2238-6114

REVISTA ELETRÔNICA

LEI GERAL DE PROTEÇÃO DE DADOS

Tribunal Regional do Trabalho da 9ª Região
V.10 - n.97 - Março/21

Expediente

TRIBUNAL REGIONAL DO TRABALHO
9ª REGIÃO

PRESIDENTE

Desembargador
SÉRGIO MURILO RODRIGUES LEMOS

VICE-PRESIDENTE

Desembargador
CÉLIO HORST WALDRAFF

CORREGEDORA REGIONAL

Desembargadora
NAIR MARIA LUNARDELLI RAMOS

CONSELHO ADMINISTRATIVO BIÊNIO 2019/2020

Desembargador Arnor Lima Neto (Diretor)
Desembargador Aramis de Souza Silveira (Vice-Diretor)
Juiz Titular Fernando Hoffmann (Coordenador)
Juiz Titular Luciano Augusto de Toledo Coelho (Vice-Coordenador).
Desembargador Arion Mazurkevic
Desembargador Cássio Colombo Filho
Juíza Titular Ana Paula Sefrin Saladini
Juíza Titular Sandra Mara Flügel Assad
Juíza Substituta Vanessa Maria Assis de Rezende
Juiz Substituto Roberto Wengrzynovski
Juiz Roberto Dala Barba Filho (Presidente da AMATRA IX)

TRT-9ª REGIÃO
Paraná

Edição temática
Periodicidade Mensal
Ano X – 2021 – n.96

COLABORADORES

Secretaria Geral da Presidência
Assessoria da Direção Geral
Assessoria de Comunicação Social

FOTOGRAFIAS E IMAGENS

Assessoria de Comunicação
Acervos digitais (Creative Commons)

APOIO À PESQUISA

Daniel Rodney Weidman Junior

SETOR DE DIAGRAMAÇÃO E PUBLICAÇÕES DIGITAIS

Patrícia Eliza Dvorak

CURITIBA - PARANÁ
ESCOLA JUDICIAL

Catalogação: Sônia Regina Locatelli - Analista Judiciário - CRB9/546

R454 Revista Eletrônica do Tribunal Regional do Trabalho do Paraná [recurso eletrônico]. / Tribunal Regional do Trabalho do Paraná. - n. 1 (out. 2011)- . - Dados eletrônicos. - Curitiba, 2019-

Mensal
ISSN 2238-6114
Modo de acesso: http://www.mflip.com.br/pub/escolajudicial/

1. Direito do trabalho - periódicos. 2. Processo do trabalho - periódicos. I. Título

.

CDU: 331:347.9(05)

EDIÇÕES PUBLICADAS

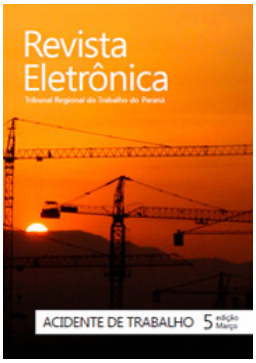
CLIQUE PARA ACESSAR

1ª edição
Ação Civil Pública

2ª edição
Revista Íntima

3ª edição
Normas Internacionais

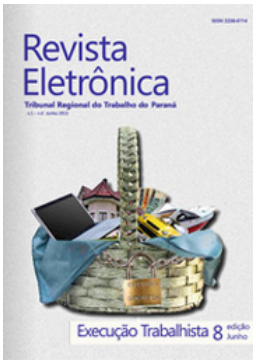
4ª edição
Substituição Processual



5ª edição
Acidente de Trabalho

6ª edição
Normas Coletivas

7ª Edição
Conciliação



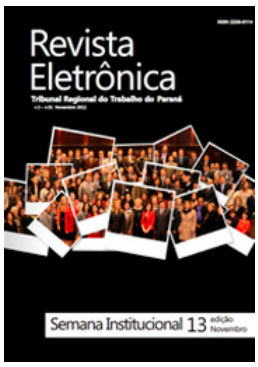
8ª edição
Execução Trabalhista

9ª edição
Conciliação II

10ª edição
Terceirização

11ª edição
Direito Desportivo

12ª edição
Direito de Imagem



13ª edição
Semana Institucional

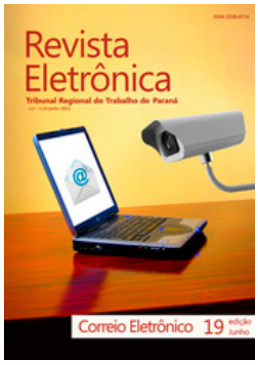
14ª edição
Índice

15ª edição
Processo Eletrônico

16ª edição
Assédio Moral e
Assédio Sexual

17ª edição
Trabalho Doméstico

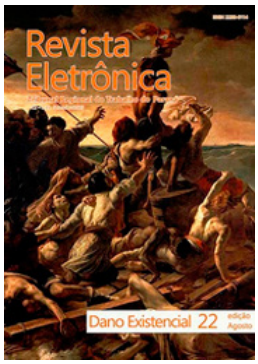
18ª edição
Grupos Vulneráveis



19ª edição
Correio Eletrônico

20ª Edição
Aviso Prévio Proporcional

21ª edição
Dano Moral

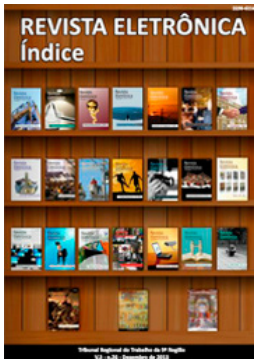


22ª edição
Dano Existencial

23ª edição
Meio Ambiente
do Trabalho

24ª edição
70 anos da CLT

25ª edição
Ética



26ª edição
Índice

27ª edição
Trabalho e HIV

28ª edição
Direito e Sustentabilidade

29ª edição
Copa do Mundo

30ª edição
Trabalho Infantil e Juvenil

31ª edição
Ações Anulatórias

32ª Edição
Trabalho da Mulher

33ª edição
Teletrabalho

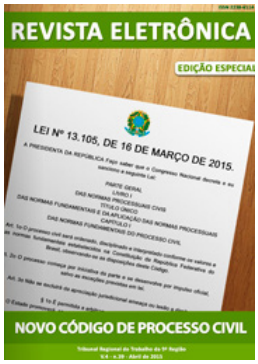
34ª edição
Execução Trabalhista II

35ª edição
Terceirização

36ª edição
Índice

37ª edição
Equiparação Salarial

38ª edição
Dano Moral Coletivo



39ª edição
Novo Código de
Processo Civil

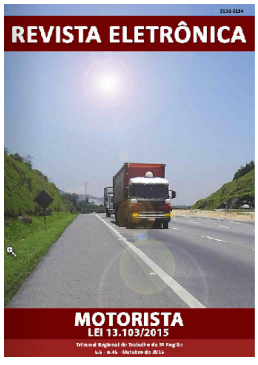
40ª edição
Recursos Trabalhistas

41ª edição
O FGTS e a Prescrição

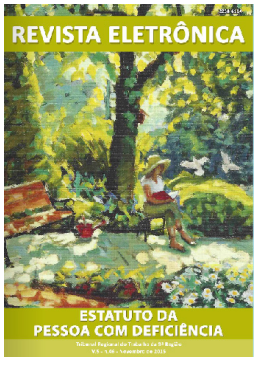
42ª edição
Discriminação no Trabalho

43ª edição
Dumping Social

44ª Edição
O Novo CPC e o
Processo do Trabalho



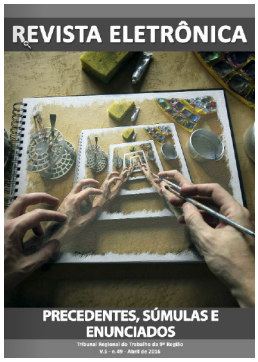
45ª edição
Motorista



46ª edição
Estatuto da Pessoa
com Deficiência

47ª edição
Índice

48ª edição
Convenção 158 da OIT



49ª edição
Precedentes, Súmulas e Enunciados

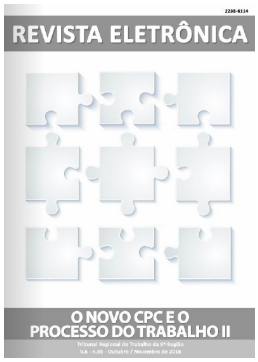
50ª edição
Execução Trabalhista e o Novo CPC

51ª edição
Negociação Coletiva do Trabalho

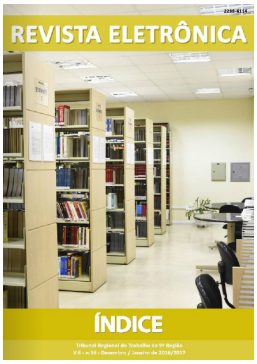
52ª edição
Trabalho Doméstico II

53ª edição
Mediação

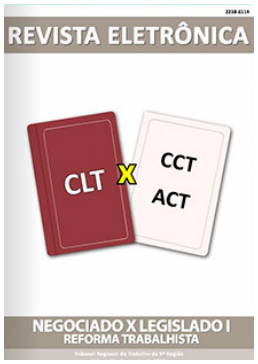
54ª edição
Súmulas Trabalhistas



55ª edição
O Novo CPC e o Processo do Trabalho II

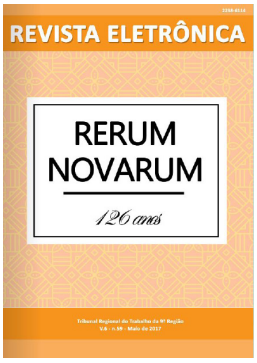


56ª Edição
Índice



57ª edição
Negociado x Legislado I

58ª edição
Negociado x Legislado II



59ª edição
Rerum Novarum

60ª edição
O Trabalho do Preso

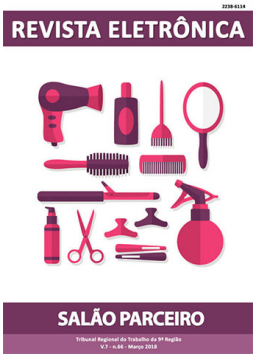
61ª edição
Reforma Trabalhista

62ª edição
Reforma Trabalhista II

63ª edição
Reforma Trabalhista III

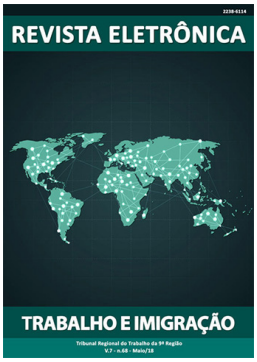
64ª edição
Segurança e Saúde no Trabalho

65ª edição
Índice

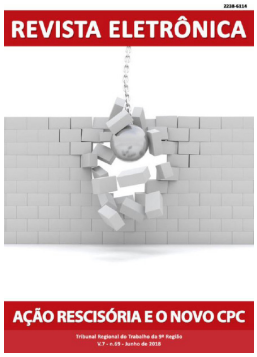


66ª edição
Salão Parceiro

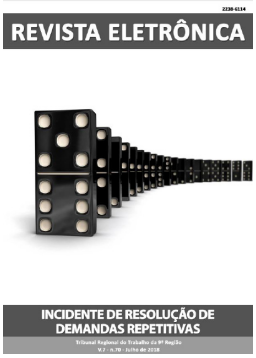
67ª edição
Reforma Trabalhista IV



68ª edição
Trabalho e Imigração



69ª Edição
Ação Rescisória e o Novo CPC



70ª edição
Incidente de Resolução de Demandas Repetitivas

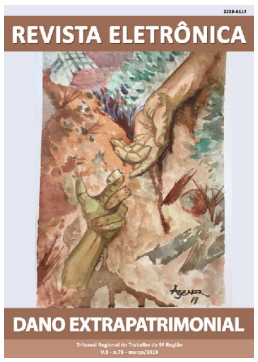
71ª edição
Contribuição Sindical

72ª edição
Terceirização: Antes e Depois da Reforma Trabalhista

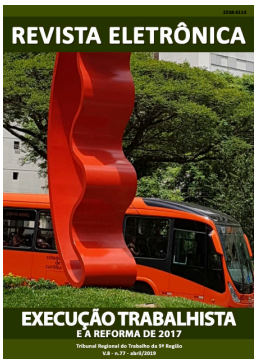
73ª edição
Arbitragem Trabalhista

74ª edição
Trabalho Intermitente

75ª edição
Teletrabalho e a
Reforma Trabalhista



76ª edição
Dano Extrapatrimonial



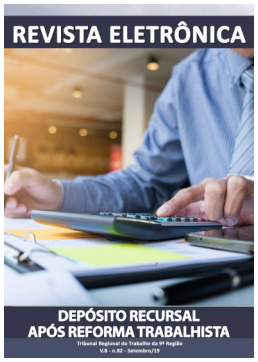
77ª edição
Execução Trabalhista
e a Reforma de 2017

78ª edição
Direitos Humanos
Trabalhistas

79ª edição
Incidente de Assunção
de Competência

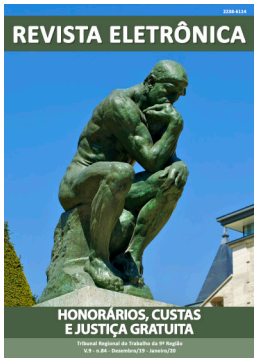
80ª edição
Pejotização

81ª edição
100 Anos da OIT



82ª edição
Depósito Recursal após
Reforma Trabalhista

83ª edição
A Mulher e o Direito do
Trabalho

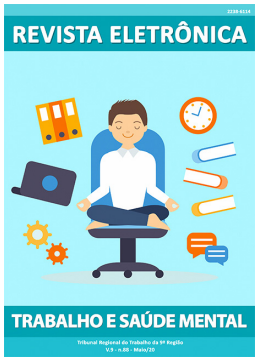


84ª edição
Honorários, Custas e Justiça
Gratuita

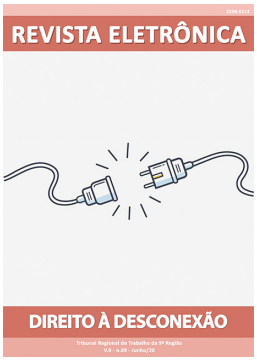
85ª edição
Transação Extrajudicial

86ª edição
4ª Revolução Industrial

87ª edição
Trabalho Rural



88ª edição
Trabalho e Saúde Mental



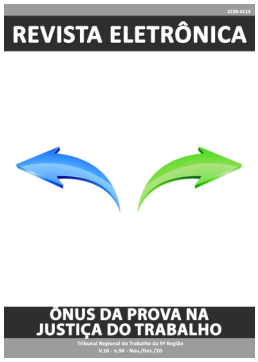
89ª edição
Direito à Desconexão

90ª edição
Processo Judicial Eletrônico

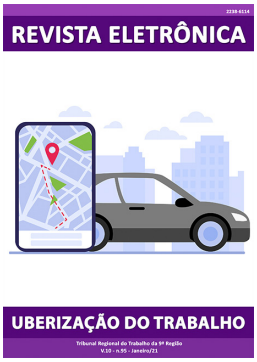
91ª edição
Compliance nas Relações de Trabalho

92ª edição
Repercussão Geral

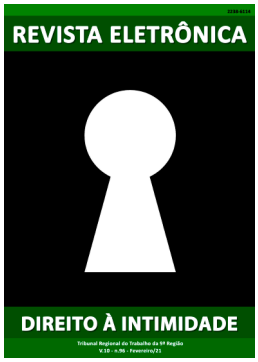
93ª edição
COVID-19 e as Relações de Trabalho



94ª edição
Ônus da Prova na Justiça do Trabalho



95ª edição
Uberização do Trabalho



96ª edição
Direito à intimidade

Número de Acessos das edições

03/2021

	Tema	
		0
1	Ação Civil Pública	66195
2	Revista Íntima	46129
3	Normas Internacionais	85247
4	Substituição Processual	58318
5	Acidente de Trabalho	52651
6	Normas Coletivas	43741
7	Conciliação	45545
8	Execução Trabalhista	54328
9	Conciliação II	24222
10	Terceirização	40039
11	Direito Desportivo	42221
12	Direito de Imagem	22874
13	Semana Institucional	6450
14	Índice	21057
15	Processo Eletrônico	19748
16	Assédio Moral e Sexual	19503
17	Trabalho Doméstico	31567
18	Grupos Vulneráveis	20796
19	Correio Eletrônico	17233
20	Aviso Prévio	12539
21	Dano Moral	21087
22	Dano Existencial	28324
23	Meio Ambiente do Trabalho	19535
24	70 Anos da CLT	9495
25	Ética	13813
26	Índice	12874
27	Trabalho e HIV	17537
28	Sustentabilidade	20988
29	Copa do Mundo	19115
30	Trabalho Infantil	35150
31	Ações Anulatórias	35134
32	Trabalho da Mulher	49966
33	Teletrabalho	24729
34	Execução Trabalhista	32186
35	Terceirização II	35354
36	Índice	16556
37	Equiparação Salarial	29740
38	Dano Moral Coletivo	41457
39	Novo Código de Processo Civil	53395
40	Recursos Trabalhistas	13272
41	O FGTS e a Prescrição	18191
42	Discriminação no Trabalho	25506
43	Dumping Social	13882
44	O Novo CPC e o Processo do Trabalho	27394
45	Motorista	35267
46	Estatuto da Pessoa com Deficiência	17722
47	Índice	10265
48	Convenção 158 da OIT	14014
49	Precedentes, Súmulas e Enunciados	9842
50	Execução Trabalhista e o Novo CPC	14070
51	Negociação Coletiva do Trabalho	9203
52	Trabalho Doméstico II	7066
53	Mediação	3400
54	Súmulas Trabalhistas	4457
55	O Novo CPC e o Processo do Trabalho II	4522
56	Índice	5773
57	Negociado x Legislado I	7508
58	Negociado x Legislado II	6523
59	Rerum Novarum	3550
60	O Trabalho do Preso	3744
61	Reforma Trabalhista	13422
62	Reforma Trabalhista II	14455
63	Reforma Trabalhista III	8446
64	Segurança e Saúde no Trabalho	3256
65	Índice	3797

66	Salão Parceiro	2880
67	Reforma Trabalhista IV	4648
68	Trabalho e Imigração	2083
68	Ação Rescisória e o Novo CPC	3081
70	Incidente de Resolução de Demandas Repetitivas	4276
71	Contribuição SIndical	2781
72	Terceirização: Antes e Depois da Reforma Trabalhista	2777
73	Arbitragem Trabalhista	2092
74	Trabalho Intermitente	3627
75	Teletrabalho e a Reforma Trabalhista	3030
76	Dano Extrapatrimonial	4213
77	Execução Trabalhista e a Reforma de 2017	2684
78	Direitos Humanos Trabalhistas	2216
79	Incidente de Assunção de Competência	1190
80	Pejotização	2364
81	100 Anos da OIT	2555
82	Depósito Recursal após Reforma Trabalhista	1933
83	A Mulher e o Direito do Trabalho	1292
84	Honorários, Custas e Justiça Gratuita	1722
85	Transação Extrajudicial	2338
86	4ª Revolução Industrial	1749
87	Trabalho Rural	835
88	Trabalho e Saúde Mental	1022
89	Direito à Desconexão	1092
90	Processo Judicial Eletrônico	950
91	Compliance nas Relações de Trabalho	1523
92	Repercussão Geral	802
93	COVID-19 e as Relações de Trabalho	1871
94	Ônus da Prova na Justiça do Trabalho	1401
95	Uberização do Trabalho	1585
96	Direito à Intimidade	786

Carta ao leitor

A edição deste mês da Revista Eletrônica traz o tema Lei Geral de Proteção de Dados.

Abrindo a série de artigos desta edição, os autores Luciano Ehlke Rodrigues, Luiz Eduardo Gunther e Rodrigo Thomazinho Comar analisam como vem ocorrendo o tratamento de dados pessoais sensíveis na era digital e o direito à privacidade, bem como o papel do Estado nesta seara.

O segundo artigo, escrito pela autora Rosane Gauriau examina o tratamento de dados pessoais na fase pré-contratual, durante o contrato de trabalho e ao fim da relação laboral, à luz da LGPD e do RGPD, à partir da contribuição do direito do trabalho francês e brasileiro.

No terceiro artigo o autor Luiz Carlos Buchain apresenta as noções gerais sobre a LGPD, avaliando dentro das operações e das pessoas submetidas ao regime legal, os dados pessoais, o tratamento, o arquivo, o titular, o controlador, o operador e o terceiro.

A autora Bruna de Sá Araújo busca, no quarto artigo, analisar a aplicação efetiva na LGPD nas decisões proferidas pelos Tribunais Regionais do Trabalho, desde a vigência da referida lei.

Patricia Peck Garrido Pinheiro, autora do quinto artigo analisa os principais desdobramentos da sanção da Lei 13.709/18, a Lei Geral de Proteção de Dados Pessoais do Brasil (LGPD).

Nosso último artigo é escrito pelo autor Antônio Carlos Aguiar e visa examinar a proteção de dados no contrato de trabalho.

Como registro especial a Lei Geral de Proteção de dados é apresentada na íntegra.

Desejamos a todos boa leitura!

Grupo de Pesquisa da Revista Eletrônica.

Sumário

ARTIGOS

REGISTRO ESPECIAL

A PROTEÇÃO E O TRATAMENTO DOS DADOS PESSOAIS SENSÍVEIS NA ERA DIGITAL E O DIREITO À PRIVACIDADE: OS LIMITES DA INTERVENÇÃO DO ESTADO

Luciano Ehlke Rodrigues
Luiz Eduardo Gunther
Rodrigo Thomazinho Comar

RESUMO

O presente estudo visa analisar como vem ocorrendo o tratamento de dados pessoais sensíveis na era digital e o direito à privacidade, bem como o papel do Estado nesta seara. A metodologia utilizada baseou-se na coleta de dados por meio de artigos científicos e de revisão bibliográfica, com a utilização do método dedutivo-dialético. O objetivo foi investigar como o cidadão brasileiro está se preparando para a aplicação da Lei Geral de Proteção de Dados (LGPD). Para tal desiderato será abordada a Lei 13.709/2018, que entrará em vigor em agosto de 2020, bem como o direito fundamental à privacidade, sendo necessário estabelecer uma ancoragem da temática na Constituição Federal de 1988 e no rol de direitos fundamentais jungidos nesse ordenamento maior. A contribuição deste artigo, portanto, destina-se a analisar os limites da intervenção do estado no tratamento dos dados pessoais sensíveis dos cidadãos brasileiros sem que se desproteja o direito à privacidade.

Palavras-chave: era da informação; tráfego de dados; tecnologia.

Luciano Ehlke Rodrigues

Professor do Centro Universitário Internacional - Uninter; Mestre em Direito Empresarial e Cidadania pelo UNICURITIBA; Advogado Trabalhista há 20 anos. Especialista em Direito e Processo do Trabalho (UNICURITIBA e EMATRA/PR).

Luiz Eduardo Gunther

Professor do Centro Universitário Curitiba – UNICURITIBA; Desembargador do Trabalho no TRT9; Doutor pela UFPR e Pós-Doutor pela PUCPR; Membro do Conselho Científico da Revista Jurídica – UNICURITIBA e do Conselho Editorial da Editora Juruá e do Instituto Memória;

Rodrigo Thomazinho Comar

Mestre em Direito Empresarial e Cidadania pela Faculdade de Direito do Centro Universitário Curitiba-UNICURITIBA. Especialista em Direito Processual Civil pela Pontifícia Universidade Católica do Paraná-PUCPR. Graduado pela Universidade Estadual de Londrina- UEL.

ABSTRACT

This study aims to analyze how the processing of sensitive personal data in the digital age and the right to privacy has been taking place, as well as the role of the State in this area. The methodology used was based on data collection through scientific articles and bibliographic review, using the deductive-dialectic method. The objective was to investigate how the Brazilian citizen is preparing for the application of the General Data Protection Law (LGPD). To this end, Law 13.709 / 2018, which will come into force in August 2020, as well as the fundamental right to privacy, will be addressed, and it will be necessary to establish an anchorage of the theme in the Federal Constitution of 1988 and in the list of fundamental rights joined in this larger order. . The contribution of this article, therefore, is intended to analyze the limits of the state's intervention in the treatment of sensitive personal data of Brazilian citizens without compromising the right to privacy.

Keywords: information age; data traffic; technology.

1 INTRODUÇÃO

Desde os primórdios da Humanidade, o homem sempre esteve intimamente ligado à ideia de evolução e conquistas. Um ponto de destaque na história do homem consiste na incessante busca pelo desconhecido, cabendo destacar, dentre tantos acontecimentos marcantes, a primeira vez em que o homem chegou à lua, quando estavam a bordo da Apollo 11, os astronautas Neil Armstrong, Edwin Aldrin e Michael Collins, em 16 de julho de 1969. A necessidade constante de conquistas marcou a tônica de vários séculos da Humanidade e ainda continua.

Inúmeros fatos permearam a vida humana, mas o século XXI proporcionou avanços em diversos ramos, em especial, o da Tecnologia da Informação, quando a máquina de escrever foi substituída pelos antigos PC´s até chegarmos à era dos celulares e tablets que permeiam o dia-a-dia dos seres humanos nos quatro cantos do Mundo.

Necessário destacarmos que nossa memória nos leva a associar fatos a personagens que os representaram, sendo certo que para este marco histórico e importante para a humanidade acima descrito, a marca do homem foi o registro de sua pegada na Lua, tido como uma comprovação física, palpável e visível de sua conquista. De toda sorte, será mais fácil lembrarmos de Neil Armstrong, enquanto os nomes de Edwin Aldrin e Michael Collins -- embora respeitáveis porquanto estiveram presentes nessa notável expedição -- insistam em cair no esquecimento.

Avançando um pouco no tempo, na segunda década do século XXI, aquilo que até então era conhecido como pegadas físicas, com o advento da Sociedade da Informação preconizada por CASTELLS (1998) e da Internet, são, hoje, transformadas em rastros naquilo que o homem pós-moderno tem denominado de "A era digital".

Necessário se faz, portanto, que seja abordada uma análise do conceito de dados pessoais sensíveis e de como a união europeia (EU) vem normatizando o tratamento desses dados. Mister se faz analisar o direito à privacidade e sua previsão legal no artigo 5º, X, da Constituição da República Federativa do Brasil de 1988 (CRFB).

Por fim, o objetivo do presente estudo reside em investigar quais os limites da Intervenção do Estado no tratamento dos Dados Pessoais Sensíveis dos cidadãos e possíveis conflitos com o Direito à Privacidade.

Partindo-se desse norte, será necessário investigar como a General Data Protection Regulation (GDPR) trata do tema na EU, bem como a Lei 13.709/2018[1], também conhecida como Lei Geral de Proteção de Dados (LGPD) regulará esse relevante tema e impactará a vida de pessoas naturais e pessoas jurídicas de direito privado e público, conforme definido no art. 1º da referida lei. Ao final, procuraremos apresentar os resultados e/ou contribuições do presente estudo ao qual nos propusemos a incursionar.

2 A ERA DIGITAL E OS DADOS PESSOAIS SENSÍVEIS

O mundo tecnológico e a world wide web (web) -- nome pelo qual a rede mundial de computadores internet se tornou conhecida a partir de 1991, quando se popularizou devido à criação de uma *interface gráfica* que facilitou o acesso e estendeu seu alcance ao público em geral -- vem prospectando milhões de pessoas que se vêem encantadas com a informação que lhes é colocada de forma instantânea. Neste contexto, cabe destacar que os acessos na web acabam por deixar rastros e as informações processadas por meios eletrônicos, também conhecidas como dados que são compartilhados pelo globo terrestre em frações de segundos merecem a atenção da comunidade acadêmica.

Se antes da Revolução tecnológica os seres humanos utilizavam-se de cartas, telegramas e ligações telefônicas para interagirem com o Mundo, o que demandava um certo tempo, a forma de comunicação na Era digital avançou rapidamente.

Hoje em dia, o compartilhamento de informações através das mídias sociais, como é o caso do Facebook, são o novo contexto.

Ocorre que tal compartilhamento de informações pode trazer sérios riscos ao vazamento de dados pessoais em caso de fragilidade do sistema ou ataques de hackers, por exemplo, ou ainda quando os dados pessoais alcançam conotação de mercadoria.

Os rastros são detectados no mundo tecnológico por meio de dados que são trafegados por meio da rede mundial de computadores. Para buscar dinamizar esse instantâneo tráfego de dados, a União Europeia se reuniu e editou o GDPR, ou seja, um Regulamento Geral de Proteção de Dados em 2018, visando dinamizar o tratamento dos dados pessoais sensíveis dos cidadãos no âmbito dos países integrantes da EU e conferir maior proteção aos dados pessoais que circulam no ambiente digital. Neste espectro é que o presente artigo buscará contribuir cientificamente trazendo elementos e conceitos a respeito da era digital, dados pessoais sensíveis e seu tratamento, direito à privacidade e os limites da intervenção do Estado neste tema.

A referida comunidade europeia revelou ao mundo sua preocupação com a forma como os dados pessoais sensíveis são tratados e buscou estabelecer todo um arcabouço normativo que era tratado pela Diretiva 45/96/CE e em 2018 foi alterado pela GDPR para tratar da questão afeita à Proteção de Dados.

1 Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 10. jun. 2019

A importância e atualidade da discussão reside no fato de que o Brasil publicou em dezembro de 2018, a Lei 13.709/2018[2], que entrará em vigor em agosto de 2020 e causará profundas modificações na forma como as empresas, o Estado e terceiros vem dando ao tratamento dos dados pessoais sensíveis dos brasileiros, inclusive com a previsão de aplicação de multa de até 50 milhões de reais a cargo da Autoridade Nacional de Proteção de Dados (ANPD), em casos em que restar evidenciada a ocorrência de descumprimento da LGPD, o que passará por futuras definições da respectiva ANPD vinculada à Presidência da República do Brasil.

2.1 OS DADOS PESSOAIS SENSÍVEIS – CONCEITO E CONSIDERAÇÕES

Primeiramente, cabe destacar que a própria Diretiva 95/46/CE[3] traz uma definição de dados pessoais sensíveis de acordo com o artigo 2º, como se tratando de qualquer informação relativa a uma determinada pessoa singular identificada ou identificável.

A referida diretiva europeia conceitua como dado pessoal identificável como todo aquele que possa ser identificado de forma direta ou indireta, complementando a aludida normativa europeia que: "[...], nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social (Diretiva 95/46/CE, np)."

Na mesma linha da Diretiva da EU, o poder legislativo elaborou a Lei 13.709/2018 que estabelece um regramento específico no que se refere ao tratamento de dados pessoais sensíveis no Brasil, lei esta que ficou conhecida como Lei Geral de Proteção de Dados, que entrará em vigor somente em agosto de 2020, em face da "*vacatio legis*" de 18 meses estabelecida por nosso legislador.

Segundo Pinheiro (2018, p. 26), os dados pessoais sensíveis podem ser conceituados da seguinte forma:

> São dados que estejam relacionados a características da personalidade do indivíduo e suas escolhas pessoais, tais como origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente a saúde ou a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

O artigo 5º, incisos I e II da Lei 13.709/2018, define dados pessoais sensíveis da seguinte forma:

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> **II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; (negritos nossos)**

2 Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 10. jun. 2019

3 Disponível em: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046>. Acesso em: 12.dez.2019

Mais adiante, em se tratando das Diretivas da União Europeia, BRAVO (2007, p. 156) destaca a proibição expressa do processamento de determinados dados pessoais:

> O art. 8.1 da Diretiva 95/46/CE proíbe o processamento dos dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, o pertencimento a sindicatos, assim como o tratamento de dados relativos à saúde ou à sexualidade. Seu apartado 5 proíbe o processamento de dados relativos à condenações criminais.
> [...] levando em conta os princípios de determinação e limitação da finalidade, legitimidade e proporcionalidade, poder-se-á autorizar um tratamento de tais dados, se de acordo com as seguintes particularidades:

O mesmo autor prossegue seu raciocínio esclarecendo que:

> - Os dados relativos à vida sexual só poderão ser objeto de processamento quando seja necessário para determinação da responsabilidade dos empregadores de uma acusação de assédio sexual.
> - Os dados relativos aos antecedentes penais só poderão ser processados se for necessário com respeito às funções particulares do emprego em questão. Nestes casos, prevê-se o necessário controle prévio por parte da autoridade nacional de controle, para evitar abusos e excessos, assim como verificar a pertinência do processamento.

DONEDA (2010, p. 191) procurou ampliar a questão relativa à proteção de qualquer dado pessoal e não somente do dado sensível concluindo que:

> qualquer dado pessoal e não somente o dado sensível é passível de, em determinadas circunstâncias, dar origem à discriminação ou ao controle, diminuindo as liberdades de escolha de uma pessoa. Os efeitos geralmente atribuídos ao tratamento indiscriminado dos dados sensíveis também podem ocorrer quando da manipulação de dados não sensíveis – tanto é que os dados não sensíveis também merecem proteção, apenas em uma escala inferior.

O mesmo autor continua seus ensinamentos a respeito dos motivos dos dados sensíveis merecerem uma proteção diferenciada, nos seguintes termos:

> O motivo dos dados sensíveis merecerem uma proteção mais intensa é justamente uma consideração probabilística de que tais dados são mais afeitos a apresentarem problemas mais graves quando de sua má utilização – daí exatamente o fato de denominá-los como “sensíveis” em relação aos demais, enfatizando sua peculiaridade neste sentido (DONEDA, 2010, p. 191).

2.2 A ERA DIGITAL E SEU SURGIMENTO

A Era digital antecede o GDPR de maio de 2018 e a Lei 13.709/2018 (LGPD) Brasileira, porquanto os fatos surgem no mundo real e cabe ao legislador elaborar normas que regularão a aplicação de determinados aspectos aptos ao convívio dos homens em sociedade.

Como dissemos anteriormente, o século

XXI trouxe inúmeros avanços tecnológicos a saber: celulares (antes analógicos e atualmente os smartphones), computadores de elevado processamento conhecidos como *mainframes*, big data até a criação da inteligência artificial (IA).

Em Castells (1999), a era digital representa a cultura da virtualidade real a partir do pressuposto que tudo é possível de ser gravado em áudio e vídeo, desde eventos, festas e uma série de outras situações, melhor descritas pelo autor:

> As pessoas começaram a filmar seus eventos, de férias a comemorações familiares, assim produzindo as próprias imagens, além do álbum fotográfico. Apesar de todos os limites dessa autoprodução de imagens, tal prática realmente modificou o fluxo de mão única das imagens e reintegrou a experiência de vida e a tela. Em muitos países, da Andaluzia ao sul da Índia, a tecnologia de vídeo da comunidade local permitiu o surgimento da transmissão local rudimentar que misturava difusão de filmes de vídeo com eventos e anúncios locais, muitas vezes à margem dos regulamentos de telecomunicações (1999, p. 363).

O único meio de controlar a rede de tecnologia da informação é simples: não fazendo parte dela, porém o preço a ser pago é extremamente elevado e muitas vezes significa que aqueles que assim optam, ficarão de fora da sociedade virtual (CASTELLS, 1999).

Prossegue o referido autor, nos mostrando um exemplo de como os Estados Unidos da América utilizaram a virtualidade real na campanha presidencial de 1992:

> Na campanha presidencial norte-americana de 1992, o então vice-presidente Dan Quayle queria posicionar-se em defesa dos valores da família tradicional. Armado de suas convicções morais, iniciou um debate incomum com Murphy Brown. Murphy Brown, representada por uma ótima atriz, Candice Bergen, era a personagem principal de uma série popular de TV que (a) (re)presentava os valores e problemas de um novo tipo de mulher: a profissional solteira com os próprios critérios sobre a vida. Nas semanas da campanha presidencial, Murphy Brown (não Candice Bergen) decidiu ter um filho fora do casamento (CASTELLS, 1999, p. 395).

O mesmo autor prossegue sua narrativa se encaminhando para a surpreendente revelação no sentido de que:

> O vice-presidente Quayle apressou-se a condenar seu comportamento como impróprio, provocando revolta nacional principalmente entre as mulheres trabalhadoras. Murphy Brown (não apenas Candice Bergen) retaliou: no episódio seguinte apareceu assistindo à entrevista de televisão em que o vice-presidente Quayle a criticava e reagiu com críticas acirradas à interferência de políticos na vida das mulheres e com a defesa de seu direito a uma nova moralidade. Com isso *Murphy Brown* aumentou sua fatia de audiência, e o conservadorismo desatualizado de Dan Quayle contribuiu para a derrota eleitoral do presidente Bush. Os dois acontecimentos foram reais e, em certa medida, socialmente relevantes (CASTELLS, 1999, p. 395).

Partindo-se desse exemplo bem

articulado por Castells, podemos destacar a vital importância da velocidade das informações, na medida em que podem influenciar diretamente nas escolhas culturais, entretenimento, alimentação, plano de saúde, músicas, filmes, mas também podem influenciar negativamente ou de forma direcionada no resultado de eleições presidenciais como veremos adiante.

Um exemplo emblemático foi o caso da Cambridge Analítica, amplamente divulgado nas mídias sociais, e que estaria relacionado às eleições norte-americanas de 2016[4], segundo denúncia feita pelos jornais *The New York Times* e *The Guardian*. De acordo com a imprensa, houve uma manipulação das eleições presidenciais norte americanas através da utilização dos perfis dos eleitores no Facebook sem o consentimento destes, com a finalidade de influenciar o resultado das eleições em favor do atual Presidente Donald Thrump.

Sob a perspectiva deste fascinante Universo de Informações e suas implicações para os seres humanos que navegam pela web, os dados classificados como dados pessoais sensíveis representam um novo petróleo (Fernandes, 2017).

Segundo FERNANDES (2017), a Diretiva da União Europeia já vem se dedicando há vários anos sobre o tema afeito à proteção de dados pessoais no que se refere ao fluxo de dados, chegando a conclusão de que:

> A Diretiva 95/46/CE, do Parlamento Europeu e do Conselho da Europa, de 24 de outubro de 1995, veio a responder a esta necessidade, ao obrigar os Estados à adoção de legislação oferecendo garantias semelhantes em todo o espaço europeu, e ao regrar os procedimentos quanto aos fluxos de dados pessoais para países que não os da União Europeia, tendo este passado a ser classificado de modo diferenciado, consoante ofereçam, ou não, um nível de proteção adequado. (FRAZÃO, np)

FRAZÃO (2018, np) tem divulgado uma série de artigos[5] acerca da Lei Geral de Proteção de Dados, revelando profunda preocupação acerca da destinação dos dados pessoais: "Passando para o exame do texto da lei, a primeira observação importante é que fica claro que o regime de proteção de dados não tem por finalidade apenas a de tutelar a privacidade dos usuários."

Podemos observar claramente da narrativa da autora que já no artigo 1º da Lei 13.709/2018, o seu objetivo visa proteger "os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (FRAZÃO, 2018, np)."

Com relação ao artigo 2º, o referido e novel diploma legal alusivo à Lei Geral de Proteção de dados elenca uma série de fundamentos aos quais busca proteger, quais sejam:

> além da privacidade, a

4 Por meio de denúncia dos jornais The New York Times e The Guardian, através do aplicativo Facebook, teria ocorrido a utilização de dados de cerca de 50 milhões de pessoas e teriam sido utilizados sem o consentimento delas para utilização na Campanha Eleitoral Pró-Trump através de análise do perfil pessoal de cada usuário. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml.>. Acesso em 18.ago. 2019.

5 Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-principais-repercussoes-para-a-atividade-empresarial-29082018>. Acesso em 02.abr.2019

> autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa; a livre concorrência e a defesa do consumidor; os direitos humanos; o livre desenvolvimento da personalidade; a dignidade e o exercício da cidadania pelas pessoas naturais.

Merece especial destaque as reflexões e ponderações lançadas por Frazão quanto às cautelas da lei preconizadas pelo legislador ordinário:

> Ao se referir expressamente ao livre desenvolvimento da personalidade, à cidadania e à dignidade, a lei certamente procura evitar muitas das destinações atuais que vêm sendo conferidas aos dados pessoais, os quais, processados por algoritmos, são capazes de fazer diagnósticos e classificações dos usuários que, por sua vez, podem ser utilizados para limitar suas possibilidades de vida. Mais do que isso, a partir de tais dados, as empresas podem discriminar usuários ou mesmo tentar manipular suas opiniões, crenças ou valores em vários âmbitos, inclusive o político (FRAZÃO, 2018, np).

Segundo Pinheiro (2018, p. 25), é possível conceituar o tratamento de dados da seguinte forma:

> Toda operação realizada com algum tipo de manuseio de dados pessoais: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, edição, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Para Castells (1999, pág. 69), a Era da Informação passou a modificar os seres humanos de uma forma profunda, causando uma integração entre mentes e máquinas, na medida em que:

> Assim, computadores, sistemas de comunicação, decodificação e programação genética são todos amplificadores e extensões da mente humana. O que pensamos e como pensamos é expresso em bens, serviços, produção material e intelectual, sejam alimentos, moradia, sistemas de transporte e comunicação, mísseis, saúde, educação ou imagens. A integração crescente entre mentes e máquinas, inclusive a máquina de DNA, está anulando o que Bruce Mazlish chama de a "a quarta descontinuidade" (aquela entre seres humanos e máquinas), alterando fundamentalmente o modo pelo qual nascemos, vivemos, aprendemos, trabalhamos, produzimos, consumimos, sonhamos, lutamos ou morremos (CASTELLS, 1999, p. 69).

O mesmo autor continua seu raciocínio, afirmando que:

> Com certeza, os contextos culturais/institucionais e a ação social intencional interagem de forma decisiva com o sistema tecnológico, mas esse sistema tem sua própria lógica embutida, caracterizada pela capacidade de

> transformar todas as informações em um sistema comum de informação, processando-as em velocidade e capacidade cada vez maiores e com custo cada vez mais reduzido em uma rede de recuperação e distribuição potencialmente ubíqua (CASTELLS, 1999, p. 69).”

A Lei 13.709/2018, que entrará em vigor em setembro de 2020 (nas disposições gerais e principiológica), excetua o tratamento de dados pessoais nas seguintes situações, conforme podemos observar no artigo 4º, inciso I, quando for realizado por: a) realizado por pessoa natural para fins exclusivamente particulares e não econômicos; bem como para fins jornalísticos e artísticos, além de acadêmicos, “ aplicando-se a esta hipótese os arts. 7º e 11 desta Lei”. (BRASIL, 2018).

No mesmo artigo, porém no inciso III, também existe exceção para o tratamento de dados pessoais quando for realizado para fins exclusivos envolvendo segurança pública, defesa nacional, segurança do estado, ou ainda atividades de investigação e repressão de infrações penais.

Em prosseguimento, o inciso V do mesmo artigo também excetua o tratamento de dados pessoais quando estes forem:

> IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

Por fim, ainda merece destaque o §1º da LGPD, que faz referência ao inciso III acima destacado, no seguinte sentido:

> § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

Quando o legislador trouxe a inaplicabilidade da Lei Geral de Proteção de Dados para os casos previstos no art. 4º e parágrafos, podemos divisar que prevaleceu a segurança pública, segurança do Estado ou atividades de investigação e repressão de infrações penais.

Todavia, se não houver o treinamento dos operadores responsáveis pelo tratamento dos dados pessoais sensíveis dos cidadãos brasileiros, evidencia-se um grande risco de vazamento desses dados gerando insegurança jurídica e prejuízos de ordem judicial em razão de demandas judiciais vindicando o pagamento de danos morais em decorrência de tais situações.

4 OS LIMITES DA INTERVENÇÃO DO ESTADO NO TRATAMENTO DOS DADOS PESSOAIS SENSÍVEIS

A Lei Geral de Proteção de Dados, como visto acima, estabelece responsabilidade ao Estado em caso de tratamento, divulgação e manipulação de dados sem o consentimento do titular, conforme podemos inferir da leitura do artigo 1º da Lei 13.709/2018:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por **pessoa jurídica de direito público** ou privado, com o **objetivo de proteger os direitos fundamentais de liberdade e de privacidade** e o livre desenvolvimento da personalidade da pessoa natural.
> Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e **devem ser observadas pela União, Estados, Distrito Federal e Municípios**. (Incluído pela Lei nº 13.853, de 2019) (grifo nosso)

Para JUNIOR e FAUSTINO (2019, p. 302) ao tratarem do tema relativo ao uso de aplicativos de serviços para a saúde pública e a proteção de dados pessoais dos usuários a situação é extremamente delicada, porquanto em se tratando de um país como o Brasil com mais de 210 milhões de habitantes[6], a isso se soma a falta de qualificação dos operadores dos dados, trazendo risco de violação à privacidade de uma gama enorme de usuários, pontificando os autores que:

> A privacidade está ligada a dignidade da pessoa humana, princípio também insculpido na Constituição Federal em seu art. 1o, inciso III e está intimamente ligada com a confidencialidade nos casos envolvendo dados sensíveis relativos à saúde das pessoas, onde no ambiente da internet e das aplicações de internet, a possibilidade da violação da privacidade ganha níveis exponenciais, quer seja pela falta de zelo daqueles que realizam o tratamento dos dados pessoais, quer seja dos próprios usuários, [...]

Mais adiante, os mesmos autores (JUNIOR e FAUSTINO, 2019, p. 306-307), no que se refere especificamente aos dados envolvendo a saúde dos usuários do Sistema Único de Saúde (SUS), que representa dados pessoais sensíveis de uma elevada camada da população brasileira, o risco de vazamento de dados é preocupante, sendo relevante para o presente estudo citar parte das inquietações manifestadas pelos articulistas quanto ao aplicativo E-Saúde lançado em junho de 2016 pelo Ministério da Saúde em âmbito nacional:

> Esse aplicativo ou solução oferece uma série de informações que possuem relação com os dados dos usuários do Sistema Único de Saúde (SUS) como, por exemplo, dados do cartão nacional de saúde, lista de medicamentos retirados em unidades de saúde, informações sobre o cartão de vacinação, lista de exames realizados, dentre outros.
> As informações são centralizadas em um banco de dados e será possível o estreitamento e análise das informações dos usuários em consonância com a utilização de unidades de saúde pública espalhadas pelo Brasil.

Prosseguem na narrativa os mesmos autores salientando quanto as implicações do aplicativo e-Health ou e-Saúde, destacando que:

> Esse aplicativo foi uma das primeiras ações do Estado direcionadas para a população utilizando tecnologia integrada com os serviços de saúde no formato conhecido como e-Health ou e-Saúde, com a possibilidade

6 Disponível em: <https://www.ibge.gov.br/apps/populacao/projecao/index.html?utm_source=portal&utm_medium=popclock>. Acesso em: 10.dez. 2019.

> de operações que envolvem o ciclo completo de tratamento de dados pessoais, onde o aplicativo vai armazenar todo o histórico de saúde de cada usuário com base nos dados no cartão SUS.

Para os autores, no exemplo acima, o risco na proteção e tratamento de dados foi evidente, na medida em que o aplicativo e-Saúde utilizado pela Prefeitura de São Paulo em 2016[7], demonstrou-se vulnerável no que se refere à forma de tratamento desses dados pessoais, quanto mais em se tratando de prontuários médicos de usuários do sistema de saúde que se utilizaram e se ainda continuam a pertencer ao Sistema Único de Saúde (SUS), porquanto não se vislumbra a necessária segurança das informações, ferindo-se, por esse modo, a privacidade de cada um dos usuários que foi exposta na rede de internacional de computadores (internet).

No exemplo acima ocorrido em 2016 (HERNANDES, 2017) resta evidente que não houve consentimento por parte dos titulares dos dados pessoais sensíveis quanto ao vazamento de prontuários médicos de pacientes da rede pública de saúde que estavam sob a guarda e responsabilidade da Prefeitura de São Paulo.

Conquanto o uso da tecnologia no século XXI já seja uma realidade irrenunciável, dado que em pleno final da segunda década do Século XXI é praticamente impossível a não conexão das pessoas por meio de aplicativos e sistemas eletrônicos (whatsapp, iFood, facebook, instagram, uber, 99, cabify, glovo, pje, projudi, e-proc, e-doc, além de milhares de app´s) o exemplo acima em relação ao vazamento de dados pessoais de pacientes (prontuário médico) na Internet abre uma verdadeira "caixa de Pandora" quanto aos objetivos desse breve estudo, na medida em que retomamos a seguinte indagação: Quais os limites para a intervenção do estado no tratamento dos dados pessoais sensíveis dos cidadãos brasileiros sem que ocorra violação ao direito à privacidade?

A tecnologia e a era digital vieram para facilitar o acesso às informações, porém, exigem, em contrapartida, um mínimo de investimento e proteção para os usuários titulares desses dados pessoais sensíveis, os quais, sem o consentimento específico, não podem ser divulgados por qualquer meio, quanto mais na rede mundial de computadores, porquanto a visualização desses dados fere o direito à privacidade consagrado no artigo 5º, X, da Constituição Cidadã de 1988.

7 Segue a parte complementar que retrata o caso ocorrido na Prefeitura de São Paulo em 2016, envolvendo o vazamento de dados pessoais de usuários do SUS por meio do aplicativo e-Saúde: Embora bastante interessante a solução, em uma pesquisa básica no site do Ministério da Saúde ou no próprio aplicativo e-Saúde, não é possível localizar a política de privacidade e os termos de usos, descriminando de forma transparente como serão tratados os dados pessoais do usuário, que tipo de dado pessoal será armazenado efetivamente, quem terá acesso a esses dados, possibilidade de exclusão de dados por parte dos usuários, e, principalmente, a respeito do consentimento dos usuários (pacientes) no que tange à forma de tratamento desses dados pessoais. Embora a solução seja bastante interessante como parte de uma política pública relacionada ao gerenciamento de dados de saúde dos usuários do sistema, esse aplicativo oferece claros riscos aos usuários, devido a não exposição de como esses dados pessoais serão tratados por parte do poder público e qual a extensão desse tratamento, ficando uma lacuna nesse sentido, dessa forma podendo surgir possibilidades de compartilhamento desses dados pessoais dos usuários, bem como episódios de vazamento de dados pessoais sensíveis nos moldes do que ocorreu na Prefeitura de São Paulo no ano de 2016 (HERNANDES, 2016), onde dados pessoais, e até mesmo dados de prontuário médico de pacientes da rede pública municipal de saúde foram expostos na internet sem a autorização, por conta de não estarem protegidos por mecanismos de segurança digital.

Gomes (2011, p. 615-616) cita o entendimento de Carlos Ari Sundfeld de que: "nos novos tempos, o Poder Legislativo faz o que sempre fez: edita leis, frequentemente com alto grau de abstração e generalidade.

Prossegue o referido autor justificando sua afirmação anterior, da seguinte forma:

> Só que, segundo os novos padrões da sociedade, agora essas normas não bastam, sendo preciso normas mais diretas para tratar das especificidades, realizar o planejamento dos setores, viabilizando a intervenção do Estado em garantia do cumprimento ou a realização daqueles valores: proteção do meio ambiente e do consumidor, busca do desenvolvimento nacional, expansão das telecomunicações nacionais, controle sobre o poder econômico – enfim, todos esses que hoje consideramos fundamentais e cuja persecução exigimos do Estado.

Justamente para que esse tratamento de dados pessoais não seja absoluto por parte da Intervenção do Estado na vida dos cidadãos brasileiros é que foi aposta ressalva no §1º no sentido de que o tratamento de dados pessoais, previsto no inciso III, será objeto de legislação específica dentro de critérios de proporcionalidade e que tais informações (dados pessoais sensíveis) a serem tratadas deverão ser as estritamente necessárias ao atendimento do interesse público, os princípios gerais de proteção e os direitos do titular previstos na Lei 13.709/2018.

5. CONSIDERAÇÕES FINAIS

A conclusão que podemos divisar é a de que existe profunda preocupação do legislador com relação aos abusos no tratamento de dados pessoais sensíveis de todos os cidadãos brasileiros, porquanto o direito à privacidade foi erigido à categoria de direito fundamental na Constituição da República Federativa do Brasil de 1988, de acordo com o artigo 5º, X[8].

Procuramos demonstrar que a Era Digital trouxe grandes avanços na forma como as pessoas e os países se comunicam de modo instantâneo e mais prático. Contudo, o tratamento dos dados pessoais sensíveis no Mundo Pós-Moderno deve obedecer a regramentos legais bem específicos, além de exigir o prévio consentimento dos titulares desses dados, sob pena de acarretar o dever de indenizar e incidirem os infratores em elevadas multas que ficarão a cargo da Autoridade Nacional de Proteção de Dados.

A Lei 13.709/2018, que entrará em vigência em agosto de 2020, representa –, ainda que de forma tardia em relação à Europa e diversos países da América Latina, porquanto muitos países já possuem há vários anos regramento específico para o tratamento de proteção dos dados pessoais sensíveis de seus cidadãos[9] – um importante marco legal após a Lei do marco Civil da Internet, para regular tal temática de uma forma um pouco mais criteriosa.

O exemplo trazido em relação ao vazamento de dados pessoais sensíveis corporificados nos prontuários médicos de pacientes usuários do SUS pela Prefeitura do Estado de São Paulo é fato inconteste de que

8 Art. 5º. Omissis:
...
X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

9 Argentina, Chile, Uruguai, por exemplo.

o assunto é extremamente sério na medida em que pode trazer um desprestígio do Brasil frente ao cenário mundial.

Além disso, representa um alerta de risco na segurança da informação digital, bem como para a própria economia do país, porquanto não se vislumbra como o nosso país possa oferecer segurança jurídica de investimento para empresas estrangeiras sem que comprove que está alinhado – de forma efetiva – com o GDPR e as normativas da EU em relação ao respeito ao tratamento dos dados pessoais sensíveis.

Por outro prisma, na perspectiva da cidadania de cada um dos brasileiros é vital que o Estado, as empresas e toda a sociedade estejam cientes de seus direitos, mas, sobretudo, de seus deveres no que tange aos ditames da Lei Geral de Proteção de Dados que, como dito anteriormente, entrará em vigência a partir de agosto de 2020 e afetará a todos.

Nestes aspectos, uma das contribuições desse estudo foi que o Estado enquanto detentor da titularidade da Autoridade Nacional de Proteção de Dados (ANPD), deve envidar esforços para utilizar o critério pedagógico e informativo a todos os destinatários das regras estabelecidas pela Lei 13.709/2018, e, acima de tudo, cumpra seu papel de ente público que segue os princípios da Administração Pública afeitos à Legalidade, Impessoalidade, Moralidade e Publicidade, atingindo-se a almejada eficiência dentro de valores que se coadunam com a moral e a ética tão caros em nosso país, afunilando-se no princípio vetor da Dignidade da Pessoa Humana (art. 1º, III, CRFB/88).

É nesta conjugação entre o direito e a tecnologia que àquele se confere o importante atributo de velar pelo cumprimento da legalidade também no mundo cibernético.

REFERÊNCIAS

BRASIL. Lei n.º 13.709/2018. Lei Geral de Proteção de Dados. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 10 jun. 2019

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 10 dez. 2019.

BUENO, Chris. Chegada do homem à Lua comemora 40 anos com nova missão. **Cienc. Cult.**, São Paulo, v. 61, n. 3, p. 19-20, 2009. Disponível em: <http://cienciaecultura.bvs.br/scielo.php?script=sci_arttext&pid=S0009-67252009000300008&lng=en&nrm=iso>. Acesso em: 18.aug.2019.

BRAVO, Álvaro A. Sanchez. **A proteção dos dados pessoais dos trabalhadores: Perspectiva Comunitária Europeia.** Revista do Tribunal Regional do trabalho da 15ª Região. n°. 30, Campinas, 2007. p. 153-160. Disponível em: <https://portal.trt15.jus.br/documents/124965/2647700/R+30-2007.pdf/27615c99-c09f-40ed-a17a-3c2c95edd63d>. Acesso em 02 dez. 2019.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. ***Espaço Jurídico,*** Joaçaba, v. 12, n. 02, p. 91-108, 2011. Disponível em: <https://editora.unoesc.

edu.br/index.php/espacojuridico/article/viewFile/1315/658>. Acesso em: 28 dez. 2019.

CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 1999.

União Europeia. **DIRETIVA 45/96/CE**. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046>. Acesso em: 12.dez.2019.

GOMES, Joaquim B. Barbosa. Agências Reguladoras: A Metamorfose do Estado e da Democracia Uma Reflexão de Direito Constitucional e Comparado). In: CLEVE, Clemerson Merlin; BARROSO, Luís Roberto (org.). **Doutrinas Essenciais. Direito Constitucional. Volume VI. Constituição Financeira, Econômica e Social**. São Paulo: Revista dos Tribunais, 2011.

FERNANDES, David Augusto. Dados pessoais: Uma Nova Commodity, ligados ao Direito à intimidade e a Dignidade da Pessoa humana. **Revista Jurídica – Unicuritiba**. vol. 04, n°. 49, Curitiba, 2017. pp. 360-392. Disponível em: <http://revista.unicuritiba.edu.br/index.php/RevJur/article/view/2298/1428>. Acesso em 05. jun. 2019

FRAZÃO, Ana. **Nova lgpd: as demais hipóteses de tratamento de dados pessoais**. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/ -19092018 Publicado em 19/09/2018>. Acesso em 02.abr. 2019

GONÇALVES, Tânia Carolina Nunes Machado; VARELLA, Marcelo D. Os desafios da Administração Pública na disponibilização de dados sensíveis. **Rev. direito GV**. São Paulo, v. 14, n. 2, p. 513-536, aug. 2018. Disponível em: om <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1808-24322018000200513&lng=en&nrm=iso>. Acesso em: 05. nov. 2019. http://dx.doi.org/10.1590/2317-6172201821.

HARARI, Yuval Noah. **21 lições para o século 21**. Tradução: São Paulo: Companhia das Letras, 2018.

HERNANDES, Raphael. Gestão Haddad expõe na internet dados de pacientes da rede pública. In: **Folha de São Paulo.** 2016. Disponível em <http://www1.folha.uol.com.br/cotidiano/2016/07/1788979-gestao-haddad-expoe-na-internet-dados-de-pacientes-da-rede-publica.shtml>. Acesso em 30. jul. 2019.

BARRETO JUNIOR, Irineu Francisco; FAUSTINO, André. Aplicativos de serviços de saúde e proteção dos dados pessoais dos usuários**. Revista Jurídica** vol. 01, n°. 54, Curitiba, 2019. p. 292 – 316. DOI: 10.6084/m9.figshare.7841105. Disponível em: <http://revista.unicuritiba.edu.br/index.php/RevJur/article/view/3311/371371803>. Acesso em 06 jun. 2019.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018**. São Paulo: Saraiva Educação, 2018.

REINALDO FILHO, Demócrito. A Diretiva Europeia sobre proteção de dados pessoais. Uma análise de seus aspectos gerais. **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 18, n. 3507, 6 fev. 2013. Disponível em: <https://jus.com.br/artigos/23669>. Acesso em: 9 jan. 2020.

SILVA, Letícia Brum da; SILVA, Rosane Leal da. **A PROTEÇÃO JURÍDICA DE DADOS PESSOAIS NA INTERNET: análise comparada do tratamento jurídico do tema na União Europeia e no Brasil**. Disponível em: <http://www.publicadireito.com.br/artigos/?cod=e4d8163c7a068b65>. Acesso em 17. ago. 2019.

Publicado originalmente na Revista Relações Internacionais do Mundo Atual - v. 2, n. 27 (2020) - UniCuritiba

TRATAMENTO DE DADOS PESSOAIS E RELAÇÃO LABORAL: CONTRIBUIÇÕES DO RGPD E DO DIREITO DO TRABALHO FRANCÊS

Rosane Gauriau

RESUMO

O presente artigo visa examinar o tratamento de dados pessoais na fase pré-contratual, durante o contrato de trabalho e ao fim da relação laboral, à luz da LGPD, e do RGPD, à partir da contribuição do direito do trabalho francês. Não se tem por objetivo comparar a LGPD e o RGPD, tampouco o direito do trabalho francês e brasileiro. Pretende-se examinar, tão somente, a experiência francesa de aplicação do RGPD e a partir dela cogitar sobre suas possíveis contribuições (ou não) ao direito do trabalho brasileiro. Enfim, sem a pretensão de exaurir a questão, serão analisadas algumas noções fundamentais e regras específicas para o tratamento de dados pessoais no contexto das relações laborais, no RGPD e na LGPD.

PALAVRAS-CHAVE:. LGPD, RGPD, França, Brasil, relação laboral, Proteção de Dados

ABSTRACT

This paper aims to address a short study about data protection during in the employment relationship based on GDPR, LGPD and French labor law. We will not compare LGPD and GDPR, nor even French and Brazilian labor law, but only, the GPDR's French experience and its possible contribution to Brazilian labor law. Finally, to understand the issue, we will examine some definitions and specific rules linked to data protection in the labor law context.

KEYWORD: LGPD, GDPR, France, Brazil, employment relationship, data protection.

SUMÁRIO

Rosane Gauriau

Pesquisadora. Doutora em Direito (summa cum laude) pela Université Paris 1- Sorbonne. Mestre em Droit des Entreprises, Université d'Angers. Membre associée do Centre Jean Bodin, recherche juridique et politique, CJB, EA n° 4337, Université d'Angers, SFR Confluences.

1-Introdução

Os recentes (mega)vazamentos de dados pessoais no Brasil e no mundo ilustram a "fragilidade dos procedimentos de segurança da informação e a ineficiência das normas jurídicas que têm por objeto a tutela de dados pessoais" (BURITI, 2021). O *Big data* é um mercado estratégico e lucrativo (CAPRIOLI, 2009; DUBOIS, 2017)

Dados pessoais estão presentes e acessíveis em todo tempo e lugar: smartphones, tabletes e computadores coletam, classificam e comercializam contatos, localização, som, imagem, hábitos e perfil. Uma mina de ouro para muitas empresas que os utilizam para analisar, orientar, otimizar o marketing, a publicidade e influenciar preferências políticas, sindicais ou de consumo.[1]

Este tipo de "mercantilização" dos dados pessoais invade o direito à intimidade e à vida privada das pessoas, razão pela qual, em diversos países, uma legislação específica foi elaborada para proteger os dados pessoais.

A implementação do RGPD (*Règlement Général sur la Protection des Données*)[2] no âmbito da União Europeia (UE) e do LGPD (Lei Geral de Proteção de Dados Pessoais) no Brasil insere-se nesse contexto, pois visam regular o tratamento dos dados das pessoas físicas garantindo-lhes seus direitos e liberdades fundamentais.

2- Considerações iniciais

LGPD e RGPD. A Lei Geral de Proteção de Dados Pessoais (LGPD)[3], Lei nº 13.709, de 14 de agosto de 2018, em vigor desde 18 de setembro de 2020[4], dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado. Inspirada na legislação europeia[5], a LGPD define as hipóteses de uso legítimo de dados pessoais por terceiros e estabelece os mecanismos de sua proteção. Seu objetivo é proteger os direitos fundamentais, como o direito à intimidade, privacidade e o livre desenvolvimento da personalidade da pessoa natural[6], bem como o direito de acesso igualitário ao ambiente virtual (PAMPLONA FILHO, 2020, p.4)

No âmbito da União Europeia, o Regulamento Geral de Proteção de Dados (RGPD)[7], Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, em vigor desde 25 de maio de 2018, é o texto de referência na matéria. Sendo um regulamento europeu, o RGPD é obrigatório e diretamente aplicável a todos os 27 Estados-Membros da UE. Na França, a Lei n° 2018-493

1 How Companies Learn Your Secrets. Disponível em: http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html ?_r=l&hp=&pagewanted=all). Acesso: 14 fev. 2021. The Great DMP Debate. Disponível em: https://www.adexchanger.com/data-exchanges/the-great-dmp-debate/ Acesso: 14 fev. 2021. What is a Data Management Platform, or DMP? Disponível em: https://digiday.com/media/what-is-a-dmp-data-management-platform/ Acesso: 14 fev. 2021.

2 Regulamento Geral de Proteção de Dados, em inglês GDPR, General Data Protection Regulation.

3 V. : art.5, X da CF e Lei nº 12.965 de 23 de abril de 2014 (Marco Civil da Internet). E ainda, a Decisão 15/20 do Conselho do Mercado Comum (CMC), MERCOSUL.

4 Exceto no que se refere às sanções administrativas que entrarão em vigor em 1º de agosto de 2021.

5 No particular da Diretiva 95/46/CE da União Europeia vigente à época da apresentação do projeto de lei (PL 4060/2012, Dep. Milton Monti - PR/SP).

6 LGPD: arts. 1 e 17 .

7 Revogou a Diretiva 95/46/CE.

de 20 de junho de 2018[8] adaptou a *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*[9] ao RGPD.

O RGPD cria um conjunto harmonizado de regras aplicáveis a qualquer tratamento de dados da pessoa física que ocorra na União Europeia. O objetivo é o de contribuir para a realização de um espaço de liberdade, segurança e justiça, para o progresso econômico e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas[10]. Aplicável, particularmente, às questões civis e comerciais, o RGPD estipula regras relativas à privacidade dos titulares dos dados e à livre circulação desses dados: protege as liberdades e direitos fundamentais dos indivíduos e, em particular, o direito à proteção de dados pessoais[11], intimidade e vida privada[12].

Segundo o RGPD , "dados pessoais" são quaisquer informações relativas a uma pessoa singular identificada ou identificável[13] ("titular dos dados"). "Tratamento"[14] é uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, etc. Os princípios da proteção de dados protegem também os "dados sensíveis"[15] e pseudoanonimizados[16], mas não se aplicam às informações anônimas[17]. Ressalte-se que, a proteção das pessoas físicas relativamente ao tratamento de seus dados pessoais é um direito fundamental reconhecido em diversos textos[18], dentre eles, o artigo 8°, n°1, da Carta dos Direitos Fundamentais da União Europeia e o artigo 16, n°1, do Tratado sobre o Funcionamento da União Europeia (TFUE) .

De modo similar, a LGPD considera que "dado pessoal" é toda a informação relacionada à pessoa natural identificada ou identificável[19]. "Tratamento de dados" é toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação,

8 V. também : Décret d'application n°2018-687 du 1er août 2018 ; Ordonnance n°2018-1125 du 12 décembre 2018; Décret n° 2019-536, 29 mai 2019. Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'Informatique, aux fichiers et aux libertés. Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel.

9 Que já tratava, à época, de questões relativas ao digital e tratamento de dados.

10 RGPD : Considerando (Consid.) n°s 1 e 2.

11 RGPD: Consid. n° 14.

12 RGPD, art. 1°.

13 RGPD : Consid. 26, 30 e art. 4.§1. Identificável é pessoa singular que possa ser determinada, direta ou indiretamente por meio, e.g., de seu nome, dados de localização, ou outros elementos específicos de sua identidade física, genética, mental, econômica, cultural ou social.

14 RGPD : Art .4°, §2.

15 RGPD : Consid. n° 10, 51 e arts. 4°, § 14, 9°, §§1° e 4°, 11, §§ 1°, 2°, "b" e art. 8° da Loi du 6 janvier 1978.

16 RGPD: Consid. n°26, 28, 29, 75, 78 e arts. 4°, §5°, 25, 32 e 40.

17 RGPD: Consid. n° 26.

18 P. ex. Diretiva (UE) 2012/58/CE do Parlamento Europeu e do Conselho (12/7/2012), modificada pela Diretiva 2009/136/CE do Parlamento e do Conselho (25/11/2009), Convenção STE108 (28/1/1981) e seu protocolo adicional.

19 LGPD: art.5°, I.

modificação, comunicação, transferência, difusão ou extração[20].

Campo de aplicação. Em regra geral, a LGPD[21] aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

1/ a operação de tratamento seja realizada no território nacional;

2/ a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;

3/ ou os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

Aplica-se também às empresas com sede no exterior, desde que a operação de tratamento de dados seja realizada no território nacional. Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta. Logo, "é irrelevante o país sede da empresa, o meio de tratamento de dados, a localização dos dados (...) a nacionalidade de seu titular, bastando que (...) os dados se encontrem em território brasileiro no momento da coleta" (PAMPLONA FILHO, 2020, p.11).

A LGPD não se aplica, dentre outros, ao tratamento de dados pessoais realizado por pessoa natural para fins particulares e não econômicos. Ou ainda, o tratamento de dados realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, atividades de investigação e repressão de infrações penais [22].

O RGPD aplica-se a toda organização, pública ou privada, de qualquer porte (empresa, Ministério, comunidade, associação, etc.) que processa dados pessoais de pessoa física em seu nome ou não, e estabelecido da União Europeia, ou que, se não estiver estabelecido em seu território, vise diretamente os residentes europeus.

Sanção e fiscalização. O cumprimento e fiscalização da RGPD e do LGPD, na França e no Brasil faz-se, principalmente, por meio de órgãos administrativos: a CNIL e a ANPD, respectivamente.

Na França, a Comissão Nacional de Informática e Liberdades (*Commission Nationale de l'Informatique et des Libertés -CNIL*) foi criada pela *Loi n° 78-17 du 6 janvier 1978* e tem por missão garantir a proteção dos dados pessoais em suporte físico ou digital, de natureza pública ou privada. Trata-se de uma autoridade administrativa independente que atua em nome do Estado, sem a ele estar subordinado. A CNIL tem a função de alertar, aconselhar e informar tanto o Poder Público, quanto os indivíduos em geral. Por fim, tem poder de controle e sanção[23]. As deliberações da CNIL são muito importantes, regularmente citadas e observadas pelo Governo, órgãos públicos e Juízes em suas decisões.

No Brasil, a ANPD (Autoridade Nacional de Proteção de Dados) é o órgão da Administração Pública Federal, vinculada à Presidência da República, responsável por zelar pela proteção de dados pessoais e por

20 LGPD: art 5°, X.

21 LGPD: arts. 3° e 4°.

22 LGPD: art. 4°.

23 Disponível em : https://www.cnil.fr/. Acesso: 13 fev. 2021.

implementar e fiscalizar o cumprimento da LGPD[24]. A ANPD tem natureza jurídica transitória[25]. Logo, não tem a mesma autonomia e liberdade da CNIL. A ANPD se articula com outras entidades e órgãos públicos no exercício das suas competências[26]. Tanto a LGPD quanto a RGPD preveem sanções administrativas, civis e penais por seu descumprimento[27].

Tratamento de dados e relações de emprego[28]. O dados pessoais gerados no ambiente laboral necessitam, como todo dado pessoal, de proteção e tratamento.

O Código do Trabalho francês já cuidava, antes do advento do RGPD, sobre o tratamento dos dados pessoais dos empregados em diversos dispositivos, como, por exemplo, no artigo L. 1221-9 do Código do Trabalho, que especifica que nenhuma informação pessoal relativa a um candidato a um emprego pode ser recolhida por um dispositivo que não tenha sido previamente levado ao seu conhecimento. Ou ainda, o artigo L. 1221-6 do mesmo Código, que prevê que as informações recolhidas por ocasião do recrutamento apenas podem ser utilizadas para avaliar a capacidade ou as aptidões profissionais do candidato.

O RGPD em seu artigo 88 reforça esse direito dos trabalhadores. O dispositivo cuida do tratamento de dados no contexto das relações de trabalho: os Estados-Membros podem estabelecer no seu ordenamento jurídico, por lei ou em convenções coletivas, normas mais específicas para garantir a defesa dos direitos e liberdades, relativamente ao tratamento de dados pessoais dos trabalhadores, no contexto laboral, principalmente para efeitos de recrutamento, execução do contrato de trabalho[29] e cessação da relação de trabalho. Tais regras devem incluir medidas adequadas e específicas para salvaguardar a dignidade, os interesses legítimos e os direitos fundamentais do titular dos dados, com especial relevo para a transparência do tratamento de dados, a transferência de dados pessoais num grupo empresarial ou num grupo de empresas envolvidas numa atividade económica conjunta e os sistemas de controle no local de trabalho[30].

A LGPD contrariamente ao RGPD não cuidou expressamente do tratamento de dados nas relações de trabalho, mas não há dúvidas de que a lei se aplica às relações de emprego, por haver coleta de dados pessoais no ambiente laboral.

Dentre os princípios e fundamentos, direitos e obrigações que consagra a LGPD[31] e que podem ser aplicados às relações de trabalho, vale destacar: o princípio da dignidade, não discriminação, autodeterminação informativa[32],

24 Art. 55-A e seg. da LGPD, Lei n° 13.853, de 14/8/2019 e Decreto n°10.474, 26/8/2020.

25 LGPD: art. 55-A.

26 LGPD: art 55-K, parágrafo único.

27 Cf. Capitulo VIII da LGPD e Capitulo VIII da RGPD.

28 Aqui entendidas as relações laborais que tratem de dados pessoais do empregado.

29 RGPD: art. 88, §1°: "(...) incluindo o cumprimento das obrigações previstas no ordenamento jurídico ou em convenções coletivas, de gestão, planejamento e organização do trabalho, de igualdade e diversidade no local de trabalho, de saúde e segurança no trabalho, de proteção dos bens do empregador ou do cliente e para efeitos do exercício e gozo, individual ou coletivo, dos direitos e benefícios relacionados com o emprego".

30 RGPD: Art. 88, §2°.

31 LGPD: Arts 2° e 6°.

32 "Segundo JJ Gomes Canotilho a autodeterminação informativa se traduz, fundamentalmente, na faculdade de o particular determinar e controlar a utilização dos seus dados pessoais. Trata-se de um direito fundamental, visto que diretamente ligado à privacidade e intimidade (art. 5º, X, da CF/88)". PINHEIRO e BOMFIM, 2020.

boa-fé, lealdade; a liberdade de expressão, de informação, de opinião; o direito à intimidade e à vida privada, à inviolabilidade da honra e da imagem. E, ainda, o livre acesso, exatidão, clareza, qualidade, atualização, integridade, confidencialidade, conservação, transparência, adequação, proporcionalidade e limitação das finalidades no tratamento dos dados pessoais. Enfim, o interesse público, segurança, proteção, prevenção, responsabilização e prestação de contas, sempre observado o devido processo legal.

> (...) a espinha dorsal da proteção de dados pessoais, é, basicamente, formada por cinco princípios, a saber: a) princípio da publicidade: a existência de banco de dados deve ser de conhecimento do público; b) princípio da exatidão: as informações devem ser fiéis à realidade e deve haver a possibilidade de atualizá-las periodicamente; c) princípio da finalidade: utilizar os dados para fins determinados - o qual deve ser comunicado ao titular antes da coleta; d) princípio do livre acesso: o interessado deve poder ter acesso aos ficheiros que contêm seus dados, além de poder controlá-los – de acordo com o princípio da exatidão; e) princípio da segurança física e lógica: os dados devem ser protegidos contra extravios, destruições, modificações, transmissões ou acessos não autorizados (PAMPLONA FILHO, 2020, p.8)

Ambos, o RGPD e a LGPD, tratam, ainda que nem sempre sob o mesmo enfoque[33], por exemplo, do princípio da *accountability* ou princípio da responsabilização e da prestação de contas[34], da nomeação e papel do encarregado de dados (*Data Protection Officer*[35]) ou ainda, da avaliação de impacto em matéria de proteção de dados[36] (*Data Protection Impact Assessment*).

Consentimento. Segundo o RGPD[37], o consentimento é a manifestação de vontade, livre, específica, informada e explícita pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento. No mesmo sentido, a LGPD afirma que o consentimento é a manifestação de vontade livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada[38]. Como consequência, os contratos (compreendido o contrato de trabalho) deverão evitar:

> (...) termos técnicos e textos demasiadamente longos. [Logo, as] informações [devem ser] claras, objetivas, inteligíveis, de fácil acesso, expressas acerca dos tipos de dados que estão sendo coletados naquela operação, os quais serão armazenados e os que serão descartados, por quanto tempo permanecerão arquivados, de

33 Sobre as principais diferenças entre a LGPD e o RGPD, verificar quadro comparativo de: RUARO, 2020.

34 RGPD: art. 5°. LGPD: art. 6º, §10.

35 RGPD: arts. 37 a 39. LGPD: arts. 5°, VIII e 41.

36 "Relativamente ao relatório de impacto a LGPD não deixou claro em quais situações o controlador será obrigado a realizar um relatório de impacto à proteção de dados pessoais, delegando a uma regulamentação posterior o tratamento desta matéria. O RGPD prevê um relatório de impacto à proteção de dados pessoais, quando o tratamento resultar em um elevado risco para o direito e a liberdade das pessoas, em determinadas hipóteses". V. RUARO, 2020.

37 RGPD : Consid. n°s 32, 33, 42, 43 e arts.4°,11, §§ 6° e 7° .

38 LGPD: art 5°, VII.

> que forma serão mantidos e, sobretudo para quais finalidades serão utilizados após a coleta e durante o tempo que estiverem em seu poder (PAMPLONA FILHO, 2020, p.13).

Assim, tanto no RGPD[39] quanto na LGPD, as cláusulas que versarem sobre a política de tratamento de dados da empresa devem ser destacadas no documento apresentado ao titular dos dados, de forma a garantir a observância dos princípios da finalidade, transparência e segurança. São excluídas todas as formas de consentimento passivo ou genérico, sob pena de nulidade do ato.

> (...) deve ser assegurado ao titular dos dados a indicação pontual e específica de quais dados ele deseja consentir e para qual finalidade específica, em detrimento da prática de mercado materializada pelo '*all or nothing*'. A granularidade, portanto, é a possibilidade de indicação específica e pontual e é um mecanismo revelador da liberdade do consentimento exigida pelo art. 5º, XII, da LGPD (PINHEIRO e BOMFIM, 2020).

O consentimento, segundo a LGPD, pode ser revogado a qualquer momento mediante manifestação expressa do titular[40]. De preferência, o consentimento deverá ser fornecido por escrito e constar de cláusula destacada das demais cláusulas contratuais, como por exemplo, por meio de um termo de consentimento para que o empregado[41] concorde expressamente com o conteúdo da política de tratamento de dados do empregador (normalmente, no contexto laboral, o controlador é o empregador)[42].

Em caso de alteração de informação, o controlador deverá informar o titular destacando as alterações feitas. O titular poderá, nos casos em que o seu consentimento for exigido, concordar, discordar da alteração ou revogar seu consentimento. Se o titular dispõe do direito à informação de seus dados pessoais, há hipóteses em que seu consentimento é dispensado[43], por exemplo, para o cumprimento de uma obrigação legal ou em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária[44].

> Isso ocorre, por exemplo, quando há determinações emanadas da lei para a empresa fornecer os dados do empregado (titular dos dados) para cadastro no e-social, ou até mesmo quando decorrer de uma decisão judicial determinando o fornecimento de dados para pagamento de uma pensão alimentícia, ou até mesmo uma determinação do Ministério Público em uma fiscalização. Nessas hipóteses, obviamente, dispensa-se a obtenção do consentimento do titular, eis que o tratamento decorre de uma obrigação

39 RGPD: Art.8°, § 4°.

40 LGPD: art. 18, §6°.

41 Trabalhador e empregado são empregados como sinônimos.

42 Cabe ainda ao empregador os deveres de prevenção e não discriminação, impedindo a utilização dos dados para fins ilícitos e discriminatórios (...), incluindo ainda a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais, sob pena de sua responsabilização. PAMPLONA FILHO, 2020, p. 26

43 RGPD: arts. 6° a 9° e 18. LGPD: art. 7º, §§4° a 7°, 11, 18 e 27.

44 P.ex.. Exame toxicológico para o motorista profissional (art.168, § 6°, da CLT), atestado de antecedentes criminais para o vigilante (arts. 12 e 16, VI, da Lei n° 7.102/1983 c/c art. 4°, I da Lei n. 10.826/2003). Cf., ainda: IRR 24300-58.2013.5.13.0023. SBDI-1 Plena J. 20/04/2017, Rel. Min. Augusto César Leite de Carvalho.

> legal. Entretanto, por cautela caberá à empresa informar expressamente por escrito no formulário de contratação essas possibilidades de fornecimento de dados decorrentes da lei, primando pelo princípio da informação preconizado pela LGPD (PAMPLONA FILHO, 2020, p.14).

Ressalte-se, enfim, que tanto na França quanto no Brasil[45], a liberdade do consentimento no contexto laboral é vista com reservas. Isso porque, é sabido que o empregado raramente pode dar, recusar ou revogar livremente o seu consentimento. *Primo*, em razão da dependência financeira do empregado *vis-à-vis* do empregador. *Secundo*, em razão da relação de subordinação que preside o contrato de trabalho e cria, indiscutível, desequilíbrio entre as partes.

> [O] consentimento (...) no âmbito das relações de trabalho é cercado de preocupações. Isso porque o art. 5º, XII, proclama que o consentimento deve ser entendido como a 'manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada'. A expressão 'livre' pressupõe verdadeira opção do titular dos dados, pressuposto que despertará dúvida sobre sua ocorrência no âmbito de uma relação como a trabalhista, marcada pelo desequilíbrio de poder e, em regra, pela dependência econômica. Não serão raras as alegações de que o empregado não teve legítima escolha, a ele tendo sido imputado o consentimento como fator condicionante de manutenção do vínculo de emprego.
>
> (...) caso o empregador pretenda obter o consentimento, é necessário observar o art. 8º, caput e § 1º, da LGPD, que estipula que o consentimento deve ser fornecido 'por escrito ou por outro meio que demonstre a manifestação de vontade do titular' e que, caso seja fornecido por escrito, deve 'constar de cláusula destacada das demais cláusulas contratuais'. Logo, sempre deverá ser expresso o consentimento (...).Algumas empresas têm inserido cláusula específica e destacada nos contratos formais de trabalho, mas, considerando a natureza de contrato de adesão do contrato de trabalho e que é delas o ônus de comprovar a validade do consentimento (art. 8º, § 2º) seria ainda mais prudente a celebração de um documento em apartado (PINHEIRO e BOMFIM, 2020).

Feitas essas considerações inicias, iremos examinar o tratamento de dados na relação individual de trabalho[46], à luz da LGPD e do RGPD, à partir da interpretação que lhe confere o Direito do Trabalho francês. *In casu*, o interesse pelo direito comparado não é o de importar o sistema estrangeiro, mas de observar quais lições podem ser aproveitadas a fim de construir um sistema próprio à realidade brasileira[47]. Assim, serão analisados, primeiramente, o tratamento de dados laborais

45 Posição adotada pelo Article 29 Data Protection Working Party, WP 249, Opinion 2/2017 on data processing at work (§ 6.2.). 8 de junho de 2017. Disponível em https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169. Acesso: 6 fev. 2021.

46 A LGPD contrariamente ao RGPD não faz menção ao tratamento de dados pelas convenções coletivas de trabalho e participação de instituições representativas do pessoal. Consid. n° 155, arts. 9° e 88.

47 V. p.ex: Kelsen (Teoria Pura do Direito) e R. Alexy (El concepto y la validez del derecho y otros ensayos, Teoría del discurso y derechos humanos ou Teoría de la Argumentación Jurídica: La Teoría del Discurso Racional como Teoría de la Fundamentación Jurídica).

na fase que antecede o contrato de trabalho, fase pré-contratual (I). Em seguida, durante o contrato de trabalho, fase contratual (II) e, enfim, após a ruptura do contrato de trabalho, fase pós-contratual (III):

3- Tratamento de dados e relação empregatícia

I/ TRATAMENTO DE DADOS: FASE PRÉ-CONTRATUAL

Recrutamento e Seleção. Segundo o Código do Trabalho francês[48], as informações relativas aos candidatos não podem ser coletadas por um dispositivo que não lhes tenha sido informado previamente. As informações apenas podem ser utilizadas para avaliar a capacidade ou aptidões profissionais para o cargo proposto. Os métodos e técnicas empregados por ocasião do recrutamento devem ser adequados, proporcionais e em relação com a finalidade a ser alcançada. Os resultados coletados são confidenciais[49]. Nas empresas com mais de 50 empregados, essas informações serão fornecidas preservando o anonimato e conforme os moldes fixados por Decreto do *Conseil d'État.*[50]

Esses dispositivos, interpretados à luz do RGPD, demandam do empregador uma proteção reforçada dos dados pessoais do candidato (titular dos dados) durante o recrutamento: ou seja, são excluídas todas as informações sobre a vida privada do candidato, a menos que a informação tenha vínculo direto e necessário com o cargo em questão. A seleção de candidatos que envolva uma avaliação do comportamento humano, que forneça uma definição do perfil ou personalidade do candidato, com base por exemplo, em sua situação econômica, localização, estado de saúde ou civil, opinião política, religião ou convicções, filiação sindical ou orientação sexual só deverá ser permitida em condições específicas e mediante consentimento do candidato. Recorde-se que o consentimento do candidato, nesta fase, bem como em todas as fases da relação laboral deve ser livre, expresso e inequívoco. O candidato deve, sempre, fornecer as informações de boa-fé[51].

Acrescente-se ainda que, segundo o RGPD, o responsável pelo tratamento de dados deverá fornecer ao candidato, dentre outras, todas as informações necessárias para assegurar um tratamento equitativo e transparente de seus dados, tendo em vista as circunstâncias e o contexto específicos em que eles serão tratados. Sempre que os dados pessoais forem suscetíveis de ser legitimamente comunicados a outro destinatário ou utilizados para outro fim que não aquele para o qual tenham sido recolhidos, o responsável pelo tratamento deverá fornecer ao candidato informações sobre a finalidade da coleta, bem como todas as informações necessárias à compreensão do tratamento de dados. O candidato tem o direito de acessar os dados coletados sobre a sua saúde, e.g., resultados de seus exames ou avaliações médicas[52].

Como consequência, os questionários

48 Arts. L.1221-6 a L.1221-9; L.1121-1; L.1222-3 e L.1222-4.

49 Arts. 9° do Código Civil francês e 226-1 e ss. do Código Penal francês.

50 Mais alta Corte Administrativa da Jurisdição Administrativa francesa.

51 RGPD: art. 5º, §1°, "c".

52 Consid. n°s, 39, 58, 60, 71, 78 e arts. 5°, §1°, "a"; 12; 13, §2°e 26, §1°.

apresentados ao candidato devem observar o princípio da minimização de dados e as questões devem estar diretamente relacionadas a oferta de emprego. Deve ser-lhe informada a finalidade da coleta dos dados, forma e duração do tratamento, a identificação e informações de contato do controlador, se haverá compartilhamento de dados e para qual finalidade, além das responsabilidades dos agentes de tratamentos e os direitos do titular dos dados (direito de acesso, retificação e oposição).

Durante essa fase, o recrutador deve respeitar a vida privada do candidato, bem como observar os princípios de lealdade, minimização, transparência, equidade, proporcionalidade e adequação no tratamento de dados.

Em caso de desfecho negativo da candidatura, o recrutador deve informar ao candidato se pretende manter o seu currículo e arquivos (contendo dados pessoais), bem como, dar-lhe a possibilidade de autorizar ou solicitar a sua destruição. O recrutador, se for o caso, deverá justificar por que certas informações necessitam conservação.

A experiência francesa pode inspirar o Direito do Trabalho brasileiro[53]. Assim, por exemplo, os dados pessoais coletados por ocasião de um recrutamento e seleção no Brasil (p.ex. identificação pessoal) ou dados sensíveis (p.ex. filiação sindical ou dados relativos à saúde) devem ser tratados com cautela, a fim de evitar discriminação ou afronta à vida privada do candidato. Os princípios supramencionados, bem como o consentimento do titular, devem ser respeitados e observados. Findo o processo seletivo, o recrutador deverá informar claramente aos candidatos não selecionados a política de utilização dos dados fornecidos e, principalmente, o que será feito com seus dados, documentos, currículos e eventual conservação (PAMPLONA FILHO, 2020, p.25)

Algoritmos, recrutamento e seleção. *Quid* da seleção por algoritmo? Segundo o RGPD, o titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar[54]. Não se trata, portanto, de proibir o uso de algoritmos, mas de limitar e enquadrar sua utilização.

Alinhada ao RGPD, a LGPD afirma que o titular dos dados tem direito de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial[55]. Em razão do princípio da transparência, recomenda-se a elaboração de relatório de impacto sobre a proteção de dados pessoais, a fim de evitar eventual contencioso de discriminação.

53 Arts. 17 a 20 LGPD.

54 RGPD: art 22.

55 LGPD: art.20 e §1°.

II/ TRATAMENTO DE DADOS: FASE CONTRATUAL

Execução do contrato de trabalho. É na fase contratual que o empregado terá conhecimento da política de tratamento de dados da empresa e dará (ou não) o seu consentimento expresso. Consequentemente, as cláusulas contratuais devem ser redigidas de modo a comprovar a transmissão de informações acerca do tratamento de dados do empregado.

O Código do Trabalho francês[56] afirma que nenhuma informação sobre um empregado pode ser coletada por um dispositivo que não lhe tenha sido previamente informado. A exigência de boa-fé e lealdade nas relações de trabalho proíbe o uso de meios clandestinos de controle do empregado. Assim, o controle por geolocalização, biometria ou vídeo/áudio-vigilância não pode ser utilizado se não estiver em conformidade com o RGPD. A coleta ilegal desses dados pelo empregador pode implicar violação da obrigação de lealdade[57], da vida privada e intimidade do empregado, culminando em sanções administrativas ou penais.

Tanto o RGPD quanto a LGPD aplicam-se aos documentos que contenham dados pessoais e dados sensíveis, a exemplo dos dados bancários para pagamento de salários, dados relativos à remuneração para fins de pensão alimentícia, dados relativos à saúde, como exames ocupacionais e atestados médicos, ficha de registro do empregado, filiação sindical etc. Recomenda-se, pois, que os formulários, questionários e os contratos de trabalho sejam adequados às exigências da LGPD, "sob pena de burla à necessária adequação dos dados coletados à teleologia justificada, de modo a permitir o livre acesso de modo gratuito e com qualidade, exatidão, clareza, transparência e segurança, cabendo às empresas a obrigação de prestação de contas (*accountability*)" (PAMPLONA FILHO, 2020, p.26).

Rememore-se que é direito do empregado, na qualidade de titular dos dados pessoais, o acesso facilitado às informações sobre o tratamento de seus dados que devem ser disponibilizados de forma clara, adequada e ostensiva pelo empregador. Dentre outros, devem ser-lhe informados seus direitos na qualidade de titular dos dados e a finalidade específica do tratamento; forma e duração do tratamento, observados os segredos comercial e industrial; identificação e informações de contato do controlador; informações acerca do uso compartilhado de dados pelo controlador e a finalidade; responsabilidades dos agentes que realizarão o tratamento, etc. O empregado pode, a qualquer momento, durante a execução do contrato e mediante requisição, acessar, confirmar, corrigir seu dados incompletos, inexatos ou desatualizados, bem como solicitar o bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o LGPD ou revogar seu consentimento[58]. Ele tem o direito de se opor a uma medida de definição de perfil, direito à portabilidade dos seus dados, direito à limitação do tratamento, e, enfim, direito de acesso, retificação, bloqueio[59] ou eliminação[60].

56 Artigo L.1222-4 do Código do Trabalho.

57 Artigo L.1222-1 do Código do Trabalho.

58 LGPD: art. 18.

59 LGPD: arts. 7° a 12, 15 a 22. RGPD: Consid. n°s 32, 42, 43 e art. 4°, §11.

60 Quanto ao direito ao esquecimento digital, o RGPD faz a ele expressamente menção, dentre outros,

Dentre os diversas questões relativas ao tratamento de dados pessoais e sensíveis durante a execução do contrato de trabalho, destacamos a vigilância e o monitoramento dos trabalhadores (a), uso da biometria (b), do *BYOD* (c) e dos dados relativos à saúde do trabalhador (d):

a-Vigilância e monitoramento de empregados. Na França, à luz do RGPD, da legislação[61], das deliberações da CNIL[62] e da jurisprudência[63], em regra geral, não é permitido o monitoramento permanente dos empregados (p.ex. vigilância constante por vídeo, *webcam* ou dispositivos de áudio), salvo em circunstâncias especiais e devidamente justificadas. Tal como acontece com qualquer tratamento de dados pessoais, um sistema de monitoramento do tempo de trabalho ou das atividades realizadas pelos empregados, à distância ou *in loco,* deve ter uma finalidade clara, definida, além de ser proporcional e adequado aos fins a que se destina. Os empregados e o *Comité social et économique*[64] (CSE) devem ser informados acerca de toda forma de monitoramento e vigilância. Isso porque, os empregados também têm direito ao respeito da vida privada no local de trabalho. Assim sendo, um sistema de vigilância permanente é excessivo e desproporcional, principalmente porque existem meios alternativos e menos intrusivos para alcançar tal fim. Igualmente excessivo e desproporcional é o compartilhamento permanente da tela e/ou uso de *keyloggers*[65], ou ainda, a obrigação do empregado de realizar ações, regularmente, para demonstrar sua presença atrás de sua tela, como clicar a cada X minutos em um aplicativo, ou tirar fotos em intervalos regulares e enviá-las ao empregador[66].

Câmeras podem ser instaladas nas entradas e saídas de edifícios, saídas de emergência e vias de circulação. Elas também podem filmar áreas onde mercadorias ou bens valiosos são armazenados. Mas não devem filmar os trabalhadores (o rosto) em seu local de trabalho, exceto em circunstâncias especiais (p.ex., é permitida a filmagem do caixa bancário em atividade, mas não o seu rosto). As câmeras também não devem filmar as áreas de descanso ou banheiros. Se as imagens puderem ser acessadas remotamente, pela Internet ou pelo celular, por exemplo, esse acesso deve ser protegido. Por fim, a gravação de som é reservada a situações específicas, limitadas e justificada pela finalidade (p.ex., uma agressão

nos Considerandos n°s 65 e 66 e no art.17. Sobre o tema, o STF, afirmou ser incompatível com a Constituição Federal a ideia de um direito ao esquecimento. Eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso. RE-1010606-RJ, Plenário, j. 11/02/2021, Rel. Min. Dias Toffoli.

61 P.ex. : arts. 5°, §1°, "c", 9°, §4° e 11,1, §2°,"b" do RGPD. Arts. 8°, II, §9° de la Loi du 6 janvier 1978. Arts. L.1121-1, L.1221-6 a L.1221-9; L.1121-1; L.1222-3 , L.1222-4 e L.2323-47 do Código do Trabalho. Art. 9° do Código Civil. Arts. 226-1 e ss. do Código Penal.

62 Disponível em: https://www.cnil.fr/. Acesso : 13 fev. 2021.

63 Cour de cassation. Chambre sociale, 19 déc. 2018, arrêt n° 17-14.631, Publié au bulletin. Conseil d'État, 10me - 9ème chambres réunies, 15 déc. 2017, 403776, Publié au recueil Lebon.

64 Instância representativa do pessoal. Art. L. 2312-38 do Código do Trabalho.

65 Keyloggers :software que permite registrar todas as teclas digitadas por uma pessoa em um computador.

66 Esses processos, segundo a CNIL, são particularmente invasivos e equivalem a um monitoramento permanente e desproporcional das atividades dos empregado. Disponível em: https://www.cnil.fr/fr/la-videosurveillance-videoprotection-au-travai.l Acesso : 15 fev. 2021.

do trabalhador no local de trabalho)[67].

A CNIL aconselha[68], pois, que antes da implantação de qualquer ferramenta de monitoramento ou controle, seja realizado um teste de adequação e proporcionalidade para determinar se todos os dados são realmente necessários, a fim de garantir que as eventuais violações do direito à privacidade sejam reduzidas ao mínimo necessário à consecução da atividade profissional. Informações claras e específicas devem ser fornecidas aos empregados sobre qualquer monitoramento ou controle realizado no ambiente de trabalho, bem como as finalidades, objetivos e as circunstâncias de tal monitoramento ou controle, uma vez que essas atividades podem afrontar a privacidade dos empregados.

A LGPD, como o RGPD, não proíbe o monitoramento por câmeras de vídeo interno e externo do ambiente da empresa. Da leitura da LGPD pode-se concluir que o tratamento do dados coletados pelo monitoramento deve ser necessário, justificado, proporcional, transparente e adequado aos fins a que se destina. Tal como ocorre no RGPD, o empregado deve ser informado do monitoramento, de preferência por escrito, sobretudo porque o uso de dados coletados por meio de um sistema de vídeo-vigilância ou o uso de dados de um sistema de geolocalização que monitore (de modo sistemático ou pontual) o empregado pode violar sua intimidade e vida privada no ambiente de trabalho. Uma avalição de impacto pode ser realizada. A questão será, certamente, objeto de pronunciamento seja pelo Poder Judiciário, seja pela ANPD.

b- Biometria. Dado pessoal sensível a biometria merece tratamento particular pelo empregador. À luz do RGPD[69], o controle da jornada por meio de registro de ponto eletrônico pelo uso de biometria deverá ser previamente autorizado pelo empregado e seu uso restrito ao fim a que se destina, vedada a utilização para outra finalidade, sem o consentimento expresso do trabalhador. Na França, a CNIL interpretando o RGPD, a legislação[70] e a jurisprudência[71] estabelece os procedimentos a serem adotados para a utilização de dados biométricos impostos pelo empregador (de direito público ou privado) ao seu pessoal (em sentido *lato*: empregados, estagiários, trabalhadores temporários, voluntários, etc.), a fim de controlar o acesso ao local de trabalho. Como todo tratamento de dados sensíveis, o uso da biometria deve ser justificado, proporcional e adequado aos fins a que se destina. O responsável pelo tratamento dos dados deve tomar as medidas adequadas (de segurança e conservação) para fornecer ao empregado todas as informações necessárias sobre os dados coletados. Uma avaliação de impacto sobre a proteção de dados deve ser efetuada pelo responsável do tratamento antes da implementação da biometria. Enfim, o uso

67 Disponível em: https://www.cnil.fr/fr/la-videosurveillance-videoprotection-au-travail . Acesso : 13 fev. 2021.

68 Idem.

69 RGPD: Consid. n°s 51, 53, 91 e arts. 4°, §14; 9°, §1° e §4°.

70 V. arts. 5°, §1°, « c », 9°, §4° e 11, §§1°, 2°, « b » do RGPD. Art. 8°, § 2°e 9° de la loi du 6 janvier 1978 modifiée. Art. L.1121-1 do Código do Trabalho. Règlement type relatif à la mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail. Disponível em: https://www.cnil.fr/sites/default/files/atoms/files/deliberation-2019-001-10-01-2019-reglement-type-controle-dacces-biometrique.pdf. Acesso: 15 fev. 2021.

71 Ver nota de rodapé n° 64.

de dados biométricos só será permitido para controlar o acesso ao local de trabalho[72].

A LGPD[73], no mesmo sentido, afirma que os dados biométricos são dados pessoais sensíveis, e tal como previsto no RGPD, seu uso deve ser enquadrado aos fins a que se destina (p.ex., o controle do ponto eletrônico[74]) e mediante informação/consentimento do trabalhador. Nesse tema, também, recomenda-se uma avaliação de impacto sobre a proteção de dados sensíveis.

c- *BYOD* . Em razão da atual pandemia de Covid-19 e da generalização do teletrabalho, muitos trabalhadores passaram a utilizar o próprio equipamento tecnológico para teletrabalhar (comumente denominado "*BYOD- Bring Your Own Device"*), o que suscita questionamentos acerca do tratamento de dados e da vida privada, à luz do RGPD e LGPD.

A utilização de equipamentos de informática de uso pessoal em contexto profissional apresenta inconvenientes para empregados e empregador. Para empregados, tendo em vista a dificuldade em estabelecer limites claros entre os dados pessoais (vida privada) e dados profissionais. Para o empregador, em razão do risco de divulgação de informações sigilosas que possam transitar nos dispositivos pessoais de seus empregados ou seu possível uso inadequado por terceiros (amigos, familiares, etc.) e, ainda, "a (im) possibilidade de monitorar os dispositivos pessoais do empregado, dada a eventual violação de sua privacidade e intimidade" (FINCATO e FRANK, 2020, p. 69 e 71). Se o empregador é, em princípio, livre para acessar os dados contidos no equipamento profissional confiado ao empregado, porque presume-se de natureza profissional, esse não é o caso quando se tratar de dados constantes do equipamento pessoal do empregado. Ressalte-se que, o empregador é responsável pela segurança dos dados pessoais de sua empresa e os dados de seus empregados, inclusive quando estão armazenados em dispositivos pessoais sobre os quais não possui controle físico ou jurídico, mas que autorizou o uso (por seus empregados). Enfim, o uso de *BYOD* não isenta o empregador de sua obrigação de fornecer a seus empregados os equipamentos e infraestrutura necessários para o desempenho de atividades, pois ferramentas pessoais só devem ser usadas excepcionalmente no contexto profissional.

Ressalte-se que, à luz do RGPD e da LGPD, o uso de equipamento pessoal (*BYOD*) não é uma forma de "tratamento de dados pessoais", mas ele pode gerar dados pessoais. Consequentemente, o recurso ao *BYOD* não altera as obrigações dos responsáveis pelo controle dos dados coletados, tampouco os princípios que regem esse tratamento (principalmente, os da transparência, adequação, minimização, proporcionalidade e finalidade). Evidentemente, deve haver o consentimento expresso do empregado quanto ao tratamento e eventual compartilhamento de seus dados pessoais coletados.

Recorrer ao *BYOD* é, portanto, uma decisão que exige ponderação das vantagens

72 Disponível em: https://www.cnil.fr/fr/lacces-aux-locaux-et-le-controle-des-horaires-sur-le-lieu-de-travail. Acesso 15 fev. 2021. Acesso 15 fev. 2021. Disponível em: Sobre o reconhecimento facial: https://rm.coe.int/lignes-direectrices-sur-la-reconnaissance-faciale/1680a134f4. Acesso: 19 fev. 2021.

73 LGPD: art.5°, II.

74 V. art. 74 da CLT e Portaria n° 1.510 de 21 de agosto de 2009 do Ministério do Trabalho e Emprego.

e desvantagens apresentadas por esse uso que confunde os limites entre a vida pessoal e profissional e põe em risco a segurança de dados pessoais dos trabalhadores, empresa, clientes e terceiros. Recomenda-se, pois, a elaboração de relatório de impacto sobre a proteção de dados pessoais.

d- Saúde. Nos termos dos artigos L. 4121-1 e L. 4122-1 do Código do Trabalho francês, o empregador tem a obrigação de proteger a saúde e a segurança de seus empregados devendo implementar todos os meios necessários para tornar efetivo esse direito. No Brasil, igualmente, o empregador deve tomar as medidas necessárias para a redução de riscos inerentes ao trabalho por meio das normas de saúde, higiene e segurança (art. 7º, XXII), proteção do meio ambiente do trabalho (arts. 200, VIII e 225, *caput*), além das normas de proteção e segurança previstas nos arts. 154 a 201 da CLT e das Normas Regulamentadoras de Segurança e Saúde no Trabalho, sem olvidar as garantias previstas na Constituição Federal, principalmente, a proteção dos direitos fundamentais contidos no arts. 5º e 6° (e.g. direito à vida, segurança, saúde, integridade, repouso, vida privada, etc.) .

A regra geral, segundo o RGPD[75], é a proibição do tratamento de dados relativos à saúde, salvo, por exemplo, se o tratamento for necessário para proteger os interesses vitais do titular dos dados[76], ou por motivos de interesse público[77] no domínio da saúde pública[78], ou se o tratamento for necessário para efeitos de medicina preventiva ou de medicina do trabalho, para a avaliação da capacidade de trabalho do empregado, diagnóstico médico, tratamentos de saúde[79], sempre com fundamento na legislação da UE ou na legislação do Estado-Membro, observada a proporcionalidade e a salvaguarda dos direitos fundamentais do titular dos dados.

Essas regras do RGPD devem ser conciliadas com a obrigação legal acima mencionada, sobretudo em tempos de pandemia da Covid-19. Assim, exceções legais podem ser invocadas pelo empregador para o tratamento de dados pessoais relativos à saúde, no âmbito do combate à Covid-19, garantida a sua utilização apenas para tais fins específicos[80].

Esclareça-se que, no tema, as autoridades francesas[81] parecem posicionar-se no sentido de que os empregadores não devem estabelecer um tratamento sistemático e generalizado dos dados de saúde de seus empregados, além daquele que for solicitado pelas autoridades de saúde pública, a fim de preservar o direito à vida privada e evitar discriminação. A CNIL[82], à luz do RGPD[83], recorda a obrigação do empregador de estar particularmente vigilante quanto à utilização, em princípio proibida, mas autorizada excepcionalmente, dos dados sensíveis como os dados de saúde, em matéria

75 RGPD: art. 9.

76 RGPD: art. 9°, §2°, "c".

77 RGPD: art. 9°, §2°, "g".

78 RGPD: art. 9°, §2°, "i".

79 RGPD: art. 9°, §2°, "h".

80 A corroborar, cite-se o Preâmbulo do RGPD e Considerando n° 46. Derrogações à proibição do artigo 9.º estão previstas nos Considerandos n°s 52 e 54 do RGPD.

81 A CNIL, em particular.

82 Disponível em: https://www.cnil.fr/sites/default/files/atoms/files/referentiel-grh.pdf. Acesso: 15 fev. 2021.

83 RGPD: arts. 9, §2° e 88.

de saúde ocupacional. Isso porque, esses dados só podem ser processados para fins específicos (p.ex. gestão do serviço de saúde ocupacional, acidentes de trabalho, doenças profissionais ou medidas de segurança específicas).

De modo similar, extrai-se da LGPD que o tratamento de dados pessoais sensíveis somente poderá ser realizado para a tutela da saúde, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária e com o consentimento do empregado, salvo hipóteses legais[84]. É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis relativos à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde ou de assistência farmacêutica[85].

Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas, mantidos em ambiente controlado e seguro, conforme as práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas[86]. O acesso aos dados em questão será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.

Aqui, também, a experiência francesa pode ser útil ao jurista brasileiro, pois os princípios de minimização, adequação, proporcionalidade e transparência no tratamento de dados, que informam o RGPD (e também a LGPD) podem ser aplicados durante a execução do contrato de trabalho, a fim de conciliar o direito do empregado de proteger seus dados pessoais (sobretudo os dados sensíveis, caracterizados por seu elevado potencial discriminatório) e o direito do empregador de conservar esses dados, por razões legais ou interesse público.

III/ TRATAMENTO DE DADOS: FASE PÓS CONTRATUAL

A ruptura do contrato de trabalho, por qualquer motivo, requer a observância dos preceitos da LGPD e do RGPD.

O empregado tem, portanto, o direito de solicitar a eliminação de seus dados pessoais quando da rescisão contratual. Todavia, da leitura dos artigos 15 e 16 da LGPD conclui-se que pode ser autorizada a sua conservação, mesmo sem a autorização do empregado, por exemplo, para o cumprimento de obrigação legal ou regulatória pelo controlador/empregador[87]. Nesse caso, o arquivamento da documentação do ex-empregado pode ser admitido, observado o prazo prescricional de 2 anos ou prazo superior para alguns documentos, em razão de fiscalização e auditoria do trabalho[88], como por

84 LGPD: art. 7° e §5°.

85 LGPD: art.11.

86 LGPD: art. 13.

87 P.ex..: "guarda de informações ficais, tributárias, trabalhistas, previdenciárias, observado os respectivos prazos prescricionais. PAMPLONA FILHO, 2020, p. 15.

88 "(...) alguns desses dados devem ser armazenados por prazo indeterminado, pois poderão ser requeridos em eventuais fiscalizações das condições de trabalho pelos Auditores-Fiscais do Trabalho ou no âmbito de reclamações trabalhistas, inclusive a pedido do Ministério Público do Trabalho (...) Os dados que envolvam atas da Comissão Interna de Prevenção de Acidentes (CIPA), o registro de empregados e o livro de Inspeção do Trabalho devem ser armazenados por prazo

exemplo os dados de depósito do FGTS.

No mesmo sentido, o RGPD afirma que o responsável pelo tratamento de dados deve justificar quem a eles pode ter direito e por quais motivos, pois esses mesmos dados podem ser utilizados após a rescisão do contrato de trabalho, de modo desleal ou abusivo. Deverá, igualmente, estar atento às medidas de privacidade e aos procedimentos técnicos adequados de forma a garantir que o tratamento de dados esteja em conformidade com o RGPD. Enfim, com vistas a prevenir contencioso, o responsável pelo tratamento deverá ser capaz de demonstrar que tomou todas as medidas necessárias para proteger a coleta de dados do ex-empregado (inclusive dos clientes ou terceiros com quem ele trabalhou) e evitar, assim, possível responsabilização civil ou administrativa. Recomenda-se, por exemplo, que por ocasião da rescisão contratual conste cláusula de confidencialidade, lealdade e menção especial sobre o sigilo dos dados de clientes e terceiros[89].

Essa interpretação do RGPD *à la française*, parece-nos, poder inspirar o jurista brasileiro quando da elaboração dos documentos relativos à rescisão contratual.

4- Considerações finais

O "mundo digital" modificou nossas interações com a sociedade, família e amigos. A atual pandemia acelerou esse quadro : o *homo numericus* (COMPIÈGNE, 2010) em evolução antes da pandemia consolidou sua presença na *net*. Enaltecido pelas redes sociais, ele descortina sua vida privada no "mundo virtual" como jamais o "mundo físico" conheceu, indicando ao "mundo jurídico" que essa noção evoluiu. Paradoxalmente, ao mesmo tempo em que descortina sua vida privada, o *homo numericus* requer o controle desses dados. *Maître et Seigneur dans son Royaume,* ele aceita fazer concessões de divulgação e acesso a suas informações, aceita a invasão da sua *privacy,* mas a condição que não haja mercantilização dessas informações pessoais (CASILLI, 2015).

Nessa arena do *Big Data,* tanto a LGPD quanto o RGPD tem por finalidade a proteção de direitos e liberdades fundamentais da pessoa humana, principalmente o direito à intimidade e à vida privada. Eles permitem que o *homo numericus* se reaproprie de seus dados pessoais, controle os métodos de compartilhamento e de acesso de suas informações, limitando, assim, o confisco de seus dados pessoais pelas grandes plataformas digitais(CASILLI, 2018). Ambos, exigem das relações empregatícias adaptações: lealdade, transparência e proporcionalidade no tratamento de dados.

A experiência francesa nos convida a refletir sobre os caminhos a seguir, a fim de garantir a efetividade desses direitos, fazer evoluir o direito pátrio alinhando-o às exigências internacionais de proteção e segurança jurídica de dados pessoais.

5- Referências Bibliográficas

AGUIAR, Antônio Carlos. A proteção de dados no contrato de trabalho. *Revista Ltr: legislação do trabalho*. São Paulo, SP, v. 82, n. 6, p. 655-

indeterminado. Por sua vez, dados envolvendo a relação de emprego como acordos de compensação, recibos de férias, de pagamento de salário, dentre outros, devem ser armazenados pelo período de 5 anos, prazo correspondente à prescrição trabalhista." Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2020/09/25/lei-geral-de-protecao-de-dados-lgpd-e-o-direito-trabalho/ Acesso: 12 fev. 2021.

89 RGPD: arts. 12 a 21.

661, jun., 2018.

ALVES, Amauri Cesar; ESTRELA, Catarina Galvão. Consentimento do trabalhador para o tratamento de seus dados pelo empregador: análise da subordinação jurídica, da higidez da manifestação de vontade e da vulnerabilidade do trabalhador no contexto da LGPD. *Síntese*, v. 31, n. 375, p. 25-39, 2020.

BENSOUSSAN, Alain.(2019) *Informatiques et Libertés*. 3ed. Éditions Francis Lefebvre.

BURITI, C.R.. A ineficiência do Direito na prevenção de vazamentos de dados pessoais Disponível em: https://www.jota.info/opiniao-e-analise/artigos/vazamentos-dados-pessoais-05032021. Acesso: 6 mar. 2021.

CALEGARI, Luiz Fernando. A influência da LGPD nas Relações de Trabalho: a necessidade de as empresas se adequarem à nova legislação. *Síntese,* v. 31, n. 375, p. 21-24, 2020.

CAPRIOLI, E. L'enjeu de la protection des données à caractère personnel en matière de publicité ciblée. *Comm. com. Élec.,* n° 6, comm. 60, juin/2009.

COMPIÈGNE, Isabelle. *Chapitre V. Qui est l'homo numericus*? In *La société numérique en question(s).* (dir.) de Compiègne Isabelle. Éditions Sciences Humaines, 2010, p. 59-70.

CASILLI, A. *Quelle protection de la vie privée face aux attaques contre nos libertés numériques?* 2015. Disponivel em : https://www.casilli.fr/2015/02/07/7013. Acesso em :16 fev. 2021.

_____. *Le RGPD, Un premier pas dans la bonne direction*. Libération, 2018. Disponível em : http://www.casilli.fr/tag/donnees-personnelles/ Acesso em: 16 fev. 2021.

DESBARATS, Isabelle. Les objets connectés au travail : quelles régulations pour quels enjeux? *Dr. Soc*. 2021, 139.

DERBLI, Ludimila Santos. O transplante jurídico do Regulamento Geral de Proteção de Dados da União Europeia ("GDPR") para o Direito brasileiro. *Revista Eletrônica do Programa de Pós-graduação da Câmara dos Deputados,* Brasília, v. 12, n. 30, p. 181-193, set./dez. 2019.

DERIEUX, Emmanuel. Réseaux sociaux et responsabilité des atteintes aux droits de la personnalité. *RLDI*/100, n° 3334, p. 77-89, jan., 2014.

_____ ; GRANCHET, Agnès. (2010) *Vie privée et droit à l'image*. 6e éd. Droit des médias. Droit français, européen et international. LGDJ, Lextenso.

DUBOIS, L. GAULLIER, F. Publicité ciblée en ligne, protection des données à caractère personnel et ePrivacy: un ménage à trois délicats. *Légicom* 2017, 69.

FINCATO, Denise; FRANK, Marina Silveira. *Bring Your Own Device (BYOD*) e suas implicações na relação de emprego: reflexões práticas. *Revista eletrônica [do] Tribunal Regional do Trabalho da 9ª Região,* Curitiba, PR, v. 9, n. 89, p. 66-82, jun., 2020.

FINKELSTEIN, Maria Eugenia; FINKELSTEIN,

Claudio. Privacidade e Lei Geral de Proteção de Dados Pessoais. *Revista de Direito Brasileiro*, Florianópolis, v. 9, n. 23, p. 284-301, maio/ago. 2019.

GOULART, Guilherme Damasio. Limites do *BYOD*: entre o poder do empregador e a proteção dos direitos da personalidade do empregado. *Revista de Direito do Trabalho*, São Paulo, SP, v. 40, n. 159, p. 71-86, set./out., 2014.

GOUTTENOIRE, Abel. *Le régime du contrôle du télétravailleur par la donnée. À propos des questions/réponses de la CNIL sur le télétravail du 12 novembre 2020*. *RDT* 2021, 88.

GUNTHER, Luiz Eduardo; COMAR, Rodrigo Thomazinho; RODRIGUES, Luciano Ehlke. A proteção e o tratamento dos dados pessoais sensíveis na era digital e o direito à privacidade : os limites da intervenção do Estado. *Rev. Relações Internacionais no mundo atual,* Curitiba, v. 2, n. 27, p. 1-17, 2020.

LE MOINE, L., Intimité et vie privée du travailleur connecté : ' BYOD', capteurs, sécurité des données dans l'entreprise numérique. *La lettre innovation et prospective de la CNIL*, n 7, juin, 2014.

PAMPLONA FILHO, Rodolfo; CONI JUNIOR, Vicente Vasconcelos. A Lei Geral de Proteção de Dados Pessoais e seus impactos no Direito do Trabalho. *Direito Unifacs: debate virtual*, Salvador, n. 239, p. 1-42, maio, 2020.

PELLEGRINI, François. Sécurité et hygiène numérique des professionnels. *Dalloz IP/IT*, 2019, 233.

PINHEIRO, Iuri; BOMFIM, Vólia. A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho. 01/10/2020. Disponível em: http://trabalhoemdebate.com.br/artigo/detalhe/a-lei-geral-de-protecao-de-dados-e-seus-impactos-nas-relacoes-de-trabalho. Acesso em : 10 fev. 2021

RAMOS, Lara Castro Padilha; GOMES, Ana Virgínia Moreira. Lei geral de proteção de dados pessoais e seus reflexos nas relações de trabalho. *Scientia Iuris*, Londrina, v.23, n.2, p. 127-146, jul., 2019.

REIS, Beatriz de Felippe. A cultura de *compliance* em matéria de proteção de dados e sua adoção no âmbito laboral = *The culture of compliance in relation to data protection and its adoption in the context of labor*. *Revista de direito do trabalho e seguridade social,* São Paulo, SP, v. 46, n. 214, p. 323-340, nov./dez., 2020

RUARO, Regina Linden. Algumas reflexões em torno do RGPD, em especial quanto ao consentimento, com alusões à LGPD (um exercício interpretativo). *In Direitos Fundamentais e Justiça*. Belo Horizonte: Fórum, ano 14, n. 42, p. 219-249, jan./jun. 2020.

_____; GLITZ, Gabriela Pandolfo Coelho. Panorama geral da Lei Geral de Proteção de Dados Pessoais no Brasil e a inspiração no Regulamento Geral de Proteção de Dados Pessoais Europeu. *Revista de Estudos e Pesquisas*, Brasília, v. 6, n. 2, p. 340-356, jul./dez., 2019.

SOUSA, Duarte Abrunhosa e; GONÇALVES, Rui Coimbra. Da necessidade de conservação de

dados pessoais dos trabalhadores no período pós-contratual = *The need to retain workers' personal data in the post-contractual period. Revista de direito do trabalho e seguridade social*. São Paulo, SP, v. 46, n. 212, p. 119-145, jul./ago., 2020.

TEYSSIÉ, B. (dir.).(2013) *La communication numérique, un droit, des droits*. Éditions Panthéon-Assas.

A LEI GERAL DE PROTEÇÃO DE DADOS: NOÇÕES GERAIS

Luiz Carlos Buchain

RESUMO

A LGPD tem por objetivo proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A "sociedade de informações" extrai dos cidadãos uma gama crescente de dados pessoais que são oferecidos "gratuitamente" aos fornecedores de bens e serviços. Os dados pessoais são direitos de personalidade que decorrem do princípio geral da dignidade da pessoa humana.

Daí decorre que o controle e disponibilização dos dados pessoais na *web* tornou-se um grande desafio para a sociedade a medida em que, através da *internet*, é possível detectar as preferências do usuário. O que se leva em conta é a possibilidade de grupos empresariais e do próprio governo conquistarem poder econômico e politico sobre o indivíduo a partir da disponibilidade de suas informações. Aqui está em jogo a limitação e a legitimação do controle de dados pessoais e a tutela das liberdades individuais e a eficiência administrativa e empresarial.

Assim, são dois conceitos contraditórios em questão: o respeito aos direitos fundamentais dos indivíduos e o exercício da livre empresa. Ao mesmo tempo em que estimula o mercado de dados, a lei o regula de forma a garantir aos indivíduos o controle sobre seus dados.

O quadro jurídico para proteção de dados pessoais, através da legislação específica, tem sua eficácia, em larga medida, dependente da eficiência da Autoridade Nacional de Proteção de Dados (ANPO) e do Conselho Nacional de Proteção de Dados pessoais e privacidade.

PALAVRAS-CHAVE

Dados. Proteção de dados. Controlador. Operador. Titular. Informação.

Luiz Carlos Buchain

Possui graduação em Ciências Jurídicas e Sociais pela Pontifícia Universidade Católica do Rio Grande do Sul (1986), mestrado em DIREITO CIVIL pela Universidade Federal do Rio Grande do Sul (1996) e doutorado em DIREITO ECONÔMICO pela Universidade Federal do Rio Grande do Sul (2005). Atualmente é professor adjunto II da Universidade Federal do Rio Grande do Sul e advogado - Buchain Sociedade Individual de Advocacia.

INTRODUÇÃO

A LGPD tem por objetivo proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A proteção de dados pessoais[1] não se reduz somente a proteção da vida privada, com a qual está intimamente ligada mas, também, com a liberdade e o livre desenvolvimento da personalidade da pessoa natural. A Constituição de 1988, ao reconhecer o princípio da dignidade humana[2] (art. 1º, III) protegeu todos os direitos de personalidade, além de positivar garantias como o direito à liberdade de expressão (art. 5º, IX), o direito à informação (art. 5º, XV), a inviolabilidade da vida privada,[3] a intimidade (art. 5º, X), a garantia de Habeas Data (art. 5º, LXXII), a proibição de invasão de domicílio (art. 5º, XI) e a violação de correspondência (art. 5º, XII).

A atual "sociedade de informações" em que vivemos, intimamente ligada à utilização das Tecnologias de Informação e Comunicações – TIC – conhecidas como o acesso à *internet*, telefones móveis, televisão interativa, entre outros, extraem dos cidadãos/usuários uma gama crescente de dados pessoais que são

1 Danilo Doneda ensina que nem todo dado é considerado pessoal. Sua caracterização como pessoal exige a característica fundamental de ter um vínculo com a pessoa e revelar um aspectos objetivos de seu titular: "Este vínculo significa que a informação se refere às características ou ações desta pessoa, que podem ser atribuídas a ela em conformidade com a lei, como no caso do nome civil ou do domicílio, ou então que são informações provenientes de seus atos, como os dados referentes ao seu consumo, informações referentes às suas manifestações, como sobre opiniões que manifesta e tantas outras". DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico. Joaçaba, v. 12.n.2, jul./dez. 2011, p.93.

2 É, portanto, em virtude da existência de uma cláusula geral e aberta de proteção e promoção da personalidade, que, no caso brasileiro, tem sido fundada especialmente no princípio da dignidade da pessoa humana, que se adota o entendimento de que o rol de direitos especiais de personalidade (sejam eles previstos na legislação infraconstitucional, sejam eles objeto de reconhecimento expresso na Constituição Federal, não é de cunho taxativo. SARLET, Ingo Wolfgang. Curso de Direito Constitucional, 3ª ed, p. 400. Ed. RT. SP-SP, 2013.

3 Inicialmente, nos EUA, o direito a privacidade se relacionava com a propriedade privada. Num segundo momento, a partir do artigo The Right to Privacy publicado por Samuel D. Warren e Louis D. Brandeis (1890), a privacidade passou a ser relacionada a proteção à inviolabilidade da personalidade. Assim, "o princípio que protege escritos pessoais e outras produções pessoais, não é contra o furto ou a apropriação física, mas contra toda forma de publicação, é na realidade não o princípio da propriedade privada, mas o da inviolabilidade da personalidade". Shapiro, 1996 apud DONEDA, Danilo. Da privacidade à Proteção dos dados Pessoais. Rio de Janeiro. Renovar. 2006.

oferecidos "gratuitamente" aos fornecedores de bens e serviços. Os dados pessoais são direitos de personalidade que decorrem do princípio geral da dignidade da pessoa humana[4]. Ademais, os dados podem ser utilizados para fins contrários ao Direito e a moral, como forma de perseguição política ou opressão econômica. Além disso, os dados coletados podem ser incorretos e representar erroneamente uma pessoa.

A TIC permite que uma infinidade de informações e dados dos cidadãos sejam extraídos da *web* justamente porque o funcionamento da rede é caracterizado por uma ampla liberdade de expressão e inclusão de dados pessoais, de forma que até mesmo os hábitos e preferências do usuário da *web* podem ser colecionados pelos fornecedores de bens e serviços. Trata-se do *superinformacionismo*[5], caracterizado pela imensa quantidade de informações que circulam na internet, permitindo facilmente a obtenção de rápidas informações sobre qualquer assunto ou pessoa.

Daí por que o controle e disponibilização dos dados pessoais na *web* tornou-se um grande desafio para a sociedade a medida em que, através da *internet*, é possível detectar as preferências do usuário, sejam artísticas, musicais, hábitos de vida, viagens, orientação sexual, crenças religiosas, etc. O que se leva em conta é a possibilidade de grupos empresariais e do próprio governo conquistarem poder econômico e politico sobre o indivíduo a partir da disponibilidade de suas informações. O grande desafio em questão é a limitação e a legitimação[6] do controle de dados pessoais[7] como forma de equilibrar as relações entre a tutela das liberdades individuais e a eficiência administrativa e empresarial.

Embora a proteção aos direitos e garantias fundamentais previstos na CF/88 tenham aplicação imediata (art. 5º, §1º da CF), e que tais direitos e garantias possam ter sua raiz identificada no princípio da dignidade da pessoa humana - verdadeira cláusula geral constitucional de tutela e promoção da pessoa humana - o fato é que a autoaplicabilidade das regras constitucionais não se mostram suficientes para garantir o efetivo direito dos cidadãos à proteção de seus dados. Essa estreita relação entre dignidade, privacidade e liberdade exige do poder público uma robusta tutela das informações relativas as pessoas tanto para afastar terceiros da esfera privada quanto para garantir os direitos fundamentais do cidadão.

4 "A tutela da personalidade – convém, então, insistir – não pode se conter em setores estanques, de um lado os direitos humanos e de outro as chamadas situações jurídicas de direito privado. A pessoa, à luz do sistema constitucional, requer proteção integrada, que supere a dicotomia direito público e direito privado e atenda à cláusula geral fixada pelo texto maior, de promoção da dignidade humana". A tutela da personalidade no ordenamento civil – constitucional brasileiro. TEPEDINO, Gustavo. https://www.academia.edu/31740015/A_tutela_da_personalidade_no_ordenamento_civil-constitucional_brasileiro Acesso em 06 de junho de 2019

5 Diz-se que a informação passou a ser insumo da produção, possuindo um papel tão importante quanto a força de trabalho e o capital.

6 A legitimação à obtenção da informação está intimamente ligada com o princípio do CONSENTIMENTO na utilização de dados pessoais. Art. 7º, I e art. 8º, § 5º da LGPD.

7 A necessidade de se proteger juridicamente os dados pessoais do cidadão se origina do fato de que dados possuem um grande valor econômico, possibilitando sua comercialização. As novas técnicas de informática conferem à intimidade um novo conteúdo. Os dados traduzem dados de personalidade e revelam comportamentos e preferências do cidadão, o que permite traçar um perfil psicológico e comportamental do indivíduo.

De outra forma, tanto o direito comum[8] quanto o direito civil, o CDC[9] ou mesmo o Marco Civil da Internet (lei 12.965/14), se revelaram insuficientes para abranger todas as hipóteses em que os dados merecem tratamento, especialmente porque a legislação citada não abarca toda a esfera de proteção necessária da vida privada: não conferem a pessoa natural a possibilidade de se opor a coleta de dados, de ter acesso aos dados e nem mesmo ser informado sobre a natureza e finalidade do tratamento de seus dados.

Empresas utilizam-se desses dados para produzir a chamada *publicidade comportamental* e desenvolver novas maneiras de rastrear os consumidores. Ao obter essas informações essenciais[10] para sua publicidade seletiva (realizada a partir dos dados coletados, em especial na *internet* e seu histórico de navegação) estas tornam-se a uma importante fonte de renda de diversas empresas.

Entretanto, é importante notar que o próprio legislador promoveu o diálogo entre a Lei Geral de Proteção de Dados Pessoais e o CDC, ao expressamente prever como fundamento da proteção de dados a defesa do consumidor (art. 2º, VI); ao estabelecer a possibilidade de que os direitos dos titulares de dados, quando também consumidores, possam ser igualmente exercidos perante organismos de defesa do consumidor (art. 18, § 8º); e ao determinar (art. 45) que as hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente. Por fim, a complementariedade das leis é consolidada (art. 64), o qual estabelece que os direitos e princípios expressos na LGPD não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que o Brasil seja parte[11].

Por essas razões, mostrou-se necessário criar um quadro legal específico para a proteção de dados pessoais visando conferir ao cidadão instrumentos legais que lhe permitam proteger-

8 Em legislação esparsa encontra-se diversos dispositivos regulando a proteção de dados. Entre outras, cita-se: CCB, CDC (art. 43), Lei de Interceptação Telefônica/ Telemática (L. 9.96/96), Lei Geral de Telecomunicações (L.9.472/97), lei de Habeas Data (L. 9.507/97), Lei do Sigilo das Operações de Instituições Financeiras (LC 105/01), Lei do Cadastro Positivo (L. 12.414/11), Lei de Acesso as Informações (L. 12.527/11), Lei de Invasão de Dispositivos Informáticos - lei Carolina Dieckman (L. 12.737/12), Marco Civil da Internet (L. 12.965/14) e na Política de Dados Abertos do Governo Federal (D. 8.777/16), Lei do cadastro positivo (Lei n. 12.414/2011, o sigilo dos agentes do fisco (art. 198 do CTN) e LC 105/01, que permite às autoridades administrativas a quebra do sigilo bancário até mesmo sem autorização judicial. Art. 6º da LC 105/2001.

9 Acerca da regulação da matéria pelo CDC, Claudia Lima Marques já afirmava a existência do direito a autoregulação de dados do consumidor: "Um direito de dispor de seus próprios dados pessoais foi positivado pelo CDC e transparece no art. 43, §§ 2º e 3º. O consumidor brasileiro tem direito de dispor de seus dados pessoais, de acessá-los e de saber que estes existem em algum banco de dados público ou privado...". Lima Marques, Claudia. Contratos no código de defesa do consumidor. 5ª ed. Ed. RT. SP-SP, 2006. p.829.

10 Há empresas dedicadas até mesmo a rastrear os passos dos consumidores em locais públicos, a partir de sinais de wi-fi de smartphones, fornecendo subsídios aos empresários para traçar o perfil dos consumidores visando oferecer-lhes produtos e serviços. Trata-se do FX Flow Intelligence. Conforme https://portalnovarejo.com.br/2015/09/7-tecnologias-para-monitorar-habitos-de-consumo/ acesso em 07/05/2019.

11 Conforme ensina Cláudia Lima Marques, deve-se aplicar a teoria do diálogo das fontes para aplicação simultânea de toda a legislação sobre o assunto. O diálogo das fontes é definido como sendo "a aplicação simultânea, coerente e coordenada das plúrimas fontes legislativas, leis especiais (como o Código de Defesa do Consumidor, a lei de seguro-saúde) e gerais (como o CC/2002 (LG/2002/400)), com campos de aplicação convergentes, mas não mais iguais". MARQUES, Claudia Lima; et al., Manual de Direito do Consumidor. São Paulo: Ed. RT, 2008, p. 85-88.

se contra o abuso da exploração dos dados pessoais[12].

A generalização do uso da informática e da coleta de dados pessoais criou um novo e crescente mercado para sua troca entre agentes econômicos e, ao mesmo tempo, criou novos riscos tanto para a vida privada[13] quanto, de uma maneira mais genérica, aos direitos e liberdades individuais. Além disso, esse novo modelo econômico de economia digital, cujos exemplos globais são o *Goggle* (buscas na internet) e o *Facebook*[14] (redes sociais), está fortemente apoiado na exploração do comércio de dados, exigindo da sociedade a criação de um instrumento legislativo para regular esse verdadeiro mercado digital.

O direito de acesso e conhecimento dos dados pessoais abarca diversas posições jurídicas, conforme ensina Ingo Sarlet[15], expostas como sendo "a) o direito de acesso e conhecimento dos dados pessoais existentes em registros (bancos de dados); b) direito ao não conhecimento, tratamento, utilização e difusão de determinados dados pessoais pelos Estado ou por terceiros, aqui incluído o direito de sigilo quanto aos dados pessoais; c) direito ao conhecimento da identidade dos responsáveis pela coleta, armazenamento, tratamento e utilização dos dados; d) o direito ao conhecimento da finalidade da coleta e eventual utilização dos dados; e) direito a ratificação e, a depender do caso, de exclusão de dados pessoais armazenados em banco de dados".

Assim, são dois conceitos contraditórios[16] em questão – o respeito aos direitos fundamentais dos indivíduos em face da liberdade de circulação de dados e exercício da livre empresa[17] no mercado – que a nova legislação visa conciliar. Ao mesmo tempo em que estimula o mercado de dados (em especial o digital), o regula de forma a garantir aos indivíduo o controle sobre seus dados.[18] A

12 A LGPD, conforme disposto em seu artigo 18, garante aos indivíduos o direito de autodeterminação, ou seja, o direito a decidir por si próprio quando e dentro de quais limites seus dados pessoais poderão ser utilizados.

13 "Em causa, portanto, está o controle por parte do indivíduo sobre as informações que em princípio apenas lhe dizem respeito, por se tratar de informações a respeito de sua vida pessoal, de modo que se poderá mesmo dizer que se trata de um direito individual ao anonimato." SARLET, Ingo Wolfgang. Curso de Direito Constitucional, 3ª ed, p. 409. Ed. RT. SP-SP, 2013

14 O Facebook chegou a 127 milhões de usuários no Brasil. Conforme http://agenciabrasil.ebc.com.br/economia/noticia/2018-07/facebook-chega-127-milhoes-de-usuarios-no-brasil Acesso em 07/05/2019

15 SARLET, Ingo W; MARINONI, Luiz Guilherme: MITIDIERO, Daniel. Curso de Direito Constitucional. São Paulo, Revista dos Tribunais, 2014, p. 433/434.

16 Exemplifica o conflito entre os direitos fundamentais e a livre circulação de dados a decisão proferida em sede de apelação em ação coletiva proposta pelo Ministério Público, (AC 70069420503), Rel. Des. Ney Weidmann Neto, disponível em: www.tjrs.jus.br. Acesso em 07/05/2019, que não há abusividade na coleta de dados por empresas destinadas a formação de banco de dados dos consumidores, destinados a prospecção de cliente, ações de marketing e telemarketing. O fundamento empregado à decisão foi o de que os dados coletados e comercializados, apesar de serem privativos, "são comumente fornecidos por qualquer cidadão na prática dos atos da vida civil, não se tratando de informações de natureza totalmente sigilosa ou confidencial. Não há, no caso, qualquer ofensa à privacidade ou a qualquer outro direito fundamental dos consumidores." Aqui o TJRS não abordou a questão da autodeterminação informativa, sendo o julgamento anterior a vigência da LGPD.

17 "Por outro lado, como os direitos fundamentais irradiam efeitos imediatos, ou horizontais, para as relações interpessoais entre entes privado, pode haver conflito ou colisão com outros direitos fundamentais, como o direito à propriedade, à liberdade de contratar ou à liberdade de exercício de trabalho ou profissão." CUEVA, Ricardo Villas Bôas. A insuficiente proteção de dados pessoais no Brasil. Revista de Direito Civil Contemporâneo. Vol. 13/2017, p. 59-67. Out-Dez 2017

18 Aqui vale lembrar que a LGPD adota o princípio da finalidade (também chamado de princípio da autodeterminação informativa), ou seja, os dados pessoais coletados são ou devem ser destinados a um fim específico onde haja correlação necessária entre o uso dos dados pessoais e a finalidade comunicada aos interessados quando da coleta dos dados. Trata-se, pois,

autodeterminação veda sua utilização para fins outros que não aquele para os quais o titular ofereceu seu expresso consentimento.

O quadro jurídico para proteção de dados pessoais[19], através da legislação específica, tem sua eficácia, em larga medida, dependente da eficiência da Autoridade Nacional de Proteção de Dados (ANPO) e do Conselho Nacional de Proteção de Dados pessoais e privacidade.

1. CAMPO DE APLICAÇÃO MATERIAL

O objeto de proteção conferida pela lei 13.709/18 está circunscrito num campo de aplicação material e territorial.

A proteção de dados se aplica a todo o universo de operações de tratamento de dados pessoais, com as exceções previstas no art. 4º da LGPD. Dentre as exceções previstas na lei temos: *(i)* o uso não econômico de dados por pessoa física, *(ii)* dados realizados para fins jornalísticos, artísticos ou acadêmicos e *(iii)* dados utilizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão a infrações penais. Há ainda a hipótese de exceção prevista no inciso IV do art. 4º da LGPD, segundo o qual não se aplica a lei aos dados "provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.".

1.1. OPERAÇÕES SUBMETIDAS AO REGIME LEGAL

A nova lei se aplica, de um lado, ao tratamento automatizado de dados pessoais e, de outro, a tratamentos não automatizados, ou seja, aqueles ainda realizados através de fichários ou meios similares. Inicialmente deve-se definir algumas noções:

1.1.1. A NOÇÃO DE "DADOS PESSOAIS"

A lei define "dado pessoal" como informação relacionada a pessoa natural identifica ou identificável"(art. 5º, I)[20] e, de outro lado, como "dado pessoal sensível" aquele sobre origem racial ou étnica, convicção religiosa, opinião política, filiação sindicato ou organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dados genético ou biométrico, quando vinculado a uma pessoa natural (art. 5º, II).

Sob outro aspecto, a lei considera não identificável, ou "anonimizado", os

de um desdobramento do direito à privacidade.

19 Exemplo de normas de primeira geração são as leis do Estado Alemão Hesse (1970), a lei de dados da Suécia (1973), o Estatuto de Proteção de Dados do Estado alemão de Rheiland-Pfalz (1974) e a lei federal de Proteção de Dados da Alemanha (1977). Nos EUA foram aprovados, nesse mesmo período, o Fair Credit Reporting Act (1970), o Freedom for Information Act (1966) e o Privacy Act (1974). Em 1976, Portugal foi o primeiro país a estabelecer em sua constituição o direito fundamental à autodeterminação informativa (art. 35).

20 Segundo a teoria do mosaico, é irrelevante o fato de a informação do indivíduo pertencer à esfera da intimidade e vida privada, pois o que interessa é sua utilização. Assim, há dados que possuem aparência de inofensivos à violação, porém, quando colocados com outros dados, apresentam risco de violação da privacidade do cidadão. Nesse sentido BARROS, Bruno M. Correa de, OLIVEIRA, Clarissa T. Lovatto, SANTOS, Rafael de. O direito à privacidade: uma reflexão acerca do anteprojeto de proteção de dados pessoais. Revista Videre, Dourados, MS, v.9, n.17.1. semestre de 2017. p. 21.

dados relativos a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (art. 5º, III). Assim, dados identificadores, tais como um endereço IP, é suscetível de identificar, ao menos indiretamente, uma pessoa física. O endereço IP é exemplo de dado pessoal porquanto existem meios técnicos e legais que permitem ao provedor de internet obter os dados cadastrais de um determinado usuário, através de seu endereço IP.

1.1.2. A NOÇÃO DE "TRATAMENTO"

A noção de "tratamento" é definida pela lei (art. 5º, X) como "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, transferência, difusão ou extração."

Além da clara extensão da lista de operações qualificadas como "tratamento" , é preciso notar que a redação adotada pelo legislador (empregando a expressão "como as que se referem ...") confere a esta lista uma natureza ilustrativa e não limitativa, atribuindo a essa definição um caráter extremamente largo. Na realidade, nenhuma operação escapa do conceito de "tratamento" tendo ela por objeto dados pessoais. Apenas nas hipóteses em que a operação em tratamento se valha de outros dados, tais como dados anonimizados, por exemplo, será possível excluir a incidência da Lei Geral de Proteção de Dados.

Assim, está posto pela lei que toda e qualquer operação, não importando sua natureza, mas que colha dados pessoais, constitui um bem sob "tratamento"[21].

Além disso, estão excluídos do regime de proteção de dados pessoais: a) tratamento de dados realizado por pessoa natural para fins exclusivamente particulares e não econômicos ou, b) realizados para fins exclusivamente jornalísticos, artísticos e acadêmicos. Já as atividades de segurança pública, defesa nacional, segurança do Estado

ou investigação e repressão de infrações penais serão ser regidos por legislação específica que deverá observar o princípio da necessidade e proporcionalidade no trato dos dados, além do devido processo legal e a proteção e os direitos do titular previstos na lei 13.709/18.

1.1.3. A NOÇÃO DE "ARQUIVO"

A nova lei se aplica ao "tratamento de dados pessoais, inclusive nos meios digitais..."(art. 1º), o que abrange tanto o tratamento de dados automatizados (digitais) quanto aqueles consubstanciados em arquivos não automatizados. Nota-se que a preocupação do legislador foi a de estender a proteção de dados a todos os meios possíveis, independentemente da tecnologia utilizada para o tratamento.

A definição de "arquivo" pode ser dada como sendo todo o conjunto de dados

21 Quanto a tutela do sigilo de dados previsto na CF/88 e seu âmbito de aplicação, devemos lembrar a decisão do STF que, ao julgar o HC 83.168-1, rel. Min. Sepúlveda Pertence, reafirmou seu entendimento de que o inciso XII do art. 5º da Constituição protege a comunicação de dados, e não os dados em si mesmos. Esta interpretação tem sido criticada por dificultar o reconhecimento do direito fundamental à proteção de dados pessoais.

organizados, ainda que esta organização seja temporária ou desprovida de estabilidade no tempo e independentemente da tecnologia empregada no tratamento.

1.2. AS PESSOAS SUBMETIDAS AO REGIME LEGAL

O objetivo da lei é "proteger os direitos fundamentais de liberdade, privacidade e do livre desenvolvimento da personalidade da pessoa natural"[22] cujos dados são objeto de tratamento, impondo obrigações a todas as pessoas intervenientes nesse tratamento: controlador e operador (agentes de tratamento) e encarregado.

1.2.1 O "TITULAR"

Segundo a LGPD, o "titular" é a pessoa natural[23] a quem se referem os dados pessoais que são objeto de tratamento", ou seja, a pessoa física identificada ou identificável. (art. 5º, V).

O titular dispõe do direito básico à proteção de dados pessoais em dupla dimensão: a) tutela da personalidade contra os riscos que ameacem sua personalidade em face da coleta, processamento, utilização e circulação dos dados pessoais, e, b) a atribuição ao titular do direito a garantia do poder de controlar o fluxo de seus dados na sociedade. Esse conceito envolve tanto um aspecto subjetivo (controle dos dados pelo titular) quando um aspecto objetivo (proteção contra os riscos causados pelo tratamento dos dados pessoais).

Somente as pessoas físicas são objeto da proteção legal. Além disso, para reconhecer-se a legitimidade de uma pessoa física a proteção da LGPD será necessário determinar se os dados tratados permitem sua identificação, direta ou indireta, sem o que o fato não estará submetido ao regime da lei.

Importante questão não tratada pela LGPD é aquela que diz respeito a cessação dos direitos do "titular" pela sua morte, nada especificando se poderiam ou não serem transferidos aos seus herdeiros. É regra aceita no direito nacional a de que os herdeiros do falecido, através de seu espólio, são parte legítima para defender diversos direitos. Assim, aos herdeiros da vítima dos danos decorrentes da "proteção de dados" deverá ser garantida a via legal para obter as reparações devidas.

Nesse sentido há o julgamento da T3 - TERCEIRA TURMA do STJ[24] que versa sobre

22 Inicialmente, o direito a privacidade era compreendido como um fenômeno coletivo, pois os danos causados pelo processamento impróprio dos dados são difusos. Posteriormente, a privacidade, até então compreendida como o "direito a ser deixado em paz" (*right to be alone*), passa a significar o direito de controle dos dados pessoais pelo indivíduo, o qual decide quando e onde seus dados podem circular. (Princípio da autodeterminação). Por fim, a privacidade e a proteção dos dados passa a se vincular a ideia de igualdade, em razão do crescente risco de seu uso com fins discriminatórios pelo Estado ou pelo mercado.

23 "Passou-se a compreender a proteção a autodeterminação informativa como fenômeno não apenas privado, mas, também, coletivo, já que em certas circunstâncias, os danos decorrentes da violação desse direito podem ser caracterizados como difusos, a exigir mecanismos jurídicos de tutela coletiva". CUEVA, Ricardo Villas Bôas. A insuficiente proteção de dados pessoais no Brasil. Revista de Direito Civil Contemporâneo. Vol. 13/2017, p. 59-67. Out-Dez 2017.

24 REsp 1209474 / SP
Data do Julgamento 10/09/2013
DJe 23/09/2013
RJP vol. 54 p. 155
RSTJ vol. 232 p. 216
Ementa - RECURSO ESPECIAL. RESPONSABILIDADE CIVIL. DANO MORAL. CONTRATO DE CARTÃO DE CRÉDITO CELEBRADO APÓS A MORTE DO USUÁRIO. INSCRIÇÃO INDEVIDA NOS ÓRGÃOS DE PROTEÇÃO AO CRÉDITO. EFICÁCIA POST MORTEM DOS DIREITOS DA PERSONALIDADE. LEGITIMIDADE ATIVA DA VIÚVA PARA

o direito a indenização da viúva e do espólio por força da inserção de nome de falecido no cadastro de inadimplentes por suposta contratação de cartão de crédito após a morte do usuário. No caso, o aresto atribui legitimidade ativa à viúva para o pedido declaratório de "inexistência de contrato de cartão de crédito" e o respectivo "pedido de indenização" pelos prejuízos decorrentes da ofensa à imagem do falecido marido (aplicação do art. 12, parágrafo único, do Código Civil). Entretanto, o tribunal negou a legitimidade ativa do espólio para o pedido indenizatório, pois o contrato fora celebrado posteriormente a su morte, momento em que a personalidade do *de cujus* já não existia. *Mutatis mutandis*, os herdeiros de pessoa falecida podem ser considerados parte legítima para requerem, por exemplo, a retirada do consentimento dada pelo falecido[25] ao tratamento de seus dados pessoais.

.....

POSTULAR A REPARAÇÃO DOS PREJUÍZOS CAUSADOS À IMAGEM DO FALECIDO. INTELIGÊNCIA DO ARTIGO 12, PARÁGRAFO ÚNICO, DO CÓDIGO CIVIL.

1. Contratação de cartão de crédito após a morte do usuário, ensejando a inscrição do seu nome nos cadastros de devedores inadimplentes.
2. Propositura de ação declaratória de inexistência de contrato de cartão de crédito, cumulada com pedido de indenização por danos morais, pelo espólio e pela viúva.
3. Legitimidade ativa da viúva tanto para o pedido declaratório como para o pedido de indenização pelos prejuízos decorrentes da ofensa à imagem do falecido marido, conforme previsto no art. 12, parágrafo único, do Código Civil.
4. Ausência de legitimidade ativa do espólio para o pedido indenizatório, pois a personalidade do "de cujus" se encerrara com seu óbito, tendo sido o contrato celebrado posteriormente.
5. Doutrina e jurisprudência acerca do tema.
6. Restabelecimento dos comandos da sentença acerca da indenização por dano moral.
7. RECURSO ESPECIAL PARCIALMENTE PROVIDO.

25 Segundo a RGPD em sua consideranda 27: "O presente regulamento não se aplica aos dados pessoais de pessoas falecidas. Os Estados-Membros poderão estabelecer regras para o tratamento dos dados pessoais de pessoas falecidas".

Outra decisão paradigmática da Segunda Seção do STJ (RECURSO ESPECIAL nº 1.304.736 - RS (2012/0031839-3), rel. Min. Luiz Felipe Salomão – regime de recursos repetitivos) diz respeito a dados pessoais tratados por empresas que praticam o sistema de *scoring* (histórico de crédito) - o STJ definiu que não se faz necessária a autorização do consumidor para a tomada de seus dados por empresas que fornecem o serviço de *scoring*[26] de pontuação para fins creditícios. Ao mesmo tempo, a decisão confere aos titulares da informação interesse de agir, para a exibição de documentos, sempre que o titular pretender conhecer e fiscalizar documentos próprios ou comuns de seu interesse e em posse do controlador. O STJ considerou legítimo o sistema de *scoring* pela aplicação do art. 5º, IV, e pelo art. 7º, I, da Lei n. 12.414/2011 (lei do cadastro positivo). Note-se que o disposto no art. 7, X da LGPD expressamente autoriza o tratamento de dados pessoais para a "proteção do crédito", remetendo a matéria para o disposto na legislação pertinente.

Nesse sentido se manifesta Claudia Lima Marques[27] ao afirmar que "a elaboração, organização, consulta e manutenção de banco de dados sobre consumidores e sobre consumo não são proibidas pelo CDC – ao contrário, são reguladas por este, logo, permitidas".

.....

26 A matéria é objeto da súmula 550 editada pela Segunda Seção do STJ. Julgamento em 14/10/2015, DJe 19/10/2015, RSTJ vol. 243 p. 1093.
Enunciado - A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo.

27 Lima Marques, Claudia. Contratos no código de defesa do consumidor. 5ª ed. Ed. RT. SP-SP, 2006. p.822.

1.2.2 O "CONTROLADOR" e SUA DEFINIÇÃO

A definição de "controlador" é fixada na LGPD como sendo a pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados. Trata-se daquele que determina as finalidades e os meios de tratamento. O "controlador" corresponde a pessoa que toma a iniciativa e controla os meios técnicos ou humanos necessários a implementação do tratamento.

A noção de "controlador" é central no tema *proteção de dados*. É sobre ele que recai a maior parte das obrigações legais como, por exemplo, o de fornecer ao titular todos os seus dados por ele tratados[28] (art. 18), bem como a de reparar danos patrimoniais ou morais, pessoais ou coletivos, causados a outrem em razão do exercício da atividade de tratamento de dados. (art. 42).

1.2.2.1 MÉTODO DE AUTENTICAÇÃO e RESPONSABILIDADE

Há situações complexas nas quais será necessária aplicação de um método que permita identificar qual a entidade que age na qualidade de "controlador".

Como regra geral, o controlador deverá, primeiramente, ser considerado como a sociedade e não a pessoa que age em seu nome. A pessoa física será considerada controladora quando agir em nome próprio. A regra geral é a de que uma empresa ou um organismo público será responsável pelas operações de tratamento realizadas a seu encargo, no campo de sua atividade ou do risco empresarial assumido. Mesmo nas hipóteses em que uma pessoa física, através de uma empresa ou organismo público, utilizar dados para fins pessoais, a empresa ou o organismo deverá ser responsabilizada por atos de prepostos ou pela falta de "segurança" no tratamento dos dados pessoais (art. 44).

Uma segunda situação poderá ocorrer quando uma sociedade empresária fixa a finalidade do tratamento de dados (o resultado esperado), enquanto uma outra sociedade decida sobre os meios a serem empregados (o modo de chegar ao resultado pretendido). Trata-se da contratação, pelo controlador, de prestadores de serviços (denominados pela lei como *operadores*), os quais serão solidariamente responsáveis pelos danos causados (art. 42, I) quando descumprirem a LGPD ou quando não tiverem seguido as instruções lícitas do "controlador" (nesses casos o "operador" se equipara ao "controlador").

Uma terceira situação seria aquela em

28 Acerca da proteção de dados e seu "controlador" há interessante situação quanto aos "programas estaduais de nota fiscal". Com o fito de incentivar o cidadão a exigir a nota fiscal em suas compras, os Estados cadastram os consumidores em seus sistemas, usualmente através de seus CPFs, para concederem-lhes certos benefícios (como o desconto em tributos, p. ex.) a partir de seu consumo (e emissão da respectiva nota fiscal). Desse momento em diante, o Estado passa a receber todas as informações constantes nas notas fiscais de consumo dos cidadãos. Para além do valor da compra e sua data, o Estado colhe informações sobre todas as mercadorias adquiridas pelo cidadão, seu preço individual e até mesmo as marcas consumidas. Todos esses dados são armazenados no banco de dados das Secretarias da Fazenda. Tais informações vão muito além do necessário para o simples incentivo da emissão da nota fiscal. A rigor, o Estado precisaria apenas do valor gasto, o estabelecimento fornecedor e o CPF do cidadão. Estamos diante de situação em que o tratamento de dados pelo operador vai muito além da sua necessidade, indo de encontro ao próprio princípio da necessidade (art. 6º, III da LGPD). Nesse sentido Machado, Jorge e Bioni, Bruno Ricardo. A proteção de dados pessoais nos programas de Nota Fiscal: Um estudo de caso no "Nota Fiscal paulista". LIINC em Revista, Rio de Janeiro, v. 12, n.2, p.350-364, novembro de 2016. http://www.ibict.br/liinc.

que se faz necessário identificar a entidade que exerceu a decisão de indicar o operador. Aqui vislumbram-se três hipóteses:

a) Situação em que a designação do controlador resulta de uma competência expressamente prevista em lei. Essa hipótese poderá ocorrer junto a órgãos da administração pública quando, por exemplo, um decreto autorize uma certa pessoa pública a implementar um tratamento, conferindo-lhe a determinação da finalidade e dos meios a serem empregados.

b) Uma segunda situação seria aquela em que inexiste disposição legal designando, expressamente, a identidade do controlador, o que nos remete às regras gerais do direito para determinar sua identidade. Assim, por exemplo, a regra geral de que o empregador responde pelos atos do empregado ou de que uma associação responde por seus membros ou aderentes.

c) Não sendo suficientes esses dois primeiros critérios, ainda nos cabe aplicar o método das "circunstâncias fáticas". Assim, analisam-se os termos dos contratos para enquadrar as relações entre seus partícipes na operação de tratamento. Além dos termos do contrato propriamente ditos, poderá ser levado em conta o efetivo grau de controle exercido por um partícipe na operação, a própria "imagem" da operação dada aos titulares e as expectativas que essa imagem poderia ter-lhes suscitado. Esses e outros elementos servirão de base para a indicação do controlador.

1.2.3 O "OPERADOR"

A LGPD define o "operador" como "a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (art. 5º, VII). Assim, a qualificação de "operador" exige da pessoa em causa o preenchimento de duas condições fundamentais: a) que seja uma entidade jurídica distinta do "controlador" e, portanto, dotada de personalidade jurídica própria e, b) que aja "em nome do controlador" . Esta segunda noção guarda alguma similitude com o contrato de mandato e significa que o *operador* deverá rigorosamente respeitar a LGPD e se limitar a obedecer as instruções lícitas do "controlador", sob pena de responsabilidade solidária (art. 42, I).

Resta daí que será encargo do operador provar, para elidir sua responsabilidade solidária, que seguiu rigorosamente a LGPD e as instruções lícitas do controlador. Nessa hipótese caberá ao operador o dever de esclarecer aos titulares que age em nome do controlador além do dever de avaliar a licitude de suas instruções.

Finalmente, todos os operadores devem zelar tanto pela obediência a LGPD quanto para que o contrato celebrado com o controlador aborde precisas e lícitas instruções à execução contratual, tudo como forma de elidir sua responsabilidade solidária prevista no art. 42, I da LGPD.

Interessa notar que no ARE 660.861 RG / MG o STF julgou, em regime de repercussão geral, que o provedor da internet[29] *Goggle* é responsável pelo pagamento de indenização por danos morais sofridos pela vítima (recorrente), em virtude da criação,

29 O art. 5º, VII, do Marco Civil da Internet, define aplicações de internet como "o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet", sendo, portanto, o provedor de aplicações de Internet qualquer entidade que proporcione ao usuário da grande rede mundial de computadores algo funcional, seja qual for a finalidade.

por terceiros, de conteúdo considerados ofensivos no sítio eletrônico de relacionamento *Orkut*. O prestador de serviço de um site de relacionamento (operador/*google*) que permite a publicação de mensagens na internet (pelo controlador/*orkut*), sem que haja um efetivo controle, ainda que mínimo, ou dispositivos de segurança[30] para evitar que conteúdos agressivos sejam veiculados, sem ao menos possibilitar a identificação do responsável pela publicação, deve responsabilizar-se pelos riscos inerentes a tal empreendimento. Observe-se que a responsabilidade neste caso foi apurada de forma objetiva, tendo em vista a incidência do Código de Defesa do Consumidor.

Entretanto, através do Marco Civil da Internet (lei 12.965/14, art. 19 e 21) o legislador dispôs que o provedor de aplicações de internet somente poderá ser responsabilizado civilmente se, após ordem judicial especifica, não tornar indisponível o conteúdo. Essa nova disposição tem o condão de alterar o conceito expresso pelo ARE 660.861 RG / MG do STF de que a mera publicação do conteúdo por terceiros acarretaria a responsabilidade objetiva do provedor

1.2.4. O TERCEIRO

Embora não haja a qualificação direta de terceiro na LGPD (art. 16, I), este pode ser definido como toda a pessoa física ou jurídica, além do titular, do controlador e do operador que, sob autoridade direta do controlador ou do operador, seja habilitada a tratar os dados. A noção de terceiro deve ser interpretada como designativa de sujeito desprovido de legitimidade ou autorização originais para tratar os dados pessoais, mas para quem é "autorizada a transferência" dos dados, desde que respeitados os requisitos e tratamento de dados dispostos na LGPG (art. 16, III).

A princípio, um terceiro recebedor de dados pessoais, de maneira lícita ou não, será equiparada a um novo controlador e, portanto, responsável pelos dados recebidos.

1.3. O CAMPO DE APLICAÇÃO TERRITORIAL

A transferência de dados pessoais tem um caráter internacional e estreitamente vinculado com o comércio eletrônico nacional e internacional. De acordo com *McKinsey Globral Institute* [31] "Ao longo dos últimos anos, o comércio eletrônico tem mudado a face do varejo: enquanto as vendas on-line crescem a taxas de dois dígitos em países desenvolvidos, o comércio tradicional permanece estável. Isso obriga os varejistas a repensar o papel de sua rede física de lojas". Verifica-se um constante crescimento do comércio de bens por meios eletrônicos.

Em decorrência da estrutura descentralizada da internet, as transações informacionais são realizadas por cruzamento de informações entre diversas jurisdições. Nesse sentido, a lei procura evitar a transferência

30 O aresto ainda observa que serviço prestado pelo provedor (Google) exige a elaboração de mecanismos aptos a impedir a publicação de conteúdos passíveis de ofender a imagem de pessoas, evitando-se que o site de relacionamento configure um meio sem limites para a manifestação de comentários ofensivos. Ainda que o fato ofensivo tenha sido elaborado por terceiros, não se exclui a responsabilidade do provedor em fiscalizar o conteúdo do que é publicado e se os usuários estão observando as políticas elaboradas pelo próprio site.

31 https://www.mckinsey.com/br/our-insights/blog-made-in-brazil/o-papel-das-lojas-fisicas-em-um-mundo-digital Acesso em 22 de julho de 2019.

internacional de dados à países cujas jurisdições apresente um menor grau de tutela a sua proteção.

Sabidamente, muitas empresas internacionais adotam países conhecidos como *data haven* para realizar o processo de transferência, tratamento e armazenamento de dados, ou seja, em países que se caracterizam por não terem leis de proteção de dados ou disporem de leis mais brandas que não asseguram reais garantias a tutela dos dados pessoais.

A intenção do legislador nacional é de cobrir essa lacuna através da aplicação da lei nacional em caráter extraterritorial e, além disso, exigir que as empresas sejam obrigadas, ao se utilizarem de fornecedores no exterior, a garantir aos titulares dos dados forma idêntica de proteção oferecida pela lei nacional.

A aplicação extraterritorial[32] da LGPD resulta do disposto em seu art. 3º, o qual determina sua aplicação a qualquer operação de tratamento de dados feita por pessoa natural ou jurídica, pública ou privada, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que se verifique um dos três critérios distintos:

a) Tratamento de dados realizado no Brasil;

Nessa hipótese valerá o critério territorial, ou seja, todo tratamento de dados realizados no país estará sujeita a LGPD.

b) O tratamento de dados tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados para indivíduos localizados no território brasileiro.

Nesse caso, o tratamento dos dados pessoais poderá ser realizado em território alienígena, ou seja, estrangeiro. Imporá a aplicação da LGPD o fato do objetivo do tratamento ser destinada a oferecer bens ou serviços para qualquer pessoa situada no território nacional. É o caso, v.g., de sites chineses que oferecem produtos à brasileiros, em português, com entrega domiciliar no país.

c) Os dados pessoais objeto do tratamento tenham sido coletados no Brasil.

Aqui igualmente desimporta o local onde se deu o tratamento. Valerá a LGPD em todas as hipóteses em que os dados sejam coletados no país, o que implica numa tentativa de garantir efeitos extraterritoriais a lei brasileira.

Como se depreende do texto legal, o critério empregado pelo legislador pátrio para fixar a competência da LGPD despreza os "meios" de tratamento de dados, o país de sua sede (do "tratamento") ou o país onde estejam localizados os dados.

Tendo em vista os critérios empregados pela LGPD, seu campo de aplicação cobrirá praticamente todos os atos de tratamento realizados no Brasil ou que sejam destinados a pessoas situadas no seu território.

Importa analisar a extraterritorialidade das normas, questão ligada ao seu caráter instrumental e à implementação de políticas públicas. Através da extraterritorialidade

32 "Na atualidade, os típicos elementos referenciais de Estado não subsistem ..... Em contraposição ao território, ocorre a desterritorialização, onde as conexões informáticas se travam no espaço virtual, sem levar em consideração o local onde se situam os sujeitos que estão conectados à Internet. Assim, pode-se efetuar um contrato por meio de comércio eletrônico com alguém que se situa na outra esfera do mundo." Limberger, Têmis. Proteção dos Dados Pessoais e Comércio Eletrônico: Os Desafios do Século XXI. Revista de Direito do Consumidor. Vol. 67/2008, p.215

os países procuram estender seu poder regulamentar para todas as condutas que, de alguma forma, possam gerar efeitos em seu território[33].

A questão da jurisdição assume grande relevância, pois para garantir a extraterritorialidade os Estados precisam assegurar a aplicação de sua lei interna sobre condutas eventualmente praticadas fora de seu território, mas que nele produzem efeitos. Trata-se do princípio dos efeitos (*effects doctrine*) segundo o qual há incidência da lei nacional do local onde se verificam as consequências da prática ilegal. O que importa, neste caso, não é a nacionalidade ou domicílio dos partícipes da ilegalidade, mas o local (país) onde se produzirão seus efeitos; já o critério da *territorialidade* implica na aplicação da norma nacional para práticas ilegais ocorridas no próprio território nacional. A lei brasileira claramente se vale dos dois princípios quando diz que a lei aplica-se a qualquer operação de tratamento ..... independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados desde que operação de tratamento seja realizada no território nacional ou se os dados tratados tenham sido coletados no território nacional (territorialidade) ou se a atividade de tratamento tenha por objetivo a oferta de bens e serviços ou o tratamento de dados de indivíduos localizados no país (princípio dos efeitos).

O critério dos efeitos acaba por estender a jurisdição de um país sobre condutas que não se verificaram em seu território, mas cujos efeitos ali se dão[34]. A extraterritorialidade da lei brasileira não impede que a mesma conduta seja julgada pela lei estrangeira, ou seja, a lei vigente no local em que se deu o tratamento de dados. De outro modo, a lei brasileira poderá pretender julgar, no Brasil, os responsáveis pelos tratamento de dados realizados no exterior (mas cujos efeitos se dão no país), fato que poderá suscitar conflito positivo de jurisdição. A questão se revolverá no plano do direito internacional.

CONCLUSÃO

Após a fundamentação do direito a proteção de dados, que se caracteriza como uma espécie de direitos de personalidade, impõe-se descrever seus efeitos como sendo tanto de caráter negativo (direito de defesa), quanto de caráter positivo (direito à prestação). É um direito negativo ao delimitar uma esfera de proteção que não poderá sofrer a intervenção do poder estatal ou privado, exigindo a abstenção desses entes nesse sentido. Será positivo porque também enseja que o Estado tome condutas positivas tendentes a garantir ao cidadão a proteção desse direito.

33 Embora os países pretendam aplicar sanções ou expedir ordens a empresas ou pessoas físicas sediadas ou domiciliadas no exterior, os efeitos extraterratoriais da lei nacional sofrem limitações impostas pela soberania dos outros países, especialmente através das chamadas blocking laws destinadas a impedir que em território nacional se produzam efeitos de ordens proferidas por autoridades

34 Nesse sentido Daniela Copetti Cravo sobre a extraterritorialidade do Regulamento Geral da Proteção de Dados Europeu: "O primeiro ponto de destaque do Regulamento é a extensão dada à proteção, que pode alcançar agentes que não tem presença na União Europeia, desde que os dados de um residente da União Europeia sejam processados em decorrência da oferta de um produto ou serviço. A outra hipótese é quando o comportamento de um indivíduo na União Europeia seja monitorado, o que demonstra a possibilidade, nas duas hipóteses, de aplicação extraterritorial do Regulamento. CRAVO, Daniela Copetti. Direito a Portabilidade de Dados. Rio de Janeiro, Lumen Juris, 2018. p. 28/29.

Desta forma, sob o ponto de vista negativo, nenhuma lei poderá eliminar esse direito da ordem jurídica, pois se trata de um direito constitucional fundamental. Desde a o ponto de vista de seu caráter positivo, caberá ao Estado o dever de garantir ao cidadão a proteção de dados pessoais, múnus que o Estado se desincumbe através da promulgação da LGPD.

Ainda deve-se concluir com a alusão a eficácia vertical e horizontal[35] do direito a proteção de dados, aplicando-se tanto a ordem pública quanto a privada. Sua aplicação vertical deriva da própria ordem constitucional através da previsão do *habeas data*, que assegura o conhecimento de informações relativas à pessoa do impetrante, constantes de registros públicos ou bancos de dados de entidades governamentais ou de caráter público (art. 5º, LXXII da CF/88). A eficácia horizontal se dá nas próprias relações jurídicas entre particulares. Registre-se, aqui, que todos os bancos de dados privados possuem caráter público, ainda que seja gerido por organismo privado, pois trata-se da uma espécie de direito fundamental à proteção da personalidade, uma vez que os dados armazenados dizem respeito a privacidade do titular.

Desta forma, somente deixa de ser cadastro *público* aqueles utilizados por pessoas físicas destinadas o uso não econômico, dados realizados para fins jornalísticos, artísticos ou acadêmicos e dados utilizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão a infrações penais.

O reconhecimento da eficácia horizontal da LGPD é essencial para a proteção da personalidade num sistema econômico onde a informação pessoal se constitui num insumo de excepcional relevância para que grandes empresas tomem suas decisões de investimento, estratégia, produção, distribuição e locação de pontos de venda a partir de acurada análise das informações obtidas sobre a renda, preferências e comportamento dos cidadãos.

A LGPD vem regular a proteção de dados e reconhecer que a informação – dados pessoais – transformou-se em verdadeiro insumo da produção, adquirindo tanta relevância quanto o capital e o trabalho. Esse quadro evolutivo proporcionou a solidificação da sociedade de informação, onde as conexões realizadas através das Tecnologias da Informação e Comunicação (TIC), tendo como suporte a *internet*, promover a informação e da difusão de dados.

Desta forma, deve-se reconhecer que, para além da defesa da privacidade, o que se protege e se regula através da LGPD é o poder de acesso e o controle das informações pelo cidadão.

BIBLIOGRAFIA

BARROS, Bruno M. Correa de., BARROS, Clarissa T. Lovatto, OLIVEIRA, Rafael Santos de. O direito à privacidade: uma reflexão acerca do anteprojeto de proteção de dados pessoais. Revista Videre, Dourados, MS, v.9, n.17.1. semestre de 2017. p. 21.

CRAVO, Daniela Copetti. Direito a Portabilidade

35 Quando se fala nas eficácias vertical e horizontal, pretende-se aludir à distinção entre a eficácia dos direitos fundamentais sobre o Poder Público e a eficácia dos direitos fundamentais nas relações entre os particulares.

de Dados. Rio de Janeiro, Lumen Juris, 2018.

CUEVA, Ricardo Villas Bôas. A insuficiente proteção de dados pessoais no Brasil. Revista de Direito Civil Contemporâneo. Vol. 13/2017, p. 59-67. Out-Dez 2017.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro. Renovar. 2006.

LIMA MARQUES, Claudia. Contratos no código de defesa do consumidor. 5ª ed. Ed. RT. SP-SP, 2006.

MASSO, Fabiano Del; ABRUSIO, Juliana e FLORÊNCIO FILHO, Marco Aurélio. Marco civil da internet. Lei 12.965/14. Ed. Revista dos Tribunais. São Paulo. 2014.

MACHADO, Jorge e Bioni, Bruno Ricardo. A proteção de dados pessoais nos programas de Nota Fiscal: Um estudo de caso no "Nota Fiscal paulista". LIINC em Revista, Rio de Janeiro, v. 12, n.2, p.350-364, novembro de 2016. http://www.oboct.br/liinc

MARQUES, Claudia Lima; et al., Manual de Direito do Consumidor. São Paulo: Ed. RT, 2008, p. 85-88.

MENDES, Gilmar. Curso de direito constitucional. 2ª ed. São Paulo. Saraiva, 2008.

OPICE BLUM, Renato; NOBREGA MALDONADO, Viviane. Comentário ao GDPR. Ed. RT, SP-SP, 2018.

OPICE BLUM, Renato; NOBREGA MALDONADO, Viviane. LGPD Lei Geral de Proteção de Dados. Comentário. Ed. RT, SP-SP, 2019.

RODOTÁ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro, Renovar. 2008.

SARLET, Ingo Wolfgang. Curso de Direito Constitucional, 3ª ed, p. 400. Ed. RT. SP-SP, 2013.

TEPEDINO, Gustavo. A tutela da personalidade no ordenamento civil – constitucional brasileiro.

https://www.academia.edu/31740015/A_tutela_da_personalidade_no_ordenamento_civil-constitucional_brasileiro

https://www.mckinsey.com/br/our-insights/blog-made-in-brazil/o-papel-das-lojas-fisicas-em-um-mundo-digital

https://portalnovarejo.com.br/2015/09/7-tecnologias-para-monitorar-habitos-de-consumo/

http://agenciabrasil.ebc.com.br/economia/noticia/2018-07/facebook-chega-127-milhoes-de-usuarios-no-brasil

http://www.ibict.br/liinc.

Publicado originalmente na Revista dos Tribunais, São Paulo, ano 108, n.1010, p. 209-229, dez.2019

APLICAÇÃO DA LGPD PELOS TRIBUNAIS TRABALHISTAS: ANÁLISE DA JURISPRUDÊNCIA RECENTE

Bruna de Sá Araújo

SUMÁRIO: INTRODUÇÃO. 1. RETROSPECTO SOBRE AS PRIMEIRAS REGULAMENTAÇÕES DE PROTEÇÃO DE DADOS EM OUTROS PAÍSES. 2. REGULAMENTAÇÃO DA PROTEÇÃO DE DADOS NO BRASIL. 3. A APLICAÇÃO DA LGPD PELOS TRIBUNAIS TRABALHISTAS. CONCLUSÃO. REFERÊNCIAS BIBLIOGRÁFICAS.

INTRODUÇÃO

Na vida em sociedade, os indivíduos se identificam perante terceiros de forma cotidiana. Ao utilizar o transporte aéreo ou serviços bancários para realizar transações monetárias, por exemplo, qualquer cidadão deve necessariamente fornecer dados pessoais, por determinação legal. Muitas outras situações de identificação, entretanto, decorrem de costumes sociais.

A autenticação biométrica para ingresso em academias ou registro de ponto do trabalhador, bem como a identificação em caixas de supermercado para a obtenção de descontos no preço, são práticas realizadas de forma voluntária pelos consumidores desses estabelecimentos comerciais, sem qualquer exigência legal.

Essas são apenas algumas das muitas situações em que são fornecidos dados pessoais a terceiros em práticas que se tornaram rotineiras e que, via de regra, não despertam no indivíduo qualquer preocupação sobre o destino, a finalidade de uso ou a segurança das suas informações pessoais.

Com efeito, a proteção de dados já era discutida e regulamentada em outros países, a Declaração da ONU dos Direitos Humanos (1948) e a Declaração Europeia dos Direitos do Homem (1950) são consideradas as primeiras declarações internacionais subscritas por países europeus que mencionam a privacidade e o direito à sua proteção.

A Lei nº 12.965/2014 (Marco Civil da Internet) é considerada a primeira legislação vigente no território brasileiro,

Bruna de Sá Araújo

Advogada, especialista em Direito do Trabalho e Processo do Trabalho pelo IPOG e pela Universidade Federal de Goiás, pós-graduada em Direito Previdenciário pela Fasam.

a dispor expressamente sobre a questão dos dados pessoais, ao tratar temas como neutralidade da rede, retenção de dados e funções sociais da internet, como liberdade de expressão, transmissão de conhecimento e responsabilidade civil.

Todavia, desde o ano de 2020 passou a viger no país lei mais específica e aprofundada sobre o tema da proteção de dados; trata-se da Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018[1], com as alterações promovidas pela Lei nº 13.853/2019, que dispõe sobre a proteção de dados pessoais.

A LGPD é considerada um marco jurídico regulatório inédito no Brasil e atinge todas as instituições públicas e privadas, que agora terão que se adaptar a essa nova regulamentação, que tem como princípio proteger os direitos fundamentais de liberdade e privacidade dos cidadãos brasileiros.

O art. 1º da Lei Geral de Proteção de Dados prevê que a sua aplicação também abarca as "pessoas jurídicas de direito público". Dessa forma, urge discutir e regulamentar o alcance dessa diretriz às publicações de dados realizadas pelos Tribunais Trabalhistas, órgãos que detêm uma enorme quantidade de dados de pessoas físicas e jurídicas.

Com a implantação e expansão do Processo Judicial Eletrônico (PJe) em meados de 2010, o Judiciário passou a gerir uma quantidade colossal de dados pessoais e sensíveis de diversos cidadãos jurisdicionados. Assim, considerando que o Poder Judiciário, como parte do Estado, é guardião de dados, busca-se analisar no presente artigo a aplicação efetiva na LGPD nas decisões proferidas pelos Tribunais Regionais do Trabalho, desde a vigência da referida lei.

1. RETROSPECTO SOBRE AS PRIMEIRAS REGULAMENTAÇÕES DE PROTEÇÃO DE DADOS EM OUTROS PAÍSES

A Declaração da ONU dos Direitos Humanos (1948)[2] e a Declaração Europeia dos Direitos do Homem (1950)[3] são consideradas as primeiras declarações internacionais subscritas por países europeus que mencionam a privacidade e o direito à proteção. Entretanto, tratavam de maneira vaga e superficial sobre a proteção dos dados pessoais.

Por outro lado, a Convenção nº 108 do Conselho da Europa[4] estabeleceu a proteção de indivíduos quanto ao processamento automático de tratamento de dados, objetivando instituir métodos mais criteriosos como a previsão das "garantias relativas à coleta e tratamento de dados pessoais". Assim, a referida convenção proíbe,

"na ausência de garantias jurídicas adequadas, o tratamento de dados 'sensíveis', tais como dados sobre a raça, a opinião política, a saúde, as convicções religiosas, a vida sexual ou o registo criminal de uma pessoa."

No ano de 1995, com o objetivo de

1 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 14 mar. 2021.

2 Disponível em: https://nacoesunidas.org/direitoshumanos/declaracao/. Acesso em: 14 mar. 2021.

3 Disponível em: https://www.echr.coe.int/Documents/Convention_POR.pdf. Acesso em: 14 mar. 2021.

4 Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37. Acesso em: 14 mar. 2021.

aperfeiçoar e dar efetividade à Convenção nº 108, a União Europeia promulgou a Diretiva nº 95/46/CE[5], que pretendia estabelecer, harmonizar e promover igualdade no tratamento de dados pessoais pelos Estados-Membros. Por se tratar de uma diretiva, seria necessário que cada Estado adotasse o texto comunitário em seu direito interno, o que ensejou diferentes níveis de proteção em cada um dos países europeus.

No entanto, o Regulamento (UE) nº 2.016/679 do Parlamento Europeu e do Conselho[6], relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, decidiu revogar a Diretiva nº 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

Dois anos mais tarde, o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia, com 11 capítulos e 99 artigos, entrou em vigor, atualizando, harmonizando e adaptando a antiga Diretiva Europeia de Proteção de Dados às mais novas formas de uso massivo de dados pessoais, tais como os modelos de negócio baseados em tecnologias de *big data*, inteligência artificial e aprendizado de máquina. O regulamento estabelecia as regras relativas ao tratamento, por uma pessoa, uma empresa ou uma organização, de dados pessoais relativos a pessoas.

Nos artigos 4º, itens 13, 14 e 15, e 9º, além dos Considerandos 51 a 56 do GDPR, há previsão sobre os denominados dados sensíveis, que são os dados pessoais que revelem origem racial ou étnica, opiniões políticas e convicções religiosas ou filosóficas; filiação sindical; dados genéticos, dados biométricos tratados simplesmente para identificar um ser humano; dados relacionados com a saúde; dados relativos à vida sexual ou à orientação sexual da pessoa.

Em relação ao tratamento de dados, o artigo 4º, itens 2 e 6, da GDPR inclui o recolhimento, o registro, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, comparação ou interconexão, a limitação, o pagamento ou a destruição de dados pessoais. Tal previsão é aplicável ao tratamento dos dados pessoais, seja por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em arquivos (ficheiros).

2. REGULAMENTAÇÃO DA PROTEÇÃO DE DADOS NO BRASIL

Sem especificar a questão relacionada à proteção de dados, a Constituição da República Federativa do Brasil traz no *caput* do art. 5º a proteção à segurança de brasileiros e estrangeiros residentes no país. Considerando os direitos fundamentais sob uma ótica expansionista, também poderia ser incluída nesse conceito a proteção de dados.

O inciso X do referido artigo dispõe que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas (...)". Assim, sob um viés expansionista protetivo, o direito à privacidade também se relaciona diretamente com a proteção de dados.

5 Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 14 mar. 2021.

6 Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679. Acesso em: 14 mar. 2021.

Outra importante legislação sobre o tema no país é o Marco Civil da Internet (Lei nº 12.965), sancionado em 2014[7]. Voltado inteiramente para o uso da internet no país, o Marco Civil traz princípios, garantias, direitos e deveres dos usuários da rede, além de diretrizes sobre como o Estado deve atuar. Ao lado da privacidade, alguns dos outros principais temas abordados pela lei são: neutralidade da rede, retenção de dados e funções sociais da internet, como liberdade de expressão, transmissão de conhecimento e responsabilidade civil.

O princípio da privacidade é conceituado como a garantia de inviolabilidade das comunicações dos usuários. Nesse contexto, a Lei do Marco Civil atribui o dever de sigilo de suas informações ao provedor do recurso de internet. A isenção de tal garantia pode acontecer somente por meio de ordem judicial, quando forem imprescindíveis para a elucidação de ações ilícitas, bem como na tentativa de identificação dos seus responsáveis.

A lei mais específica e aprofundada sobre o tema da proteção de dados é a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/201816, com as alterações promovidas pela Lei nº 13.853/2019, que dispõe sobre a proteção de dados pessoais. A LGPD entrou em vigor no dia 18 de setembro de 2020, após o presidente Jair Bolsonaro sancionar o Projeto de Lei de Conversão nº 34/2020, originado da Medida Provisória nº 959/2020.

Ao editar a MP, em abril de 2020, o governo incluiu, em seu art. 4º, um dispositivo que previa o adiamento da entrada em vigor da LGPD, para maio de 2021. Como tem força de lei, assim que foi publicada a MP, a vigência da LGPD foi adiada. No entanto, ao passar pela análise do Congresso Nacional, o dispositivo em comento não foi aprovado.

A LGPD visa preservar o direito constitucional à liberdade e à privacidade que todos os cidadãos brasileiros têm, assim como protegê-los de danos causados por rupturas desses direitos. A LGPD se aplica a qualquer tratamento de dados ocorrido (total ou parcialmente) em solo brasileiro, ou que tenha por objetivo vender produtos e serviços nacionais. Além disso, a lei é direcionada para tratamentos com fins comerciais, ou seja, trocas e outros tratamentos de dados entre pessoas físicas sem objetivos de compra ou venda de produtos e serviços não se enquadram.

A lei elucida que o direito à privacidade e à liberdade não impede a coleta, o uso e outros tratamentos de dados para fins jornalísticos, artísticos ou acadêmicos. Por conseguinte, preserva-se a liberdade de imprensa, da arte e da ciência.

O art. 5º é considerado um dos mais importantes da lei, pois estabelece a definição de conceitos fundamentais básicos para a compreensão do texto como um todo, tais como dado pessoal, dado pessoal sensível, dado anonimizado, banco de dados, titular, controlador, operador, encarregado, agentes de tratamento, tratamento, anonimização, consentimento, bloqueio, eliminação, transferência internacional de dados, uso compartilhado de dados, relatório de impacto à proteção de dados pessoais, órgão de pesquisa e autoridade nacional.

A lei ainda traz a determinação de que o

7 BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. (Marco Civil da Internet). Disponível em: https://legislacao.presidencia. gov.br/atos/?tipo=LEI&numero=12965&ano=2014&ato=93eUTRE9ENVpWTdb6. Acesso em: 14 mar. 2021.

titular tem direito de solicitar informações sobre a finalidade, a duração e a forma de tratamento dos dados, assim como saber se seus dados estão sendo ou foram compartilhados com outros agentes.

3. A APLICAÇÃO DA LGPD PELOS TRIBUNAIS TRABALHISTAS

Antes da difusão da internet, no final da década de 1980, a coleta de dados era mais trabalhosa, uma vez que o Poder Judiciário e os operadores do Direito produziam documentos físicos e inexistiam métodos acessíveis de análise, organização e classificação de dados.

Atualmente, com o advento da Quarta Revolução Industrial e a informatização de quase todo o sistema processual brasileiro, além da obrigatoriedade legal de publicidade da quase totalidade dos processos, acarretou-se uma grande quantidade de dados gerados pelo Judiciário, consolidados nas versões *online* dos diários oficiais ou nos próprios sites dos Tribunais.

Contudo, ao disponibilizar essa grande quantidade de dados, inclusive os chamados dados sensíveis e os dados pessoais, indaga-se se o Poder Judiciário não estaria infringindo as normativas nacionais e internacionais mencionadas alhures sobre proteção de dados.

A indagação e sua resposta são preocupantes, uma vez que o Poder Judiciário, como parte do Estado e guardião de dados sensíveis e pessoais de inúmeros cidadãos jurisdicionados, não poderia disponibilizar tais dados, sem limites claros e restritivos dispostos na legislação aplicável.

É cediço que no Brasil os processos e seu conteúdo são públicos, com exceção dos processos que tramitam em segredo de justiça. Em regra, sem assinatura eletrônica dos procuradores ou membros do Judiciário, não é possível que o cidadão comum consiga ler o teor dos autos eletrônicos se não for parte envolvida e possuir a senha de acesso.

Por outro lado, é notório que a jurisprudência e as decisões ficam disponíveis no Diário Oficial e banco de decisões do Tribunal, de modo que inúmeros dados pessoais e dados pessoais sensíveis ficam disponíveis ao público em geral, violando o direito à privacidade e proteção de dados de diversos cidadãos.

Pensando justamente nessa violação aos dados pessoais e sensíveis das partes litigantes dos processos trabalhistas, e ainda, considerando que a LGPD aplica-se às pessoas jurídicas de direito público, incluído os órgãos do Poder Judiciário, nota-se cada vez mais jurisprudência sobre o tema, indicando que os Magistrados e Tribunais Regionais do Trabalho estão aplicando efetivamente a letra da lei.

A juíza da 3ª Vara do Trabalho de Belo Horizonte do TRT da 3ª Região determinou nos autos de uma reclamatória trabalhista, que a disponibilização do dado em prova judicial implicará em presunção de consentimento quanto à forma de tratamento disciplinado pelo titular, prevalecendo de imediato, bem como para efeito do disposto no art. 7º, I, da Lei n. 13.709/2019 (LGPD), no que se refere ao consentimento do fornecimento do dado pelo titular (RT-0010083-28.2021.5.03.0003).

No TRT da 14ª Região, o juiz da Vara do Trabalho de Jaru-RO tem decidido que, após a vigência da Lei Geral de Proteção de Dados, a ata de audiência não poderá servir como alvará por conter dados sensíveis do reclamante e de seus patronos (RT-0000266-25.2020.5.14.0081).

Recentemente, o juiz Willian Alessandro Rocha da Vara do Trabalho de Poá-SP, do TRT da 2ª Região, verificou em uma reclamatória trabalhista que foram juntados documentos no processo relacionados à saúde da reclamada, bem como os documentos relacionados à saúde do patrono da autora continham dados sensíveis, nos termos do artigo 5º, II, da LGPD. Assim, considerando a proteção dos dados disponíveis no órgão público, o juiz determinou que a Secretaria da Vara incluísse os referidos documentos em sigilo, deixando acessível somente para os patronos das partes (RT-1000300-56.2020.5.02.0391).

O juiz da 3ª Vara do Trabalho de Lages-SC, do TRT da 12ª Região, homologou em dezembro de 2020 um pedido de produção antecipada de provas, formulado por um Sindicato obreiro em face de uma empresa de transportes. O Sindicato elencou justificativas referentes a não apresentação de alguns documentos, dentre elas os elevados custos para digitalização de mais de 130 mil documentos e a possível violação da LGPD com a divulgação de dados sensíveis dos empregados (PAP-0002963-39.2020.5.12.0060).

O Tribunal Superior do Trabalho publicou no dia 12 de março de 2021, o Ato Conjunto TST.CSJT.GP n. 4, no qual instituiu a Política de Privacidade e Proteção de Dados Pessoais no âmbito do TST e do Conselho Superior da Justiça do Trabalho. Em seu artigo 7º, o ato estabelece que:

"O Tribunal Superior do Trabalho e o Conselho Superior da Justiça do Trabalho poderão, nas atividades voltadas ao estrito exercício de suas competências legais e constitucionais, proceder ao tratamento de dados pessoais independentemente de consentimento".

No referido ato, também ficou estabelecido que o exercício da função de Controlador no âmbito do TST e do CSJT será atribuído ao Ministro Presidente (art.13); a função de Encarregado pelo tratamento de dados Pessoais será exercida por Juiz Auxiliar indicado pelo Presidente do TST (art. 15); definiu que serão operadores as pessoas naturais ou jurídicas, de direito público ou privado, que realizarem operações de tratamento de dados pessoais em nome do respectivo controlador (art. 18).

A proteção de dados também é observada nas decisões de tribunais estrangeiros, a partir de 2019, a França proibiu a divulgação de estatísticas sobre decisões judiciais, consoante a regra do artigo 33 da referida Lei francesa, que também adicionou dispositivos a outras leis, como o Código Penal. O artigo 33 estabelece.

"(...) que os dados de identidade de magistrados e servidores do Judiciário não podem ser reutilizados com o objetivo ou efeito de avaliar, analisar, comparar ou prever suas práticas profissionais, reais ou supostas."

O artigo 33 (V) da Lei nº 2013-111, que foi modificado pela Lei nº 2019- 222, determina que as decisões dos tribunais judiciais são disponibilizadas gratuitamente ao público em formato eletrônico, mas sujeitos às disposições especiais que regem o acesso e a publicidade das decisões judiciais: os nomes e sobrenomes das pessoas singulares mencionadas na decisão, quando são partes ou terceiros, ficam ocultos antes da disponibilização ao público.

O artigo também prevê que, quando a divulgação dos dados for suscetível de prejudicar a segurança ou o respeito da privacidade dessas pessoas ou sua comitiva, também estará oculto qualquer elemento que permita identificar as partes, os terceiros, os magistrados e os membros do registro.

A premissa da qual a lei parte é que, ao restringir o acesso a dados pessoais e liberar o acesso aos dados de conteúdo, a justiça francesa estaria conciliando a publicidade das informações jurídicas com a proteção à intimidade das pessoas envolvidas[8].

A retirada dos nomes e sobrenomes das pessoas físicas mencionadas nas decisões francesas a partir de 2019, independentemente do fato de serem partes ou terceiros, antes da disponibilização ao público, visa atender as determinações do Regulamento Geral de Proteção de Dados (GDPR). A Lei francesa levou em consideração o fato de que são dados sensíveis aqueles que não podem ser disponibilizados ao público, tratando-se de uma forma de proteção dos envolvidos.

Desse modo, o Regulamento Geral de Proteção de Dados (GDPR) determina que, se a divulgação de outras informações colocar em risco a segurança ou o respeito pela vida privada dessas pessoas ou seus arredores, não deverão ser publicadas, assim como qualquer informação que identifique as partes ou terceiros.

CONCLUSÃO

Em plena vigência no Brasil desde o dia 18 de setembro de 2020, a Lei Geral de Proteção de Dados (LGPD) enseja ampla discussão sobre problemáticas oriundas da necessidade de proteção de dados. O presente artigo buscou discutir a questão que afeta os Tribunais trabalhistas do país, demonstrando que tais órgãos já estão se adequando à nova legislação que regula de forma específica a proteção de dados, ainda que de forma pontual.

Partindo de um estudo aprofundado sobre as primeiras regulamentações sobre proteção de dados no mundo, demonstrou-se que o tema em questão foi discutido e regulado com maior profundidade em países da União Europeia e América.

De maneira superficial, no Brasil, o art. 5º, caput e inciso X, da Constituição Federal prevê a proteção e inviolabilidade dos brasileiros e estrangeiros residentes no país, sem especificar se tal proteção abrangeria a proteção de dados. Em 2014, foi sancionada a Lei nº 12.965, chamada de Marco Civil da Internet, que dispõe sobre temas como neutralidade da rede, retenção de dados e funções sociais da internet, como liberdade de expressão, transmissão de conhecimento e responsabilidade civil.

A lei mais específica e aprofundada sobre o tema da proteção de dados é a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, com as alterações promovidas pela Lei nº 13.853/2019, que dispõe sobre a proteção de dados pessoais. A LGPD visa preservar o direito constitucional à liberdade e à privacidade que todos os cidadãos brasileiros têm, assim como protegê-los de danos causados por rupturas desses direitos.

As inovações tecnológicas permitiram a informatização de quase todo o sistema processual brasileiro e ampliou a publicidade das decisões judiciais. Soma-se a isso a grande quantidade de dados gerados pelo Judiciário, consolidados nas versões online dos diários oficiais ou nos próprios sites dos tribunais.

Apesar de vigente desde setembro de 2020, a pouca jurisprudência encontrada nos repositórios dos Tribunais Regionais do Trabalho de todo o país indicam a aplicação esparsa

8 CORRÊA, Fernando; TRECENTI, Julio; NUNES, Marcelo Guedes. A lei francesa de acesso a dados judiciários: algumas reflexões. Disponível em: https://www.migalhas.com.br/depeso/304441/a-leifrancesa-de-acesso-a-dados-judiciarios-algumas-reflexoes. Acesso em: 14 mar. 2021.

e pontual da LGPD, revelando que o assunto precisa ser melhor debatido e efetivamente aplicado pelos magistrados trabalhistas.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. (Marco Civil da Internet). Disponível em: https://legislacao. presidencia.gov.br/atos/?tipo=LEI&numero=12965&ano=2014&ato=93eUTRE9ENVpWTdb6. Acesso em: 14 mar. 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709. htm. Acesso em: 14 mar. 2021.

CORRÊA, Fernando; TRECENTI, Julio; NUNES, Marcelo Guedes. A lei francesa de acesso a dados judiciários: algumas reflexões.

MORAES, Alexandre de. Direito constitucional. 32. ed. São Paulo: Atlas, 2016.

NOVELINO, Marcelo. Direito constitucional. 2. ed. São Paulo: Método, 2008.

ORSINI, Adriana Goulart de Sena. Jurimetria e predição: notas sobre uso dos algoritmos e o Poder Judiciário. In: Futuro do trabalho: efeitos da revolução digital na sociedade, Brasília: ESMPU, 2020.

Internet

A Declaração Universal dos Direitos Humanos. Disponível em: https://nacoesunidas.org/direitoshumanos/declaracao/. Acesso em: 14 mar. 2021.

A lei francesa de acesso a dados judiciários: algumas reflexões. Disponível em: https://www.migalhas.com.br/depeso/304441/a-lei-francesa-de-acesso-a-dados-judiciarios-algumas-reflexoes. Acesso em: 14 mar. 2021.

Convenção Europeia dos Direitos do Homem. Disponível em: https://www.echr.coe.int/Documents/Convention_POR.pdf. Acesso em: 14 mar. 2021.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37. Acesso em: 14 mar. 2021.

Décision nº 2019-778 DC. Disponível em: https://www.conseil-constitutionnel.fr/ decision/2019/2019778DC.htm. Acesso em: 14 mar. 2021.

Directiva 95/46/CE do Parlamento Europeu e do Conselho. Disponível em: https://eur-lex. europa. eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 14 mar. 2021.

LGPD comentada. Disponível em: https://guialgpd.com.br/lgpd-comentada/. Acesso em: 14 mar. 2021.

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. Disponível em: https://eurlex.europa.eu/legal-content/PT/TXT/?uri=-CELEX%3A32016R0679. Acesso em: 14 mar. 2021.

NOVA LEI BRASILEIRA DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) E O IMPACTO NAS INSTITUIÇOES PÚBLICAS E PRIVADAS

Patricia Peck Garrido Pinheiro

Resumo

O presente estudo visa analisar os principais desdobramentos da sanção da Lei 13.709/18, a Lei Geral de Proteção de Dados Pessoais do Brasil (LGPD). Para isso, pontuamos as transformações contextuais que resultaram no surgimento de um regulamento específico para a proteção de dados no país, como o amplo desenvolvimento tecnológico, o aumento da importância da informação dentro do contexto contemporâneo e a insegurança dos dados no mundo digital. Os principais impactos no ambiente jurídico e nas relações negociais também são analisados, sempre com o viés comparativo da lei nacional com o regulamento europeu, o General Data Protection Regulation (GDPR).

Palavras-chave

Direito digital – Proteção de dados – Privacidade – Dados pessoais – Sociedade digital – Lei de Proteção de Dados Pessoais

Sumário

Introdução

A Lei 13.709/18 (LGL\2018\7222), assinada pelo presidente Michel Temer no dia 14 de agosto de 2018, é o marco legal da proteção de Dados Pessoais do Brasil. Conhecida também pela sigla LGPD, a Lei Geral de Proteção de Dados, é originária do PLC 53/18, que por sua vez foi resultante da união de outros dois projetos, e estabeleceu um prazo de 18 meses de adaptação às novas

Patricia Peck Garrido Pinheiro

Doutora em Direito Internacional e Propriedade Intelectual pela USP, PhD

regras contados da data de sua publicação.

Criada como meio de fortalecer a proteção da privacidade dos usuários e de seus dados pessoais, a lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado. Um dos grandes destaques trazidos com a novidade é que, a partir das novas regras, os cidadãos poderão ter acesso a informações de como seus dados são coletados, processados e armazenados. Ou seja, o objetivo é proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

O surgimento dessa lei específica sobre proteção dos dados pessoais decorre das novas necessidades da sociedade digital que exige mais transparência das relações, considerando a sustentação do modelo atual de negócios onde a informação passou a ser a principal moeda de troca utilizada pelos usuários para ter acesso a determinados bens, serviços ou conveniências.

De acordo com a definição da LGPD, tratamento é compreendido como toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle, modificação, comunicação, transferência, difusão ou extração.

Assim como o *General Data Protection Regulation* (GDPR), o regulamento de proteção aos dados da União Europeia, a LGPD exige que toda e qualquer transação envolvendo dados que estejam em território nacional (do Brasil), independentemente de sua cidadania ou origem, sejam abarcadas pelas novas regras. Isso significa que todas as empresas que fazem operação de tratamento de dados – independentemente do meio de tratamento, do país de sua sede ou do país de origem dos dados, desde que estejam localizados no país – passem a ficar obrigadas à respeitar a LGPD.

Essa nova realidade pode modificar bastante o cenário mercadológico não só em âmbito nacional, mas também global, tendo em vista que os modelos de negócios desenvolvidos com base no uso de dados precisarão instituir novos procedimentos de tratamento que obedeçam às novas regras.

Evolução informacional: o aumento da importância da informação

Com o desenvolvimento social, a informação foi ganhando cada vez mais importância na sociedade, de modo que, a partir da Revolução Informacional ao fim do século XX, essa importância tornou-se bastante significativa culminando em um modelo econômico totalmente centrado nas bases de dados. Conforme já apontava Manuel Castells, em sua obra "Sociedade em Rede", faz parte da realidade da sociedade em rede a constante inovação tecnológica, sendo que as adaptações necessárias a tais inovações passam a seguir o mesmo ritmo acelerado das novidades técnicas[1].

É possível observar que a informação já era notada como um dos ativos de grande relevância da sociedade até antes mesmo do surgimento da Era Digital. Bruno Ricardo Bioni pontua esse fato em sua obra *Proteção de dados pessoais: a função e os limites do consentimento*:

Antes mesmo da criação da Internet, já

se havia constatado o papel de centralidade da informação para otimizar o desenvolvimento econômico. Com o *taylorismo*, passou-se a estudar o próprio processo de produção, investindo-se, por exemplo, em treinamento dos operários para se alcançar melhores taxas de produtividade. Portanto, desde a sociedade industrial, já se reconhecia a informação como um fator determinante para a geração de riquezas[2].

Apesar dessa notável constatação, o que não se imaginava é que a sociedade iria modificar tanto as suas relações em razão do desenvolvimento técnico-científico que as suas redes de relação se desfragmentariam em diversos grupos com possibilidade de comunicação e interação praticamente independentes de tempo e espaço.

Conforme afirma Hugo Moreira Lima Sauaia, em sua obra *A proteção dos dados pessoais no brasil*,

> [...] há um rompimento das redes de segurança, tecidas e sustentadas agora individualmente, o apoio oferecido anteriormente pela família, pelos amigos próximos [...] onde se poderia buscar auxílio para remediar as lesões provenientes do trabalho e das limitações humanas, parece não mais subsistir[3].

Esse rompimento é sentido também no que concerne à segurança e à estabilidade das relações, trazendo reflexos diretos ao funcionamento da sociedade. O que se observou foi que, com o advento da Internet e a disseminação de seu uso, a relações sociais se tornaram mais fluídas e instáveis, caracterizadas como relações líquidas, impalpáveis e imprevisíveis, na visão de Bauman[4].

Essa instabilidade foi transmitida aos meios digitais que, por sua própria natureza virtualizada, tornaram as noções de ação e reação inerentes ao comportamento humano menos identificáveis. Por outro lado, os riscos tornaram-se menos visíveis, dificultando assim a proteção das pessoas no meio digitalizado.

A risco crescente à segurança da informação e a necessidade de ter um maior padrão de controle para proteção das informações pessoais depositadas em confiança nas instituições, passaram a exigir uma regulamentação que pudesse trazer algumas garantias mínimas para os titulares bem como alguns novos direitos que permitissem o seu empoderamento no tocante a um maior poder de decisão sobre o uso de suas informações pessoais.

Daí o surgimento do movimento contemporâneo em prol da proteção dos dados pessoais em todo o mundo e a a construção de um novo framework legal através de legislações específicas, com grande necessidade de harmonização para se adaptarem às normas já existentes bem como adequar os modelos de negócios do contexto digital da economia para que a proteção de dados pessoais seja possível de forma efetiva e eficaz e com respeito aos direitos fundamentais prevalentes no documento constitucional:

> [..] a compreensão das mais diversas legislações acerca da proteção dos dados pessoais dentro da nova realidade digital precisou evoluir e foi se modificando ao longo dos últimos 30 anos, resultando em reflexos diretos na seara jurídica – seja na resolução de conflitos ou na criação de mecanismo

> de suporte para as questões digitais, como: como realizar um contrato na esfera digital? Como proteger a privacidade dos cidadãos dentro do mundo virtual? Qual a responsabilidade das empresas frente ao manuseio e tratamento das informações fornecidas pelos clientes?[5]

A proteção de dados pessoais e a sua relação com os direitos fundamentais

O surgimento da LGDP no Brasil tem íntima relação com a necessidade de atualização do arcabouço regulatório nacional frente aos impactos socioeconômicos trazidos com a evolução tecnológica. De forma mais ampla, pode-se afirmar que o nascimento de regulações específicas para a proteção dos dados pessoais em países de todo o mundo é resultado da associação: evolução x expansão dos direitos humanos com a atualização e consequente adaptação de documentos internacionais de proteção aos direitos humanos[6].

Com isso em vista, afirma-se que os instrumentos de regulação dos dados pessoais surgem com o objetivo de proteger direitos fundamentais como: privacidade, intimidade, honra, direito de imagem e a dignidade humana. Acrescenta-se ainda que tais mecanismos têm ligação direta com a internacionalização dos direitos humanos vivenciada pelo mundo contemporâneo, conforme pontua Leandro Alvarenga Miranda, em sua obra *Proteção de dados pessoais e o paradigma da privacidade*: "A preocupação com a privacidade é histórica e remonta aos primórdios das culturas hebraica, grega e chinesa. [...] a evolução das normas e a criação da codificação vieram acompanhadas da consolidação dos direitos individuais do homem"[7].

Tal relação é tão clara que o GDPR aponta no art. (1) que toma por base o artigo 8º, n. 1 da Carta dos Direitos Fundamentais da União Europeia e o artigo 16º, n. 1 do Tratado sobre o funcionamento da União Europeia para a criação do novo regulamento de proteção de dados europeu.

E, embora o instrumento regulatório brasileiro não faça menção direta à documentos específicos que originam o seu teor, é notável a influência de alguns tratados internacionais de que o Brasil é signatário e que – de certa forma – trazem a questão dos dados pessoais em seu texto.

Entre esses documentos é possível citar: a Convenção de Berna de 1886 que já trazia a questão da base de dados em seu texto, ainda que de maneira indefinida e incipiente; o Acordo sobre Aspectos dos Direitos de Propriedade Intelectual relacionados ao Comércio (TRIPS – aprovado no Brasil em 1994) pontua no artigo 10 (2) que as compilações de dados devem receber o mesmo tratamento da criação intelectual, embora não se aprofunde em relação à proteção pessoal dos dados compilados.

A proteção aos direitos fundamentais também é visualizada através o art. 2º da LGPD, no qual são mencionados princípios encontrados no texto constitucional brasileiro como cerne do desenvolvimento de todo e qualquer tratamento de dados pessoais. Dentre os artigos constitucionais que podem ser relacionados com os princípios apontados no art. 2º da LGPD destacam-se os art. 3º, I, II; art. 4º, II; art. 5º, X, XII; art. 7º, XXVII; art. 219[8].

Da mesma forma, o GDPR pontua que o regulamento toma por base os direitos

fundamentais e que visa proteger e garantir a privacidade, liberdade, segurança, justiça das pessoas, assim como promover o progresso econômico e social, além de garantir a segurança jurídica dos países, através do preâmbulo (1), (2), (13)[9] e art. 1º (2)[10].

Breve histórico da proteção de dados pessoais no Brasil

O Brasil já previa certa proteção aos dados pessoais em suas normas internas através dos seguintes: i) Código de Defesa do Consumidor – no art. 43[11]; ii) Decreto 7.962 de 2013 (LGL\2013\2685) (Comércio Eletrônico) – no art. 4º, VII[12]; iii) Marco Civil da Internet – no art. 7º, I, III, VII, VIII, IX, X, XI e art. 11[13] § 1º, § 2º[14].

Todavia, com o rápido desenvolvimento e expansão da tecnologia em todo o mundo, surgiu a necessidade de criação de leis específicas para a proteção desses dados. Isso porque na nova realidade da Era Digital, os dados são uma nova forma de riqueza, de modo que a atuação das empresas dentro do contexto digital passou a necessitar da criação de mecanismos de regulação e proteção dos dados pessoais dos usuários.

Em 2018, o Brasil passou a fazer parte do grupo dos países dotados de um Lei Geral de Proteção de Dados (LGPD) através da sanção da Lei 13.709, de 14 de agosto de 2018 (LGL\2018\7222). Nota-se que o principal objetivo da lei foi a atualização dos mecanismos regulatórios do país frente às necessidades surgidas com o desenvolvimento e expansão da tecnologia e aumento cada vez mais expressivo da coleta, processamento, transmissão e armazenamento de dados no ambiente virtual.

Também é necessário pontuar que a "corrida" aprovação da lei foi visivelmente influenciada pelo início da vigência do GDPR em 25 de maio de 2018, tendo em vista que a discussão em torno da regulamentação de dados pessoais teve início em 2010 no Brasil, por meio da abertura de uma consulta pública por parte do Ministério da Justiça. O resultado desta consulta foi a criação do Projeto de Lei 4.060, de 2012, que mais à frente recebeu em anexo o Projeto de Lei 5.276 de 2016.

Depois de muita conversa e questionamentos acerca das ideias propostas chegou-se ao Projeto de Lei da Câmara 53/18 que gerou a Lei 13.709. É notável que o texto da LGPD é amplamente inspirado pelo GDPR, embora o regulamento nacional seja mais enxuto e traga em seu conteúdo regras mais abertas do que o proposto pela União Europeia.

Ao sancionar a Lei 13. 709/2018 o Presidente Temer vetou alguns artigos que se mostravam incongruentes com a Constituição Nacional, como a criação de um órgão regulador, procedimento que só pode ser iniciado pelo executivo e estava com um erro em sua iniciativa ao ser proposto pela Câmara.

Com a atualização do corpo legislativo nacional em relação à proteção de dados pessoais, a LGPD passa a trazer completa proteção aos dados pessoais em qualquer mídia ou suporte, com a exigência do consentimento prévio e expresso para as hipóteses de tratamento (a não ser que recaia em alguma exceção) e não mais apenas aos capturados em plataforma digital (como podia haver o entendimento neste sentido no tocante a interpretação do Marco Civil da Internet), conforme deixa claro o art. 1º[15].

Determinações da nova lei de proteção

de dados

Na medida em que a economia digital gira em torno dos dados pessoais, é preciso delimitar alguns limites e melhores práticas, para proteção do consumidor e evitar inclusive concorrência desleal. As novas regras vêm com um escopo de permitir que a livre iniciativa possa inovar desde que siga uma cartilha de valores que estejam condizentes com o respeito aos direitos humanos fundamentais, mas acima de tudo, que aja com a máxima transparência possível no tocante ao uso (tratamento) dos dados pessoais.

Toda a redação da regulamentação de proteção de dados pessoais tem como principal linha condutora a transparência. Ou seja, mesmo nas hipóteses em que não é exigido o consentimento prévio e expresso há que ser transparente sempre.

Assim, a regulamentação traz novos direitos para os titulares e, por sua vez, obrigações às empresas, como: permitir que o usuário tenha a possibilidade de acesso ao dado que está sendo tratado, de retificação, portabilidade dos dados para outra empresa, apagamento até oposição ao tratamento realizado.

Além disso, exige aplicação de medidas técnicas e administrativas que garantam a proteção dos dados pessoais, mesmo sem detalhais quais sejam, procedimentos de governança, atualização de políticas e normas e camada de gestão, já que é preciso nomear uma pessoa que será responsável pela relação com as autoridades.

As organizações devem estar prontas para cumprir essas adequações, com um canal apropriado para receber e dar andamento às solicitações de modo que alcance todos os seus sistemas e empresas para as quais os dados foram compartilhados. Ou seja, precisam avaliar seu ambiente e verificar se está preparada para estar aderente à legislação.

Claramente que a LGPD também traz exceções: a lei não se aplica quando o tratamento dos dados é realizado por uma pessoa física, para fins exclusivamente particulares e não econômicos, para fins exclusivamente jornalísticos e artísticos, e para tratamentos realizados para fins de segurança pública e defesa nacional.

Um outro aspecto relevante a citar é o de que o dano anonimizado, conforme previsto pelo artigo 5º, não é considerado um dado pessoal, logo, deixa de estar passível de proteção conforme a lei.

Caso haja infrações, as sanções administrativas envolvem advertência, com indicação de prazo para adoção de medidas corretivas; multa simples, de até 2% do faturamento da empresa (limitada, no total, a R$ 50 milhões por infração); publicização da infração após devidamente apurada e confirmada a sua ocorrência; bloqueio dos dados pessoais a que se refere a infração até a regularização da atividade de tratamento pelo controlador; eliminação dos dados pessoais a que se refere a infração; suspensão parcial ou total do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 meses, suspensão, proibição parcial ou total do exercício da atividade de tratamento dos dados pessoais.

Relevância da lei em um contexto globalizado

Como já foi destacado, um dos fatores que pressionou essa corrida legislativa em

vários países foi a entrada em vigor do General Data Protection Regulation (GDPR) na União Europeia, em maio deste ano. Isso porque o Estado que não possui lei de mesmo nível pode passar a sofrer algum tipo de barreira econômica ou dificuldade de fazer negócios com os países da região. Considerando o contexto econômico atual, este é um luxo que a maioria das nações, especialmente os da América Latina, não podem se dar.

Os efeitos da GDPR são principalmente econômicos, sociais e políticos. É apenas uma das muitas regulamentações que vão surgir nesta linha, onde se busca trazer mecanismos de controle para equilibrar as relações dentro de um cenário de negócios digitais sem fronteiras.

Portanto, não apenas virão regras sobre proteção de dados pessoais, mas também sobre demais usos de tecnologia com alto impacto na sociedade, tais como a Inteligência Artificial, a robotização, o Blockchain, entre outros. Há uma grande preocupação em um modelo de "dados abertos" (*Open Society*) com cibersegurança. Pois não dá mais para continuar com puxadinhos digitais, como quando vimos casos de vazamentos de dados que foram mantidos anos em segredo.

A importância da lei, resumidamente, é o estabelecimento de segurança jurídica para os envolvidos no processo de tratamento de dados, deixando mais claro quais os controles que devem ser aplicados e quais as obrigações e responsabilidades das partes, porque apesar de termos alguma legislação setorial (como as resoluções do Banco Central aplicáveis às Instituições Financeiras, por exemplo), era necessária uma lei que pudesse alcançar a todos, em todos os setores econômicos.

Considerando que o atual estágio tecnológico impõe a análise massiva de dados, a economia digital depende do tratamento de dados pessoais, em especial, serviços e produtos altamente especializados. Afinal, a grande questão não é proibir ou demonizar o uso de dados pessoais pelas empresas. O desafio é fazer isso de forma equilibrada, protegendo a privacidade dos cidadãos, mas sem inviabilizar a inovação e os negócios.

O cidadão deve ter o direito de ser proprietário da sua própria informação e poder negociar livremente a mesma. O governo e as empresas podem tratar dados, mas o indivíduo tem o direito de saber quais dados estão sendo coletados e com quem estão sendo compartilhados e para quais finalidades. Deve haver uma base de princípios e regras a serem seguidas, e respeitar a capacidade jurídica de se contratar e a liberdade para tanto. Por isso, novamente, o princípio norteador é o da transparência muito mais que qualquer outro.

Afinal, as relações negociais dependem diretamente dos dados se desenvolverem, para garantir a segurança jurídica das partes, evitar golpes, fraudes, inadimplência e oferecer melhores experiências na oferta de produtos e serviços, otimizando mão de obra e especializando negócios. Informação verdadeira e transparente, utilizada de forma legítima e proporcional, garante crescimento econômico e social.

Planejamento estratégico e aplicabilidade

Passada a primeira etapa de ter uma lei ou regra sobre o tratamento dos dados, agora é hora de educar o mercado. Esse tipo de legislação é evolutiva e leva um tempo de amadurecimento. Apesar do prazo que foi

conferido de adaptação, é sabido que levará mais tempo para promover toda a mudança necessária de modo a se atender as novas exigências.

Além disso, a conformidade à proteção de dados é o tipo de projeto contínuo, que exigirá uma revisitação da pauta periodicamete, visto que os negócios estão também em transformação, assim como a tecnologia, trazendo inovação e novas funcionalidades, logo o que é feito hoje sofrerá alterações em curto espaço de tempo e os procedimentos bem como a documentação sobre proteção de dados pessoais, precisará de atualização em intervalos não superiores a dois anos, especialmente no tocante às políticas de privacidade, termos de uso e contratos.

Logo, ter a lei é apenas o começo de uma longa jornada que teremos que atravessar tanto no âmbito público como privado. Atender aos requisitos da nova lei exige investimento, atualização de ferramentas de segurança de dados, revisão documental, melhoria de processos e, acima de tudo, mudança de cultura.

Mostrar aos gestores, profissionais das áreas de compliance, jurídico, analytics, ciência de dados, tecnologia da informação, segurança da informação, negócios e marketing a importância de estarmos alinhados com o contexto de Transformação Digital, ao garantir a competitividade econômica com os países que já regulamentaram os ativos mais valiosos da Sociedade da Informação.

Mais que isso, é incorporar uma cultura empresarial que aplique e valorize as melhores práticas de gestão para atingir a compliance de dados. Enaltecer as razões e a necessidade de mecanismos de controle para equilibrar as relações dentro de um cenário de negócios digitais sem fronteiras. A linha mestra é a garantia da liberdade, mas a base é a transparência.

Os bens de conhecimento estão nas grandes bases de dados e para esse tratamento é necessário transparência, reter dados pessoais com a justificativa legal compatível e anomização. Vamos mostrar como construir uma cultura de proteção para manter a valorização dos ativos intangíveis e das ações. O investidor precisa de proteção e de blindagem legal do patrimônio e da reputação. Vivemos uma nova era de mais responsabilidade, onde tecnologia e informação resultam em poder.

Desdobramentos e consequências

A LGPD traz um grande impacto social e econômico, especialmente sobre sistema da pequena empresa e startups. Tanto por que traz exigências que aumentam os custos empresariais e passam a ter que entrar na prioridade dos gestores (*road map)* mas como também exigem alguns processos de governança corporativa (de TI, de Segurança de Informação, de Gestão de Dados) que não eram tão comuns neste ambiente e que podem até dificultar (burocratizar) suas atividades que estão mais acostumadas com leveza e velocidade.

Ademais, o cidadão, que é o titular precisará saber mais sobre o que é proteção de dados pessoais, o que vai exigir investimento em campanhas educativas e orientativas.

O conceito de *privacy by design* é um grande desafio para ser implementado e deve passar a ser ensinado nas Universidades, pois é a melhor forma de garantir a sustentabilidade do modelo trazido pelo novo Marco Legal.

Um fator de complexidade adicional na temática da proteção de dados pessoais é não

ser um Tratado Internacional. Ou seja, acaba exigindo que as instituições e as empresas precisem realizar todo um trabalho de análise comparada das legislações para poderem se adequar dependendo de como é o seu modelo operacional.

Apesar de vivermos uma sociedade globalizada, da internet ser um grande território internacional e de se querer permitir o livre fluxo de dados, em matéria de proteção de dados pessoais acabou-se utilizando os mecanismos das leis nacionais e dos regulamentos regionais, e esta é a maior crítica que se pode ter quanto ao desdobramento que se teve deste assunto. Vamos esperar que para o futuro, os temas de grande impacto como da Inteligência Artificial possam alcançar um tratamento mais internacional e evitar a solução país a país.

Bibliografia

AGÊNCIA CÂMARA NOTÍCIAS. Comissão discute marco regulatório para a proteção de dados pessoais. *Agência Câmara Notícias*, maio 2017. Disponível em: [www2.camara.leg.br/camaranoticias/noticias/ciencia-e-tecnologia/534978-comissao-discute-marco-regulatorio-para-a-protecao-de-dados-pessoais.html]. Acesso em: mar. 2018.

ALCANTARA, Larissa de. *Tecnologia e inovação*: big data e internet das coisas. São Paulo: Bok2, 2017.

ARTICLE 19. *Proteção de dados pessoais no Brasil*: análise dos projetos de lei em tramitação no Congresso Nacional. 2016. Disponível em: [http://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Prote%C3%A7%C3%A3o-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf]. Acesso em: mar. 2018.

ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE SOFTWARES. *Brasil, país digital [site*]. Disponível em: [https://brasilpaisdigital.com.br/]. Acesso em: mar. 2018.

BAUMAN, Zygmunt. *O mal-estar da pós-modernidade.* Rio de Janeiro: Zahar, 1997.

BIONI, Bruno Ricardo. *Proteção de dados pessoais:* a função e os limites do consentimento. Rio de Janeiro: Forense, 2018.

CASTELLANO, Ana Carolina H.; FORNARA, Matheus Tormen. Startaups, Cibersegurança e Proteção de Dados. *Jota*, 25 maio 2017. Disponível em: [www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/startups-ciberseguranca-e-protecao-de-dados-25052017]. Acesso em: mar. 2018.

CASTTELLS, Manuel. *A sociedade em rede.* São Paulo: Paz e Terra, 2009.

COSTA, Larissa Carolina Lotufo da; COSTA, Vinicius Lotufo da. *Regulamentação da proteção de dados pessoais no Brasil:* breve histórico, impactos legais e realidade brasileira. In: Anais do I Congresso de Direito Propriedade Intelectual e Desenvolvimento Econômico-Social. Franca: Unesp, 2018.

COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais Comentada.* São Paulo: Ed. RT, 2018.

GREENWALD, Glenn. Why privacy matters? *Ted Talks*, 10.10.2014. Disponível em: [www.youtube.com/watch?v=pcSlowAhvUk]. Acesso em: mar. 2018.

LEMOALLE, Edouard; CARBONI, Guilherme. Lei Europeia de Proteção de Dados e seus efeitos no Brasil. *Jota*, 12.02.2018. Disponível em: [www.jota.info/opiniao-e-analise/artigos/lei-europeia-de-protecao-de-dados-pessoais-gdpr-e-seus-efeitos-no-brasil-12022018]. Acesso em: mar. 2018.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coord.). *Comentários ao GDPR*: Regulamento Geral de Proteção de Dados da União Europeia. São Paulo: Ed. RT, 2018.

MIRANDA, Leandro Alvarenga. *A proteção de dados pessoais e o paradigma da privacidade*. São Paulo: All Print Ed., 2018.

PINHEIRO, Patrícia Peck. *Direito digital*. 6. ed. rev. atual e amp. São Paulo: Saraiva, 2016.

PINHEIRO, Patricia Peck. *Proteção de dados pessoais:* comentários à Lei n. 13. 709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

REUTERS. Privacy issues emerge as major business risk for Facebook. *New York Times*, 19.03.2018. Disponível em: [www.reuters.com/article/us-facebook-privacy-costs-analysis/privacy-issues-emerge-as-major-business-risk-for-facebook-idUSKBN1GW01F]. Acesso em: mar. 2018.

ROSATI, Florencia; PETRINELLI, Ludmilla. Tracking privacy trends in Latin America in the age of the GDPR. *Cecile Park Media*, fev. 2017. Disponível em: [www.ebv.com.ar/images/publicaciones/dplfebruary2017estudiobeccarvarela.pdf]. Acesso em: mar. 2018.

SAUAIA, Hugo Moreira Lima. *A proteção de dados pessoais no brasil.* Rio de Janeiro: Lumen Juris, 2018.

SOUZA, Carlos Affonso; LEMOS, Ronaldo; BOTTINO, Celina (Coord.). *Marco civil da internet:* jurisprudência comentada. São Paulo: Ed. RT, 2017.

1 CASTTELLS, Manuel. *A sociedade em rede*. São Paulo: Paz e Terra, 2009.

2 BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2018. p. 9.

3 SAUAIA, Hugo Moreira Lima. *A proteção de dados pessoais no Brasil*. Rio de Janeiro: Lumen Juris, 2018. p. 12.

4 BAUMAN, Zygmunt. *O mal-estar da pós-modernidade*. Rio de Janeiro: Zahar, 1997.

5 COSTA, Larissa Carolina Lotufo da; COSTA, Vinicius Lotufo da. Regulamentação da Proteção de Dados Pessoais no Brasil: breve histórico, impactos legais e realidade brasileira. *Anais do I Congresso de Direito Propriedade Intelectual e Desenvolvimento Econômico-Social*. Franca: Unesp, 2018.

6 PINHEIRO, Patricia Peck. *Proteção de dados pessoais*: comentários à Lei n. 13. 709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

7 MIRANDA, Leandro Alvarenga. *A proteção de dados pessoais e o paradigma da privacidade*. São Paulo: All Print Ed., 2018. p. 19-20.

8 Art. 3º Constituem objetivos fundamentais da República Federativa do Brasil: I – construir uma sociedade livre, justa e solidária; II – garantir o desenvolvimento nacional.Art. 4º A República Federativa do Brasil rege-se nas suas relações internacionais pelos seguintes princípios: [...] II – prevalência dos direitos humanos.
Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; [...] XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; [...]
Art. 7º São direitos dos trabalhadores urbanos e rurais, além de outros que visem à melhoria de sua condição social: [...] XXVII – proteção em face da automação, na forma da lei.
Art. 219. O mercado interno integra o patrimônio nacional e será incentivado de modo a viabilizar o desenvolvimento cultural e socioeconômico, o bem-estar da população e a autonomia tecnológica do País, nos termos de lei federal. Parágrafo único. O Estado estimulará a formação e o fortalecimento da inovação nas empresas, bem como nos demais entes, públicos ou privados, a constituição e a manutenção de parques e polos tecnológicos e de demais ambientes promotores da inovação, a atuação dos inventores independentes e a criação, absorção, difusão e transferência de tecnologia.

9 (1) A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. [...](2) Os princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente o direito à proteção dos dados pessoais. O presente regulamento tem como objetivo contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união económica, para o progresso económico e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares.
(13) A fim de assegurar um nível coerente de proteção das pessoas singulares no conjunto da União e evitar que as divergências constituam um obstáculo à livre circulação de dados pessoais no mercado interno, é necessário um regulamento que garanta a segurança jurídica e a transparência aos operadores económicos, incluindo as micro, pequenas e médias empresas, que assegure às pessoas singulares de todos os Estados-Membros o mesmo nível de direitos suscetíveis de proteção judicial e imponha obrigações e responsabilidades iguais aos responsáveis pelo tratamento e aos seus subcontratantes, que assegure um controlo coerente do tratamento dos dados pessoais,

sanções equivalentes em todos os Estados-Membros, bem como uma cooperação efetiva entre as autoridades de controlo dos diferentes Estados-Membros. [...]

10 Artigo 1.º Objeto e objetivos [...] 2. O presente regulamento defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais.

11 Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de 5 (cinco) dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público. § 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores. § 6º Todas as informações de que trata o *caput* deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor.

12 Art. 4º Para garantir o atendimento facilitado ao consumidor no comércio eletrônico, o fornecedor deverá: [..] VII – utilizar mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor.

13 Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I – inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; [...] III – inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; [...] VII – não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; VIII – informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; IX – consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; X – exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre

as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei; XI – publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet; [...] Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. § 1º O disposto no *caput* aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil. § 2º O disposto no *caput* aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

14 PINHEIRO, Patrícia Peck. *Direito digital*. 6. ed. rev. atual e amp. São Paulo: Saraiva, 2016.

15 Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, *inclusive nos meios digitais*, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural", grifo nosso.

Publicado originalmente na Revista dos Tribunais, São Paulo, v.108, n.1000, p.309-323, fev.2019.

A PROTEÇÃO DE DADOS NO CONTRATO DE TRABALHO

Antônio Carlos Aguiar

RESUMO

As mudanças sociais que impactaram em grande medida o Mundo do Trabalho são inevitáveis e já se consolidaram. Os novos desafios envolvem, nesse cenário, também, os dados pessoais, petróleo do século XXI, antes mesmo de se formar qualquer vínculo de trabalho e após o encerramento da relação. Essa nova dinâmica e os fundamentos legais que se formaram exige a transição do direito social restrito para a aplicação prático-estrutural atual, se fazendo necessária a compreensão dos novos atores nessa nova realidade que nos desafia com novos desdobramentos jurídicos e factuais que devem ser avaliados sob as perspectivas jurídico-protetivas.

Palavras chave: direito do trabalho; impactos tecnológicos; proteção de dados; privacidade; autodeterminação informativa.

1. Introdução: Purgatório de Dante

"Só para lembrar, Henry Ford aplicou os princípios da administração científica de Taylor e Fayol em sua empresa e revolucionou o mundo. Temos produtos em nossas casas graças à implementação de três paradigmas fundamentais dessa escola: 1. Linha de produção com a micro divisão de atividades; 2. Adestramento da mão de obra para a execução de tarefas simples; 3. Controle dos 'tempos e movimentos' em busca de maior produtividade. Em outras palavras, uma estrutura organizacional hierárquica na qual há uma turma que mantenha e pensa, outra que obedece e vigia uma terceira com juízo suficiente para executar tudo isto".

E ainda hoje as empresas e, portanto, os efeitos reflexivos desta padronização organizacional se espraiam perante os contratos de trabalho, adotam essas regras. Isso, em um ambiente de trabalho onde a um simples clique, é possível, via internet, ter acesso a tudo, desde manuais, dicas, questionários, chegando a impressoras digitais que replicam (muito) mais barato o produto que o empregado "adestrado pelo modelo tradicional de linha de produção" trabalha diuturnamente.

Aqui está um dos pontos principais de destaque a ser enxergado e visitado: o limbo

Antônio Carlos Aguiar

Doutor em Direito do Trabalho pela Pontifícia Universidade Católica de São Paulo – PUC/SP. Mestre em Direito do Trabalho pela Pontifícia Universidade Católica de São Paulo – PUC/SP. Especialista em Direito do Trabalho pela Universidade de São Paulo – USP

estrutural que cerca as relações de trabalho neste momento de transição (em velocidade exponencial) do recém passado ao presente (novo e pouco conhecido), com a precária utilização, na grande maioria das vezes, de instrumentos que não já não mais se encaixam neste status quo pós-moderno.

Vivenciamos o Purgatório de Dante, utilizando-se de licença poética, o meio do caminho – entre esse passado e o futuro (já presente) –, ou seja: "Saídos do Inferno, e da Terra, por um longo e tortuoso caminho subterrâneo, atravessado por um arroio que eles acompanham contra sua corrente, e chegados ao ar livre da praia do Purgatório, Dante e Virgílio se encantam com a visão da noite estrelada, especialmente com as quatro estrelas que correspondem, no céu austral, à constelação da Ursa Menor no céu setentrional. Encontram, logo mais, o guardião do Purgatório, que é Catão de Útica, o famosos legista da república de Roma antiga, o qual interpela, maravilhado e suspeitoso pela maneira insólita de sua chegada ao Purgatório, vindo necessariamente do Inferno, mas acaba aceitando as explicações de Virgílio e fornecendo-lhes todos os ensinamentos para seu novo cometimento" .

Precisamos conversar com o Guardião. Por favor, Catão de Útica do Purgatório Digital nos atenda.

Necessitamos de uma espécie de guia que se materialize por meio de um observatório digital das relações de trabalho, em especial, que nos faça compreender e trabalhar com todas as miudezas, desdobramentos e efeitos (positivos e negativos) que fazem parte do chamado petróleo do século XXI, segundo a revista britânica The Economist, vale dizer, os dados pessoais: por quem, como e por que. Caminhemos por entre os estágios dessa montanha .

2. Primeiro estágio: fase pré-contratual

Atualmente até a busca por uma ocupação ou recolocação profissional está diferenciada. Quem ainda manda pelo correio ou entrega pessoalmente um currículo expresso? Aliás, cabe outra pergunta: o que mesmo deve conter neste currículo (digital)?

Hoje por meio do espaço cibernético encontra-se tudo. Ele é tutorial. Um grande "supermercado digital" demonstrando as praticidades do como fazer. Vídeos explicativos, aulas, manuais, pórticos exemplificativos, etc. Uma interessante vitrine de mecanismos de atuação variados. A pergunta (outra) que fica é: mecanismo de ajuda/apoio ou de padronização/stantardlização? Estaríamos impedindo que Óblio possa manifestar e ser auto-criativo?

Comporte-se bem e adequadamente. Entrevistas de candidatos a emprego. Quantas "dicas" são dadas/oferecidas aos candidatos, a fim de que "se comportem bem" numa entrevista. Que impressionem. Apresentem o "seu melhor". Que apresentem suas "qualificações e qualificativos" que retratem quem ele é (ou quer/deva ser). E todas essas informações serão "guardadas numa 'caixinha'".

Essa abordagem é identificada para destacar que a base de informações obtidas, antes mesmo do início de uma relação de trabalho, por parte do empregador (pelo mercado e/ou mídias sociais), é indutiva e, por via reflexiva, invasiva na vida da (na) vida privada do entrevistado; da nossa vida...

Passam por esse estágio perguntas pessoais, personalíssimas, que, por vezes,

vão bem além daquilo que necessária e obrigatoriamente deveria o empregador ter acesso informativo para a prestação de um serviço que poderá (ou não) num futuro ser-lhe fornecido.

Vão desde com quem mora: filhos, cônjuge, pais, amigos, etc., até para que time torce; religião que professa; opinião política, redes sociais que está presente, gostos, cultura, prática esportiva, hobby, rituais, amigos (network), e daí por diante, passando, é claro, pelo básico, ou seja, escolaridade e experiência profissional anterior, tudo por meio de mecanismos "científicos" de avaliação e "constatação" direta, como: capacidade profissional, experiência, formação direta e indireta (nível de empatia, comportamento em equipe, resiliência e empregabilidade), por exemplo.

Aliás, no que se refere à experiência anterior, juntamente com o grau técnico de sua avaliação, são acompanhados questionamentos outros, como a razão da sua saída, procedidos do porquê da escolha de um novo e eventual empregador, acrescidos, de modo sútil e aparentemente inocente, de outras perguntas, que têm o fito de saber se o candidato tem algum tipo de vício, se apresenta algum problema de saúde pessoal e/ou familiar, se tem espírito questionador, tudo devidamente atrelado aos seus hábitos nos empregos anteriores, como qual frequência/necessidade de uso de smartphone, como entende as ordens e orientações recebidas, faltas ao serviço e assim por diante.

Questiona-se, ainda, onde mora e a distância de sua casa até a empresa, bem como quantas conduções são necessárias ao deslocamento, não somente para fins de cálculos relacionados a custos, como com vale transporte, mas, também, como um meio de monitoramento relacionado a futuros e possíveis atrasos.

Ao final, a entrevista é encerrada e dela advém um resumo, um fechamento opinativo quanto à avaliação (subjetiva ou por meio de algum programa – ou algoritmo) da personalidade do candidato: pessoa calma, paciente, "resiliente", "promissora", agitada, ansiosa, dinâmica, criativa, com iniciativa, identificando – segundo os critérios de quem o avaliou – os seus pontos positivos e negativos.

Esse relatório conclusivo serve à contratação ou não da pessoa.

As perguntas que ficam a partir desse complexo processo, são: qual o destino dessa profícua e detalhada fonte de informações dessa pessoa? Qual o compromisso de sigilo daqueles que as obtiveram, que estiveram envolvidos neste procedimento? Qual a garantia do entrevistado de que seus dados pessoais não serão abertos (ou conhecidos) por terceiros? Qual a proteção jurídica desses dados pessoais? Qual a diferenciação de tratamento (se existente) dessas informações, entre os contratados e os não-contratados (e o critério de acesso)? Se existente, qual ou quais os motivos jurídicos para isso?

3. Segundo estágio: vigência do contrato de trabalho.

Parabéns: você foi aprovado na entrevista, de candidato torna-se um colaborador efetivo. Passa, muitas vezes, a ter convênio médico e a empresa, prestadora desses serviços, ilimitado acesso a toda a sua condição físico-mental (por vezes, da sua família também). Internamente,

tem direito ao uso de ferramentas digitais (e espaço para arquivamento de fotos, vídeos e outros documentos pessoais), tudo e por óbvio, armazenado e guardado por constantes backups efetuados pelo empregador em suas máquinas (os computadores, smarthphones, tablets, etc. continuam sendo de propriedade do empregador) – pelo menos, essa é a regra (que, claro, comporta exceções).

Se o empregado prestar serviços externos ou em home office poderá (se não houver explícita ordem em sentido contrário) se utilizar de rede wi-fi pública e/ou gratuita. Estará (o risco é grande e efetivo), contudo, trabalhando e possivelmente disponibilizando informações confidenciais para quem não deveria nesta hipótese. Será que ninguém lhe disse que isso não era seguro? Não há alguma política interna ou disposição contratual alertando-o para esse fato de risco? A necessidade dessas prévias comunicativas é importantíssima, diante dos reflexos negativos que podem desdobrar-se da sua (má) utilização.

Por falar em política interna será que há alguma disciplinando como ele deve usar (ou não usar) os aparelhos que lhe são ofertados para o trabalho, como computadores, smarthphones, tablets, etc.? E mais: que eles serão considerados como ferramenta de trabalho e, portanto, sujeitos à fiscalização e controle? Condição que implica análise e verificação de (por) terceiros de fatos, fotos e comportamentos íntimos?

Ou mais ainda: que o empregador poderá, ao longo do contrato, obter informações estritamente pessoais relacionadas ao comportamento geral do empregado, geradoras de fórmulas que lhe permitem avaliar e assegurar a sua produtividade, influenciando diretamente na sua carreira profissional, sem que tenha possibilidade de um "contraditório" quanto ao subjetivo entendimento daquele que detém acesso a essas informações?

Ainda com relação ao uso do wi-fi aberto para clientes apenas com senha sem identificação, a empregadora teria explicitado sobre os riscos de a sua utilização poder ser tratada em determinadas situações como crime virtual – além do acesso indevido por terceiros das informações contidas no aparelho? – como, por exemplo, um roubo de identidade e de senha, com a utilização das informações pessoais para realizar compras online ou efetuar transações financeiras de forma indevida. Ou, então: a) falsa identidade; b) calúnia, injúria ou difamação na internet; c) estelionato; d) pirataria; e) discriminação (comentários preconceituosos de cunho racista, sexista, homofóbico, transfóbico, etc.); e) pedofilia.

A lista é grande.

4. Terceiro estágio. "Fim do casamento": depois da rescisão contratual

Terminada a relação teria o empregado um salvo conduto relativo a uma espécie de direito ao esquecimento? Seus dados pessoais são seus e de mais ninguém. Logo, tudo que estiver (se previamente autorizado para tanto) guardado em seu maquinário deverá ser-lhe entregue por meio de pendrive ou mídia equivalente, com garantia de não armazenamento por parte do empregador.

Há de se observar, ainda, outros aspectos periféricos e reflexivos supervenientes ao fim do contrato, não diretamente ligados ao arquivo/guarda de "coisas" pessoais. A

relação profissional que foi mantida entre empregado e empregador é originária de um contrato sinalagmático, limitado tão somente àqueles que o constituíram, à vista do seu caráter de direitos e obrigações exclusivas aos envolvidos. Salvo informações de índole estatal, que obrigatoriamente devem ser guardadas e eventual ou periodicamente repassadas à fiscalização do Estado, a fidúcia contratual obriga as partes que respeitem a individualidade personalíssima do contrato. Não é juridicamente admissível e possível repassar a terceiros dados e/ou informações sem a anuência do seu titular.

O que fica, para estudo e avaliação jurídica, é o como, ou seja, a instrumentalização de mecanismos eficazes de controle, para efetividade deste comando ético, à vista da ruptura contratual havida no relacionamento entre as partes. Único, diga-se de passagem, elo jurídico e factual que as ligava.

Sem dúvida alguma, é importantíssima a celebração de mecanismos jurídicos de vazão eficaz para essa garantia. Eles podem perpassar por aditivos contratuais; compromissos expressos pós-contratuais, com cláusulas restritivas de liberdade; acordos coletivos de trabalho; políticas internas de compliance; e tudo mais que tenha o condão de limitar (pelo menos mitigar) o conteúdo comunicativo dessas informações/dados pessoais e profissionais dos envolvidos ausentes, diante da ruptura do laço contratual.

Não há aqui que se esperar bom senso ou outra medida moral subjetiva. Deve-se, ao contrário, exteriorizar e expressar categoricamente os entendimentos e seus limites. Somente assim, se terá o respeito jurídico necessário e a possibilidade de reparo, diante de uma eventual e futura infração.

5. Proteção de dados: uma garantia jurídica

Quando se fala em proteção, dentro de um contexto social permeado por questões tecnológicas, o que está em jogo não é a construção de meios e formas que garantam ao indivíduo (a pessoa humana) uma proibição plena quanto ao acesso à sua vida privada; à sua intimidade (algo como: me deixe em paz).

O que é possível e deve ser respeitado é outro modo garantidor, qual seja o controle. Dispositivos legais que delimitem o acesso e uso dos seus dados pessoais, formadores da sua identidade e personalidade, que protejam o segredo (se assim a pessoa o quiser) sobre esses dados; sobre o fluxo dessas informações.

Muito embora no Brasil não exista uma regulamentação específica acerca da proteção de dados, a tutela privada de direitos da personalidade do trabalhador tem sua garantia, com vistas à proteção da dignidade da pessoa humana. Para tanto, observam-se as disposições principiológicas da Constituição Federal, Consolidação das Leis do Trabalho e Marco Civil da Internet.

Por sua vez, a União Europeia, em 27 de abril de 2016, editou normas que compõem o agora chamado General Data Protection Regulation (GDPR). De acordo com o estabelecido, as organizações que manipulam e tratam dados pessoais da Comunidade Europeia tiveram até maio de 2018 para se adequar às novas regras, dois anos após a edição . O GDPR é composto por:

a) Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho – relativo à proteção das pessoas singulares no que diz

respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) ;

b) Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho – 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 ;

c) Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho de 27 de abril de 2016 – relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave .

Em relação ao âmbito de aplicação, devemos ter em mente que o GDPR aplica-se a empresas brasileiras que tratam dados de cidadãos europeus, como, por exemplo, empresas que tenham matriz ou filial europeia, com sistema integrado para tratamento de dados .

Numa relação de emprego, como bem alerta e destaca Tatiana de Almeida Granja , estão presentes princípios próprios do Direito do Trabalho, que impõem limites aos poderes do empregador (direção, hierárquico e de fiscalização), garantidores, portanto, da proteção de dados. Neste sentido, ao destacar, primeiramente, o princípio da irrenunciabilidade de Direitos, ela o faz citando outros dois autores:

Primeiro, a jurista Maria Belén Cardona Rubert , que identifica as possibilidades de tratamento de dados sensíveis:

> "O empresário unicamente poderá proceder ao tratamento automatizado destes dados sensíveis quando, pela natureza do posto, o trabalhador deva realizar tarefas carregadas de um indubitável conteúdo ideológico, devendo ser excluída esta possibilidade no caso de se tratar de tarefas neutras, já que a aptidão para executar ditas prestações não depende da participação do trabalhador na tendência ou linha ideológica da empresa e, portanto, são ilícitas todas as indagações realizadas pelo empresário dirigidas a obter informação relativa a ideologia, crenças religiosas, afinidade política ou sindical do candidato ao emprego ou do trabalhador do quadro que tenha que desenvolver ou desenvolva atividades ideologicamente neutras".

Depois, traz à tona o entendimento de Daniel Martínez Fons :

> "[...]. no que se refere aos dados especialmente protegidos, deve-se ter em conta que a exigência do consentimento na coleta e no tratamento de dados sensíveis não substitui nem neutraliza os direitos fundamentais à intimidade, liberdade religiosa, ideológica e sindical na relação de trabalho. Efetivamente, o requerimento empresarial ao trabalhador de qualquer informação relativa a algum dos aspectos agora citados se sujeita ao princípio da proporcionalidade. Isto significa que deve ser comprovado um interesse relevante no conhecimento da

informação".

A seguir, trata do princípio da qualidade dos dados, evidenciando que por esse princípio "os dados coletados devem ser adequados, necessários e proporcionais (não excessivos) e adequados à finalidade de tratamento a que se destinam. Além disso, eles devem ser, de fato, necessários, indispensáveis e não excessivos ao propósito do tratamento. [...] deve haver proporcionalidade entre as naturezas dos dados levantados e o objetivo do tratamento de dados. Insta registrar que as três exigências relacionadas à qualidade dos dados – adequação, pertinência ou necessidade e proporcionalidade em sentido estrito – correspondem aos três elementos do Princípio da Proporcionalidade".

Depois, completa com o Princípio da Informação, onde "é obrigação do empregador informar a existência e a finalidade do tratamento. É também necessário informar os meios e as fontes que serão utilizadas na obtenção dos dados, bem como as consequências da negativa de consentimento e/ou fornecimento das informações. [...] é mister demonstrar a idoneidade e garantir a transparência do tratamento de dados de caráter pessoal".

Outro princípio por ela relacionado refere-se ao Princípio do Consentimento, onde "em qualquer espécie de tratamento de dados, o consentimento do indivíduo tem importância capital. Trata-se do princípio que legitima todo o tratamento. Ele permite que o afetado controle a utilização de seus dados pessoais, o que se denomina direito à autodeterminação informativa".

Especificamente com relação a esse princípio, uma vez mais, ela se vale das assertivas e preciosas lições de Daniel Martínez Fons , para quem:

> […] o consentimento da pessoa afetada é princípio essencial da relação de tratamento de dados […]. A aplicação de tecnologias que permitam coletar, armazenar e tratar dados de caráter pessoal exige, com caráter geral, o consentimento do afetado […]. Trata-se, portanto, de acordo com a doutrina, do "informed consent", isto é, um consentimento informado e plenamente consciente sobre a relação jurídico-privada que se constrói entre o responsável do ficheiro e o afetado (tradução e grifos nossos).

E completa a relação com os princípios: (i) Princípio da Dignidade da Pessoa Humana; (ii) Princípio da Não-Discriminação; e (iii) Princípio da Boa-Fé.

Para um real e efetivo efeito garantidor, hão de ser habilitados e reconhecidos alguns direitos suplementares: (a) direito de acesso; (b) direitos de retificação e de cancelamento; e (c) direito de oposição.

O empregado tem de ter acesso às informações que lhe dizem respeito. Deve-lhe ser facilitado o conhecimento, com simplicidade de caminhos para obtenção de todas as informações que concernem à sua vida (pessoal e profissional).

Neste sentido, Daniel Martínez Fons assegura que:

> […] não cabe impor restrições indiretas que desestimulem o exercício do direito de acessar; de maneira que se deve rejeitar qualquer prática neste sentido, tais como circunscrever o exercício do direito fora da jornada de trabalho ou que o tempo investido não seja considerado tempo de trabalho, submeter a questionários

> os trabalhadores que querem acessar, nem, enfim, estabelecer um registro autônomo dos trabalhadores que fazem uso de sua faculdade.

Quanto à periodicidade, Tatiana de Almeida Granja, entende que deve ser fixado "um intervalo mínimo entre os acessos dos trabalhadores aos seus próprios dados, evitando transtornos para a organização decorrentes de sucessivos e despropositados acessos [...] com o estabelecimento de exigências mínimas que demonstrem a legitimidade de interesse".

Por óbvio, quando houver necessidades excepcionais e justificáveis, esse período pode sofrer alterações para atender essas legitimas urgências.

Embora não haja regulamentação específica na legislação brasileira (fora da relação de trabalho) há de se interpretar que a tutela dos direitos privados abarca a proteção do trabalhador, com base nas garantias constitucionais, Código Civil e Consolidação das Leis do Trabalho.

Os dados poderão ser objeto de correção (Direitos de retificação e de cancelamento), por meio de cancelamento (exclusão física do dado) ou, em alguns casos, pelo simples bloqueio ao acesso.

Há, ainda, a possibilidade do exercício do Direito de oposição, facultado ao empregado apresentar justificativas legítimas para exposição e/ou manutenção de seus dados pessoais, uma espécie de jus resistentiae no contrato de trabalho.

Note-se que esse procedimento de controle é indispensável dentro do seio da sociedade eminentemente digital que vivemos. Como alerta, Fernanda Bruno, professora e pesquisadora da UFRJ, "os contornos modernos que conhecemos e herdamos – a separação público/privado e a definição de papéis em cada uma dessas esferas, a valorização da família, os direitos do indivíduo, a inviolabilidade do domínio privado, o direito ao segredo, à solidão, a proteção ao anonimato etc – foram resultado de embates na definição das relações entre o estado e a sociedade civil, o indivíduo e o coletivo. Logo, a privacidade, não sendo uma condição "natural", está sujeita a variações, mas estas não seguem um princípio "evolutivo" que levaria a sua extinção (como quer Zuckerberg, presidente do Facebook), mas são (e foram sempre) o efeito de embates sociais, políticos, econômicos. A história da privacidade é uma história política do cotidiano, onde a micro e a macro-política não cessam de se misturar. É nesse sentido que se deve compreender as recentes transformações nos seus limites. A privacidade hoje está em disputa. Não se trata de afirmar que ela existe ou deixou se existir, mas de compreender os discursos, forças e práticas que hoje disputam pelo sentido, valor e experiência da privacidade. Essa disputa é especialmente sensível no campo das redes distribuídas de comunicação. Assim, é preciso entrecruzar a disputa em torno da privacidade e as disputas políticas, econômicas, sociais, cognitivas e estéticas que se travam no âmbito dessas redes, de seus "bens" materiais e imateriais, de seus modelos de comunicação, circulação e produção de informação, conhecimento, cultura etc. Não raro (embora não necessariamente) os que clamam pelo fim da privacidade também clamam pelo controle da liberdade e do anonimato, ou pelo controle das práticas de compartilhamento e colaboração na rede ".

O importante, sem dúvida alguma, é o cuidado e a forma como são tratadas, divulgadas e destinadas às informações provenientes de dados pessoais do trabalhador (antes, durante e após a relação de emprego), na medida em que esses dados pessoais (e sua publicidade) estão sob um invólucro digital de duas ordens:

a) Uma primeira que pode ser chamada de mais superficial e visível, "onde as pessoas geram e disponibilizam voluntariamente e sobre os quais usualmente têm o controle do seu grau de visibilidade e publicidade (conforme as ferramentas disponibilizadas aos usuários, e nas quais inscrevem-se as nuances éticas da política de privacidade desses serviços e ambientes)"; e

b) uma segunda camada, que chamaremos de profunda, de dados que podem ou não conter meios de identificação dos indivíduos que os geraram. "Agregados em bancos de dados e submetidos a técnicas de mineração e profiling, tais dados geram mapas e perfis de consumo, interesse, comportamento, sociabilidade, preferências políticas que podem ser usados para os mais diversos fins, do marketing à administração pública ou privada, da indústria do entretenimento à indústria da segurança, entre outros. Neste caso, o controle do indivíduo sobre os seus próprios dados é bem menos evidente e a noção de privacidade (nos seus termos jurídicos) não dá conta da complexidade de questões sociais, políticas e cognitivas envolvidas" .

Logo, a proteção e guarda dos dados deve ser feita de maneira própria e complexa e não de modo amador e subjetivo, até porque o Marco Civil da Internet exige a proteção da privacidade do usuário, mas pede a manutenção, por um ano, de registros que possam identificar os autores dos acessos.

6. LGPD: Legislação Brasileira

A lei 13.709 de 14 de agosto de 2018 disciplinou a proteção de dados, dispondo sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Sendo assim, pode-se considerar como fundamentos legais (a) o respeito à privacidade; (b) a autodeterminação informativa; (c) a liberdade de expressão, de informação e de opinião; (d) a inviolabilidade da intimidade, da honra e da imagem; (e) o desenvolvimento econômico e tecnológico e a inovação; (f) a livre-iniciativa, a livre concorrência e a defesa do consumidor; (g) os diretos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Estão excluídos da aplicação da lei alguns meios de tratamento de dados realizados exclusivamente para fins artísticos, jornalísticos e acadêmicos. As informações relativas exclusivamente à segurança pública, defesa nacional e atividades de investigação, repressão de infrações penais.

Dentre os princípios que regem a legislação têm-se a (a) finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular,

sem possibilidade de tratamento posterior de forma incompatível com essas finalidades, (b) adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento, (c) necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados, (d) livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais, (e) qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento, (f) transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial, (g) segurança: 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, (h) prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais, (i) não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos, (j) responsabilização e prestação de contas: 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.

Foi explícita ao disciplinar conceitos, partícipes e elementos integrativos de toda a cadeia relacionada à proteção de dados, considerando: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico; V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); IX - agentes de tratamento: o controlador e o operador; X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento,

armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo; XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada; XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados; XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado; XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro; XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados; XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco; XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

A LGPD prevê que o tratamento de dados só pode ser realizado nas seguintes hipóteses:

a) mediante o fornecimento de consentimento pelo titular;

b) para o cumprimento de obrigação legal ou regulatória pelo controlador;

c) pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

d) para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

e) quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

f)para o exercício regular de direitos em processo judicial, administrativo ou arbitral;

g) para a proteção da vida ou da incolumidade física do titular ou de terceiros;

h) para a tutela da saúde, exclusivamente, em procedimento realizado

por profissionais de saúde, serviços de saúde ou autoridade sanitária;

i) quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

j) para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

A lei ainda determina que o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados. Referidas informações devem ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso à finalidade específica do tratamento, sua forma e duração, observados os segredos comercial e industrial, com identificação e informações de contato do controlador, bem como sobre as informações acerca do uso compartilhado e responsabilidades dos agentes que realizarão o tratamento.

O controlador (pessoa física ou jurídica, de direito público ou privado), a quem compete as decisões referentes ao tratamento de dados pessoais, tem de obrigatoriamente indicar o encarregado pelo tratamento de dados pessoais. Esse encarregado será o responsável por aceitaras reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providencias, receber comunicações da autoridade nacional de proteção de dados, bem como orientar os funcionários da entidade sobre as praticas que devem ser tomadas em relação à proteção de dados pessoais.

7. Conclusão: Proteção de Dados de mármore, não de murta.

A importância deste viés contratual quanto à proteção de dados, tem relevância estrutural e transversal, tanto que gerou até a criação de uma profissição nova e moldada à sua gerência e aplicabilidade, como é o caso do "diretor de proteção de dados". Em matéria específica sobre o tema, publicada no jornal O Estado de S. Paulo, destacou-se que "bancos, seguradoras, agências de publicidade e marketing e veículos de comunicação, todos procuram o mesmo profissional [..,] Data Protection Officer (diretor de proteção de dados, em tradução livre) ou DPO. Trata-se de responsável por elaborar estratégias sobre como coletar e proteger dados pessoais contra ciberataques, uma das novas exigências do Regulamento Geral Sobre Proteção de Dados Pessoais (GDPR). [...]. Com a entrada em vigor da GDPR, a União Europeia espera que o DPO seja capaz de dizer "não" a um presidente executivo que esteja a infringir as regras impostas pela legislação" .

O equilíbrio entre as inovações digitais, comércio eletrônico e vida privada tem de existir e ser regulado. Todo esse processo de publicidade direcionada, assistentes pessoais, redes sociais e serviços de geolocalização estão imbricados nos estágios acima relacionados e próprios da relação de emprego (melhor: de trabalho, em sentido lato), o que exige, portanto, precaução e definição de regras comportamentais contratuais com o fito de mitigar abusos e excessos, preservando-se a dignidade da pessoa humana.

O Regulamento Geral Sobre Proteção de Dados (GDPR) é um grande balizador do "como"

tratar o tema, uma vez que regulamenta direitos que incluem o acesso aos dados, retificação, direito ao esquecimento, direito à informação em caso de sinistro – como vazamento de dados –, direito à limitação de tratamento e, finalmente, direito à portabilidade de dados. Esse último muito inovador. O usuário vai poder transferir seus dados de um banco para outro, por exemplo, sem burocracia .

O momento, assim, valendo-se, aqui, da metáfora trazida por Leandro Karnal (lembrando Padre Vieira) é transformador: deve-se dar plena segurança jurídica à proteção de dados, lapidando-a em mármore e não de murta.

Destaca Karnal: "O padre Vieira criou uma ideia em seu Sermão do Espírito Santo, em 1657. Alguns povos, pensava o inaciano, são de difícil mudança e resistem à pregação do Evangelho. Diz o português que: 'Há umas nações naturalmente duras e constantes, as quais dificultosamente recebem a fé e deixam os erros de seus antepassados; resistem com armas, duvidam com o entendimento, repugnam com a vontade, cerram-se, teimam, argumentam, replicam, dão grande trabalho até se renderem; mas, uma vez rendidos, uma vez que receberam a fé, ficam nelas firmes, como estátuas de mármore; Não é necessário trabalhar mais nelas'. No caso desses povos, a conquista espiritual seria muito complexa e demorada. Uma vez realizada a tarefa hercúlea, a nova imagem seria dura como pedra e os convertidos ficariam apegados de forma definitiva à Boa-Nova. Haveria outros povos, como os indígenas do Brasil, que teriam comportamento oposto. Seria dóceis e receptivos ao novo modelo religioso. A facilidade da adesão seria acompanhada pela pouca constância no caminho de Jesus. Imediatamente cristianizados e com rapidez voltando às crenças antepassadas. No caso em questão, em vez de mármore, seria como esculpir em um arbusto, a murta, planta sobre a qual o jardineiro hábil pode produzir formas inventivas. Passadas algumas semanas (Vieira fala em 4 dias), o arbusto perde o modelo e retorna ao estado natural. No mundo clássico, a murta era dedicada à deusa Vênus/Afrodite, reforçando sua mutabilidade. Os 'gentios' do Novo Mundo eram alunos ambíguos: aceitariam tudo que lhes ensinavam e, teimosos, permanecem apegados ao seu universo de valores" .

Mais do que fundamental, imprescindível, se torna, assim, o respeito à garantia do controle de dados pessoais, por meio de políticas específicas e adequadas.

Referências bibliográficas

AGUIAR, Antonio Carlos. Direito do Trabalho 2.0: digital e disruptivo. São Paulo, LTr. 2018

ALIGHIERE, Dante, A Divina Comédia, Purgatório, Tradução e notas Italo Eugenio Mauro, Editora 34, São Paulo, 1998, 4ª reimpressão 2000.

ALMEIDA, Tatiana de. O Desafio da Proteção aos Dados pessoais do Trabalhador: a relação de trabalho. Disponível em: <http://direitoeti.com.br/artigos/o-desafio-da-protecao-aos-dados-pessoais-do-trabalhador-a-relacao-de-trabalho/> Acesso em 27 mai. 2018.

ALVES, Rubem. Concerto para corpo e alma. Papirus Editora. São Paulo, 2002.

BRUNO, Fernanda. O fim da privacidade

em disputa. Disponível em: <http://revistapontocom.org.br/edicoes-anteriores-artigos/o-fim-da-privacidade-em-disputa> Acessado em 27 mai.2018.

CARDONA RUBERT, Maria Belén. Informática y contrato de trabajo. Valencia: Tirant lo Blanch, 1999 apud GRANJA, Tatiana de Almeida. O desafio da proteção aos dados pessoais do trabalhador: a relação de trabalho. Disponível em: <http://direitoeti.com.br/artigos/o-desafio-da-protecao-aos-dados-pessoais-do-trabalhador-a-relacao-de-trabalho/> Acesso em 27 mai. 2018.

COLL, C; MONEREO, C (Org). Psicologia da educação virtual: aprender e ensinar com as tecnologias da informação e da comunicação. Tradução Naila Freitas. Porto Alegre: Armed

DUARTE, Roberto Dias, in Quem mexeu no meu currículo? Jornal O Estado de S. Paulo, 23 de outubro de 2011, p. 2, Caderno Empregos.

MARTÍNEZ FONS, Daniel. Tratamiento y protección de datos de los trabajadores en la relación de trabajo. Derecho social y nuevas tecnologías. Madrid: Consejo General del Poder Judicial, 2005 apud GRANJA, Tatiana de Almeida. O desafio da proteção aos dados pessoais do trabalhador: a relação de trabalho. Disponível em: <http://direitoeti.com.br/artigos/o-desafio-da-protecao-aos-dados-pessoais-do-trabalhador-a-relacao-de-trabalho/> Acesso em 27 mai. 2018.

Publicado originalmente na Revista Ltr : legislação do trabalho : Vol. 82, n. 6 (jun. 2018)

LEI GERAL DE PROTEÇÃO DE DADOS
LEI Nº 13.709, DE 14 DE AGOSTO DE 2018

Lei Geral de Proteção de Dados Pessoais (LGPD). (Redação dada pela Lei nº 13.853, de 2019)

O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. (Incluído pela Lei nº 13.853, de 2019)

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I - o respeito à privacidade;
II - a autodeterminação informativa;
III - a liberdade de expressão, de informação, de comunicação e de opinião;
IV - a inviolabilidade da intimidade, da honra e da imagem;
V - o desenvolvimento econômico e tecnológico e a inovação;
VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

I - a operação de tratamento seja realizada no território nacional;
II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (Redação dada pela Lei nº 13.853, de 2019)
III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:

I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
II - realizado para fins exclusivamente:

a) jornalístico e artísticos; ou
b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;

III - realizado para fins exclusivos de:

a) segurança pública;
b) defesa nacional;
c) segurança do Estado; ou
d) atividades de investigação e repressão de infrações penais; ou

IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.
§ 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.
§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.
§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público. (Redação dada pela Lei nº 13.853, de 2019)

Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 13.853, de 2019)
IX - agentes de tratamento: o controlador e o operador;
X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e (Redação dada pela Lei nº 13.853, de 2019)
XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. (Redação dada pela Lei nº 13.853, de 2019)

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
VII - segurança: 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;
VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X - responsabilização e prestação de contas: 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.

CAPÍTULO II
DO TRATAMENTO DE DADOS PESSOAIS

Seção I
Dos Requisitos para o Tratamento de Dados Pessoais

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;
II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019)
IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

§ 1º (Revogado). (Redação dada pela Lei nº 13.853, de 2019)
§ 2º (Revogado). (Redação dada pela Lei nº 13.853, de 2019)
§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.
§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.
§ 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas

nesta Lei.
§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.
§ 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei. (Incluído pela Lei nº 13.853, de 2019)

Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.
§ 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.
§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.
§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.
§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.
§ 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I - finalidade específica do tratamento;
II - forma e duração do tratamento, observados os segredos comercial e industrial;
III - identificação do controlador;
IV - informações de contato do controlador;
V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
VI - responsabilidades dos agentes que realizarão o tratamento; e

VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

§ 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.
§ 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.
§ 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.

Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I - apoio e promoção de atividades do controlador; e
II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.
§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Seção II
Do Tratamento de Dados Pessoais Sensíveis

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;
b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
e) proteção da vida ou da incolumidade física do titular ou de terceiro;
f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019)
g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.
§ 2º Nos casos de aplicação do disposto nas alíneas “a” e “b” do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.
§ 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.
§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: (Redação dada pela Lei nº 13.853, de 2019)

I - a portabilidade de dados quando solicitada pelo titular; ou (Incluído pela Lei nº 13.853, de 2019)
II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo. (Incluído pela Lei nº 13.853, de 2019)
§ 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários. (Incluído pela Lei nº 13.853, de 2019)

Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando

exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.
§ 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.
§ 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.

Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

§ 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais.
§ 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro.
§ 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.
§ 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Seção III
Do Tratamento de Dados Pessoais de Crianças e de Adolescentes

Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.
§ 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.

§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.
§ 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.
§ 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.
§ 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Seção IV
Do Término do Tratamento de Dados

Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
II - fim do período de tratamento;
III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou
IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

I - cumprimento de obrigação legal ou regulatória pelo controlador;
II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

CAPÍTULO III
DOS DIREITOS DO TITULAR

Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I - confirmação da existência de tratamento;
II - acesso aos dados;
III - correção de dados incompletos, inexatos ou desatualizados;
IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019)
VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.
§ 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.
§ 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.
§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:

I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou
II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

§ 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.

§ 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional. (Redação dada pela Lei nº 13.853, de 2019)
§ 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.
§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.

Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:

I - em formato simplificado, imediatamente; ou
II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

§ 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.
§ 2º As informações e os dados poderão ser fornecidos, a critério do titular:

I - por meio eletrônico, seguro e idôneo para esse fim; ou
II - sob forma impressa.

§ 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.
§ 4º A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos.

Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (Redação dada pela Lei nº 13.853, de 2019)

§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.
§ 3º (VETADO). (Incluído pela Lei nº 13.853, de 2019)

Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

CAPÍTULO IV
DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

Seção I
Das Regras

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

I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;
II - (VETADO); e
III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e (Redação dada pela Lei nº 13.853, de 2019)
IV - (VETADO). (Incluído pela Lei nº 13.853, de 2019)

§ 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento.
§ 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput deste artigo de instituir as autoridades de que trata a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .
§ 3º Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº

9.507, de 12 de novembro de 1997 (Lei do Habeas Data) , da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo) , e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .
§ 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.

§ 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo.

Art. 24. As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal , terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.

Parágrafo único. As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos deste Capítulo.

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

Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:

I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) ;
II - (VETADO);
III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.
IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou (Incluído pela Lei nº 13.853, de 2019)
V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde

que vedado o tratamento para outras finalidades. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Os contratos e convênios de que trata o § 1º deste artigo deverão ser comunicados à autoridade nacional.

Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto:

I - nas hipóteses de dispensa de consentimento previstas nesta Lei;
II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; ou
III - nas exceções constantes do § 1º do art. 26 desta Lei.

Parágrafo único. A informação à autoridade nacional de que trata o caput deste artigo será objeto de regulamentação. (Incluído pela Lei nº 13.853, de 2019)

Art. 28. (VETADO).

Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do poder público a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei. (Redação dada pela Lei nº 13.853, de 2019)

Art. 30. A autoridade nacional poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais.

Seção II
Da Responsabilidade

Art. 31. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.

Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

CAPÍTULO V
DA TRANSFERÊNCIA INTERNACIONAL DE DADOS

Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:

I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;
II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:

a) cláusulas contratuais específicas para determinada transferência;
b) cláusulas-padrão contratuais;
c) normas corporativas globais;
d) selos, certificados e códigos de conduta regularmente emitidos;

III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;
IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;
V - quando a autoridade nacional autorizar a transferência;
VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;
VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou
IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração:

I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;
II - a natureza dos dados;
III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;
IV - a adoção de medidas de segurança previstas em regulamento;
V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e
VI - outras circunstâncias específicas relativas à transferência.

Art. 35. A definição do conteúdo de cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do caput do art. 33 desta Lei, será realizada pela autoridade nacional.

§ 1º Para a verificação do disposto no caput deste artigo, deverão ser considerados os requisitos, as condições e as garantias mínimas para a transferência que observem os direitos, as garantias e os princípios desta Lei.
§ 2º Na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação da autoridade nacional, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento, quando necessário.
§ 3º A autoridade nacional poderá designar organismos de certificação para a realização do previsto no caput deste artigo, que permanecerão sob sua fiscalização nos termos definidos em regulamento.
§ 4º Os atos realizados por organismo de certificação poderão ser revistos pela autoridade nacional e, caso em desconformidade com esta Lei, submetidos a revisão ou anulados.
§ 5º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no caput deste artigo serão também analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos §§ 1º e 2º do art. 46 desta Lei.

Art. 36. As alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no inciso II do art. 33 desta Lei deverão ser comunicadas à autoridade nacional.

CAPÍTULO VI
DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS

Seção I
Do Controlador e do Operador

Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados

pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, 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.

Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

Art. 40. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.

Seção II
Do Encarregado pelo Tratamento de Dados Pessoais

Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.
§ 2º As atividades do encarregado consistem em:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
II - receber comunicações da autoridade nacional e adotar providências;
III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

§ 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.
§ 4º (VETADO). (Incluído pela Lei nº 13.853, de 2019)

Seção III
Da Responsabilidade e do Ressarcimento de Danos

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

§ 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
§ 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.
§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:

I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

I - o modo pelo qual é realizado;

II - o resultado e os riscos que razoavelmente dele se esperam;
III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

CAPÍTULO VII
DA SEGURANÇA E DAS BOAS PRÁTICAS

Seção I
Da Segurança e do Sigilo de Dados

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;
III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
IV - os riscos relacionados ao incidente;
V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:

I - ampla divulgação do fato em meios de comunicação; e
II - medidas para reverter ou mitigar os efeitos do incidente.

§ 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Seção II
Das Boas Práticas e da Governança

Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.
§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

I - implementar programa de governança em privacidade que, no mínimo:

a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
g) conte com planos de resposta a incidentes e remediação; e
h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.

§ 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.

CAPÍTULO VIII
DA FISCALIZAÇÃO

Seção I
Das Sanções Administrativas

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: ()

I - advertência, com indicação de prazo para adoção de medidas corretivas;
II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
III - multa diária, observado o limite total a que se refere o inciso II;
IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
VI - eliminação dos dados pessoais a que se refere a infração;
VII - (VETADO);
VIII - (VETADO);
IX - (VETADO).
X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)
XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)
XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019)

§ 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:

I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
II - a boa-fé do infrator;
III - a vantagem auferida ou pretendida pelo infrator;
IV - a condição econômica do infrator;
V - a reincidência;
VI - o grau do dano;
VII - a cooperação do infrator;
VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
IX - a adoção de política de boas práticas e governança;
X - a pronta adoção de medidas corretivas; e
XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais

definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica. (Redação dada pela Lei nº 13.853, de 2019)

§ 3º O disposto nos incisos I, IV, V, VI, X, XI e XII do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011. (Promulgação partes vetadas)

§ 4º No cálculo do valor da multa de que trata o inciso II do caput deste artigo, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.

§ 5º O produto da arrecadação das multas aplicadas pela ANPD, inscritas ou não em dívida ativa, será destinado ao Fundo de Defesa de Direitos Difusos de que tratam o art. 13 da Lei nº 7.347, de 24 de julho de 1985, e a Lei nº 9.008, de 21 de março de 1995. (Incluído pela Lei nº 13.853, de 2019)

§ 6º As sanções previstas nos incisos X, XI e XII do caput deste artigo serão aplicadas: (Incluído pela Lei nº 13.853, de 2019)

I - somente após já ter sido imposta ao menos 1 (uma) das sanções de que tratam os incisos II, III, IV, V e VI do caput deste artigo para o mesmo caso concreto; e (Incluído pela Lei nº 13.853, de 2019)

II - em caso de controladores submetidos a outros órgãos e entidades com competências sancionatórias, ouvidos esses órgãos. (Incluído pela Lei nº 13.853, de 2019)

§ 7º Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo. (Incluído pela Lei nº 13.853, de 2019)

Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa.

§ 1º As metodologias a que se refere o caput deste artigo devem ser previamente publicadas, para ciência dos agentes de tratamento, e devem apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, que deverão conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos nesta Lei.

§ 2º O regulamento de sanções e metodologias correspondentes deve estabelecer as circunstâncias e as condições para a adoção de multa simples ou diária.

Art. 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional. ()

Parágrafo único. A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento.

CAPÍTULO IX
DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

Seção I
Da Autoridade Nacional de Proteção de Dados (ANPD)

Art. 55. (VETADO).

Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República. (Incluído pela Lei nº 13.853, de 2019)

§ 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República. (Incluído pela Lei nº 13.853, de 2019)
§ 2º A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD. (Incluído pela Lei nº 13.853, de 2019)
§ 3º O provimento dos cargos e das funções necessários à criação e à atuação da ANPD está condicionado à expressa autorização física e financeira na lei orçamentária anual e à permissão na lei de diretrizes orçamentárias. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-B. É assegurada autonomia técnica e decisória à ANPD. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-C. A ANPD é composta de: (Incluído pela Lei nº 13.853, de 2019)

I - Conselho Diretor, órgão máximo de direção; (Incluído pela Lei nº 13.853, de 2019)
II - Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)
III - Corregedoria; (Incluído pela Lei nº 13.853, de 2019)

IV - Ouvidoria; (Incluído pela Lei nº 13.853, de 2019)
V - órgão de assessoramento jurídico próprio; e (Incluído pela Lei nº 13.853, de 2019)
VI - unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-D. O Conselho Diretor da ANPD será composto de 5 (cinco) diretores, incluído o Diretor-Presidente. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Os membros do Conselho Diretor da ANPD serão escolhidos pelo Presidente da República e por ele nomeados, após aprovação pelo Senado Federal, nos termos da alínea 'f' do inciso III do art. 52 da Constituição Federal, e ocuparão cargo em comissão do Grupo-Direção e Assessoramento Superiores - DAS, no mínimo, de nível 5. (Incluído pela Lei nº 13.853, de 2019)
§ 2º Os membros do Conselho Diretor serão escolhidos dentre brasileiros que tenham reputação ilibada, nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados. (Incluído pela Lei nº 13.853, de 2019)
§ 3º O mandato dos membros do Conselho Diretor será de 4 (quatro) anos. (Incluído pela Lei nº 13.853, de 2019)
§ 4º Os mandatos dos primeiros membros do Conselho Diretor nomeados serão de 2 (dois), de 3 (três), de 4 (quatro), de 5 (cinco) e de 6 (seis) anos, conforme estabelecido no ato de nomeação. (Incluído pela Lei nº 13.853, de 2019)
§ 5º Na hipótese de vacância do cargo no curso do mandato de membro do Conselho Diretor, o prazo remanescente será completado pelo sucessor. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-E. Os membros do Conselho Diretor somente perderão seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Nos termos do caput deste artigo, cabe ao Ministro de Estado Chefe da Casa Civil da Presidência da República instaurar o processo administrativo disciplinar, que será conduzido por comissão especial constituída por servidores públicos federais estáveis. (Incluído pela Lei nº 13.853, de 2019)
§ 2º Compete ao Presidente da República determinar o afastamento preventivo, somente quando assim recomendado pela comissão especial de que trata o § 1º deste artigo, e proferir o julgamento. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-F. Aplica-se aos membros do Conselho Diretor, após o exercício do cargo, o disposto no art. 6º da Lei nº 12.813, de 16 de maio de 2013. (Incluído pela Lei nº 13.853, de 2019)

Parágrafo único. A infração ao disposto no caput deste artigo caracteriza ato de improbidade administrativa. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-G. Ato do Presidente da República disporá sobre a estrutura regimental da ANPD. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Até a data de entrada em vigor de sua estrutura regimental, a ANPD receberá o apoio técnico e administrativo da Casa Civil da Presidência da República para o exercício de suas atividades. (Incluído pela Lei nº 13.853, de 2019)
§ 2º O Conselho Diretor disporá sobre o regimento interno da ANPD. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-H. Os cargos em comissão e as funções de confiança da ANPD serão remanejados de outros órgãos e entidades do Poder Executivo federal. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-I. Os ocupantes dos cargos em comissão e das funções de confiança da ANPD serão indicados pelo Conselho Diretor e nomeados ou designados pelo Diretor-Presidente. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-J. Compete à ANPD: (Incluído pela Lei nº 13.853, de 2019)

I - zelar pela proteção dos dados pessoais, nos termos da legislação; (Incluído pela Lei nº 13.853, de 2019)

II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei; (Incluído pela Lei nº 13.853, de 2019)
III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)
IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; (Incluído pela Lei nº 13.853, de 2019)
V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação; (Incluído pela Lei nº 13.853, de 2019)
VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; (Incluído pela Lei nº 13.853, de 2019)
VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; (Incluído pela Lei nº 13.853, de 2019)
VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis; (Incluído pela Lei nº 13.853, de 2019)

IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; (Incluído pela Lei nº 13.853, de 2019)

X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial; (Incluído pela Lei nº 13.853, de 2019)

XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei; (Incluído pela Lei nº 13.853, de 2019)

XII - elaborar relatórios de gestão anuais acerca de suas atividades; (Incluído pela Lei nº 13.853, de 2019)

XIII - 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; (Incluído pela Lei nº 13.853, de 2019)

XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento; (Incluído pela Lei nº 13.853, de 2019)

XV - arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas; (Incluído pela Lei nº 13.853, de 2019)

XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público; (Incluído pela Lei nº 13.853, de 2019)

XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942; (Incluído pela Lei nº 13.853, de 2019)

XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei; (Incluído pela Lei nº 13.853, de 2019)

XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso); (Incluído pela Lei nº 13.853, de 2019)

XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos; (Incluído pela Lei nº 13.853, de 2019)

XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; (Incluído pela Lei nº 13.853, de 2019)

XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos

e entidades da administração pública federal; (Incluído pela Lei nº 13.853, de 2019)
XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e (Incluído pela Lei nº 13.853, de 2019)
XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Ao impor condicionantes administrativas ao tratamento de dados pessoais por agente de tratamento privado, sejam eles limites, encargos ou sujeições, a ANPD deve observar a exigência de mínima intervenção, assegurados os fundamentos, os princípios e os direitos dos titulares previstos no art. 170 da Constituição Federal e nesta Lei. (Incluído pela Lei nº 13.853, de 2019)
§ 2º Os regulamentos e as normas editados pela ANPD devem ser precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório. (Incluído pela Lei nº 13.853, de 2019)
§ 3º A ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados, conforme legislação específica, e o tratamento de dados pessoais, na forma desta Lei. (Incluído pela Lei nº 13.853, de 2019)
§ 4º A ANPD manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD. (Incluído pela Lei nº 13.853, de 2019)
§ 5º No exercício das competências de que trata o caput deste artigo, a autoridade competente deverá zelar pela preservação do segredo empresarial e do sigilo das informações, nos termos da lei. (Incluído pela Lei nº 13.853, de 2019)
§ 6º As reclamações colhidas conforme o disposto no inciso V do caput deste artigo poderão ser analisadas de forma agregada, e as eventuais providências delas decorrentes poderão ser adotadas de forma padronizada. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública. (Incluído pela Lei nº 13.853, de 2019)
Parágrafo único. A ANPD articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-L. Constituem receitas da ANPD: (Incluído pela Lei nº 13.853, de 2019)

I - as dotações, consignadas no orçamento geral da União, os créditos especiais, os créditos adicionais, as transferências e os repasses que lhe forem conferidos; (Incluído pela Lei nº 13.853, de 2019)
II - as doações, os legados, as subvenções e outros recursos que lhe forem destinados; (Incluído pela Lei nº 13.853, de 2019)
III - os valores apurados na venda ou aluguel de bens móveis e imóveis de sua propriedade; (Incluído pela Lei nº 13.853, de 2019)
IV - os valores apurados em aplicações no mercado financeiro das receitas previstas neste artigo; (Incluído pela Lei nº 13.853, de 2019)
V - (VETADO); (Incluído pela Lei nº 13.853, de 2019)
VI - os recursos provenientes de acordos, convênios ou contratos celebrados com entidades, organismos ou empresas, públicos ou privados, nacionais ou internacionais; (Incluído pela Lei nº 13.853, de 2019)
VII - o produto da venda de publicações, material técnico, dados e informações, inclusive para fins de licitação pública. (Incluído pela Lei nº 13.853, de 2019)

Art. 56. (VETADO).
Art. 5 7. (VETADO).

Seção II
Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

Art. 58. (VETADO).

Art. 58-A. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto de 23 (vinte e três) representantes, titulares e suplentes, dos seguintes órgãos: (Incluído pela Lei nº 13.853, de 2019)

I - 5 (cinco) do Poder Executivo federal; (Incluído pela Lei nº 13.853, de 2019)
II - 1 (um) do Senado Federal; (Incluído pela Lei nº 13.853, de 2019)
III - 1 (um) da Câmara dos Deputados; (Incluído pela Lei nº 13.853, de 2019)
IV - 1 (um) do Conselho Nacional de Justiça; (Incluído pela Lei nº 13.853, de 2019)
V - 1 (um) do Conselho Nacional do Ministério Público; (Incluído pela Lei nº 13.853, de 2019)
VI - 1 (um) do Comitê Gestor da Internet no Brasil; (Incluído pela Lei nº 13.853, de 2019)
VII - 3 (três) de entidades da sociedade civil com atuação relacionada a proteção de dados pessoais; (Incluído pela Lei nº 13.853, de 2019)
VIII - 3 (três) de instituições científicas, tecnológicas e de inovação; (Incluído pela Lei nº 13.853, de 2019)

IX - 3 (três) de confederações sindicais representativas das categorias econômicas do setor produtivo; (Incluído pela Lei nº 13.853, de 2019)
X - 2 (dois) de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais; e (Incluído pela Lei nº 13.853, de 2019)
XI - 2 (dois) de entidades representativas do setor laboral. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Os representantes serão designados por ato do Presidente da República, permitida a delegação. (Incluído pela Lei nº 13.853, de 2019)
§ 2º Os representantes de que tratam os incisos I, II, III, IV, V e VI do caput deste artigo e seus suplentes serão indicados pelos titulares dos respectivos órgãos e entidades da administração pública. (Incluído pela Lei nº 13.853, de 2019)
§ 3º Os representantes de que tratam os incisos VII, VIII, IX, X e XI do caput deste artigo e seus suplentes: (Incluído pela Lei nº 13.853, de 2019)

I - serão indicados na forma de regulamento; (Incluído pela Lei nº 13.853, de 2019)
II - não poderão ser membros do Comitê Gestor da Internet no Brasil; (Incluído pela Lei nº 13.853, de 2019)
III - terão mandato de 2 (dois) anos, permitida 1 (uma) recondução. (Incluído pela Lei nº 13.853, de 2019)

§ 4º A participação no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será considerada prestação de serviço público relevante, não remunerada. (Incluído pela Lei nº 13.853, de 2019)

Art. 58-B. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade: (Incluído pela Lei nº 13.853, de 2019)

I - propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD; (Incluído pela Lei nº 13.853, de 2019)
II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)
III - sugerir ações a serem realizadas pela ANPD; (Incluído pela Lei nº 13.853, de 2019)
IV - elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e (Incluído pela Lei nº 13.853, de 2019)
V - disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população. (Incluído pela Lei nº 13.853, de 2019)

Art. 59. (VETADO).

CAPÍTULO X
DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 60. A Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet) , passa a vigorar com as seguintes alterações:

"Art. 7º .....

.....

X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais;

....." (NR)

"Art. 16. .....

.....

II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais." (NR)

Art. 61. A empresa estrangeira será notificada e intimada de todos os atos processuais previstos nesta Lei, independentemente de procuração ou de disposição contratual ou estatutária, na pessoa do agente ou representante ou pessoa responsável por sua filial, agência, sucursal, estabelecimento ou escritório instalado no Brasil.

Art. 62. A autoridade nacional e o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep), no âmbito de suas competências, editarão regulamentos específicos para o acesso a dados tratados pela União para o cumprimento do disposto no § 2º do art. 9º da Lei nº 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional) , e aos referentes ao Sistema Nacional de Avaliação da Educação Superior (Sinaes), de que trata a Lei nº 10.861, de 14 de abril de 2004 .

Art. 63. A autoridade nacional estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados.

Art. 64. Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Art. 65. Esta Lei entra em vigor: (Redação dada pela Lei nº 13.853, de 2019)

I - dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e (Incluído pela Lei nº 13.853, de 2019)

I-A – dia 1º de agosto de 2021, quanto aos arts. 52, 53 e 54; (Incluído pela Lei nº 14.010, de 2020)

II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos. (Incluído pela Lei nº 13.853, de 2019)

Brasília , 14 de agosto de 2018; 197º da Independência e 130º da República.

MICHEL TEMER

Torquato Jardim
Aloysio Nunes Ferreira Filho
Eduardo Refinetti Guardia
Esteves Pedro Colnago Junior
Gilberto Magalhães Occhi
Gilberto Kassab
Wagner de Campos Rosário
Gustavo do Vale Rocha
Ilan Goldfajn
Raul Jungmann
Eliseu Padilha

NORMAS PARA PUBLICAÇÃO

Prezados autores,

A Revista Eletrônica do Tribunal Regional do Trabalho da 9ª Região, Revista Científica de periodicidade mensal é divulgada exclusivamente por meio eletrônico a partir do site www.trt9.jus.br. Adota temática singular a cada edição e se destina a publicar artigos acórdãos, sentenças, condensa entendimentos jurisprudenciais sumulados ou organizados em orientações, resenhas, convida para publicação observadas as seguintes normas.

1. Os artigos ou decisões devem ser encaminhados à análise do Conselho Editorial, para o e-mail **revistaeletronica@trt9.jus.br**

2. Os artigos serão técnico-científicos, focados na área temática de cada edição específica, sendo divulgada a sequência dos temas eleitos pela Escola Judicial do TRT-9ª Região, mediante consulta;

3. Os artigos encaminhados à Revista Eletrônica devem estar digitados na versão do aplicativo Word, fonte Calibri corpo 12, espaçamento entrelinhas 1,5, modelo justificado, com títulos e subtítulos em maiúsculas alinhados à esquerda, em negrito. A primeira lauda conterá o título do artigo, nome, titulação completa do autor, referência acerca da publicação original ou sobre seu ineditismo e uma foto;

4. Os artigos encaminhados à publicação deverão ter de preferência entre 8 e 12 laudas, incluídas as referências bibliográficas. Os artigos conterão citações bibliográficas numeradas, notas de rodapé ordenadas e referências bibliográficas observarão normas vigentes da ABNT, reservando-se o Conselho Editorial da Revista Eletrônica o direito de adaptar eventuais inconsistências, além de estar autorizado a proceder revisões ortográficas, se existentes;

5. A publicação dos artigos não implicará remuneração a seus autores, que ao submeterem o texto à análise autorizam sua eventual publicação, sendo obrigação do Conselho Editorial informá-los assim que divulgada a Revista Eletrônica;

6. O envio de artigos ou decisões não pressupõe automática publicação, sendo sua efetiva adequação ao conteúdo temático de cada edição da Revista Eletrônica pertencente ao juízo crítico-científico do Conselho Editorial, orientado pelo Desembargador que organiza as pesquisas voltadas à publicação.

7. Dúvidas a respeito das normas para publicação serão dirimidas por e-mails encaminhados à **revistaeletronica@trt9.jus.br**

Respeitosamente.

CONSELHO EDITORIAL


TRT-9ª REGIÃO
Escola Judicial