demais legislações afetas ao tema.

Para que a atividade fiscalizatória ocorra de maneira eficaz, com qualidade e eficiência, é necessário assegurar que os Tribunais de Contas executem suas competências constitucionais e legais com o devido alinhamento aos princípios da publicidade, da supremacia do interesse público, da transparência das informações e do acesso geral às prestações de contas.

Assim, no exercício da função fiscalizatória, os Tribunais de Contas necessitam ter acesso a dados pessoais para garantir o cumprimento de sua missão constitucional. A consequência imediata seria evitar fraudes e corrupção, aumentar a arrecadação e aprimorar a qualidade dos gastos públicos.

Nessa seara, o tratamento de dados pessoais, quando no atendimento da finalidade pública, na persecução do interesse público e com o objetivo de executar as competências legais, foi disciplinado pelo artigo 23 da LGPD.

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na

> persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:
>
> I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;
>
> II. - (VETADO) e;
>
> III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei;
>
> IV. - (VETADO)

Como se percebe, há requisitos específicos previstos na LGPD quando o tratamento de dados pessoais for realizado pelo setor público, o que ocorre pelo fato de a Administração Pública estar envolta em suas atividades por princípios e interesses gerais e coletivos que se sobrepõem aos privados.

Por esse motivo, igualmente, a LGPD não previu, nesses casos, a necessidade de prévio consentimento para o tratamento e compartilhamento dos dados pessoais. Aliás, entendimento diverso criaria um verdadeiro obstáculo à atuação dos Tribunais de Contas e afrontaria o Estado Democrático de Direito.

Depreende-se, portanto, que o tratamento de dados pessoais pelos Tribunais de Contas, enquanto no exercício de suas competências fiscalizadoras, as quais indiscutivelmente têm finalidade pública, enquadra-se nas disposições do artigo 23. A interpretação do novo diploma deve se dar em consonância com o sistema constitucional, que prevê a supremacia do interesse público sobre o privado, a transparência das informações públicas e o acesso à prestação de contas.

A Lei Federal nº 12.527/2011 já previa o dever dos órgãos e das entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, de assegurar a: gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação; a proteção da informação, garantindo-se sua disponibilidade, autenticidade e integridade; e a proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso. Portanto, no que tange a esses aspectos, não há inovação.

Por outro lado, verifica-se que as novidades legislativas da LGPD, aplicáveis aos Tribunais de Contas enquanto no exercício de suas atribuições institucionais, encontram-se nos incisos I e III do artigo 23.

A previsão do inciso I do artigo 23 exige que os Tribunais de Contas passem a informar as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais. Além disso, as Cortes deverão fornecer informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos.

A leitura dessa previsão deve pautar-se pela razoabilidade e adequação, a fim de que a divulgação de tais informações não prejudique nem comprometa as atividades de fiscalização. No entanto, o seu cumprimento exigirá organização e autoconhecimento das Cortes de Contas, que deverão ter o devido domínio de seus bancos de dados.

Nesse aspecto, mostra-se imprescindível investir nos pré-requisitos estruturantes mencionados no tópico 02, a fim de que seja possível realizar o mapeamento de bases e dos fluxos, bem como ter o registro de atividades e de processos internos relacionados ao uso, processamento e operações de tratamento de dados pessoais.

Quanto à publicidade das operações de tratamento, percebe-se que a legislação deixou em aberto a possibilidade de a ANPD dispor sobre esse ponto

específico futuramente, ao prever no artigo 23, §1º, que "A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento".

Não obstante, depreende-se dos parágrafos subsequentes da Lei que o exercício de direitos por parte de titulares perante o Poder Público deverá ser assegurado desde o princípio da vigência da LGPD, em consonância com o disposto em legislações específicas, em especial as disposições constantes na Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data) , da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo), e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

Ainda que não exista regulamentação específica dispondo sobre como (e se) os Tribunais de Contas deverão atender de forma ativa ao inciso I do artigo 23, o direito dos titulares de obter tais informações, sob demanda, está expressamente previsto. Para tanto, as Cortes poderão se valer das estruturas de comunicação já existentes em suas organizações (a exemplo da Ouvidoria, dos Serviços de Informação ao Cidadão e do Protocolo), desde que permitam aos titulares de dados exercerem seus direitos de forma facilitada e gratuita.

Por sua vez, o inciso III do artigo 23 prevê que as pessoas jurídicas de direito público deverão indicar um encarregado quando realizarem operações de tratamento de dados pessoais. Conforme explicitado no tópico 3.2, a figura do encarregado é conceituada pelo artigo 5º da LGPD, e suas atividades estão disciplinadas no artigo 41 do mesmo diploma, cabendo, assim, a cada Tribunal de Contas, enquanto no papel de controlador, indicar que pessoa exercerá tais atribuições.

Na divulgação das informações relativas ao exercício do controle externo (a exemplo da publicação ativa de relatórios de auditoria, lista de gestores que tiveram contas julgadas irregulares ou parecer prévio desfavorável, lista de devedores de condenações fixadas pelas Cortes, etc), deve-se levar em consideração os princípios constitucionais, a Lei de Acesso à Informação e a própria previsão

expressa no artigo 7º, §3[24], da LGPD. Isso porque as informações constantes e resultantes dos processos de fiscalização são indiscutivelmente de interesse geral e coletivo (artigo 8º da LAI), sendo que há alto grau de relevância pública em disseminá-las para a sociedade. Tal divulgação concretiza o cumprimento ao princípio da publicidade, fomenta a participação popular e o controle social, e demonstra que os agentes públicos estão cumprindo com seu dever de prestar contas.

[24] Art. 7º, § 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.

5 LGPD E O COMPARTILHAMENTO DE INFORMAÇÕES

O tratamento de dados pelos Tribunais de Contas abrange também a comunicação e o compartilhamento de informações com terceiros.

É parte fundamental da função moderna de controle externo utilizar, de maneira controlada e ostensiva, todas as informações às quais tenha acesso para subsidiar as ações de controle em suas diversas fases: planejamento, execução, relatório e instrução, desde que alinhadas às suas funções constitucionais e legais.

O uso compartilhado de dados e informações traz eficiência às atividades desempenhadas, razão pela qual tem sido estimulado e ampliado, cada vez mais, no setor público. Nesse sentido, a LGPD estabeleceu regras específicas.

Quanto à estrutura dos dados, a LGPD prevê:

> Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

É preciso também considerar a abrangência da atuação contemporânea dos Tribunais de Contas, em que dados e informações de diversas fontes e origens, públicas ou privadas, podem ser utilizados como insumo para o cumprimento eficiente e efetivo das suas funções.

Ademais, dado o crescente número de políticas públicas multissetoriais e transversais que envolvem diversos entes da federação para a sua execução (transferências voluntárias, por exemplo), mostra-se essencial a utilização do compartilhamento de dados e informações entre instituições públicas de diferentes poderes e entes da federação.

Nesse ponto, a LGPD trouxe as seguintes previsões em seu artigo 26, caput e §1º, incisos I, IV e V:

> 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: (...)
>
> I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) ;
>
> IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou
>
> V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades. (Incluído pela Lei nº 13.853, de 2019)

Portanto, ao considerarmos o rol de funções exercidas pelos Tribunais de Contas, é necessário observar fluxos específicos de tratamento de dados conforme as hipóteses presentes nos artigos 25 e 26 acima mencionados, assim como a dissociação em classes de dados.

Assim, a adaptação das operações dos Tribunais de Contas deve ser realizada para certificar a aderência com a LGPD, havendo necessidade de adoção de medidas de resguardo.

Nesse aspecto, é relevante revisar as atribuições infralegais previstas em normativas internas (tais como Resoluções, Instruções e Portarias), bem como as disposições inseridas em termos de cooperação, convênios, acordos de cooperação técnica, de modo a deixar mais clara a necessidade de utilização de dados e informações para suporte às ações de controle, adequando inclusive os procedimentos padrão de instrução e de fiscalização.

Igualmente, mostra-se prudente a criação de controles, caso ainda não existam, para deixar claros os papéis e as responsabilidades dos profissionais que

lidam com dados e informações em diversas fases, com a intenção de cumprir fielmente o que preveem os artigos 25 e 26 (caput) da LGPD.

Dada a importância do uso de dados e informações para a atividade de controle externo, aqui inseridas não somente as de cunho pessoal, é recomendável que as Cortes de Contas avaliem a conveniência e oportunidade de criação de uma estrutura organizacional específica para a gestão de informações. Nos moldes dos *chief data officers,* presentes em agências públicas norte-americanas, tais estruturas prestam-se a tornar modernas e estáveis as atividades necessárias para suportar o uso e produção de informações para o controle externo em todo o seu ciclo de vida.

É de se avaliar a necessidade de estabelecimento de fluxo de trabalho para integração e compartilhamento de informações com a ANPD. Como já referido anteriormente, uma vez instituída a ANPD e regulamentado o seu funcionamento, será necessário verificar os procedimentos de comunicação e estabelecer um processo de trabalho interno que dê suporte às eventuais interações com a agência.

6. CONSIDERAÇÕES FINAIS

Feitas as considerações acima, tem-se como imperioso que as Cortes de Contas busquem adequar-se aos aspectos inovadores da lei, investindo em questões de segurança da informação, gestão de riscos, de processos, mapeamento de bases, fluxos e procedimentos, treinamento e capacitação de pessoal, tendo presente que o texto legislativo contribui nesse sentido.

Merece atenção, ainda, a existência da Lei da Transparência (Lei Federal nº 131/2009) e da Lei de Acesso à Informação (Lei Federal nº 12.527/2011), com as quais a LGPD deverá necessariamente dialogar, para que sejam aplicadas de forma integrada. Nesse aspecto, não devem ser olvidados os avanços dos últimos anos em termos de transparência, controle social e participação popular, os quais só foram possíveis graças ao amplo acesso e à vasta disseminação de informações.

Não é demais referir que os Tribunais de Contas, acima de qualquer nova legislação editada, devem obedecer aos princípios constitucionais que norteiam a atuação da administração pública, quais sejam: legalidade, moralidade, impessoalidade, publicidade, eficiência, razoabilidade, proporcionalidade, ampla defesa, contraditório, segurança jurídica, motivação e supremacia do interesse público. Portanto, a interpretação da LGPD no âmbito das Cortes de Cortes deve, indubitavelmente, ser feita em consonância com o aparato jurídico e constitucional já existente.

Instituto Rui Barbosa
www.irbcontas.org.br
A Casa do Conhecimento dos Tribunais de Contas

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001/2013** : tecnologia da informação : técnicas de segurança : sistemas de gestão de segurança da informação : requisitos. Rio de Janeiro: ABNT, 2013a.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002/2013 :** tecnologia da informação : técnicas de segurança : código de prática para controles de segurança da informação. Rio de Janeiro: ABNT, 2013b.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27005/2011** : metodologia para gerenciamento de riscos da segurança da informação. Rio de Janeiro: ABNT, 2011.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 31000/2018** : gestão de riscos : diretrizes. Rio de Janeiro: ABNT, 2018.

ASSOCIAÇÃO DOS TRIBUNAIS DE CONTAS DO BRASIL. **Resolução ATRICON n° 09/2018**. Aprova as diretrizes de controle externo Atricon 3218/2018 relacionadas à temática transparência dos Tribunais de Contas e dos jurisdicionados. Disponível em: http://www.atricon.org.br/normas/resolucao-atricon-no-092018/. Acesso em: 31 out. 2019.

BIONE, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento**.** Rio de Janeiro: Forense, 2019. 314p.

BRASIL. Constituição Federal (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/ConstituicaoCompilado.htm. Acesso em: 1 out. 2019.

BRASIL. **Lei n° 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 31 out. 2019.

BRASIL. **Lei n° 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 31 out. 2019.

BRASIL. **Lei n° 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em:http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 31 out. 2019.

BRASIL. **Lei n° 13.460, de 26 de junho de 2017**. Dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública. Disponível em:http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 31 out. 2019.

BRASIL. **Lei n° 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em:http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 31 de out. 2019.

BRASIL. **Lei n° 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 31 de out. 2019.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 1 out. 2019.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 1 out. 2019.

BRASIL. **Lei nº 9.507, de 12 de novembro de 1997.** Regula o direito de acesso a informações e disciplina o rito processual do *habeas data.* Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9507.htm. Acesso em: 4 out. 2019.

BRASIL. **Lei nº 9.784, de 29 de janeiro de 1999**. Regula o processo administrativo no âmbito da Administração Pública Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9784.htm. Acesso em: 1 out. 2019.

BRASIL.Tribunal de Contas da União. **Classificação da informação**. Brasília,DF : TCU, 2010. Disponível em: https://portal.tcu.gov.br/biblioteca-digital/classificacao-da-informacao.htm. Acesso em: 5 out. 2019.

BRASIL.Tribunal de Contas da União. **Manual de gestão de riscos do TCU**. Brasília,DF : TCU, 2018. Disponível em: https://drive.google.com/file/d/1YEHkCaLgyfg3qxW6tJxOxER-Q1YTte8d/view. Acesso em: 31 out. 2019.

BROCKE, Jan vom; ROSEMANN, Michael. **Manual de BPM Gestão de Processos de Negócio**. Porto Alegre: Bookman, 2013.

CAMPOS, André L. N. **Modelagem de processos com BPMN**. 2. ed., Rio de Janeiro: Brasport, 2014.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais comentada**. 2.ed. São Paulo: Thomson Reuters Revista dos Tribunais, 2019. 244p.

CUNHA**,** Juliana Falci Sousa Rocha. Direito à proteção de dados pessoais : a recente evolução legislativa brasileira. **Revista de Propriedade Intelectual. Direito Contemporâneo e Constituição - PIDCC**, Aracaju (SE), ano VIII, v. 13, n. 2, p.115-

145, jul. 2019. Disponível em: http://www.pidcc.com.br/fr/manual-de-direito-empresarial-vol-iii-3/2-uncategorised/347-direito-a-protecao-de-dados-pessoais-a-recente-evolucao-legislativa-brasileira. Acesso em: 15 out. 2019.

10 MELHORES práticas de segurança da informação : descubra pontos importantes a serem observados na hora de proteger sua empresa. disponível em: https://blogbrasil.comstor.com/10-melhores-praticas-de-seguranca-da-informacao. Acesso em: 31 out. 2019.

FORTES, Vinícius Borges. **Os direitos de privacidade e a proteção de dados pessoais na internet**. Rio de Janeiro: Lumen Juris, 2016.

10 MELHORES práticas de segurança da informação: descubra pontos importantes a serem observados na hora de proteger sua empresa. Canal Comstor. disponível em: https://blogbrasil.comstor.com/10-melhores-praticas-de-seguranca-da-informacao. Acesso em: 31 out. 2019.

GUIA para a lei geral de proteção de dados. São Paulo (SP): Mattos Filho, Veiga Filho e Quiroga Advogados, 2018. Disponível em: https://www.legiscompliance.com.br/images/pdf/cartilha_lgpd_mattosfilho.pdf. Acesso em: 29 set. 2019.

INSTITUTO DE TECNOLOGIA E SOCIEDADE (ITS Rio). **Lei geral de proteção de dados pessoais (LGPD) e setor público**: um guia da Lei 13.709/2018, voltado para os órgãos e entidades públicas. Rio de Janeiro, 2019. Disponível em: https://itsrio.org/wp-content/uploads/2019/05/LGPD-vf-1.pdf. Acesso em: 29 set. 2019.

KODAMA, Roberto. **Oficina "proteção de dados pessoais**". *In*: SEMANA DE OUVIDORIA E ACESSO À INFORMAÇÃO, 4., 2019, Rio de Janeiro. Disponível em: http://ouvidorias.gov.br/4a-semana-de-ouvidoria-e-acesso-a-informacao-arquivos/4a-semana-de-ouvidoria-e-acesso-a-informacao-apresentacoes/roberto-kodama-protecao-de-dados-pessoais.pdf/view Acesso em: 29 set. 2019.

LGPD o que muda no setor público? Campo Grande (MT): Digix, 2019. Disponível em: http://www.digix.com.br/conteudo-interno-lgpd-o-que-muda-no-setor-publico/. Acesso em: 29 set. 2019.

LIMBERGER, Têmis. **O direito à intimidade na era da informática: a necessidade de proteção dos dados pessoais**. Porto Alegre: Livraria do Advogado, 2007.

MACIEL, Moisés. **Os Tribunais de Contas no exercício do controle externo face à nova Lei Geral de Proteção de Dados Pessoais**. 2019. No prelo

MANZONI, Leonardo. **Blockchain e o aprimoramento do processo eletrônico do Tribunal de Contas do Estado de Santa Catarina**. Disponível em: https://drive.google.com/file/d/1-zLh0fgMatWmeSHL_BjiIb9-NQGAI-AR/view. Acesso em: 31 out. 2019.

MEIRELLES, Hely Lopes. **Direito administrativo brasileiro.** 43. ed. São Paulo: Malheiros, 2018. 1016 p.

MOURA, João Batista Ribas de. Os 4 riscos que fragilizam a gestão de riscos. **Revista TCU**, v. 50, n. 141, p. 42-51, jan./abr. 2018 .Disponível em: https://revista.tcu.gov.br/ojs/index.php/RTCU/article/view/1487. Acesso em: 31 out. 2019.

OLIVEIRA, Ricardo Alexandre de. Lei geral de proteção de dados pessoais e seus impactos no ordenamento jurídico. **Revista dos Tribunais**, São Paulo, ano 107, v. 998, p. 241-261, dez. 2018.

PAVANI JR., Orlando; SCUCUGLIA, Rafael. **Mapeamento e gestão por processos** - BPM. Rio de Janeiro: M.BOOKS, 2011.

PEREIRA, Mariléa. A modelagem de processo de negócio à luz dos ritos processuais existentes no Tribunal de Contas do Estado de SC. **Revista do TCU**, v. 49, n. 139, p. 84-95, maio/ago. 2017. Disponível em:

https://revista.tcu.gov.br/ojs/index.php/RTCU/article/view/1433. Acesso em: 31 out. 2019.

PEREIRA, Wallace da Silva. Fluxo de processo eletrônico. *In:* ENCONTRO NACIONAL DO INSTITUTO RUI BARBOSA, 2017, Brasília,DF. **Palestra** [...]. Tema: Inteligência e tecnologia: soluções estratégicas para os tribunais de contas. 1 video (15min11s). Publicado pelo canal do Instituto Rui Barbosa. Disponível em: https://www.youtube.com/watch?v=OeBifCPh3Ek. Acesso em: 31 out. 2019.

PINHEIRO, Patrícia Peck. **Direito digital**. 4 ed. São Paulo: Saraiva, 2010.

ROSSO, Angela Maria. **LGPD e setor público**: aspectos gerais e desafios. Disponível em: https://m.migalhas.com.br/depeso/300585/lgpd-e-setor-publico-aspectos-gerais-e-desafios. Acesso em: 29 set. 2019.

SANTA CATARINA. Secretaria de Administração do Estado. Escritório de Gestão de Processos. **Modelo de governança por processos**. Florianópolis, 2018. Disponível em: https://drive.google.com/file/d/1P9hn9WC3imC7jDhoT6ckSTRQoIOZK2ZW/view. Acesso em: 31 out. 2019.

SANTA CATARINA. Tribunal de Contas do Estado. Diretoria de Informática. **Otimizando a operacionalização do processo eletrônico**. 2013 .Disponível em: https://drive.google.com/file/d/0B6sqjeu1JyfbcEg4b3ZBUkhzcUE/view. Acesso em: 31 out. 2019.

SANTA CATARINA. Tribunal de Contas do Estado. **Resolução nº TC-0126/2016**. Dispõe sobre o processo em meio eletrônico no âmbito do Tribunal de Contas do Estado de Santa Catarina. Disponível em: http://www.tce.sc.gov.br/sites/default/files/leis_normas/RESOLUÇÃO%20N.%20TC%200126-2016%20CONSOLIDADA_0.pdf. Acesso em: 31 out. 2019.

SANTOS, Fabíola de Almeida; TALIBA, Rita. Lei geral de proteção de dados no Brasil e os possíveis impactos. **Revista dos Tribunais**, São Paulo, ano 107, v. 998, p. 225-239, dez. 2018.

SILVA, Paulo Matheus Nicolau. **Recomendações de segurança da informação para soluções de tecnologia da informação e comunicação baseadas em computação em nuvem**. Disponível em: http://bdm.unb.br/bitstream/10483/14032/1/2013_PauloMatheusNicolauSilva.pdf. Acesso em: 31 out. 2019.

SIMPÓSIO INTERNACIONAL LEI GERAL DE PROTEÇÃO DE DADOS - LGPD, 2019, FLORIANÓPOLIS (SC). Florianópolis: TJSC, 2019. Disponível em: https://www.youtube.com/watch?v=OSszD6f1rDc. Acesso em: 4 out. 2019.

UNIÃO EUROPEIA. Tribunal de Contas Europeu. **Desafios à eficácia da política da cibersegurança da UE** : documento informativo. 2019. Disponível em: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_PT.pdf. Acesso em: 29 set. 2019.

VIANA, Igor Bonfim. A proteção de dados pessoais na internet à luz do direito pátrio. Universidade Federal de Roraima. Boa Vista, 2018. Disponível em: https://www.passeidireto.com/arquivo/69640254/monografia-igor-bonfim-viana. Acesso em: 31 out. 2019.

WEBINAR: como se adequar à LGPD na prática. 1 video (49min35s). Publicado pelo canal BigData Corp. Disponível em: https://www.youtube.com/watch?v=XvUp26scook. Acesso em: 31 out. 2019.