GESTÃO DE RISCOS E OS DADOS PESSOAIS OBTIDOS POR MEDIDAS PROBATÓRIAS NO PROCESSO PENAL

RISK MANAGEMENT AND PERSONAL DATA OBTAINED BY PROBATORY MEASURES IN THE CRIMINAL PROCEDURE

Pedro Enrico de Oliveira[1]
Rafael Lima da Costa[2]

RESUMO

A gestão de riscos é fundamental para a execução de planejamento estratégico elaborado à luz da gestão de processos de negócio de toda e qualquer entidade, privada ou pública. Contudo, estudos realizados na literatura acadêmica pertinente e nos instrumentos normativos produzidos pelo Poder Judiciário brasileiro revelaram a carência de pesquisas para a gestão de riscos provocados pela coleta e manejo de dados pessoais no âmbito das medidas cautelares do processo criminal. O propósito deste artigo é verificar se, verdadeiramente, riscos são gerados no contexto apresentado e se a adoção de uma metodologia de gestão de riscos é necessária para o alcance dos objetivos institucionais do Poder Judiciário. Por meio de uma abordagem qualitativa de revisão teórica, o tema foi tratado sob uma perspectiva holística, com o propósito de integração multidisciplinar e interdisciplinar da Administração científica, da Sociologia e do Direito. Os resultados obtidos nos conduziram à confirmação de que o tratamento desses dados pessoais gera riscos de eventos danosos à gestão judiciária, à gestão processual e ao exercício da atividade jurisdicional, além de danos às instituições públicas e privadas, ao indivíduo ou à coletividade. Para conter os riscos, é imperiosa a adoção de metodologia adequada e eficaz para preveni-los, corrigi-los e mitigá-los.

Palavras-chave: Gestão de riscos. Metodologias. Poder Judiciário. Dados pessoais. Processo criminal cautelar.

ABSTRACT

Risk management is fundamental for the execution of strategic planning elaborated in light of the business process management of any and all entities, private or public. However, studies carried out in the relevant academic literature and in the normative instruments produced by the Brazilian Judicial Branch revealed the lack of research for the management of risks caused by the collection and handling of personal data within the scope of the precautionary measures in the criminal process. The purpose of this article is to verify if, truly, risks are generated in the presented context and if the adoption of a risk management methodology is necessary to reach the institutional objectives of the Judicial Branch. Through a qualitative approach of theoretical review, the theme was treated from a holistic perspective, with the purpose of integrating multidisciplinary and interdisciplinary scientific administration, sociology and the law. The results obtained led us to the confirmation that the treatment of these personal data creates risks of harmful events to the judiciary management, to the judicial

1 Mestrando Profissional em Direito e Poder Judiciário pela Escola Nacional de Formação e Aperfeiçoamento de Magistrados, Especialista em Direito Processual Civil, Especialista em Direitos Humanos, Teoria e Filosofia do Direito, Juiz de Direito do Tribunal de Justiça do Estado do Pará.
2 Aluno especial do Programa de Mestrado Profissional em Direito e Poder Judiciário da Escola Nacional de Formação e Aperfeiçoamento de Magistrados, Especialista em Direito Processual Civil, Especialista em Direito Administrativo, Juiz Federal do Tribunal Regional Federal da 1ª Região.

case management and to the exercise of the jurisdictional activity, in addition to damages to public and private institutions, to the individual or community. To restrain the risks, it is imperative to adopt an adequate and effective methodology to prevent, correct and mitigate them.

Keywords: Risk management. Methodologies. Judicial Branch. Personal data. Criminal procedure.

1 **INTRODUÇÃO**

Se o Poder Judiciário fosse uma indústria, substancial parte dos insumos empregados no processo produtivo seria desperdiçada; fadado estaria, consequentemente, à insolvência e à quebra. Esta posição é impactante, mas factível. A cultura do Poder Judiciário sempre se caracterizou pela falta de rigor metodológico na administração judiciária e de processos. Contudo, o sistema de justiça passou a ser o palco para a *judicialização da vida* (Barroso, 2009), com o aumento relevante do número de processos judiciais que nele ingressam anualmente. Torna-se, assim, necessária a adoção de métodos adequados de gestão do seu processo produtivo.

Algumas áreas de atuação do Poder Judiciário possuem destaque por atuarem no âmbito dos direitos fundamentais, como a liberdade, a intimidade, a vida privada e o patrimônio. A Justiça Criminal, assim, mesmo sendo necessária à convivência harmônica entre as pessoas, pode gerar eventos danosos na prática de seus atos.

Neste contexto fático, a presente pesquisa foi empreendida para responder aos seguintes problemas: as medidas cautelares no processo penal que promovam a coleta e o manejo de dados pessoais geram riscos que podem causar danos à gestão judiciária, à gestão processual e ao exercício da atividade jurisdicional, além de danos às instituições públicas e privadas, ao indivíduo e à coletividade? É necessária a adoção de uma metodologia de gestão de riscos adequada para tutelar esta classe processual e, assim, promover o progresso da gestão dos tribunais brasileiros?

A investigação teórica foi realizada porque se identificou a carência de estudos prévios para aferir o problema proposto, que aborda a gestão de risco na atividade jurisdicional criminal. Mais especificamente, não há projetos de gestão de riscos relativos a dados pessoais obtidos no processo penal que apontem para a metodologia mais adequada ao tratamento desses dados e tampouco a descrição de medidas técnicas e organizacionais planejadas para mitigar, prevenir ou corrigir os riscos identificados.

O Conselho Nacional de Justiça e diversos tribunais têm editado os seus próprios manuais de gestão de riscos, mas sem tratar especificamente da questão posta. Ocorre que os riscos decorrentes do manejo de dados pessoais pelo Poder Judiciário têm emergido em importância pelo avançado estágio de sua virtualização e à luz dos recentes ataques

cibernéticos a diversos tribunais brasileiros, o que estimulou, apenas a título de exemplo[3], o Conselho Nacional de Justiça a expedir a Resolução nº 360/2020, que determina a adoção de Protocolo de Gerenciamento de Crises Cibernéticas pelos órgãos do Poder Judiciário, além da Resolução nº 361, que determinou a adoção de Protocolo de Prevenção a Incidentes Cibernéticos (PPICiber/PJ), e da Resolução nº 362, que instituiu o Protocolo de Investigação para Ilícitos Cibernéticos.

Não são suficientes soluções meramente normativas, senão proposições metodológicas e objetivas de medidas contra os riscos verificáveis. Mesmo as recentes normas legais que disciplinam o tratamento de dados pessoais, como a nova Lei Geral de Proteção de Dados Pessoais (LGPD), não abordam especificamente o tema em análise. A LGPD exclui expressamente a sua aplicação para dados pessoais obtidos em decorrência de atividades de investigação e repressão de infrações penais.

A relevância do presente estudo está relacionada, de tal modo, à ampliação do acesso a dados pessoais por meio de investigações criminais ou pela própria instrução processual penal. Em razão do avanço dos equipamentos tecnológicos e principalmente da sincronização de informações em ambientes virtuais, os indivíduos estão cada vez mais concentrando seus dados pessoais no mesmo local de armazenamento. Isso torna mais dificultosa a realização da separação dos dados que são relevantes para a persecução penal pública daqueles que apenas dizem respeito à órbita privada do indivíduo. O Poder Judiciário torna-se, assim, um órgão que detém dados individuais relevantes, sem que tenha havido sequer a anuência dos seus titulares para o referido compartilhamento.

A hipótese central defendida por este artigo é a de que os dados pessoais coletados e tratados no processo criminal cautelar são elementos que geram riscos elevados para a gestão judiciária e processual e podem impedir o Poder Judiciário de atingir os seus objetivos institucionais, mormente o da prestação jurisdicional, podendo, ademais, gerar graves danos ao indivíduo e à coletividade. Consequentemente, é necessária a adoção de metodologia legítima e adequada para a gestão destes riscos e a específica descrição de medidas técnicas e organizacionais planejadas para mitigar os riscos identificados, implementando-se, assim, uma cultura de risco no âmbito do Poder Judiciário Brasileiro.

A pesquisa foi desenvolvida por meio coleta de dados em revisão teórica, os quais foram tratados pelo método qualitativo. O tema foi tratado sob uma perspectiva holística, multidisciplinar e interdisciplinar, com o propósito de integrar a Administração científica, a Sociologia e o Direito.

Este artigo foi seccionado em cinco partes. A primeira seção deste artigo é a presente introdução. A segunda seção apresenta o recorte teórico da pesquisa, apresentando o tratamento dado pela literatura científica de referência aos conceitos mais sensíveis para a formulação do problema e a compreensão da hipótese. A terceira seção promoverá a discussão

3 Disponível em: https://www.cnj.jus.br/judiciario-reforca-protecao-de-dados-de-forma-colaborativa/#:~:text=A%20Resolu%C3%A7%C3%A3o%20CNJ%20n%C2%BA%20360,no%20%C3%A2mbito%20do%20Poder%20Judici%C3%A1rio. Acesso em: 10 de jan. de 2021.

qualitativa das informações e dos dados arrecadados pela pesquisa, tratando dos riscos no contexto da Justiça Criminal e dos riscos gerados pela coleta e manejo de dados pessoais, a regulamentação da proteção de dados pessoais e uma sucinta aplicação hipotética das metodologias para a gestão dos riscos identificáveis. Por fim, a quarta e derradeira seção traz as conclusões desta pesquisa.

Por fim, esclarecemos que os exemplos que se seguirão no transcorrer deste artigo são meras ilustrações, como sói ser. O que se pretende não é exaurir as casuísticas de riscos de eventos danosos possíveis, mas, tão somente, expor a mecânica e a fluidez de como os riscos se manifestam no contexto do Poder Judiciário.

2 **MOLDURA CONCEITUAL E TEÓRICA**

2.1 DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS

Para fins de delimitação conceitual, adotaremos as definições de dado pessoal e de dado pessoal sensível previstas no artigo 5º, incisos I e II, da Lei Federal 13.709/2018, Lei Geral de Proteção de Dados (LGPD). É, portanto, dado pessoal, aquele que disponha sobre "*informação relacionada à pessoa natural identificada ou identificável*".

Por sua vez, dado pessoal sensível corresponde ao:

> 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.

Apesar de a LGPD não ser aplicável para a proteção de dados pessoais no âmbito da investigação criminal e do próprio processo penal, as definições de dados pessoais e dados pessoais sensíveis adotadas por ela seguem o modelo utilizado em outros instrumentos normativos sobre o tema, como o Regulamento Geral sobre a Proteção de Dados da União Europeia. Assim, apresenta-se adequado para o presente estudo.

2.2 CONSIDERAÇÕES GERAIS SOBRE O RISCO

Em sua relevante contribuição, Beck (1992) sustenta que, na modernidade avançada, a produção social de riquezas é sistematicamente acompanhada pela produção social de riscos. Trata-se de um incongruente estado de coisas em que o processo de modernização aumenta exponencialmente as forças produtivas e, consequentemente, são desencadeados riscos e potenciais ameaças em uma extensão desconhecida. Esta é a sociedade programada de risco descortinada pelo sociólogo alemão na década de 1980 e, embora se trate de uma tese sociológica e de conteúdo não prescritivo, a disseminação desta concepção da realidade moldou o pensamento contemporâneo sobre a gestão dos riscos.

O risco é uma situação ou evento onde algo de valor humano (incluindo-se os próprios

humanos) está em jogo e onde o resultado é incerto, consoante uma definição ontológica formulada por Rosa (1998). Este conceito, elucida o autor, aborda três elementos que estão presentes em quase todos os conceitos de risco, que são a noção de que o risco está dentro do quadro de preocupação ou interesse humano, a noção de que algum resultado desejável ou indesejável é possível de se implementar e a noção de incerteza quanto a sua ocorrência.

Beck (1992), por seu turno, traça uma abordagem menos dogmática e conceitua o risco como uma forma sistemática de lidarmos com os perigos e as inseguranças que foram introduzidos pela modernização industrial, pois a sua percepção é de que o risco pós-industrial é programado e, portanto, é uma ação. A propósito de contextualizar, os dados pessoais, no presente tempo, são coletados, armazenados, manejados e tratados por instrumentos de tecnologia introduzidos por esta referida modernização industrial e, assim, inserem-se na conjuntura de incertezas que a sociedade de risco preconiza existir.

Independente da abordagem conceitual, se ontológica ou não, o fato é que o risco é um elemento não circunstancial e, portanto, constantemente presente nas relações humanas. Este elemento poderia ser capital para manter a sociedade no estado de natureza, todavia, as relações humanas são fundadas em confiança, princípio este que, para Hobbes (2015), é um dos elementos que cumprem a função de separar o estado de natureza do contrato social. Para Serpa (2010), a confiança é um sentimento de superação de incerteza e da imprevisibilidade, mediante a assunção de certo grau de risco, em relação ao comportamento de terceiros, de tal modo que não se espera algo distinto da expectativa que tenha criado.

Neste breve esforço reflexivo de se tomar a confiança como princípio informador de uma sociedade de risco, emerge, como corolário, a concepção de que determinados riscos produzidos pela necessária modernização industrial, tais quais os que provém da coleta e manejo de dados sensíveis pelo Estado-Juiz, por exemplo, são tolerados e permitidos pela sociedade. Trata-se de confiança entre os cidadãos e entre cidadãos e o Estado, os quais sustentam legítimas expectativas que não devem ser frustradas.

Ante este contexto teórico, verifica-se que as estruturas do Estado de Direito disciplinam a tolerância da sociedade para com a prática de atividades geradoras de riscos de eventos danosos e, não por outro fundamento, o processo cautelar criminal distribuído para fins de coletar elementos probatórios, ainda que se manifeste como uma atividade estatal geradora de riscos, e, de fato, o é, justifica-se como medida legítima e de utilidade coletiva.

2.3 A GESTÃO DE RISCOS E A SUA INTEGRAÇÃO À GESTÃO DE PROCESSOS DE NEGÓCIO (*BUSINESS PROCESS MANAGEMENT* - BPM)

Seguindo a orientação da publicação metodológica Gerenciamento de Riscos Corporativos - Estrutura Integrada, lavrada pelo *Committee of Sponsoring Organization of the Treadway Commission* (COSO), com a colaboração da PricewaterhouseCoopers (BRASIL,

2007), para os propósitos a que se destina esta pesquisa, consideraremos tão somente os riscos de eventos que podem gerar impactos negativos e que, de modo consequente, podem impedir a criação de valor ou mesmo destruir o valor existente. Em contraposição a esta tendência, a gestão de riscos integrará o processo de criação e preservação de valor.

A gestão de riscos e os seus propósitos são amplamente relacionados pela literatura como essenciais para o alcance dos objetivos institucionais delineados no planejamento estratégico, por meio da gestão do processo de negócios de toda e qualquer entidade, privada ou pública. Como consequência, toda a cadeia produtiva deve ser racionalizada, dentre outros parâmetros administrativos, com fundamento no plano de gestão de riscos. Wagner e Disparte (2016) defendem que, para que ocorra maior integração da gestão de riscos dentro do léxico corporativo e trazê-la ao seu pleno potencial, a sua função necessita ser entendida como um instrumento catalisador para a eficaz tomada de decisões e não apenas como instrumento de prevenção do risco ou como uma função meramente regulatória.

Pode-se definir a gestão de riscos como o processo de identificar e avaliar os riscos, tomando medidas para reduzir tais riscos para um nível aceitável, consoante a primeira publicação do NIST *Special Publication* 800-30, *Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology* (ESTADOS UNIDOS DA AMÉRICA, 2002), clássica metodologia de gestão de riscos de sistemas de tecnologia da informação.

O processo de gestão de riscos deverá ser implementado por um método adequado para eliminar ou reduzir os riscos de eventos danosos, incrementando a possibilidade de sucesso do planejamento estratégico e o alcance dos objetivos institucionais. O método escolhido deverá ser capaz de estimular as oportunidades de melhor uso do tempo e de aperfeiçoamento da qualidade do produto ou serviço prestado, ao tempo em que provoca a diminuição do uso de recursos humanos, materiais e financeiros. Dionne (2013) sustenta que o objetivo da gestão de riscos corporativa é criar uma estrutura de referência que permita à companhia (entidade pública, na hipótese vertente neste artigo) lidar com o risco e a incerteza. A identificação, a avaliação e o processo de gestão do risco é parte do desenvolvimento estratégico de uma companhia (entidade pública, insistimos) e deve ser estruturada e planejada a partir do maior grau hierárquico da instituição.

Ao esboçarmos a visão do Poder Judiciário brasileiro sobre o conceito de gestão de riscos, verificamos que os elementos coincidem com a estrutura conceitual acima apresentada. A título de exemplo, por ser o órgão de cúpula do Poder Judiciário, elegemos o Guia de Gestão de Riscos (BRASIL, 2019) do Supremo Tribunal Federal (STF) como referência para o conceito adotado pelos demais órgãos jurisdicionais. O referido guia aponta que a gestão de riscos é composta por atividades coordenadas para orientar e apoiar a organização quanto aos riscos aos quais está exposta, a fim de criar, proteger e agregar valor, com vistas à melhoria do desempenho, à promoção da inovação e ao alcance dos objetivos. A gestão de riscos deve

contribuir para a formulação e para a execução da estratégia, auxiliando no fluxo de informações necessárias à avaliação dos cenários e à tomada de decisão, visando ao aproveitamento de oportunidades e à proteção da imagem institucional.

Uma moldura teórica muito bem sedimentada na literatura impõe a integração de uma gestão de riscos ao planejamento estratégico de uma entidade, pública ou privada. Sobre a gestão dos processos de negócio, ou *business process management* (BPM), Davenport (1993) a define como o conjunto estruturado e mensurado de ações através do tempo e do espaço, organizado por um começo e um fim, em que são identificáveis entradas e saídas definidas para produzir um específico resultado para um cliente ou mercado. Nesta estrutura de ações, empreendem-se muitos esforços na modelagem da forma como o processo produtivo é realizado e, como consequência, todo o processo está sujeito a erros em cada uma de suas etapas; com o propósito de consecução plena e exitosa da gestão dos processos de negócio, é essencial entender e gerir os riscos associados a cada etapa do planejamento.

Verifica-se que, no contexto da tomada de decisões e de execução de um planejamento estratégico de gestão, as questões relacionadas aos riscos são tradicionalmente separadas das questões operacionais do negócio, embora não o devessem ser, como preconizam Campbell & Stamp (2004) e March & Shapira (1987).

A gestão de riscos deve compor o ciclo de vida útil de um planejamento estratégico elaborado à luz de uma gestão dos processos de negócio, devendo estar integrada a cada fase e na transição entre cada fase do processo produtivo (Muehlen e Ho, 2005).

No mesmo sentido, Neiger; Churilov; Muehlen e Michael (2006) propõem uma visão holística do processo produtivo e que este seja pautado por uma cultura de risco, ao que chamam, então, de *risk-oriented process management* (gestão de processos orientada a riscos). Para tanto, sustentam que o modelo anteriormente proposto por Neiger e Churilov (2004), denominado *value-focused process engineering* (engenharia de processos com foco em valor), alinhem-se a uma gestão de processos de negócio orientada a riscos.

Concluímos que, para que inexista solução de continuidade na implantação da estrutura metodológica de gestão de riscos dentro de uma gestão de processos de negócio, a boa prática é alinhar os princípios do *business process management* (BPM) propostos por Brocke; Schmiedel; Recker; Trkman; Mertens e Viaene (2014) à gestão de riscos, posto que possuem absoluta similitude ontológica e pragmática. Segue o rol dos dez princípios e uma singela releitura à luz da gestão de riscos:

I. Princípio da consciência do contexto: a gestão de riscos deve se ajustar ao contexto organizacional;

II. Princípio da continuidade: a gestão de riscos deve ser uma prática permanente;

III. Princípio da capacitação: a gestão de riscos deve desenvolver capacidades;

IV. Princípio do holismo: a gestão de riscos deve ser inclusiva em escopo;

V. Princípio da institucionalização: a gestão de riscos deve ser incorporada na estrutura

organizacional;

VII. Princípio do envolvimento: a gestão de riscos deve integrar todos os grupos interessados;

VIII. Princípio da compreensão conjunta: a gestão de riscos deve criar um significado compartilhado;

IX. Princípio do propósito: a gestão de riscos deve contribuir para a criação de valor estratégico;

X. Princípio da simplicidade: a gestão de riscos deve ser econômica e não deve conter mais recursos do que os necessários para a aplicação pretendida;

XI. Princípio da apropriação tecnológica: a gestão de riscos deve fazer uso oportuno da tecnologia.

2.4 METODOLOGIAS DE GESTÃO DE RISCOS MAIS RELEVANTES

2.4.1 **ABNT NBR ISO 31000:2018**

No ano de 2009, a *International Organization for Standardization* (ISO) publicou o ISO 31000:2009, cuja edição em língua portuguesa foi elaborada e editada pela Comissão de Estudo Especial de Gestão de Riscos (CEE-63) da Associação Brasileira de Normas Técnicas (ABNT) e recebeu o nome de ABNT NBR ISO 31000. No ano de 2018 ocorreu uma extensa revisão, com alteração do conteúdo da metodologia.

A normalização contida nesta metodologia, consoante informado na publicação ABNT NBR ISO 31000 (BRASIL, 2018), tem o escopo de ditar diretrizes para a gestão dos riscos enfrentados pelas organizações, as quais poderão ser personalizadas para qualquer organização e conforme o seu contexto, não se limitando a um específico setor produtivo. Para mais, a norma se aplica a todo o ciclo de vida útil da entidade e a qualquer atividade, incluindo a tomada de decisão em todos os níveis.

Um de seus princípios é não uniformizar as ações de gestão de riscos, pois as suas diretrizes são genéricas. Assim, a implantação do plano e da estrutura de gestão de riscos deverá considerar as necessidades, os objetivos, a estrutura, as operações, os processos produtivos, as funções, os projetos, os produtos e serviços, os ativos e as práticas específicas empregadas pela entidade.

A norma ABNT NBR ISO 31000 compreende o guia com princípios e diretrizes de gestão de riscos, sendo complementada pela norma ABNT NBR ISO/IEC 31010, a qual fornece técnicas para avaliação e gestão de riscos, e pelo ISO Guia 73, que fornece o vocabulário básico para os termos e conceitos utilizados na gestão de riscos.

Esta metodologia se desenvolve por uma matriz circular centralizada num componente de liderança e comprometimento, que tem o propósito de implantar uma governança dos

riscos por meio de componentes de integração, concepção, implementação, avaliação e melhoria. Esta estrutura é organizada para auxiliar a entidade a integrar a gestão de riscos a sua gestão de processos de negócio (*business process management*).

A gestão de riscos, então, obedece à rotina de aplicar sistematicamente políticas, procedimentos e práticas capazes de estabelecer o contexto, identificar, analisar criticamente, avaliar e tratar os riscos, além de empreender comunicação e consulta, monitoramento, registro e relato destes riscos.

A crítica a esta metodologia é que, ao tempo em que permite que a entidade mantenha a estrutura formal de gestão de riscos já em prática e apenas adeque ou inclua os atributos da ABNT NBR ISO 31000 para averiguar a suficiência e eficácia da metodologia utilizada, deixa de estabelecer um método objetivo para esta readequação ou inclusão de atributos.

2.4.2 **COSO-IC *Internal Control - Integrated Framework* (Controle Interno - Estrutura Integrada)**

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) é uma entidade privada estadunidense fundada no ano de 1985, cujo propósito exordial é investigar eventos de fraudes em relatórios financeiros e contábeis. Desenvolve estruturas e metodologias de controles internos, gestão de riscos corporativos e prevenção de fraudes para a execução de uma governança corporativa ética.

No ano de 1992, ante a necessidade de se produzir uma metodologia de controles internos como premissa de uma sólida governança corporativa, o COSO lançou o *Internal Control - Integrated Framework*, vindo a se tornar a mais utilizada metodologia de controles internos, os quais são considerados importantes meios para se alcançar os fins planejados pela corporação. A avaliação dos riscos é tão somente um dos componentes desta metodologia, pois o seu escopo é, de fato, criar uma estrutura para o controle interno.

2.4.3 **COSO-ERM *Enterprise Risk Management - Integrated Framework* (Gerenciamento de Riscos Corporativos - Estrutura Integrada)**

Como instrumento apto a estruturar de forma mais ampla e abrangente a gestão dos riscos e, como efeito, melhorar a governança corporativa, o COSO elaborou, no ano de 2004, o *Enterprise Risk Management - Integrated Framework*, com a colaboração da PricewaterhouseCoopers, cuja última atualização ocorreu no ano de 2017.

Diferentemente da ABNT NBR ISO 31000, o *Enterprise Risk Management - Integrated Framework* somente abrange em seu escopo os riscos que possam produzir impactos negativos para a entidade.

A versão em língua portuguesa da publicação metodológica Gerenciamento de Riscos

Corporativos – Estrutura Integrada (BRASIL, 2007), lavrado pelo *The Committee of Sponsoring Organization of the Treadway Commission* (COSO), informa que esta metodologia envolve e inter-relaciona oito componentes: ambiente interno, fixação de objetivos, identificação de eventos, avaliação de riscos, resposta a risco, atividade de controle, informações e comunicações, monitoramento.

A metodologia *Enterprise Risk Management - Integrated Framework* não avalia os riscos corporativos em um processo seriado e não quebra a cadeia produtiva em diversas etapas, umas subsequentes às outras; diferentemente, realiza a avaliação sob um formato multidimensional e multidirecional, onde os oito componentes interagem entre si e se influenciam mutuamente. A representação desta metodologia se dá por uma matriz tridimensional inserida em um cubo, onde cada dimensão indica os objetivos da entidade (classificados em estratégicos, de operações, de comunicação e de conformidade), os níveis de organização da entidade (classificados em nível de organização, divisão, unidade de negócio e subsidiária) e os componentes de avaliação dos riscos, o que permite ao gestor, segundo o COSO, manter o completo domínio sobre o gerenciamento dos riscos.

O COSO avalia que esta metodologia *Enterprise Risk Management - Integrated Framework* será eficaz se cada um dos oito componentes não apresentar fraquezas significantes e os riscos se enquadrarem à quantidade de riscos que a entidade está disposta a tolerar (apetite a risco). Se pensarmos na administração pública e, mais notadamente, no exercício da atividade jurisdicional pelo Poder Judiciário e nos princípios reitores do Estado Democrático de Direito, certamente o apetite a risco é extremamente baixo e, no que importa aos cuidados que os dados pessoais coletados no contexto do processo criminal exigem, devemos considerar que este apetite a risco deve ser considerado nulo.

A gestão eficaz dos riscos nos quatro níveis da organização, observados os componentes de avaliação dos riscos, demonstra que a alta administração da entidade compreendeu até que ponto os objetivos estratégicos e operacionais não estão sendo alcançados, que a entidade realiza um processo de comunicação confiável e que todas as normais legais são observadas.

Por fim, esta metodologia informa que a sua eficácia é limitada pelas falhas humanas ou pelos erros na tomada de decisões. Cumpre-nos a crítica de que esta metodologia deveria lidar de forma mais sistemática e operacional com os riscos relacionados a fatores humanos, tais como o erro de avaliação e as fraudes, os quais, possivelmente, são os maiores provocadores de eventos danosos no âmbito da gestão judiciária e da gestão processual.

2.4.4 **INTOSAI GOV 9130 - *Guidelines for Internal Control Standards for the Public Sector – Further Information on Entity Risk Management***

The International Organization of Supreme Audit Institutions ou, em língua

portuguesa, Organização Internacional de Entidades Fiscalizadoras Superiores, é uma instituição apolítica voltada para a discussão de questões relacionadas à auditoria de entidades governamentais.

No ano de 2004, inspirado na metodologia COSO-IC *Internal Control - Integrated Framework*, o INTOSAI publicou uma estrutura de controle interno destinada exclusivamente para entidades públicas denominada GOV 9100 – *Guidelines for Internal Control Standards for the Public Sector*, consideradas as particularidades do processo produtivo e dos objetivos do setor público. Já no ano de 2007, como instrumento de complementação à estrutura de controle interno, e inspirado no COSO-ERM *Enterprise Risk Management - Integrated Framework*, o INTOSAI atualizou o seu guia de controle interno e publicou o GOV 9130 - *Guidelines for Internal Control Standards for the Public Sector – Further Information on Entity Risk Management*, contendo uma metodologia de gestão de riscos específica para entidades públicas.

As metodologias GOV 9100 e GOV 9130 são utilizadas pelo Tribunal de Contas da União (TCU) como um dos modelos de referência para suas práticas de controle interno e de gestão de riscos.

É incompleta e carece de aplicação em conjunto com as metodologias COSO-IC *Internal Control - Integrated Framework* e COSO-ERM *Enterprise Risk Management - Integrated Framework*, conforme especificado no próprio conteúdo dos guias GOV 9100 e GOV 9130.

2.4.5 **Série NIST *Special Publication* 800**

A série NIST SP 800 são publicações com diretrizes, recomendações, especificações técnicas e relatórios anuais para a segurança cibernética, formuladas pelo *National Institute of Standards and Technology* (Instituto Nacional de Padrões e Tecnologia), para subsidiar as necessidades de segurança do Governo Federal dos Estados Unidos da América, porém, as entidades não governamentais podem adotar tais publicações.

As publicações que mais interessam ao futuro desta pesquisa são a NIST SP 800-30 *Revision* 1 (*Guide for Conducting Risk Assessments*) e a NIST SP 800-37 *Revision* 2 (*Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*), pois é necessário que passemos a ter real preocupação com a segurança dos dados pessoais existentes nos sistemas de tecnologia da informação.

Em linhas gerais, a publicação NIST SP 800-30 *Revision* 1 concentra o seu foco na avaliação dos riscos para tratar os fatores de risco essenciais, tais como as fontes de ameaças e eventos, vulnerabilidades e condições predisponentes, impacto e probabilidade de ocorrência de ameaça, por exemplo. O propósito desta publicação é indicar as ações apropriadas como resposta para os riscos identificados nos sistemas de informação.

Por seu turno, a NIST SP 800-37 *Revision* 2 descreve uma estrutura de gestão de riscos e apresenta diretrizes para gerenciar os riscos produzidos pelos dados existentes em sistemas de informação. A estrutura apresentada propõe ser disciplinada e flexível, incluindo a categorização de segurança de informações; a seleção, implementação e avaliação de controle; as autorizações de sistema e controle comum; e o monitoramento contínuo.

2.4.6 **Série ISO/IEC 27000**

A série de normas ISO/IEC 27000 foi reservada pela ISO - Organização Internacional de Normalização - exclusivamente para padronizar a segurança da informação. Possui um amplo escopo de atuação, pois não trata tão somente de privacidade e problemas técnicos de segurança cibernética. As publicações desta série são relevantes para esta pesquisa, pois a principal publicação da série, a ISO 27001, apresenta as especificações para um sistema de gestão de segurança da informação.

2.4.7 **HazOp**

HazOp é a sigla para *Hazard and Operability* (Perigo e Operabilidade). Esta metodologia é a mais disseminada técnica de identificação de perigos e riscos no setor industrial. Por priorizar a identificação de falhas e fraquezas no processo produtivo, entendemos que a aplicação de sua filosofia pode ser útil para a administração pública.

A metodologia HazOp adota como princípio básico a manutenção das condições normais de operação, porquanto seguras; o desvio das condições normais, por seu turno, é o gerador dos perigos e riscos. Uma vez identificados os motivos de desvio das condições normais de operação do processo produtivo, os perigos e riscos são classificados em graus de probabilidade de ocorrência e graus de severidade dos danos. Para tanto[4], todo o processo produtivo é seccionado, questionado e discutido por uma equipe multiprofissional de diferentes setores da corporação, que deverá considerar todos os cenários possíveis e todos os desvios potenciais das condições normais, para identificar as não conformidades.

2.4.8 **Gestão de riscos na indústria aeronáutica e na aviação comercial civil**

Este tópico não foi aberto para relacionar e discutir exaustivamente as metodologias de gestão de riscos utilizadas pela indústria aeronáutica e pela aviação comercial civil, senão, apenas para trazer a discussão para dentro do contexto desta pesquisa. O que nos interessa, para tanto, é pesquisar e compreender o que estes dois setores produtivos podem contribuir para a gestão de riscos no Poder Judiciário, dada as suas notórias capacidades de antever os

4 GREENWOOD, Amanda. HAZOP: The Cornerstone of Effective Risk Management. Process Street. San Francisco, 2020. Disponível em: https://www.process.st/hazop/. Acesso em: 25 dez. 2020.

riscos, realizar prognósticos e antecipar a aplicação de soluções.

Os padrões de segurança e de gestão de riscos tanto da indústria aeronáutica, quanto da aviação comercial civil, são extremamente rígidos e complexos; as entidades responsáveis por criar padrões de gestão são respeitadas por seu rigor metodológico e pelo grau de austeridade com que cumprem o mister de promover a segurança do voo desde a concepção do projeto da aeronave. Os diversos recursos de gestão de riscos implantados são responsáveis por manter segura uma atividade de alto risco e, apenas para exemplificar, podemos citar a redundância dos sistemas embarcados no projeto de uma aeronave, a aplicação sistemática de *check-lists* para realizar o voo e o uso da inteligência artificial para antever eventos danosos.

Aviadores costumam afirmar que o voo de uma aeronave inicia antes da decolagem, o que aponta para uma cultura de risco muito bem absorvida por todos os membros das corporações e entidades que compõem este sistema. Esta cultura de gerenciamento de riscos não é realizada por um sistema *top-down*, ou seja, não parte de um gestor de nível hierárquico superior para que todos os demais níveis de organização obedeçam ou se adequem, como costuma ocorrer nos modelos clássicos de gestão, mas, sim, por meio de um esforço conjunto de todas as corporações e entidades envolvidas neste propósito.

A gestão de riscos na indústria aeronáutica e na aviação comercial civil é um processo cíclico, onde são identificados os pontos fracos para que estes sejam colocados sob controle, considerando-se que se trata de atividade potencialmente perigosa, inclusive no que importa à gestão de pessoas, financeira e de recursos das corporações.

3 **DISCUSSÃO QUALITATIVA**

3.1 RISCOS GERAIS NA JUSTIÇA CRIMINAL

A revisão teórica nos apresentou a importância de se planejar e executar um projeto de gestão de riscos, a sua integração à gestão de processos de negócio das organizações e delineou os principais métodos de gestão de riscos. Doravante, passaremos a abordar de forma não exaustiva alguns dos riscos que podem ser gerados pelo complexo sistema de Justiça Criminal brasileiro, notadamente nas etapas que integram o processo penal.

Como proteção aos direitos fundamentais, principalmente o direito à liberdade, à privacidade e à intimidade, a função jurisdicional e dos seus auxiliares na esfera criminal deve ser bem regrada e controlada (Marques, 2003).

Diversos são os riscos na Justiça Criminal, tais como a demora na entrega da tutela jurisdicional, a seletividade da punição e o ingresso indevido na esfera jurídica dos indivíduos. Esses riscos assemelham-se, em parte, àqueles elencados por Assi (2014), aplicáveis às organizações empresariais. Consistem no risco operacional, risco legal, risco de reputação, risco de tecnologia e riscos de falhas humanas e fraudes.

A ocorrência de prescrição gera o risco de reputação ao Poder Judiciário, pois traz prejuízo a sua imagem institucional perante a sociedade, atingindo, inclusive, um dos efeitos desejados pela persecução penal, que é a prevenção geral.

Quanto à demora na tramitação dos processos, além de gerar um risco de ocorrência de prescrição, o acúmulo de acervo dificulta a gestão processual e o tratamento dos dados que integram cada um dos feitos criminais. Isso acarreta risco operacional, que está relacionado com não-conformidades oriundas de deficiências nos processos internos, principalmente de controle. A falta de controle sistemático das atividades desenvolvidas pelo Poder Judiciário faz surgir os riscos de falhas humanas e fraudes, com o vazamento de informações pessoais, prejudicando a efetividade da atividade jurisdicional e os direitos individuais.

De acordo com o Relatório Justiça em Números, do Conselho Nacional de Justiça (BRASIL, 2020), o tempo médio de tramitação de um processo criminal na fase de conhecimento é de 4 anos, sendo 1 ano e 3 meses a mais do que os processos não criminais.

Já é possível constatar um tempo excessivo na tramitação dos processos antes mesmo de uma primeira manifestação estatal por meio da sentença de primeiro grau. Some-se a esse lapso temporal, aquele despendido na fase de investigação dos crimes, realizada antes do ajuizamento da ação penal. Conforme se pode extrair da pesquisa Justiça Criminal, Impunidade e Prescrição, organizada pelo Conselho Nacional de Justiça (BRASIL, 2019), o tempo médio para apuração de um crime pelo Polícia Federal é de 639 dias (1 ano e 09 meses). Entre as polícias estaduais, a que possui o maior tempo mediano de tramitação de inquéritos é a do estado do Rio de Janeiro, com 1.177 dias (3 anos e 2 meses). Já a polícia civil do estado do Acre é a mais eficiente, com média de 250 dias entre a instauração e o relatório do inquérito policial.

O fator tempo é um elemento que influencia na efetividade do processo penal, ante a possibilidade de desaparecimento dos substratos fáticos relacionados ao crime. Para reavivar esses fatos e tentar formar a culpa do imputado, os órgãos responsáveis pela persecução penal necessitam, assim, de material probatório hígido.

O controle na obtenção desses elementos probatórios e no tratamento deles pelo Poder Judiciário é fundamental. Juntamente com os elementos de prova, são colhidos, durante a investigação ou instrução processual, dados pessoais dos imputados e de terceiros, os quais podem ou não servir para o objetivo da persecução penal. Todos esses dados são geridos por diversos órgãos que compõem o sistema de Justiça, que não atuam necessariamente de forma integrada e muitas vezes não respeitam um padrão metodológico gerencial.

Considerando que 5,3 milhões de processos criminais estavam em tramitação no ano de 2019, conforme dados do Relatório Justiça em Números, do Conselho Nacional de Justiça (BRASIL, 2020), é possível concluir que o volume de dados pessoais acautelados pelo estado brasileiro é expressivo quantitativamente. Quando o processo possui dados sigilosos, a ausência de métodos gerenciais amplia o risco de má utilização desses elementos.

O risco também decorre da divergência de sistemas processuais existentes, o que obriga a tramitação de parte dos processos judiciais por meio físico e outra parte por sistemas informatizados. Alguns órgãos jurisdicionais possuem, inclusive, os dois modelos, como ocorre com o Tribunal Regional Federal da 1ª Região, maior Tribunal do Brasil em extensão territorial, que ainda conta com 41,29% dos processos em primeiro grau tramitando em meio físico, o que equivale a 1.645.092 processos[5] (BRASIL, 2021).

Essa também é a realidade em diversos tribunais estaduais brasileiros, que ainda possuem grande parcela de seu acervo de processos criminais. Para fins de exemplificação, o Tribunal de Justiça do Estado do Pará somente finalizou a implantação do Processo Judicial Eletrônico (PJe) em todas as suas varas no dia 18 de janeiro de 2021[6] (BRASIL, 2021). Essa implantação contempla, porém, apenas os novos processos, de sorte que todo o acervo anterior ainda é físico.

O processo judicial eletrônico que vem sendo implantado paulatinamente favorece a adoção de fluxos de atividades padronizadas e o controle de dados sigiloso, incluindo os pessoais. Todavia, trata-se de um sistema conectado à internet, o que amplia os riscos de vazamento dessas informações, no caso de falhas nos mecanismos de proteção, representando, assim, um risco tecnológico.

3.2 RISCOS DECORRENTES DA OBTENÇÃO DE DADOS PESSOAIS POR MEIO DE MEDIDAS CAUTELARES PROBATÓRIAS NO PROCESSO PENAL

A adoção de medidas cautelares com natureza probatória é autorizada para possibilitar o desenvolvimento de um processo penal que respeite os direitos do imputado, mas que também garanta a aplicação da lei penal.

As medidas mais utilizadas e que necessitam de autorização judicial são a busca e apreensão domiciliar, prevista no artigo 240, §1º, do Código de Processo Penal, a interceptação telefônica/telemática, disciplinada pela Lei Federal nº 9.296/1996, o afastamento do sigilo bancário, conforme a Lei Complementar nº 105/2001 e o afastamento do sigilo fiscal, disciplinado no artigo 198, do Código Tributário Nacional. Além do mais, no âmbito do enfrentamento às organizações criminosas, o artigo 3º, incisos IV, V e VI, da Lei Federal nº 12.850, autoriza todas essas medidas supramencionadas como meios de obtenção da prova.

Na execução da busca e apreensão deverão ser coletados todos os elementos que tenham relação com o crime. Isso não afasta o dever de o magistrado identificar o local e o objeto da busca e apreensão, como forma de evitar que dados pessoais, que não tenham

5 Disponível em: https://app.powerbi.com/view?r=eyJrIjoiNjQzNjAzYjktYTZkMy00YzI5LWIwNjUtYTQyZDMwZDk2ZjExIiwidCI6Ijk2MzgxOWY2LWUxYTMtNDkxYy1hMWNjLTUwOTZmOTE0Y2Y0YiJ9. Acesso em: 15 de fev. de 2021.

6 TJPA, Tribunal de Justiça do Estado do Pará. TJPA conclui 100% de implantação do PJe. Belém, 2021. Disponível em: http://www.tjpa.jus.br/PortalExterno/imprensa/noticias/Informes/1170118-tjpa-conclui-100-de-implantacao-do-pje.xhtml. Acesso em: 21 jan. 2021.

relação com a apuração, sejam indevidamente apreendidos ou que haja violação de domicílio sem a imprescindível autorização judicial.

A falta dessa individualização acarreta risco grave para a validade da investigação e da própria instrução processual, enquadrando-se no risco legal, que é exatamente a não-conformidade com os preceitos estabelecidos pelo ordenamento jurídico, mencionado por Assi (2014).

O Supremo Tribunal Federal, em 16/12/2014, no julgamento do *Habeas Corpus* 106.566 - SP, de relatoria do Ministro Gilmar Mendes[7], declarou ilegal e, portanto, nula, a apreensão de computadores (e o acesso ao seu conteúdo), por ter sido realizada em endereço de sociedade empresária que não constava expressamente declinado no mandado judicial.

A peculiaridade do caso consiste no fato de que a busca e apreensão foi efetuada no mesmo edifício identificado no mandado, porém em andar diverso. O que parece ser preciosismo representa, em verdade, o cuidado com a atuação estatal na obtenção de dados que são acobertados pelas garantias constitucionais da intimidade, vida privada, honra e a imagem das pessoas, bem como a inviolabilidade do domicílio. Se houve o acesso a dados e informações particulares em local diverso do autorizado, isso significa que não existiu prévia análise judicial da existência dos requisitos necessários à apreensão daqueles elementos específicos.

Além disso, no caso que serve de exemplo, instituição financeira foi o alvo da operação, de sorte que era detentora de dados pessoais, incluindo os de natureza financeira, relativos a milhares de clientes que não tinham qualquer relação com a persecução penal. Isso potencializa os riscos decorrentes da obtenção desses subsídios, sem o devido controle judicial. A intimidade desses clientes pode ter sido devassada em razão de busca e apreensão que posteriormente foi declarada nula. Se não se respeitou o devido processo legal para realizar a obtenção dos dados acobertados pelo direito ao sigilo, não há garantias de que o tratamento desses dados apreendidos tenha sido realizado de forma a preservar a intimidade e a privacidade dos seus titulares.

Uma adequada gestão de riscos, com a previsão de possíveis consequências geradas pela tomada de decisão, poderia ter evitado todo o desperdício de tempo e de recursos, bem como o prejuízo à credibilidade do Poder Judiciário.

Mesmo com a individualização do local e do objeto da busca e apreensão, ou seja, ainda que se trate de uma busca e apreensão legítima, os riscos oriundos da coleta de dados persistem. Há situações em que a correta triagem dos elementos de prova somente pode ser realizada posteriormente. Isso sói ocorrer em grandes operações com diversos alvos ou que tratam de organizações criminosas, em que o volume de material apreendido é muito grande e diversificado.

---

7 Disponível em: https://stf.jusbrasil.com.br/jurisprudencia/863934993/habeas-corpus-hc-106566-sp-sao-paulo-9944578-2920101000000/inteiro-teor-863935002. Acesso em: 10 de jan. de 2021.

Além de documentos físicos, como mencionado acima, relevante material probatório apreendido consiste em dados digitais, que se encontram em dispositivos eletrônicos. Para se ter uma ideia de como é relevante quantitativamente a apreensão de dados de informática, apresentam-se alguns números da chamada operação Lava-Jato, extraídos do sítio eletrônico oficial da Polícia Federal (BRASIL, 2018)[8], que serve de exemplo pela sua dimensão.

Até o dia 14/08/2017, haviam sido apreendidos e submetidos à perícia 5.754 elementos de prova. Dentre eles, a grande maioria era composto por dispositivos de armazenamento e equipamentos computacionais, quais sejam, 1.592 *pendrives* (28%); 985 discos rígidos de computador (17%); 967 telefones celulares (17%); 725 computadores (13%); 437 mídias óticas (8%); 139 cartões de memória (2%); 100 disquetes (2%); 97 *tablets* (2%); 93 CDs (2%); 77 DVDs (1%); 25 fitas magnéticas (1%); 14 cartões SIM (0,5%); 128 outros dispositivos computacionais (2%); 74 outros dispositivos de armazenamento computacional (1%). Ou seja, 68,5% de todo o material apreendido corresponde a aparelhos de onde são extraídos dados digitais ou digitalizados.

Esse aspecto prejudica ainda mais a triagem do que é pertinente por ocasião da execução da medida judicial. A identificação e a separação do material que servirá como elemento probatório dependerá, inclusive, de realização de perícia técnica, como forma de garantia da inviolabilidade da intimidade do imputado e de terceiros.

Quanto aos dados armazenados em computadores, o Supremo Tribunal Federal (RE 418.416, Rel. Ministro Sepúlveda Pertence, Tribunal Pleno, DJ 19/12/2006)[9] já decidiu acerca da viabilidade do acesso a esse conteúdo. Para isso, deve constar na decisão judicial a autorização para a apreensão dos computadores. Esse acesso não representa desrespeito à inviolabilidade de correspondência, uma vez que a aludida proteção diz respeito à comunicação, não havendo tutela sobre os dados considerados em si, mesmo que estejam armazenados em um computador.

Com relação aos dados inseridos em aparelhos de telefonia celular, notadamente em aplicativos de conversas como *Whatsapp*, *Telegram*, *Instagram*, dentre outros, o Superior Tribunal de Justiça tem se posicionado no sentido de que a apreensão realizada diretamente pela autoridade policial não autoriza o acesso ao conteúdo, sem que haja decisão judicial nesse sentido (HC 315.220/RS, Rel. Min. Maria Thereza de Assis Moura, Sexta Turma, julgado em 15/09/2015, DJe 09/10/2015)[10]. Por sua vez, em se tratando de busca e apreensão ordenada pela autoridade judiciária competente, o acesso ao conteúdo de conversas e mensagens armazenadas no aparelho celular é permitida (RHC 75.800/PR, 6ª Turma)[11].

---

8 POLÍCIA FEDERAL. Operação Lava-Jato: números. Polícia Federal. Ministério da Justiça e Segurança Pública. Brasília, 2021. Disponível em: http://www.pf.gov.br/imprensa/lava-jato/numeros-da-operacao-lava-jato. Acesso em: 2 jan. de 2021.

9 Disponível em: https://stf.jusbrasil.com.br/jurisprudencia/760712/recurso-extraordinario-re-418416-sc/inteiro-teor-100476877. Acesso em: 10 de jan. de 2021

10 Disponível em: https://www.conjur.com.br/dl/hc-315220-quebra-sigilo-telematico-dez.pdf. Acesso em: 10 de jan. de 2021

11 Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/862575507/recurso-ordinario-em-habeas-corpus-rhc-75800-pr-2016-0239483-8/inteiro-teor-862575526. Acesso em: 10 de jan. de 2021.

Impende consignar que no HC 91.867/PA, cuja relatoria coube ao Ministro Gilmar Mendes[12], o Supremo Tribunal Federal reconheceu a possibilidade de acesso por policiais militares à lista dos numerais telefônicos contida no aparelho de um indivíduo submetido à busca pessoal. Foi entendido que essa conduta não violaria a intimidade. Por outro lado, este precedente estabeleceu claros limites ao acesso do conteúdo de aparelhos celulares, que não pode alcançar dados pessoais, como mensagens, conversas gravadas e outros elementos.

Nos últimos 10 anos, com o desenvolvimento de aparelhos como os tablets e smartphones, vivenciou-se verdadeira revolução na tecnologia da informação. Grande quantidade de dados pessoais são armazenados, atualmente, em aparelhos móveis ou computadores profissionais e domésticos, quando não estão sincronizados em todos ou armazenados no ambiente virtual denominado nuvem. Por isso, a proteção atualmente conferida a eles deve se assemelhar àquela atribuída ao domicílio, dependendo sempre de aferição judicial prévia.

A esses casos não se aplicam as disposições da Lei Federal nº 9.296/1996, porquanto o acesso é feito aos dados armazenados nos aparelhos, relativos à comunicação pretérita. A interceptação ou escuta telefônica, ao seu turno, possibilitam o contato direto e em tempo real com as mensagens transmitidas, alcançando a transferência da informação, seja oral ou telemática.

A interceptação telefônica e telemática também é um instrumento gerador de relevantes riscos ligados à privacidade, à intimidade, ao devido processo legal e à própria administração judiciária. Importante consignar que o Brasil já chegou a ser condenado pela Corte Interamericana de Direitos Humanos (CIDH), no dia 06 de julho de 2009, no caso Escher e outros vs. Brasil[13], em razão de vícios e vazamento para a imprensa de dados pessoais oriundos de interceptações telefônicas autorizadas judicialmente e que alcançavam membros de associação e cooperativa agrícolas ligadas ao movimento dos trabalhadores sem-terra no estado do Paraná.

Como bem aponta Cabacinha (2020), foi reconhecido na aludida sentença, dentre outros aspectos, que o Brasil deixou de exercer seu dever de proteger o direito à vida privada, previsto no artigo 11, da Convenção Americana de Direitos Humanos (CADH). Fixou-se que o pedido de interceptação telefônica foi formulado por autoridade incompetente (Polícia Militar), a decisão judicial de deferimento não estava fundamentada e a interceptação não havia conexão com as supostas investigações. Também não houve comunicação ao órgão do Ministério Público para que pudesse ser exercido o controle da atuação do Estado.

Além de todas essas ilegalidades, ainda houve a divulgação de trechos das conversas obtidas nas interceptações telefônicas por programa jornalístico de televisão de grande amplitude nacional. A CIDH declarou que essa divulgação provocou sofrimento e temor às

12 Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=2792328. Acesso em: 10 de jan. de 2021.
13 Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf. Acesso em: 10 de jan. de 2021.

vítimas e trouxe prejuízos à imagem da associação da qual faziam parte, atentando contra o exercício do direito de livre associação, garantido no artigo 16, da CADH.

Perceba-se que a ausência de métodos estruturados para garantir um escorreito tratamento dos dados pessoais obtidos por meio da atuação estatal, além dos prejuízos aos direitos individuais, chegou a causar a responsabilização do Brasil no plano internacional. No âmbito interno, seja na esfera administrativa ou jurisdicional, não houve o reconhecimento de ilegalidades ou mesmo falhas procedimentais pelos agentes públicos envolvidos .

Assim, independente da forma como serão acessados os dados pessoais, torna-se uma questão extremamente relevante os métodos que serão utilizados para a devida identificação desses dados, com a separação daquilo que não é relevante para a investigação ou instrução processual. Além dessa identificação e separação, a garantia da inviolabilidade desses dados e devolução aos seus titulares, quando não servirem ao propósito da apuração, também merecem a devida estruturação.

Esses dados necessitam ser devidamente identificados e protegidos, como forma de garantia da intimidade, uma vez que é possível, inclusive, o compartilhamento deles com outras investigações ou processos, alcançando até mesmo procedimentos não criminais, conforme já decidiu, no dia 23/02/2016, a 1ª Turma do Supremo Tribunal Federal, no Inq 3305 AgR/RS, de relatoria do Ministro Marco Aurélio, com redação para o acórdão o Ministro Luis Roberto Barroso[14].

Assim, toda a cadeia de transmissão de dados pessoais também precisa ser acompanhada pelas autoridades competentes, com a utilização de sistemática materialmente eficiente que garanta o sigilo das informações, tanto para resguardar a higidez do material apreendido, como para impedir vazamentos prejudiciais ao imputado e a terceiros.

Sobre a proteção das provas obtidas no processo penal, merece referência a previsão contida no artigo 158-A, do Código de Processo Penal, introduzido pela Lei Federal nº 13.964, de 24 de dezembro de 2019, que trata da cadeia de custódia. A sistemática foi criada para proteger os vestígios coletados em locais ou em vítimas de crimes, como forma de garantir o rastreio de sua posse e manuseio, até o descarte.

Ainda que o disciplinamento legal gire em torno de vestígios materiais, sobre os quais poderão ser realizadas perícias técnicas, normalmente feitas em laboratório, a norma permite interpretação ampliativa para que seja aplicada a todo o tipo de elemento probatório que seja compreensível pelo sentido humano, o que inclui os dados pessoais imateriais obtidos em medidas cautelares criminais.

A preocupação é com o risco operacional que pode gerar a quebra da cadeia de custódia da prova, impedindo que se consiga reconhecer o seu valor por possível adulteração ou perecimento de elementos caracterizadores. Por outro lado, a manutenção de uma cadeia de custódia bem realizada também protege direitos fundamentais e por isso deve ser

14 Disponível em: https://stf.jusbrasil.com.br/jurisprudencia/25286561/inquerito-inq-3305-rs-stf/inteiro-teor-143454395. Acesso em: 10 de jan. de 2021.

concretizada no plano fático e não apenas normativo. Essa concretização perpassa necessariamente pela adoção de métodos adequados de gestão de riscos.

A preocupação não recai somente sobre os elementos probatórios necessários à demonstração da ocorrência de um crime e da correta identificação de seu autor, mas também sobre os dados pessoais que são obtidos juntamente com eles e que podem servir ao deslinde da causa ou não.

Para mitigar, prevenir ou corrigir esses riscos, temos defendido a adoção de metodologias de gestão de riscos, normalmente adotadas no âmbito empresarial, para o tratamento dos dados pessoais obtidos por meio de medidas cautelares no processo penal. Propugna-se que, nesse aspecto, em muito se assemelha a atuação dos órgãos jurisdicionais com a de organizações empresariais que lidam com rotinas bem estruturadas, níveis hierárquicos de organização e até mesmo com a coleta e tratamento de dados pessoais.

3.3 A REGULAMENTAÇÃO DA PROTEÇÃO DE DADOS PESSOAIS

3.3.1 **A regulamentação pela União Europeia**

Se a coleta de dados pessoais deve ser autorizada de forma bastante criteriosa e sempre balizada pela ordem normativa, o tratamento dos dados coletados merece igual ou maior atenção. A preocupação com a inviolabilidade da vida privada é compartilhada por todas as nações, notadamente em razão da facilidade com que os dados são transmitidos atualmente com o avanço da utilização da internet e outros meios tecnológicos de transmissão de informação.

No âmbito europeu, aprovou-se no ano de 2016, com entrada em vigor em 25 de maio de 2018, o Regulamento Geral sobre a Proteção de Dados – RGPD - (UE) 2016/679, que sucede a Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995. O escopo do meticuloso regulamento é promover uma segura transmissão de dados pessoais entre os integrantes da União Europeia, bem como possibilitar que tais dados também sejam compartilhados com países não membros da comunidade e organismos internacionais. A regulamentação é destinada a enquadrar o tratamento de dados de caráter pessoal tanto no setor privado, como no setor público (Degrave, 2018).

De forma mais específica para a área criminal, foi aprovada a Diretiva (EU) 2016/680, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, que tem por objetivo proteger dados pessoais e conferir o devido tratamento a eles pelas autoridades competentes para efeitos de "*prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados*" (BÉLGICA, 2016).

Essa Diretiva, assim como o RGPD, traz expressa menção à necessidade de resguardar os dados pessoais, independentemente da nacionalidade e domicílio de seu titular,

impondo que sua utilização somente se dê para finalidade específica, explícita, legítima e compatível com as disposições da Diretiva. Também apresenta como um de seus objetivos a facilitação do intercâmbio desses dados entre as autoridades competentes dos Estados-Membros, como forma de assegurar a eficácia da cooperação judiciária em matéria penal e cooperação policial (BÉLGICA, 2016).

No aspecto procedimental, a Diretiva estabelece, como forma de assegurar o tratamento devido, que todos os dados pessoais devem ser manejados com respeito a um nível adequado de segurança e confidencialidade, principalmente para evitar que pessoas não autorizadas tenham acesso a eles. Devem-se levar em conta as técnicas e tecnologias mais modernas para a proteção de dados. Também deve ser aferido o custo de aplicação da tecnologia de proteção dos dados, confrontando-a com a natureza dos dados pessoais a resguardar.

A Diretiva impõe, ainda, a criação pelos Estados-Membros da União Europeia de, pelo menos, uma autoridade de controle dos dados pessoais coletados, que deve ter natureza pública e ser tecnicamente independente. Essa autoridade de controle realizará, dentre outras atribuições, a efetiva fiscalização de todos os procedimentos de coleta e tratamento de dados pessoais, podendo realizar investigações, recomendações e corrigir não-conformidades administrativas. Deve ser permitida à autoridade de controle a comunicação à autoridade judiciária do respectivo país sobre eventuais violações à Diretiva, podendo, ainda, intervir em processos judiciais.

Visualiza-se, assim, a centralização do controle desses dados pessoais, mesmo quando obtidos em decorrência de atos investigatórios ou da persecução penal, favorecendo a transparência na fiscalização. Mas a simples regulamentação não se apresenta suficiente se não for adotada uma metodologia adequada de gestão dos dados, exatamente pelas autoridades responsáveis por isso, seja de forma centralizada ou não.

Tanto o regulamento, quanto as normas que o introduziram no âmbito dos ordenamentos jurídicos internos dos Estados-Membros da União Europeia, não especificam os métodos para o tratamento desses dados. Realmente não poderiam fazê-lo, pois se trata de um aspecto operacional que é alterado constantemente pelos avanços tecnológicos e pela identificação de novos riscos. Por outro lado, tentou-se delinear o arcabouço normativo que permitiria uma sistematização desse tratamento de dados pessoais.

Para essa finalidade, ainda no âmbito europeu, merece referência o Regulamento (EU 2017/1939), de 12 de outubro de 2017, que institui a Procuradoria Europeia com competência para "*investigar, instaurar a ação penal e deduzir acusação e sustentá-la na instrução e no julgamento contra os autores e seus cúmplices nas infrações penais lesivas dos interesses financeiros da União previstas na Diretiva (UE) 2017/1371*". Nele também é disciplinado o tratamento dos chamados dados pessoais operacionais, incluindo a respectiva avaliação de impacto, notadamente em razão da utilização de novas tecnologias, mecanismos ou

procedimentos.

A definição de dados pessoais operacionais consta no anexo do regulamento delegado (EU) 2020/2153. São aqueles relacionados à identificação de uma pessoa, tais como nome de família, nomes próprios, alcunhas ou pseudônimos, nacionalidade, local de nascimento, de residência, profissão, números de documentos de identificação, de telefone, endereço de correio eletrônico, número de contas bancárias, matrículas de veículos, referência a ativos pertencentes ou utilizados pela pessoa e referência à eventual participação em atividade criminosa.

O artigo 55º, do Regulamento (EU) 2017/1939, delineia, ainda, categoria especial de dados pessoais operacionais, que se assemelham conceitualmente aos dados sensíveis previstos na LGPD brasileira. Esses dados somente podem receber tratamento se forem complementares a outros dados pessoais obtidos e se imprescindíveis para as investigações da Procuradoria Europeia, com os devidos cuidados relativos aos direitos do titular dos dados.

Com as ressalvas mencionadas acima, os dados pessoais podem ser inseridos em um sistema de gestão de processos da Procuradoria Europeia, na forma do artigo 43º, do Regulamento (EU) 2017/1939.

Esse sistema tem por escopo, dentre outros, possibilitar o controle da licitude do tratamento de dados pessoais operacionais, bem como garantir o acesso seguro às informações sobre investigações e processos penais e permitir o cruzamento de informações e extração de dados para análise operacional e estatística.

Na hipótese de a Procuradoria Europeia desejar criar um novo ficheiro, que consiste em qualquer conjunto estruturado de dados pessoais, ela deverá realizar consulta prévia à Autoridade Europeia para a Proteção de Dados, quando a avaliação de impacto apontar para elevado risco aos direitos e às liberdades dos titulares dos dados.

A atuação da Autoridade Europeia para a Proteção de Dados é um exemplo claro de concretização de um método de gestão de riscos quanto ao tratamento de dados pessoais na seara da persecução penal. Esse órgão da União Europeia, de caráter independente, foi criado pelo Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018. A aludida Autoridade irá aferir de forma pormenorizada todos os aspectos envolvendo a coleta e o tratamento de dados pessoais operacionais, apresentando recomendações que visam diminuir os riscos para os referidos dados, como forma de proteger os direitos e as liberdades dos seus titulares.

Em um caso apreciado, que serve como paradigma, foi apresentado pela Procuradoria Europeia pedido de apreciação prévia pela Autoridade Europeia para a Proteção de Dados, dos riscos identificados em um sistema de gestão de processos (BÉLGICA, 2020). A Autoridade Europeia para Proteção de Dados realizou uma análise criteriosa de toda a documentação enviada pela Procuradoria Europeia. Na oportunidade, avaliou a conformidade da sistemática utilizada para o tratamento dos dados pessoais inseridos em um sistema de gestão de processos com o quadro jurídico aplicável.

No pedido de análise prévia, a Procuradoria Europeia já apontou os riscos que identificou para os dados pessoais. Foram apresentadas, ainda, as propostas de mitigação desses riscos, que alcançam aspectos de natureza organizacional, técnica ou mesmo legal, o que foi aferido pela autoridade consultora.

A Autoridade Europeia para Proteção de Dados chegou a elogiar a metodologia adotada pela Procuradoria Europeia, por ter incluído fatores de risco e matriz de probabilidade de impacto, bem como pela completude da descrição da situação a ser analisada, focando na abordagem dos riscos para os titulares dos dados. Apesar disso, passou a delinear uma série de comentários e recomendações sobre a metodologia adotada pela Procuradoria, assim como apresentou recomendações sobre os riscos apontados.

Não obstante o fato de que a presente pesquisa não nos permite abordar todas as recomendações apresentadas pela Autoridade Europeia para Proteção de Dados, é relevante apresentar em linhas gerais a forma de abordagem realizada pela referida Autoridade, pois é uma demonstração de como esta gestão de riscos está sendo tratada com seriedade no âmbito europeu.

O primeiro aspecto tratado foi o equívoco da Procuradoria Europeia ao abordar evento e risco como sinônimos. Foi esclarecido, então, que eventos e riscos possuem conceitos distintos, porquanto um evento já possui seu impacto e probabilidade. Por sua vez, o risco é oriundo de um evento e representa um resultado possível, normalmente negativo, de um evento. Igualmente, houve crítica quanto à insuficiência na descrição das medidas de mitigação dos riscos. Apontou-se que a falha conceitual entre eventos e riscos acarretou a falta de descrição da forma como um risco pode se materializar, impossibilitando que a medida de mitigação fosse suficientemente específica.

Perceba-se que a preocupação da Autoridade Europeia para a Proteção de Dados é com a especificação e concretização de medidas que tenham o condão de mitigar, prevenir ou corrigir os riscos que possam prejudicar os titulares dos dados pessoais em tratamento.

A referida autoridade entende não ser suficiente apenas delinear regras internas de procedimento da Procuradoria Europeia ou de processamento dos dados ou, ainda, apresentar regras acerca do oficial de proteção dos dados. É necessário que seja delineado de maneira clara qual dessas regras será aplicada quando da ocorrência de um caso particular. Ou seja, os meios de mitigação, prevenção ou correção de riscos ou de resposta para um evento devem ser sistematizados de maneira completa e concreta.

Um dos principais riscos que permeiam o tratamento de dados pessoais é o consistente no possível vazamento destes. A Procuradoria Europeia apresentou na consulta, como risco, a ausência de notificação e tratamento de violações a dados pessoais. Para esse cenário, a autoridade consultora recomenda a especificação de medidas destinadas a abordar o risco particular. Também orienta a criação de uma política de não violação de dados pessoais, possuindo características determinadas que envolvam a análise de risco, o processo de

notificação à Procuradoria Europeia e, quando aplicável, a comunicação aos titulares dos dados violados.

Quanto aos demais riscos que foram apontados pela Procuradoria Europeia, a Autoridade Europeia para Proteção de Dados passa a fazer a correlação deles com as obrigações existentes nos regulamentos que tratam da matéria. As recomendações são, então, formas de aprimorar a sistemática já proposta pela Procuradoria Europeia, sempre com o escopo de dar efetividade às normas de proteção aos dados pessoais.

O que se quis evidenciar com a apresentação, ainda que de forma superficial, da atuação do aludido órgão de consulta europeu, é que todo o processo produtivo que envolva a coleta e o tratamento de dados pessoais necessita seguir métodos de gestão de risco. Sem isso, torna-se impossível até mesmo verificar a ocorrência de eventuais violações, ante a possível fragmentação dos dados e a facilidade na sua dispersão pelos diversos meios de comunicação atualmente existentes.

3.3.2 **A busca por uma regulamentação no Brasil**

No Brasil, não obstante esteja em vigor a Lei Geral de Proteção de Dados - LGPD (Lei Federal nº 13.709/2018), não há normatização específica sobre o tratamento de dados pessoais na esfera da investigação e da persecução penal, pois expressamente excluída da LGPD, na forma do seu artigo 4º, *caput*, inciso III, alíneas "*a*" e "*d*", c/c § 1º.

Em razão, disso, foi instituída pela presidência da Câmara dos Deputados, no dia 26 de novembro de 2019, Comissão de Juristas que apresentou Anteprojeto de Lei de Proteção de Dados para a segurança pública e investigação criminal.

Como apresentado na exposição de motivos do referido anteprojeto de lei, a finalidade é delinear parâmetros à efetivação do tratamento de dados pessoais, quando estes forem obtidos em atividades de segurança pública e de persecução criminal. Seguindo as linhas gerais da Diretiva (EU) 2016/680 da União Europeia, o anteprojeto de lei brasileiro visa a proteção dos dados pessoais, evitando o seu uso indevido. Além disso, quer possibilitar o acesso de autoridades às ferramentas e às plataformas atuais utilizadas na área da segurança pública e de investigações, considerando que a troca de informações entre autoridades internacionais fica obstada pela falta de regulamentação interna.

Considerando que se trata de um anteprojeto de lei, que ainda passará por todo o processo legislativo, não se adentrará na análise detalhada sobre suas disposições. Mas é válido destacar os princípios da segurança da informação, prevenção, responsabilização e prestação de contas, indicados no artigo 6º, incisos IX, X e XII, do anteprojeto. Estes princípios representam o reconhecimento da necessidade de adoção de medidas concretas e metodologicamente adequadas para a garantia da inviolabilidade da intimidade das pessoas. Para isso, faz-se necessária a correta avaliação de riscos e a adoção de medidas de mitigação,

prevenção ou correção dos eventuais danos oriundos do tratamento de dados pessoais obtidos em investigações ou persecução penal.

A finalidade do presente estudo é exatamente analisar a possibilidade de os métodos de gestão de riscos apresentados e adotados por entidades públicas e privadas serem aplicados à proteção de dados pessoais dentro de um processo judicial, para que essa proteção não permaneça apenas no plano normativo, sendo efetivamente realizada pelas autoridades competentes.

3.4 METODOLOGIAS DE GESTÃO DE RISCOS APLICADAS À ATIVIDADE JURISDICIONAL

O Poder Judiciário já adota métodos de gerenciamento de processos de negócios (*business process management*) e a gestão dos riscos deve ser tomada como parte preponderante de um planejamento estratégico de gestão. O Conselho Nacional de Justiça (CNJ), desde o ano de sua instalação (2005), tem fomentado as boas práticas de governança no âmbito do Poder Judiciário, ainda que por modelos tecnocráticos (no sentido *top-down*) e, algumas vezes, despidos de rigores metodológicos.

Mesmo quando aplicados métodos de gestão no âmbito do Poder Judiciário, estes costumam se limitar ao aspecto da administração burocrática, que visa à organização dos servidores, às atividades desempenhadas no serviço público e à gestão de patrimônio. Quanto à tramitação de processos judiciais, que é a atividade fim do Poder Judiciário, costuma-se conceber que as regras estabelecidas em lei, que estruturam os ritos, são suficientes para a garantia de um desenvolvimento hígido e eficiente.

Como já exposto quando da apresentação dos riscos existentes na Justiça Criminal, nem sempre as normas legais conseguem prever todas as situações que podem gerar esses riscos, sendo necessária, também no acompanhamento processual, a utilização de métodos de gestão de riscos.

As normas legais preveem os limites de atuação de todos aqueles que participam da relação jurídico-processual, o que inclui o juiz, que terá a função de concretizar a norma no plano fático. Não tratam, porém, dos aspectos operacionais que giram em torno de uma decisão judicial.

É imprescindível, pois, a sistematização das atividades de forma coordenada, com a aferição prévia dos riscos que podem ser gerados em razão de cada participação individual dos servidores, dos juízes e de todos aqueles que, de alguma forma, atuem no processo. Além disso, o ambiente em que os processos judiciais tramitam deve ser adequado e eficiente.

Notadamente no âmbito do processo criminal cautelar, que é o foco de análise do presente artigo, o processamento das demandas de forma adequada e sistematizada é ainda mais importante, uma vez que as consequências da decisão judicial costumam atingir bens

jurídicos individuais relevantes e antes da efetiva formação da culpa. Desse modo, tanto a organização dos processos judiciais criminais quanto o tratamento de todos os dados que estão neles contidos, o que inclui dados pessoais colhidos nas investigações ou mesmo durante a instrução processual, necessitam de meticulosa e adequada sistematização metodológica.

Como já delineado, existem diversas metodologias de gestão de riscos, todas muito bem estruturadas. Para a Justiça criminal, a implantação de uma metodologia específica deve levar em conta a capacidade de adaptação e personalização, ante as suas peculiaridades. Em razão disso, acredita-se que a verificação da metodologia mais adequada para aplicação no âmbito da Justiça Criminal depende de uma prévia pesquisa experimental, por meio da aplicação controlada das diversas metodologias de gestão de riscos ou de seus elementos principais em unidades judiciárias com características semelhantes.

Mesmo antes dessa aplicação experimental, pode-se destacar características de algumas das metodologias que apontam para a possível adequação à gestão de riscos no âmbito do processo criminal. Então, façamos um singelo exercício racional.

A primeira delas é a relacionada a não uniformização das ações de gestão de risco contida na ABNT NBR ISO 31000:2018. Isso possibilita a desejada personalização, ante as diferenças estruturais encontradas em cada unidade judiciária brasileira. O método de gestão de risco a ser adotado deverá levar em consideração a quantidade de servidores, de auxiliares e mesmo de juízes vinculados à unidade judiciária. Também deve considerar a estrutura física da unidade e os sistemas de acompanhamento processual disponíveis.

Existem diversas unidades judiciárias, seja na Justiça estadual ou federal, que não possuem apenas competência criminal. De igual modo, ainda é comum tramitarem nessas unidades com competência ampla, processos físicos e virtuais. Assim, essa adaptabilidade da ABNT NBR ISO 31000:2018 pode ser adequada à atividade do Poder Judiciário.

A distribuição de tarefas com a consideração das características de cada servidor e a elaboração de rotinas de checagem das atividades, com comunicação direta entre juiz e servidor, para o necessário monitoramento, permitem a identificação dos riscos e não conformidades, o que pode evitar consequências graves.

Normalmente, o deferimento de uma medida cautelar de natureza probatória no processo criminal impõe o sigilo até a prática de todos os atos concretos necessários ao seu cumprimento. Se não houver uma sistematização adequada, gera-se o risco de vazamento de informações relativas à decisão, prejudicando a sua efetividade. Esse risco pode estar relacionado à atuação das pessoas que participam do processo ou mesmo do ambiente onde ele tramita.

A metodologia desenvolvida pelo COSO (ERM - *Enterprise Risk Management - Integrated Framework*), que tem por escopo realizar um controle interno das organizações, pode ser de extrema valia no âmbito do processo criminal cautelar, notadamente como forma de minimizar o risco de não conformidades no procedimento. Os oito componentes da

metodologia, já apresentados anteriormente, poderiam permitir um controle constante de todas as etapas que integram a tomada e o cumprimento de decisões judiciais no âmbito do processo criminal que impliquem na obtenção de dados pessoais.

Ao levar em conta o ambiente interno, a aplicação da metodologia em comento está em consonância com medidas que já vem sendo adotadas pelo Poder Judiciário e que precisam avançar para o incremento da segurança no tratamento dos dados coletados.

Como reconhecimento dessa necessidade, a versão 2.1.8.0 do sistema PJe, atualizado no dia 27 de novembro de 2020, adotada pelo Tribunal Regional Federal da 1ª Região, apresenta cinco novos níveis de sigilo na tramitação processual (BRASIL, 2020)[15]. Isso possibilita maior restrição do acesso aos elementos contidos nos autos eletrônicos, com o controle pelo usuário de maior nível.

Apesar de representar um avanço para a segurança dos dados pessoais contidos em processos criminais que tramitam no ambiente virtual, não se pode olvidar que ainda há grande acervo físico tramitando em diversas unidades judiciárias pelo país. Nestes casos, o controle de processos sigilosos e dos dados pessoais neles contidos não pode se limitar à identificação de processo como sigiloso em sua capa e à guarda em um escaninho diferenciado. A aplicação de método de gestão de risco que avalie a existência de falhas e fraquezas no processo produtivo se faz necessária.

É exatamente essa a principal característica da metodologia HazOp. Com ela, poder-se-ia buscar uma forma de integrar as diversas instâncias do Poder Judiciário, para a identificação de possíveis desvios operacionais do padrão esperado para as medidas cautelares probatórias no âmbito do processo criminal. Não estaria limitada essa análise, portanto, ao primeiro grau de jurisdição.

Isso de modo algum iria interferir na independência funcional, que permaneceria preservada. Do mesmo modo, não haveria antecipação de posicionamento ou mitigação do caráter revisor da instância superior. O que se poderia adotar, como forma de garantia da higidez do procedimento e do material apreendido, seria uma atuação concertada no plano da identificação prévia dos riscos, com sua classificação em graus de probabilidade de ocorrência, para guiar a atuação de cada juiz e dos demais colaboradores que participam do processo.

Além do mais, para o escorreito tratamento dos dados pessoais coletados em medidas criminais cautelares, é necessário que sejam seguidos de forma rigorosa todos os protocolos de segurança previamente traçados após a análise dos riscos. A observância aos padrões de atuação pré-estabelecidos alcança todos aqueles que, de alguma forma, são responsáveis pela condução processual, o que inclui servidores e juízes.

O nosso atual sistema de justiça não mais concebe uma atuação artesanal do juiz. Seria o plano ideal, mas impossível quando se verifica o grande volume de processos que nele

15 Disponível em: https://portal.trf1.jus.br/portaltrf1/comunicacao-social/imprensa/noticias/institucional-pje-ganhara-nova-versao-do-sistema-2.htm. Acesso em: 15 de jan. de 2021.

ingressam diariamente. Este problema é agravado em unidades judiciárias com competência ampla, como costuma ocorrer em diversas subseções judiciárias da Justiça Federal e comarcas da Justiça Estadual no interior do Brasil.

Assim, ainda que o ato decisório seja individual e necessite da atenção e dedicação do julgador, a análise processual é dividida em diversas etapas, das quais participam um número variado de pessoas. Cada integrante da cadeia produtiva deve ter o conhecimento da importância de sua atuação para o alcance dos objetivos da organização, mas não apenas isso é suficiente.

É importante que os protocolos de segurança sejam bem definidos e sistematizados em manuais de fácil compreensão, mas com a completude necessária para que todos tenham a possibilidade de realizar check-lists que evitarão não-conformidades prejudiciais à higidez do processo e aos direitos dos atingidos por ele. Essa é uma das características da gestão de riscos encontrada na indústria aeronáutica e na aviação comercial civil, que pode ser incorporada ao processo criminal cautelar.

Se dentro do processo judicial eletrônico existem mecanismos para controle do acesso aos dados ali inseridos, antes da inserção de tais informações no ambiente digital do sistema PJe o controle e gestão é determinado por cada unidade judiciária.

É comum a troca de informações entre membros da equipe antes de o ato ser inserido no processo judicial eletrônico. Garantir que esses dados estão sendo organizados e manuseados de forma segura, para evitar vazamentos, é um dos objetivos da adoção de um método adequado de gestão de risco, por ser imperioso o respeito à privacidade, notadamente em razão da repercussão que uma vida conectada em rede de computadores pode gerar (Magrani, 2019).

Não pretendemos ser exaustivos. Ao apresentar estes singelos exemplos, tivemos o propósito de demonstrar que cada metodologia necessitará ser escrutinada exaustivamente para aferir a solução mais adequada para a gestão dos riscos gerados pela coleta e pelo tratamento de dados pessoais no processo criminal cautelar.

4 **CONCLUSÃO**

A gestão de riscos é metodologia que se soma ao gerenciamento de processos produtivos e, como tal, é um instrumento legítimo e adequado para a gestão judiciária, a gestão processual e para o exercício da atividade jurisdicional.

Apresentado um pequeno rol não exaustivo de riscos de eventos danosos prováveis pela coleta e manejo de dados pessoais no âmbito do processo cautelar criminal, constatou-se que, para evitá-los ou minimizá-los, não é suficiente a simples aplicação da legislação que regulamenta os ritos processuais e a atuação judicial.

Ainda no âmbito normativo, foram expostas iniciativas no plano internacional e

interno que buscam regulamentar a proteção de dados pessoais. Com o desenvolvimento de ferramentas tecnológicas que facilitam a transmissão de dados globalmente, não se pode negar a relevância da normatização de toda conduta que atinja essa categoria de dados, principalmente porque praticada pelo próprio Estado.

Destacou-se, ainda, que, no Brasil, a Lei Geral de Proteção de Dados não tratou especificamente sobre a coleta e o tratamento de dados no âmbito da investigação e processo judicial criminal. Apesar de existir um anteprojeto que regula exatamente esta questão, destaca-se a necessidade de que a proteção não permaneça no plano normativo, sendo realizada efetivamente pelas autoridades competentes.

De modo consequente, ante a existência de riscos verificáveis e a revisão teórica sobre a gestão de riscos, é imperativa a adoção de uma metodologia adequada para a gestão dos riscos produzidos na hipótese vertente.

Neste estudo preliminar, vislumbra-se que as metodologias existentes e utilizadas para a gestão de processos de negócios podem ser aplicadas à gestão judiciária dos dados pessoais obtidos em medidas cautelares de natureza probatória. Existe, inclusive, similitude no desiderato, eis que tanto as organizações privadas, quanto as públicas, incluído nestas o Poder Judiciário, buscam satisfazer seu público-alvo, sem descurar da segurança necessária em cada etapa do processo produtivo.

Não se trata, porém, de mera tentativa de aplicação direta e irrestrita das metodologias de gestão de risco para estes específicos procedimentos judiciais. Considerando as peculiaridades da atividade jurisdicional, a adaptação das metodologias pode se fazer imprescindível.

O presente artigo não encerra esta pesquisa, pois o tema explorado merece e exige maior escrutínio científico e uma resposta pragmática e propositiva. Por tal motivo, serão promovidas novas diligências investigativas para, em momento oportuno, apresentarmos novas contribuições para a formação de uma base teórica apta a promover, efetivamente, a gestão dos riscos causados pela coleta e pelo manejo de dados pessoais no âmbito do processo cautelar de natureza criminal.

REFERÊNCIAS

ASSI, Marcos. **Controles Internos e Cultura Organizacional**. 2. ed. São Paulo: Saint Paul Editora, 2014. 191 p.

BARROSO, Luiz Roberto. Anuário iberoamericano de justicia constitucional. *In:* JUDICIALIZAÇÃO, ATIVISMO JUDICIAL E LEGITIMIDADE DEMOCRÁTICA. 13. ed. 2009.

BECK, Ulrich. **Risk Society**: Towards a New Modernity. 1. ed. Londres: Sage Publications, 1992. 272 p.

BRASIL, Superior Tribunal de Justiça. **Gestão de riscos**: Ed. rev. e atual. Brasília: STJ, 2016. 35 p. Disponível em: https://www.stj.jus.br/publicacaoinstitucional/index.php/GeR/article/view/3489/3612. Acesso em: 13 jan. 2021.

BRASIL, Supremo Tribunal Federal (STF). **Guia de gestão de riscos [recurso eletrônico]**. Brasília: STF, Secretaria de Gestão Estratégica, Escritório de Gestão Aplicada, 2019. 49 p. Disponível em: http://www.stf.jus.br/arquivo/cms/centralDoCidadaoAcessoInformacaoGestaoEstrategica/anexo/GestaodeRiscos/GuiaGestaodeRiscos.pdf. Acesso em: 13 jan. 2021.

BRASIL. Presidência da República. Lei Federal n. 13.709, de 14 de agosto de 2018. Diário Oficial da União. Brasília, 15 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 12 jan. 2021.

BROCKE, Jan vom *et al*. Ten principles of good business process management. **Business Process Management Journal**, Londres, v. 20, n. 4, p. 530-548, jul. 2014. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/BPMJ-06-2013-0074/full/html. Acesso em: 24 nov. 2020.

CABACINHA, Paulo Máximo de Castro. **O Poder Judiciário Nacional e a Corte Interamericana de Direitos Humanos**: Diálogo ou indiferença?. 1. ed. Belo Horizonte: Arraes Editores, 2020. 257 p.

CAMPBELL, Philip L.; STAMP, Jason E.. A classification scheme for risk assessment methods. **Sandia National Laboratories**, Albuquerque, p. 29, 2004. Disponível em: https://energy.sandia.gov/wp-content/gallery/uploads/sand_2004_4233.pdf. Acesso em: 23 dez. 2020.

CNJ, Conselho Nacional de Justiça. **Relatório Justiça em números 2020**: ano-base 2019. Brasília: CNJ, 2020. 267 p. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2020/08/WEB-V3-Justi%C3%A7a-em-N%C3%BAmeros-2020-atualizado-em-25-08-2020.pdf. Acesso em: 20 jan. 2021.

CNJ, Conselho Nacional de Justiça (Coord.); Núcleo de Estudos de Políticas Públicas da Universidade de São Paulo e Associação Brasileira de Jurimetria. **Relatório analítico propositivo**: Justiça Criminal, impunidade e prescrição. Brasília: CNJ, 2019. 188 p. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2018/01/6ab66f9a7c1f5c99878f04a46f8279e4.pdf. Acesso em: 20 jan. 2021.

Committee of Sponsoring Organizations of the Treadway Commission – COSO. COSO Gerenciamento de Riscos Corporativos - Estrutura Integrada: Sumário Executivo e Estrutura. **PricewaterhouseCoopers LLP**, Brasil, 2007. 141 p.

CRAWLEY, Frank; TYLER, Brian. **HazOp**: Guide to Best Practice. 3. ed. Amsterdã: Elsevier, 2015. 168 p.

DAVENPORT, Thomas H.. **Process Innovation**: Reengineering Work Through Information Technology. Boston, Mass: Harvard Business School Press, 1992. 352 p.

DEGRAVE, Élise. Le règlement général sur la protection des données et le secteur public.

Revue de droit communal, Wolters Kluwer, v. 1, p. 4-14, 2018. Wolters Kluwer.

DIONNES, Georges. Risk Management: History, Definition, and Critique. **Risk Management and Insurance Review**, v. 16, n. 2, p. 147-166, 2013. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2231635. Acesso em: 5 jan. 2021.

EDPS, European Data Protection Supervisor. **Opinion on the European Public Prosecutor's Office's prior consultation on the risks identified in the Data Protection Impact Assessment carried out on its Case Management System**. Bruxelas: EDPS, 2020. Disponível em: https://edps.europa.eu/sites/edp/files/publication/20-10-01_prior_consultation_opinion_eppo_dpia_cms_2020-0568_en.pdf. Acesso em: 29 dez. 2020.

GREENWOOD, Amanda. **HAZOP**: The Cornerstone of Effective Risk Management. **Process Street**. San Francisco, 2020. Disponível em: https://www.process.st/hazop/. Acesso em: 25 dez. 2020.

HAMMER, Michael. What is Business Process Management?. *In:* BROCKE, Jan vom; ROSEMANN, Michael. **Handbook on Business Process Management 1**: Introduction, Methods, and Information Systems. 1. ed. Berlim, Heidelberg: Springer, v. 1, 2010. 612 p. cap. 1, p. 3-16. Disponível em: https://doi.org/10.1007/978-3-642-00416-2_1. Acesso em: 13 jan. 2021.

HOBBES, Thomas. **Leviatã, ou matéria, forma e poder de um estado eclesiástico e civil**. Tradução Rosina D'Angina. 1. ed. São Paulo: Martin Claret, 2014. 544 p. Tradução de: Leviathan, or matter, form and power of a commonwalth ecclesiastical and civil.

MACHADO, Mariana Bicalho. **Taxonomia de eventos de risco operacional do Poder Judiciário**. Brasília, 2018. 48 p. Trabalho de Conclusão de Curso (Especialização em Gestão Pública) - Escola Nacional de Administração Pública (enap), Brasília, 2018. Disponível em: https://repositorio.enap.gov.br/bitstream/1/3399/1/Artigo%20Mariana%20Bicalho%20-%20Vers%c3%a3o%20Postada.pdf. Acesso em: 23 dez. 2020.

MAGRANI, Eduardo. **Entre dados e robôs**: ética e privacidade na era da hiperconectividade. 2. ed. Porto Alegre: Arquipélago Editorial, 2019. 304 p.

MARCH, James G.; SHAPIRA, Zur. Managerial Perspectives on Risk and Risk Taking. **Management Science**, v. 33, n. 11, p. 1404-1418, nov. 1987.

MARQUES, José Frederico. **Elementos de direito processual penal**. 2. ed. Campinas: Millenium, v. 1, 2003. 478 p. (revista e atualizada por Eduardo Reale Ferrari).

MUEHLEN, Michael zur *et al*. Risk Management in the BPM Lifecycle. *In:* BUSINESS PROCESS MANAGEMENT WORKSHOPS. BPM 2005. LECTURE NOTES IN COMPUTER SCIENCE. 2005. **Proceedings [...]** Berlim: Springer, 2006. Disponível em: https://doi.org/10.1007/11678564_42. Acesso em: 22 dez. 2020.

NAJI, Hafeth I.; ALI, Rouwaida Hussein; AL-ZUBAIDI, Ehsan Ali. Risk Management Techniques. *In:* EMEAGWALI, Okechukwu Lawrence. **Strategic Management**: a Dynamic View. Londres: IntechOpen, 2019. 35 p. cap. 6. Disponível em: https://doi.org/10.5772/intechopen.85801. Acesso em: 16 dez. 2020.

NEIGER, D. *et al*. Integrating risks in business process models with value focused process

engineering. *In:* EUROPEAN CONFERENCE ON INFORMATION SYSTEMS (ECIS), 14. 2006. **Proceedings [...]**. AIS Electronic Library (AISeL), 2006. Disponível em: https://aisel.aisnet.org/ecis2006/122/. Acesso em: 18 dez. 2020.

NEIGER, Dina *et al*. Goal-Oriented Business Process Modeling with EPCs and Value-Focused Thinking. *In:* BUSINESS PROCESS MANAGEMENT SECOND INTERNATIONAL CONFERENCE, BPM 2004. 2004. **Proceedings [...]** Berlim, Heidelberg: Springer, 2004. 98-115 p.

O Parlamento Europeu e o Conselho da União Europeia. Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. **Jornal Oficial da União Europeia**. Bruxelas, p. 89-131, L 119, ano 2016, 4 mai. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&from=BG. Acesso em: 29 dez. 2020.

POLÍCIA FEDERAL. **Operação Lava-Jato**: números. **Polícia Federal. Ministério da Justiça e Segurança Pública**. Brasília, 2021. Disponível em: http://www.pf.gov.br/imprensa/lava-jato/numeros-da-operacao-lava-jato. Acesso em: 2 jan. 2021.

ROSA, Eugene A. Metatheoretical foundations for post-normal risk. **Journal of Risk Research**, v. 1, n. 1, p. 15-44, 1998. Disponível em: https://doi.org/10.1080/136698798377303. Acesso em: 8 dez. 2020.

ROSEMANN, Michael *et al*. Integrating Risks in Business Process Models. *In:* 16TH AUSTRALASIAN CONFERENCE ON INFORMATION SYSTEMS (ACIS 2005), 16. 2005. **Proceedings [...]**. 2005. 1-10 p. Disponível em: https://eprints.qut.edu.au/25641/1/Integrating_risk_in_business_proces_Models_with_value_focused_process_engineering.pdf. Acesso em: 17 dez. 2020.

SERPA JR, Wagner. **Princípio da proteção à confiança legítima em matéria tributária e modulação dos efeitos das decisões judiciais**. São Paulo, 2010. 154 p. Dissertação (Mestrado em Direito Político e Econômico) - Universidade Presbiteriana Mackenzie, São Paulo, 2010. Disponível em: http://tede.mackenzie.br/jspui/handle/tede/1038. Acesso em: 4 jan. 2021.

STONEBURNER, Gary; GOGUEN, Alice; FERINGA, Alexis. **NIST Special Publication 800-30**: Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology, v. 1. 2002. 54 p.

Superior Tribunal de Justiça. Introdução à gestão de processos de trabalho: guia metodológico. **Superior Tribunal de Justiça**, Brasília, p. 59, dez. 2016. Disponível em: https://www.stj.jus.br/static_files/STJ/Institucional/Gest%C3%A3o%20estrat%C3%A9gica/3_gestao_processos_15dez16.pdf. Acesso em: 27 jan. 2021.

TJPA, Tribunal de Justiça do Estado do Pará. **TJPA conclui 100% de implantação do PJe**. Belém, 2021. Disponível em: http://www.tjpa.jus.br/PortalExterno/imprensa/noticias/Informes/1170118-tjpa-conclui-100-de-implantacao-do-pje.xhtml. Acesso em: 21 jan. 2021.

TRIBUNAL REGIONAL FEDERAL DA 1ª REGIÃO, Justiça Federal. **Dashboard - Implantação PJe**: Processos em tramitação. **Tribunal Regional Federal da 1ª Região**. Brasília, 2021. Disponível em: https://app.powerbi.com/view?r=eyJrIjoiNjQzNjAzYjktYTZkMy00YzI5LWIwNjUtYTQyZDMwZDk2ZjExIiwidCI6Ijk2MzgxOWY2LWUxYTMtNDkxYy1hMWNjLTUwOTZmOTE0Y2Y0YiJ9. Acesso em: 15 fev. 2021.

VASCONCELOS, Fernando Freire. **Gestão de risco no Poder Judiciário**. 1. ed. Belo Horizonte: Dialética, 2020. 152 p.

WAGNER, Daniel; DISPARTE, Dante. **Global risk agility and decision making**: Organizational resilience in the era of man-made risk. 1. ed. Londres: Palgrave Macmillan UK, 2016. 415 p.

WESKE, Mathias. **Business Process Management**: Concepts, Languages, Architectures. 2. ed. Berlim, Heidelberg: Springer, 2012. 403 p.