



ESCOLA
JUDICIAL
DO TRT DA 4ª REGIÃO

ESTUDOS SOBRE A LGPD

LEI GERAL DE PROTEÇÃO DE DADOS

DOUTRINA E APLICABILIDADE NO
ÂMBITO LABORAL

Artigos, Decisões & Glossário

Organizadores:

Luciane Cardoso Barzotto e Ricardo H. Martins Costa

Apoio:



PUCRS

PPG DIREITO UFRGS

ASRDT



CENTRO DE PESQUISAS
JUDICIAIS DA AMB

CDEA
UFRGS - PUCRS



OBSERVATÓRIOS
DO CDEA



UNISINOS

© Tribunal Regional do Trabalho da 4ª Região, 2022

Presidente do Tribunal Regional do Trabalho da 4ª Região
Desembargador Francisco Rossal de Araújo
Diretor da Escola Judicial do Tribunal Regional da 4ª Região
Desembargador João Paulo Lucena
Realização administrativa
TRT4 e EJUD4

Edição e editoração: Diadorim Editora
Capa: Rosana de Souza Kim Jobim
Revisão: Cris Gutkoski
Projeto gráfico: Flávio Ilha

CONSELHO CIENTÍFICO-EDITORIAL

Fabiano Menke UFRGS-CNPD (Conselho Nacional de
Proteção de Dados e Privacidade)
Luiz Eduardo Gunther Unicuitiba – TRT9
Denise Maria Schelleberger Fernandes MPT
Regina Linden Ruaro PUCRS
Gabrielle Bezerra Sales Sarlet PUCRS
Giovanni Olsson Unochapecó-CNJ
Tereza Aparecida Asta Gemignani TRT15 – Comitê Científico Enamat
Leandro Krebs Gonçalves EJUD 4

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD

E82 Estudos sobre LGPD – Lei Geral de Proteção de Dados – lei nº 13.709/2018:
doutrina e aplicabilidade no âmbito laboral [recurso eletrônico] / organizado por Luciane
Cardoso Barzotto, Ricardo Hofmeister de Almeida Martins Costa - Porto Alegre : Escola Judicial
do Tribunal Regional do Trabalho da 4ª Região. Diadorim Editora, 2022.

685 p. ; PDF ; 6MB.

ISBN: 978-65-995463-8-9 (Ebook)

1. Direito. 2. Direito digital. 3. Lei Geral de Proteção de Dados. I. Barzotto, Luciane
Cardoso. II. Costa, Ricardo Hofmeister de Almeida Martins. II. Título. III. Brasil. Tribunal
Regional do Trabalho (4ª Região) Escola Judicial do Tribunal Regional do Trabalho da 4ª Região

2022-936

CDD 340.0285

CDU 34:004

Tribunal Regional do Trabalho da 4ª Região
Avenida Praia de Belas, 1432. Prédio III. 2º andar
CEP 90110-904 - Porto Alegre - RS
Telefone: (51) 3255.2683

Qualquer parte desta publicação pode ser reproduzida, desde que citadas a fonte e a respectiva autoria. O teor dos textos publicados é de total responsabilidade dos autores, não expressando necessariamente a posição da Escola Judicial do Tribunal Regional do Trabalho da 4ª Região

3. RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS DOS TRABALHADORES: DILEMAS EM TORNO DA ANÁLISE DE RISCO

DATA PROTECTION IMPACT ASSESSMENT OF EMPLOYEES' PERSONAL DATA: DILEMMAS AROUND RISK ANALYSIS

CLAUDIA LIMA MARQUES⁵⁴ E CÍNTIA ROSA PEREIRA DE LIMA⁵⁵

Resumo

A proteção de dados pessoais parte do pressuposto da vulnerabilidade dos titulares de dados, pois estão sujeitos ao controle das atividades de tratamento de dados realizadas pelos controladores e operadores. Neste sentido, fica evidente a forte aproximação deste tema com o Direito do Trabalho, que também se estrutura a partir da vulnerabilidade dos empregados face aos empregadores. Um dos pontos de intenso debate sobre a LGPD é o relatório de impacto à proteção de dados (RIPD), pois ainda não está claro seu caráter obrigatório para todas as situações ou não, além da falta de uniformidade quanto à metodologia para análise de risco. Este artigo enfrenta o tema, evidenciando a elaboração deste documento pelo empregador diante do tratamento de dados pessoais de seus funcionários.

Palavras-Chave: Lei Geral de Proteção de Dados. Princípio da Segurança. Princípio da Prevenção. Doutrina do Diálogo das Fontes.

Abstract

The protection of personal data is based on the assumption of data subjects' vulnerability, as they are subject to the control of data processing activities carried out by controllers and operators. In this sense, one can notice the approximation of this issue with Labor Law, which is also structured on the vulnerability of employees towards employers. One of the points of intense debate about the LGPD is the data protection impact assessment (DPIA), as it is not yet clear whether it is mandatory for all situations or not, in addition to the lack of uniformity regarding the methodology for risk analysis. This article addresses these issues, highlighting the preparation of this document by the employer in view of the processing of personal data of its employees.

Keywords: Data Protection General Law. Security Principle. Prevention Principle. Laws Dialogue Doctrine.

54 Professora Titular e Diretora da Faculdade de Direito da Universidade Federal do Rio Grande do Sul. Doutora iuris utriusque (Heidelberg), L.L.M. (Tübingen). Ex-Presidente do Instituto Brasileiro de Política e Direito do Consumidor – Brasilcon. Presidente do Comitê de Proteção Internacional dos Consumidores da International Law Association ILA (Londres) e Diretora do Centro de Estudos Europeus e Alemães – CDEA (UFRGS-PUCRS-DAAD). cmarques.ufrgs@gmail.com

55 Professora Associada de Direito Civil da Faculdade de Direito da USP Ribeirão Preto – FDRP. Doutora em Direito Civil pela USP. Livre-docente em Direito Civil pela USP. Pós-doutorado em Direito Civil pela *Università degli Studi di Camerino* (Itália) e *Fordham Law School* (Nova York). Presidente do Instituto Avançado de Proteção de Dados – IAPD. cintiar@usp.br

1. Introdução

No atual contexto da sociedade informacional, é cediço que o poder econômico se mede pela capacidade de coletar e armazenar informações que identificam ou possam identificar pessoas, que são utilizadas de maneira muito criativa com evidente geração de lucros. Assim, as *big players* da economia informacional são as corporações que detêm um volume imensurável de dados pessoais, como *Google, Facebook, WhatsApp, YouTube, Amazon*, dentre outras cuja movimentação está fundada nos dados pessoais como verdadeiras *commodities*.⁵⁶

Neste contexto, fica evidente a importância de uma Lei Geral de Proteção de Dados Pessoais para equacionar e equilibrar os interesses em jogo: de um lado, a busca de lucro pelos agentes de tratamento de dados pessoais; de outro, a proteção à autodeterminação informativa.

Inicialmente, a proteção de dados pessoais era vista como um desdobramento do direito à privacidade. No entanto, Stefano Rodotà⁵⁷ caracteriza a evolução cultural e jurídica do termo “privacidade”, sistematizando tal evolução em quatro aspectos que destacam a privacidade, e hoje a proteção de dados, como um “elemento constitutivo da cidadania”, quais sejam:

- 1) do direito de ser deixado só ao direito de manter o controle sobre suas próprias informações;
- 2) da privacidade ao direito à autodeterminação informativa;
- 3) da privacidade a não discriminação;
- 4) do segredo ao controle.

Em síntese, Stefano Rodotà⁵⁸ afirma que a privacidade, na sociedade informacional, não pode ser mais apenas entendida como o “direito de ser deixado só”; em verdade, a tutela dos dados pessoais garante ao titular conhecer, controlar, identificar e interromper o fluxo de informações que lhe digam respeito.

Em outro texto, Stefano Rodotà⁵⁹ destaca uma diferença importante: o direito à privacidade possui tutela estática e negativa, enquanto a tutela dos dados pessoais, estruturada a partir de regras sobre o tratamento de dados, poderes de intervenção, dentre outras, possui uma tutela dinâmica, ou seja, surge com a coleta dos dados e permanece com eles durante a circulação e armazenamento.

56 PARISER, Eli. **The filter bubble**: how the new personalized web is changing what we read and how we think. Nova York: Penguin Book, 2011. pp. 45 – 46: “What all of this means is that your behavior is now a commodity, a tiny piece of a market that provides a platform for the personalization of the whole Internet. We’re used to thinking of the Web as a series of one-to-one relationships: You manage your relationship with Yahoo separately from your relationship with your favorite blog. But behind the scenes, the Web is becoming increasingly integrated. Businesses are realizing that it’s profitable to share data. Thanks to Acxiom and the data market, sites can put the most relevant products up front and whisper to each other behind your back.” (grifo nosso)

57w Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali. **Rivista Critica del Diritto Privato**, anno XV, n. 1, março 1997, pp. 583 – 609. pp. 588 – 591.

58 Privacy..., *op. cit.*, p. 521.

59 Tra diritti fondamentali ed elasticità della normativa: il nuovo codice sulla *privacy*. **Europa e Diritto Privato**, fasc. 01, pp. 01 – 11, Milão: Giuffrè, 2004. p. 03. No mesmo sentido: FINOCCHIARO, Giusella. **Privacy e protezione dei dati personali**: disciplina e strumenti operativi. Bologna: Zanichelli, 2012. pp. 04 – 05.

Sobre tal distinção, Giusella Finocchiaro⁶⁰ destaca que determinado dado pessoal, ainda que não seja privado, é objeto de tutela pela legislação sobre proteção de dados pessoais. Portanto, conclui que a definição de dado pessoal não faz referência direta nem indireta à privacidade. Em suma, o objeto do direito à privacidade é diverso do objeto do direito à proteção dos dados pessoais. O primeiro é assegurar o resguardo de parcela de sua vida privada; o segundo, por sua vez, é proteger os titulares de dados viabilizando o acesso e controle de suas informações (ainda que de conhecimento público) e impedindo que sejam objeto de tratamento em desacordo com as regras e códigos de condutas. Portanto, é imperiosa a análise do direito à proteção de dados pessoais como um direito autônomo.⁶¹

Além de ser um direito autônomo, a proteção de dados pessoais é um direito fundamental,⁶² merecendo toda atenção do legislador infraconstitucional e dos aplicadores do Direito. A fim de manter sempre atual a LGPD, sua base é essencialmente principiológica, trazendo em seu bojo, além da boa-fé⁶³, dez princípios balizadores das atividades de tratamento de dados pessoais. São eles: da finalidade, da adequação, da necessidade, do livre acesso, da qualidade dos dados, da transparência, da segurança, da prevenção, da não discriminação e da responsabilização e prestação de contas (art. 6º da LGPD).

Sob a ótica principiológica, é necessária a análise da implementação de mecanismos focados na identificação e mitigação dos riscos decorrentes da manipulação de dados pessoais, especialmente numa sociedade de extrema vigilância líquida exercida por meio tecnológico contra todos, buscando-se, desta forma, evitar severos danos aos titulares de dados.⁶⁴ Destaca-se, assim, a tríade de princípios trazidos na LGPD: da segurança, da prevenção e da prestação de contas.

Insculpido no art. 6º, inciso VI da LGPD, o princípio da segurança é entendido como a “utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão”. Sem dúvida, a violação de dados pessoais põe em xeque os direitos dos titulares de dados, desta maneira, os agentes de tratamento de dados possuem o ônus de estabelecer medidas eficazes para compelir os acessos não autorizados às informações pessoais dos titulares dos dados e, conseqüentemente, a ocorrência de eventuais danos⁶⁵.

60 *op. cit.*, p. 36 – 37: “Da qui l’ulteriore riprova che il diritto alla riservatezza e il diritto alla protezione dei dati personali non coincidono, con riferimento ai beni oggetto dei diritti. Nel primo caso, l’oggetto della tutela è costituito dalle vicende riservate, intese come vicende intime o familiari; nel secondo caso, l’oggetto della tutela è invece costituito dai dati e dalle informazioni, anche se privi di contenuto riservato”.

61 Cf. LIMA, Cíntia Rosa Pereira de. **Autoridade Nacional de Proteção de Dados e a Efetividade da Lei Geral de proteção de Dados**. São Paulo: Editora Almedina, 2020. p. 90.

62 A Proposta de Emenda à Constituição (PEC) nº 17/2019 pretende inserir o inciso XII-A ao art. 5º, e o inciso XXX ao art. 22 da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria.

63 Cf. MARQUES, Claudia Lima. **Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais**. 9. ed. rev. e atual. São Paulo: Revista dos Tribunais, 2019. p. 905.

64 ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**. Nova York: Public Affairs, 2019.

65 LIMA, Cíntia Rosa Pereira de. **Autoridade Nacional de Proteção de Dados e a Efetividade da Lei**

O princípio da prevenção está intimamente relacionado a este e vem descrito na LGPD (inciso VIII do art. 6º) como a “*adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais*”.

Enquanto o princípio da responsabilização e prestação de contas (inciso X, art. 6º da LGPD), também chamado de *accountability*, é a: “demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas”. A LGPD prevê, portanto, que os agentes de tratamento de dados devem observar e cumprir todas as exigências legais, mas que também devem comprovar a eficácia dessas medidas. Em outras palavras, deve ser adotado um modelo de governança capaz de assegurar o cumprimento de tais obrigações e, ao mesmo tempo, a organização e manutenção de documentos que comprovem que tais obrigações estão sendo satisfeitas.

Miriam Wimmer⁶⁶ realça que os princípios previstos na LGPD não são criações inéditas do legislador brasileiro, pois eles são inspirados em princípios já consolidados em documentos internacionais e leis de proteção de dados de outros países.

Pode-se acrescentar que estes princípios, como visto, não são criações da LGPD, pois estão insculpidos em outras leis como leis trabalhistas e o Código de Defesa do Consumidor, dentre outras, fortalecendo ainda mais a doutrina do “Diálogo das Fontes”.⁶⁷

Neste sentido, deve-se realizar o mesmo diálogo entre a LGPD e o Direito do Trabalho no que diz respeito à caracterização do Relatório de Impacto à Proteção de Dados Pessoais, hipóteses em que tal análise seja obrigatória e a metodologia empregada.

2. Do Relatório de Impacto à Proteção de Dados Pessoais e sua aplicação nas relações trabalhistas

Muito se tem falado sobre o denominado “Relatório de Impacto à Proteção de Dados”, conhecido pela sigla RIPD. Mas em que consiste este documento, quais são as hipóteses nas quais tal documento é obrigatório, qual metodologia deve ser empregada e sua importância como uma ferramenta de mitigação de riscos e prevenção nas relações trabalhistas?

Na verdade, a Lei Geral de Proteção de Dados (Lei n. 13.709/2018) fala muito pouco sobre esse documento. Este documento é mencionado dentre os conceitos elencados no art. 5º da LGPD inc. XVII, no art. 10, § 3º (quando a base legal para o tratamento de dados for o legítimo interesse) e no art. 38 (com ênfase aos dados pessoais sensíveis).

Geral de proteção de Dados. São Paulo: Editora Almedina, 2020. p. 204-206.

66 Capítulo 4 – A LGPD e o balé dos princípios: tensões e convergências na aplicação dos princípios de proteção de dados pessoais ao setor público. In: FRANCOSKI, Denise de Souza Luiz; TASSO, Fernando Antonio. **A Lei Geral de Proteção de Dados Pessoais: Aspectos Práticos e Teóricos Relevantes no Setor Público e Privado.** São Paulo: Revista dos Tribunais, 2021. pp.163 – 186. p. 166.

67 MARQUES, Claudia Lima. Superação das antinomias pelo diálogo das fontes: o modelo brasileiro de coexistência entre o Código de Defesa do Consumidor e o Código Civil de 2002. **Revista de Direito do Consumidor**, vol. 51, pp. 34-67, jul. – set., 2004; MARQUES, Claudia Lima (orgs.) **Diálogo das fontes. Do conflito à coordenação das normas do direito brasileiro.** São Paulo: Revista dos Tribunais, 2012.

Portanto, caberá à ANPD regulamentar esse tema nos termos do art. 55-J, inc. XIII da LGPD: “editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei”.

Algumas leis específicas podem exigir tal documento, por exemplo, a Medida Provisória n. 954/2020, que autorizava o compartilhamento de informações dos consumidores pelas empresas de telefonia móvel e fixa com o IBGE, cuja eficácia ficou suspensa após o julgamento das Ações Diretas de Inconstitucionalidade (ADI n. 6387, n. 6388, n. 6389, n. 6390 e n. 6393) pelo Supremo Tribunal Federal.⁶⁸

O art. 3º, § 2º da MP 954/2020 exigia o Relatório de Impacto à Proteção de Dados Pessoais nos termos da LGPD, mesmo antes da entrada em vigor da lei, *in verbis*: “A Fundação IBGE informará, em seu sítio eletrônico, as situações em que os dados referidos no *caput* do art. 2º foram utilizados e divulgará relatório de impacto à proteção de dados pessoais, nos termos do disposto na Lei nº 13.709, de 14 de agosto de 2018.”⁶⁹ Esta seria uma hipótese na qual tal documento deve ser obrigatório, pois se trata de tratamento de dados em massa; no entanto, com razão, tal Medida Provisória teve sua eficácia suspensa pelo julgamento das ADIs acima mencionadas.

2.1 Conceito e conteúdo do Relatório de Impacto à Proteção de Dados Pessoais

O inc. XVII do art. 5º da LGPD traz um conceito do que vem a ser o Relatório de Impacto à Proteção de Dados Pessoais, a saber: “documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco”.

Pode-se afirmar, portanto, que neste documento deve-se conter, minimamente: a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados (conforme o disposto no parágrafo único do art. 38 da LGPD).

O objetivo desse documento é realizar uma avaliação dos riscos às liberdades civis e aos direitos fundamentais envolvidos no tratamento de dados pessoais como consta da definição do inc. XVII do art. 5º da LGPD. No entanto, a proteção de dados pessoais é um direito fundamental, restando a pergunta se tal documento será sempre obrigatório para as atividades de tratamento de dados.

Neste documento, há a descrição do tratamento de dados, bem como a avaliação de sua necessidade e proporcionalidade aos riscos envolvidos com tal atividade. O ideal é realizar essa avaliação antes do tratamento de dados pessoais. Esse documento é um processo contínuo, pois deve ser revisitado constantemente a fim de se verificar se as medidas de segurança apontadas para mitigar os riscos continuam eficazes tendo em vista a evolução tecnológica.

68 Disponível em: https://jurisprudencia.stf.jus.br/pages/search?base=acordaos&pesquisa_inteiro_teor=false&sinonimo=true&plural=true&radicais=false&buscaExata=true&page=1&pageSize=10&-queryString=ADI%206387&sort=_score&sortBy=desc

69 Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm

2.2 Hipóteses nas quais o Relatório de Impacto à Proteção de Dados Pessoais é obrigatório

O art. 35 do GDPR traz regras específicas para o denominado “*Data Protection Impact Assessment (DPIA)*”, a saber:

1. Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação.

O WP 29 elaborou um parecer n. 248⁷⁰ sobre o tema, oferecendo diretrizes sobre este documento, além de uma relação das hipóteses nas quais este documento é obrigatório.

São nove as circunstâncias nas quais o DPIA será obrigatório:

- 1) Avaliação de crédito (*Credit Scoring*)
- 2) Criação de perfis a partir de decisões automatizadas
- 3) Monitoramento sistemático (ex. câmeras de segurança)
- 4) Tratamento de dados pessoais sensíveis
- 5) Tratamento de dados pessoais em massa
- 6) Combinação de duas ou mais operações de tratamento de dados
- 7) Tratamento de dados pessoais de vulneráveis
- 8) Tratamento de dados com aplicação de tecnologias novas
- 9) Tratamento de dados que impeça o exercício de um ou mais direitos assegurados aos titulares de dados

Na Europa, discute-se se basta constatar uma destas circunstâncias para a obrigatoriedade do DPIA, ou se basta constatar mais de uma delas. O ideal seria determinar a obrigatoriedade se coexistirem duas ou mais destas circunstâncias.

No Brasil, ainda não se tem uma definição de circunstâncias nas quais esse relatório de impacto seja obrigatório; caberá à ANPD tal definição em resolução específica sobre RIPD consoante inc. XIII do art. 55-J da LGPD.

Consoante o que dispõe a LGPD, em se tratando de tratamento de dados com base no legítimo interesse (§ 3º do art. 10 da LGPD) ou se tratando de tratamento de dados pessoais sensíveis (art. 38 LGPD), este documento é obrigatório. Nas outras situações, o Relatório de Impacto à Proteção de Dados será facultativo. Muitas implementações da LGPD estão elaborando o RIPD sempre, fundamentando no princípio da responsabilidade e prestação de contas (*accountability*). No entanto, entendemos que este documento deve ser elaborado com parcimônia, pois se deve

70 Disponível em: <https://ec.europa.eu/newsroom/article29/items/611236>

adotar a metodologia adequada, bem como as medidas de salvaguardas eficientes, caso contrário, o agente de tratamento de dados poderá produzir prova contra si mesmo, documentando algo que não existe ou impraticável.

2.3 Metodologia de análise de riscos

Quanto à metodologia, existem várias metodologias para fazer essa avaliação. A ISO 29.134 tem diretrizes para aplicar tal metodologia. Para cada risco identificado, define-se: a probabilidade de ocorrência do evento de risco, o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento. Como exemplo, os parâmetros escalares podem ser utilizados para representar os níveis de probabilidade e impacto que, após a multiplicação, resultarão nos níveis de risco, que direcionarão a aplicação de medidas de segurança.

A *Commission Nationale de l'Informatique et des Libertés (CNIL)* fornece gratuitamente uma ferramenta para efetuar de forma guiada um DPIA, mas com base no GDPR⁷¹. No Brasil, em novembro de 2020, o Ministério da Economia liderou um estudo sobre o tema, resultando no Guia de Avaliação de Riscos de Segurança e Privacidade⁷², neste documento, são oferecidos alguns modelos de matriz de risco:

GUIA DE AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

Tabela 8. Matriz de Probabilidade X Impacto (CCGD, 2020).

Probabilidade (P)	15	75	150	225
	10	50	100	150
	5	25	50	75
		5	10	15
		Impacto (I)		

Tabela 9. Legenda de cores (CCGD, 2020).

Legenda (Cor)	Classificação do nível de risco
Verde	Baixo
Amarelo	Moderado
Vermelho	Alto

71 Disponível em: <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment>

72 Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-avaliacao-de-riscos-de-seguranca-e-privacidade.pdf>

tanto, o ideal seria padronizar tal metodologia para resguardar maior segurança tanto aos agentes de tratamento de dados quanto aos titulares de dados pessoais.

3. Aspectos específicos do Relatório de Impacto à Proteção de Dados Pessoais nas relações trabalhistas

Os empregadores detêm uma série de informações sobre os trabalhadores, inclusive dados pessoais sensíveis, tais como aqueles relacionados à saúde, por exemplo, ao tratar dados relacionados a atestados de afastamento por motivo de saúde, dentre outros.

Além disso, levando-se em consideração o tamanho do empregador associando-se ao número dos empregados, o tratamento de dados pode ser considerado como tratamento de massa.

Outro ponto a ser destacado é o tratamento de dados pessoais com base no interesse legítimo, uma cláusula geral que alarga o rol previsto no art. 7º da LGPD, ou seja, as hipóteses legais nas quais está autorizado o tratamento de dados pessoais. Tema que também será regulado pela ANPD.

Desta forma, entendemos que nestas três situações acima descritas o Relatório de Impacto à Proteção de Dados passa a ser obrigatório. No entanto, deve ser elaborado de maneira técnica a fim de se evidenciar uma análise adequada sobre o nível de risco envolvido no tratamento de dados pessoais nestas circunstâncias. Não se trata de “achismo”, e sim, uma metodologia que requer domínio da arte, caso contrário, ao invés de mitigar os riscos envolvendo o tratamento de dados, pode acentuar estes riscos. Vejamos: se a análise é feita de maneira superficial a ponto de se concluir que o risco é baixo, o agente de tratamento de dados não tomará as medidas de segurança técnicas e organizacionais adequadas, favorecendo as condições para os incidentes de segurança com dados pessoais; por outro lado, se for atribuído um risco elevado de maneira leviana, há uma assunção de culpa por parte do agente de tratamento de dados que cria um risco elevado, acentuando-se as consequências da responsabilidade civil.

4. Considerações finais

A aproximação axiológica entre LGPD e o Direito do Trabalho é evidente, justificando o diálogo das fontes de maneira a manter a coesão de todo o sistema. Portanto, os princípios do Direito do Trabalho, notadamente o princípio da proteção, e os princípios elencados no art. 6º da LGPD, revelam a necessidade de aplicação coerente das normas trabalhistas e da LGPD.

Alguns exemplos explicitam esta aproximação, como o princípio da *accountability* e a possibilidade da inversão do ônus da prova prevista expressamente no § 2º do art. 42 da LGPD.

Tendo em vista o tratamento de dados pessoais relacionados aos trabalhadores, tais como os relacionados à saúde, à convicção político partidária, orientação sexual etc., ou seja, dados pessoais sensíveis (art. 5º, inc. II da LGPD), impõe um olhar cuidadoso do empregador ao monitorar os possíveis riscos para que sejam

implementadas medidas de segurança técnicas e organizacionais de modo a reduzir possíveis danos decorrentes do tratamento de dados.

Os agentes de tratamento de dados não podem realizar as atividades de tratamento de dados quando sabem ou deveriam saber do seu alto grau de periculosidade à proteção dos titulares de dados pessoais, a menos que tais riscos sejam identificados, mapeados e mitigados por medidas de segurança técnicas e organizacionais. Esta regra pode ensejar o princípio da precaução, cujo instrumento deve ser o Relatório de Impacto à Proteção de Dados Pessoais, considerado pela lei como “documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco” (inc. XVII do art. 5º da LGPD).

Diante disto, este tema deverá ser cuidadosamente regulado pela Autoridade Nacional de Proteção de Dados, atentando-se para as hipóteses nas quais tal procedimento será obrigatório para trazer clareza e segurança jurídica tanto aos agentes de tratamento de dados quanto para os titulares de dados pessoais.

REFERÊNCIAS

FINOCCHIARO, Giusella. **Privacy e protezione dei dati personali: disciplina e strumenti operativi**. Bologna: Zanichelli, 2012.

LIMA, Cíntia Rosa Pereira de. **Autoridade Nacional de Proteção de Dados e a Efetividade da Lei Geral de proteção de Dados**. São Paulo: Editora Almedina, 2020.

MARQUES, Claudia Lima (orgs.) **Diálogo das fontes. Do conflito à coordenação das normas do direito brasileiro**. São Paulo: Revista dos Tribunais, 2012.

_____. **Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais**. 9. ed. rev. e atual. São Paulo: Revista dos Tribunais, 2019.

_____. Superação das antinomias pelo diálogo das fontes: o modelo brasileiro de coexistência entre o Código de Defesa do Consumidor e o Código Civil de 2002. **Revista de Direito do Consumidor**, vol. 51, pp. 34-67, jul. – set., 2004.

PARISER, Eli. **The filter bubble: how the new personalized web is changing what we read and how we think**. Nova York: Penguin Book, 2011.

RODOTÀ, Stefano. Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali. **Rivista Critica del Diritto Privato**, anno XV, n. 1, março 1997, pp. 583 – 609.

_____. Tra diritti fondamentali ed elasticità della normativa: il nuovo codice sulla *privacy*. **Europa e Diritto Privato**, fasc. 01, pp. 01 – 11, Milão: Giuffrè, 2004.

WIMMER, Miriam. Capítulo 4 – A LGPD e o balé dos princípios: tensões e convergências na aplicação dos princípios de proteção de dados pessoais ao setor público. *In*: FRANCOSKI, Denise de Souza Luiz; TASSO, Fernando Anto-

nio. **A Lei Geral de Proteção de Dados Pessoais: Aspectos Práticos e Teóricos Relevantes no Setor Público e Privado.** São Paulo: Revista dos Tribunais, 2021. pp.163 – 186.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism.** Nova York: Public Affairs, 2019.