A LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA NA PRÁTICA EMPRESARIAL

Ana Paula de Oliveira

Advogada, pós-graduanda em Direito Civil e Direito Processual Civil pela Unicuritiba, pós-graduanda em Direito do Trabalho e Direito Previdenciário pela UNISC; Membro da Comissão de Compliance da OAB/PR, Membro do Comitê Brasileiro de Compliance e Membro da Comissão de Processo Disciplinar da Federação Paranaense de Futebol.

Dânton Zanetti

Advogado, pós-graduado em Direito Processual Civil pela PUC-PR, pós-graduado em Direito e Processo do Trabalho pela Unicuritiba, Professor na Faculdade de Direito Santa Cruz. Membro da Comissão de Inovação e Gestão da OAB/PR.

Flávio Santos Lima

Advogado, Membro da Comissão de Inovação e Gestão da OAB/PR. Advogado e Consultor na Oystr Robôs Inteligentes.

Themis Ortega Sampaio

Advogada, pós-graduada em Direito Contemporâneo pela FEMPAR, pós-graduada em Direito Civil e Direito Processual Civil pela Unicuritiba, Membro da Comissão de Inovação e Gestão da OAB/PR e Membro do Comitê Brasileiro de Compliance.

Resumo: A Nova Lei Geral de Proteção de Dados, que passa a ter vigência em agosto de 2020, surgiu como um desafio para as empresas que lidam com dados pessoais. Diante disso, nasce a necessidade de entender quais serão os caminhos para a adaptação dessas instituições. Assim, o objetivo do artigo consiste em apresentar medidas que devem ser observadas pelos empresários para estar em conformidade (*Compliance)* com a lei e proteger os usuários efetivamente. Outrossim, observou-se questões como a função do termo de uso e das políticas de privacidade, e o papel do DPO, que recai sobre a figura do encarregado.

Palavras-chave: Proteção de Dados; *Compliance*; Atividade Empresarial.

1. Introdução

O desenvolvimento tecnológico experimentado pela sociedade nas últimas décadas, ofusca o fato de que um longo percurso histórico teve de ser percorrido até que a

privacidade pudesse ser reconhecida como um bem jurídico digno de tutela Estatal, atribuindo-se aos juristas norte-americanos Samuel D. Warren e Louis D. Brandeis o primeiro artigo científico dedicado ao tema, intitulado *"The Right to Privacy"*, do ano de 1890.[1]

No referido escrito os autores sustentam que os direitos individuais derivariam da proteção da *pessoa* ou da *propriedade*, e, de tempos em tempos, alterações no cenário político, social e econômico fariam necessário reavaliar a natureza e extensão de tais bens jurídicos. Nesta esteira, ressignificando o direito à vida em face da mais nova ameaça tecnológica da época – as câmeras fotográficas instantâneas utilizadas pela imprensa – Warren e Brandeis reconhecem a privacidade como "o direito de ser deixado só".

Desde então, com a evolução das tecnologias, paulatinamente a privacidade, foi ganhando importância e reconhecimento jurídico no cenário internacional, valendo citar, exemplificativamente, documentos expressivos como a Convenção Americana dos Direitos e Deveres do Homem, de 1948, cujo artigo V estatui que "Toda pessoa tem direito à proteção da lei contra os ataques abusivos à sua honra, à sua reputação e à sua vida particular e familiar"[2], e a Declaração Universal dos Direitos Humanos, do mesmo ano, que no artigo 12 expressa que "Ninguém será sujeito à

1 WARREN, Samuel D.; BRANDEIS, Louis D. **The right to privacy.** Harvard Law Review, Vol. 4, Nº. 5. 1890, p. 193-220.

2 Disponível em: <https://www.cidh.oas.org/basicos/portugues/b.Declaracao_Americana.htm>; Acesso em 07.01.2019.

interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques".[3]

A preocupação com o tratamento de dados pessoais como desdobramento da privacidade é um efeito colateral da mudança de paradigma trazida pela "Quarta Revolução Industrial", cujo tom é dado pelo fenômeno da "informacionalização da sociedade", iniciado na década de 1970. Seus reflexos impactam diretamente tanto a atividade econômico-empresarial, quanto a atuação do próprio Estado, que, além de criar e consumir informação, controla o fluxo de informações.[4]

Diante dessa transformação exsurge a necessidade de regulamentar o uso dos dados, fenômeno que vem inspirando a edição de leis e regulamentações específicas sobre a matéria a nível global.

No Brasil, o acesso à internet é garantido por força da Lei 12.965/2014 (o "Marco Civil da Internet"), que em seu artigo 7º prevê que o "O acesso à internet é essencial ao exercício da cidadania". Mais recentemente, em 14 de agosto de 2018, foi promulgada a Lei 13.709/2018, a Lei

3 Disponível em: <https://www.unicef.org/brazil/pt/resources_10133.html>; Acesso em 07.01.2019.

4 BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade: do direito às novas tecnologias na sociedade da informação.** Rio de Janeiro: Lumen Juris, 2018, p. 13-15.

Geral de Proteção de Dados (LGDP), responsável por aprofundar a regulamentação das questões relativas ao tratamento de dados pessoais no cenário nacional.

Os impactos desta nova norma são expressivos, tanto no aspecto da tutela da privacidade e proteção dos dados pessoais de seus respectivos titulares, quanto, naturalmente, para a atividade empresarial, considerando que a LGPD impõe uma série de diretrizes para que o tratamento de dados seja realizado de forma lícita.

No presente estudo, sem a pretensão de esgotar o tema, serão abordadas algumas medidas consideradas necessárias para a adaptação das empresas diante deste novo cenário. Inicialmente, trata-se da instauração de Programas de *Compliance*, com observância de boas práticas, incluindo os princípios fundamentais, gestão de risco e até mesmo a aplicação da ISO 27001.

Em seguida, passa-se a analisar a tessitura de documentos como os "Termos de Uso" e "Políticas de Privacidade", largamente utilizados em serviços *online*. Por fim, analisa-se a figura do *Data Protection Officer (DPO)*, que recai na pessoa que exerce a função de encarregado.

2. A lei geral de proteção de dados brasileira em compliance

A nova Lei Geral de Proteção de Dados, publicada em agosto de 2018, trouxe novos desafios para as empresas que lidam com dados pessoais. Até a sua entrada em vigor,

as pessoas naturais e jurídicas que estejam sob sua abrangência devem se adequar às novas exigências legais.

Inicialmente, o empresário que usa, coleta ou armazena dados de qualquer pessoa deve observar, além da boa-fé, os princípios trazidos pela Lei 13.709/2018, no art. 6º, para se manter em *compliance*[5]. Tais princípios apresentam-se discriminados com sua aplicação prática, o que facilita a sua incorporação pelas políticas de proteção de dados.

Pode-se dizer que esses princípios foram desenvolvidos por meio de instrumentos internacionais e transnacionais, a partir do novo contexto da privacidade ligada à proteção dos dados pessoais[6] e trazidos para a legislação brasileira. Tratam-se de princípios fundamentais dos cidadãos e devem ser efetivados pelas instituições que manipulam dados. Diante disso, busca-se aqui demonstrar a concretização dos princípios mais relevantes, que servem de base para a efetividade dos demais princípios, sendo eles o princípio da finalidade, da transparência, da qualidade de dados e da segurança.

O princípio da finalidade determina que é necessária uma correlação entre o uso dos dados pessoais e o fim comunicado aos titulares quando do momento da coleta. Assim, é possível limitar o acesso de terceiro às informações

5 Conformidade (tradução livre).

6 MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental.** São Paulo: Saraiva, 2014. p. 70.

coletadas. Outrossim, também serve para definir a adequação e razoabilidade do uso de dados. Para o cumprimento deste princípio, deve a instituição estabelecer de forma expressa e limitada "a finalidade do tratamento de dados, sob pena de se considerar ilegítimo o tratamento realizado com base em finalidades amplas ou genéricas"[7].

Já o princípio da transparência, para se tornar efetivo, precisa que os bancos de dados sejam de conhecimento público. Esta ideia reafirma o preceito democrático de incompatibilidade de bancos de dados sigilosos com um Estado Democrático de Direito. Ademais, a transparência também permite o combate de práticas abusivas a partir do uso dos dados. Para estar em conformidade com esse relevante princípio, as empresas devem publicar seu nome, sede e conteúdo juntamente com o banco de dados. Essas publicações podem ser feitas em "registros públicos, diários oficiais ou meios de grande circulação sob pena de ineficácia desse direito"[8].

Ainda, importante ressaltar o princípio da qualidade dos dados. Este exige que as informações tenham tratamento leal e lícito, além de estarem adequados à finalidade declarada e possuindo conteúdo objetivo, exato e atualizado. Para isso, as empresas que tratam dados devem ter cautela com a sua gestão[9], mantendo-os sempre

7 Ibidem, p. 71

8 Idem.

9 "A Gestão de Identidades e Acessos compreende um conjunto de processos para gerenciar todo o ciclo de vida dos acessos dos usuários, in-

atualizados. Assim, é necessário que se disponha de instrumentos para garantir os direitos de acesso, retificação e cancelamento dos dados[10].

Ademais, imperioso comentar acerca do princípio da segurança, que para ser efetivo precisa de meios que possibilitem a proteção dos dados pessoais contra extravios, destruições, modificações e desvios não autorizados por seus titulares. Decorrente disto, surge o princípio da responsabilização e prestação de contas, "que visa assegurar a reparação adequada e integral dos danos materiais e morais causados ao indivíduo em razão da violação ao seu direito à privacidade"[11]

Nesse panorama, os Programas de Integridade (C*ompliance*) têm se mostrado como um ótimo caminho para superar todos os desafios de adequação, revelando-se, ainda, como estratégia para minimizar os riscos reputacionais e legais das empresas[12].

Diante da necessidade de uma atuação multidisciplinar especializada, que demanda estrutura tecnológica de

---

ternos ou externos, dentro de uma organização" (SILVA, Felipe. **Gestão de Identidades e Acessos.**In.In CABRAL, Carlos; CAPRINO, Willian (org.). Trilhas em Segurança da Informação, Caminhos e Ideias para a Proteção de Dados. Rio de Janeiro: Brasport, 2015. p.73).

10 MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental.** São Paulo: Saraiva, 2014. p. 72

11 Idem.

12 VERÍSSIMO, Carla. **Compliance: incentivo à adoção de medidas anticorrupção**. São Paulo: Saraiva, 2017. p.104.

segurança da informação, governança normativa e contratual, e ainda capacitação de equipes, há a exigência de ação imediata por parte das empresas.

Importante observar que o programa ou sistema a ser adotado, poderá ser proporcional ao porte da corporação, bem como aos riscos que ela enfrenta.

Sobre esse aspecto, a Portaria Conjunta da CGU e do Ministério da Micro e Pequena Empresa n. 2279/2015 aponta medidas de integridade com um rigor formal mais simples, a fim de garantir o comprometimento com a ética e a integridade entre as microempresas e empresas de pequeno porte[13]. Desmistifica-se assim o preceito de que "*compliance tem um custo elevado demais*" para estas empresas, tendo em vista que é possível adequá-lo às necessidades especiais de cada companhia.

Em linhas gerais, quanto maior a corporação, e maiores os riscos a que a esta estará submetida, mais complexa é a tarefa de incorporar um sistema de cumprimento normativo[14].

Em se tratando de riscos, as penalidades provenientes do descumprimento da Lei podem ser bastante danosas. São os casos, por exemplo, da publicização da infração, da aplicação de multa diária única, ou ainda de multa de até 2% (dois por cento) do faturamento da

13 Ibidem. p.174.

14 VERÍSSIMO, Carla. **Compliance: incentivo à adoção de medidas anticorrupção**. São Paulo: Saraiva, 2017.p.276.

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.

Estima-se assim que a adequação, de fato, não será tarefa fácil[15], porém a falta dela poderá importar em prejuízos incomensuráveis. Ponderando-se que o c*ompliance* tem objetivos tanto preventivos, quanto reativos[16], tais danos podem ser consideravelmente reduzidos.

Neste ínterim, tratando-se em definitivo das diretrizes de um Programa de Integridade, é possível defini-lo sob três etapas: A primeira, correspondente à formulação, ou seja, análise e valoração de riscos, definição de medidas de prevenção e a criação de uma estrutura de *compliance*. A segunda, implementação, ou seja, comunicação e detalhamento do programa, consistente em medidas organizacionais para criação de processos de *compliance*. A terceira, por fim, abrangendo a consolidação e aperfeiçoamento, estabelecendo um processo para apuração de violações, critério de sanções e avaliação continuada e aperfeiçoamento do programa[17].

---

15 FRAZÃO, Ana. **Nova LGPD: principais repercussões para a atividade empresarial**, 2018. 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: 29/09/2018.

16 VERÍSSIMO, Carla. **Compliance: incentivo à adoção de medidas anticorrupção**. São Paulo: Saraiva, 2017. p.91.

17 Ibidem, p.277.

No que tange a gestão dos riscos, consiste num processo estruturado[18]. Levantam-se os ímpetos possíveis do negócio para, em seguida, dar sequência às demais etapas, buscando formas de reduzir ou eliminar seus efeitos como, por exemplo, coibir severos danos à imagem da empresa, no caso de um eventual vazamento de dados.

BARROS aponta que "risco é composto de dois grandes componentes: a probabilidade de ocorrência e a magnitude de perda", sendo que esta última consiste em "impacto"[19]. Nesse contexto, a probabilidade de ocorrência pode ser representada pela frequência do evento danoso – ou ameaça – em determinado período de tempo. Quanto ao impacto, se revela no "comprometimento de uma das propriedades básicas da segurança de informação: confidencialidade, integridade e disponibilidade"[20].

No que tange os mecanismos para desenvolver a conformidade com a Lei Geral da Proteção de Dados, o grupo de normas 27000, publicada pela *International Organization for Standardization (ISO),* pode-se mostrar também como importante e moderna ferramenta de proteção de da-

18 BARROS, Augusto Paes de. **Gestão de Risco.**In CABRAL, Carlos; CAPRINO, Willian (org.). Trilhas em Segurança da Informação, Caminhos e Ideias para a Proteção de Dados. Rio de Janeiro: Brasport, 2015. p. 38.

19 BARROS, Augusto Paes de. **Gestão de Risco.**In CABRAL, Carlos; CAPRINO, Willian (org.). Trilhas em Segurança da Informação, Caminhos e Ideias para a Proteção de Dados. Rio de Janeiro: Brasport, 2015. p. 39.

20 Ibidem, p. 40.

dos. Estas normas definem requisitos para um sistema de gestão de segurança da informação (SGSI) bem como sua operação, em especial a ISO 27001[21].

Referida normativa trata-se de padrão internacional reconhecido e validado para segurança de informação. Entre outros aspectos, segue um sistema de gestão que avalia riscos de segurança e proteção, adota procedimentos de controle, e monitora o desempenho dos processos, atuando assim em sintonia e reforçando os programas de integridade que visam a proteção de dados e privacidade.

Assim, considerando-se os riscos do negócio e os preceitos basilares dos programas de integridade, como prevenção, processamento de informações sensíveis, e treinamento de colaboradores, pode-se enquadrar a Lei Geral da Proteção de Dados, perfeitamente como um tema de *compliance.*

Diante disso, para se manter em *compliance* efetivamente*,* as instituições ainda devem observar outras questões práticas, a exemplo da elaboração de um adequado Termo de Uso e de Políticas de Privacidade.

3. A função dos termos de uso e das políticas de privacidade

Com o advento da LGPD, quebra-se um verdadeiro paradigma na cultura de proteção meramente formal da privacidade do titular de dados, e inaugura-se uma nova

21 Ibidem, p. 52.

etapa em que se impõe a tutela material dos dados pessoais tratados em ambiente digital ou fora dele.

Isto porque, se mesmo no âmbito das relações digitais estabelecidas via *internet* havia legislação própria para regular o tema da proteção de dados– ainda que de forma incompleta, considerando que a questão da proteção de dados até então era regida pela Lei nº 12.965/2014, conhecida como "Marco Civil da *Internet*" – verificava-se abuso contumaz praticado por empresas na coleta, tratamento e exploração de dados pessoais. O cuidado no tratamento de dados realizados fora do meio digital, então, não se sujeitava a qualquer controle mínimo, mesmo havendo outras normas dispostas em leis esparsas, como o Código de Defesa do Consumidor e as leis do Cadastro Positivo (nº 12.414/2011) e de Acesso à Informação (nº 12.527/2011), sem olvidar da garantia fundamental à vida privada, assegurada no artigo 5º, X, da Constituição Federal.

A referida mudança de paradigma, traz impactos relevantes à atividade empresarial, mormente considerando que nesta "Quarta Revolução Industrial", que tem como traços marcantes a velocidade, amplitude, profundidade e impacto sistêmico (SCHWAB, 2016)[22], as relações sociais cada vez mais se desenvolvem digitalmente, razão pela qual os grandes bancos de dados, atualmente, são mantidos em nuvens (*cloudcomputing*) e outras espécies de bancos de dados ex-

22 SCHWAB, Klaus. **A quarta revolução industrial**. Tradução por Daniel Moreira Miranda. São Paulo: Edipro, 2016.

clusivamente digitais, ganhando enorme relevo atividades de '*Data Mining'* (mineração de dados)[23] e o chamado '*Big Data'* (grande volume de dados)[24], por exemplo.

Este fenômeno se deve muito em razão do amadurecimento nas últimas décadas da importância da *informação* como ativo dotado de valor financeiro e de mercado, considerados, sobretudo, os aspectos da 'maleabilidade' e 'utilidade' da informação, que exponenciam sua influência sobre as tomadas de decisão e a vida cotidiana em geral. Na análise de DONEDA, o efeito disso foi uma crescente expansão de atividades empresariais ligadas à exploração de dados, sistematização da informação e formação de bancos de dados.[25]

---

23 Segundo FREITAS e PAMPLONA (2018, p. 8), "A Mineração de Dados (*Data Mining*) tem como objetivo atender estas expectativas e pode ser definida por Fayyad, Piatetsky-Shapiro e Smyth (1996, p. 39-40) como *'nontrivialprocessofidentifyingvalid, novel, potentiallyusefulandultimatelyunderstandablepatterns in data'".*

24 Conforme FRANÇA, "Os dados das redes sociais online podem ser usados para extrair informações sobre padrões de interações interpessoais e opiniões. Esses dados podem auxiliar no entendimento de fenômenos, na previsão de um evento ou na tomada de decisões. Com a ampla adoção dessas redes, esses dados aumentaram em volume, variedade e precisam de processamento rápido, exigindo, por esse motivo, que novas abordagens no tratamento sejam empregadas. Aos dados que possuem tais características (volume, variedade e necessidade de velocidade em seu tratamento), chamamo-los de Big Data."(FRANÇA, T. C.; FARIA, F. F.; RANGEL, F. M.; FARIAS, C. M.; OLIVEIRA, J.. BigSocial Data: Princípios sobre coleta, tratamento e análise de dados sociais. Artigopublicado nos anais do XXIX Simpósio Brasileiro de Banco de Dados (SBBD) 2014.Curitiba. 2014, p. 8. Disponível em:<http://www.inf.ufpr.br/sbbdsbsc2014/sbbd/proceedings/artigos/pdfs/127.pdf>. Acesso em 10/10/2018.

25 DONEDA, Danilo. **Proteção de dados pessoais nas relações de**

Uma das consequências diretas deste modelo relacional é a proliferação dos documentos intitulados "Termos de Uso" e "Política de Privacidade", que se propõem a reger as relações dos usuários de *sites* e serviços de *internet*, inclusive no que tange às ações ligadas ao tratamento de dados pessoais, desde a coleta, passando pelo armazenamento, até sua eliminação.

Para CAVALCANTI e SANTOS (2018), "Torna-se, portanto, obrigatório adotar, desde a concepção de serviços, produtos e modelos de negócio, a prática de se garantir direitos de proteção à privacidade e aos dados pessoais. São os chamados *privacy by design* e *by default*"[26], em que o primeiro modelo permite uma adequação do formato e níveis de privacidade a ser cedida por determinado usuário, enquanto o segundo não se concebe tal possibilidade.

Com efeito, ainda é insipiente na doutrina e na própria jurisprudência pátria discussões mais aprofundadas a respeito da natureza jurídica e efeitos emanados dos documentos intitulados "Termos de Uso" e "Política de Privacidade".

Nada obstante, é possível amolda-los às ferramentas já existentes no ordenamento jurídico pátrio, em espe-

---

consumo: para além da informação creditícia. Brasília: SDE/DPDC. 2010, p. 22.

26 CAVALCANTI, Natália Peppi; SANTOS, Luiza Mendonça da Silva Belo.**A Lei Geral de Proteção de Dados do Brasil na era do Big Data.** *In* Tecnologia Jurídica & Direito Digital - II Congresso Internacional de Direito, Governo e Tecnologia. 2018, p. 358.

cial às normas pertinentes aos contratos de adesão, cuja principal característica é a existência das figuras do proponente e do aderente. O primeiro é o responsável por estabelecer cláusulas e condições contratuais, enquanto o segundo tem apenas a opção de aceitar ou rejeitar o contrato como um todo, abrindo mão da possibilidade de negociar os termos do contrato. Nas palavras de RIBEIRO e GALESKI JUNIOR (2015):

> "Nos contratos de adesão, a liberdade na fixação do conteúdo contratual, entendida como liberdade privada do contratante e contratado é parcialmente afastada, por não resultarem do livre debate entre as partes, mas provirem do fato de uma delas aceitar tacitamente cláusulas e condições previamente estabelecidas pela outra."[27]

As definições acima são inteiramente aplicáveis aos Termos de Uso e Políticas de Privacidade, eis que um determinado internauta, ao acessar um *site* de seu interesse – e, portanto, estabelecer uma relação com dada empresa, fornecedora de serviços – tem pouca, ou mesmo nenhuma possibilidade de influir na redação e nos efeitos de qualquer das cláusulas dispostas nos documentos mencionados. Resta-lhe apenas aceitá-los nos moldes em que se encontram propostos, ou rejeitá-los e, assim, ter seu acesso a informação, conteúdos, produtos, serviços, etc., limitado ou até mesmo impedido.

27 RIBEIRO, Márcia Carla Pereira; GALESKI JUNIOR, Irineu. **Teoria geral dos contratos: contratos empresariais e análise econômica.** 2ª ed. São Paulo: Editora Revista dos Tribunais. 2015, p. 58.

De outro lado, a empresa titular de determinado domínio de *internet*, ou aplicativo, mesmo atualmente, enquanto sujeita às disposições legais previstas no Marco Civil da *Internet*, tem o dever de informar àqueles que navegam em seu *site* a respeito dos dados pessoais que pretende tratar, o que, como visto, comumente é disposto nos Termos de Uso e Políticas de Privacidade.

Analisando a natureza desta relação adesiva é bem-vinda a lição de MAGRANI (2014, p. 158) ao afirmar que, "malgrado tratar-se de espaços privados, os usuários não podem sujeitar-se a termos de uso abusivos que restrinjam de forma desproporcional seus direitos garantidos na Constituição"[28], ponderando que o uso da *internet* é manifestação palpável da função social desempenhada pela atividade empresarial, e que os ambientes virtuais não mais podem ser enxergados apenas como um espaço para o mero exercício de direitos disponíveis, mas como meio de concretização de diversos direitos sociais e individuais.

Muito embora o dever, em si, quanto à proteção de dados pessoais já existisse sob o pálio do Marco Civil da Internet, a LGPD, no entanto, aprofunda – e muito – as parcas diretrizes estabelecidas naquela norma, impondo às empresas novos desafios para se adequar ao novo estandarte legal.

---

28 MAGRANI, Eduardo. **Democracia conectada: a internet como ferramenta de engajamento político-democrático**. Curitiba: Juruá. 2014, p. 158.

Como visto, sobretudo para as empresas que hospedam seus serviços na *internet*, para estar em *compliance* com a LGPD, invariavelmente terão que dispor em seus Termos de Uso e Políticas de Privacidade informações claras e transparentes a seu público a respeito da forma como o tratamento de dados pessoais será realizado, sobretudo para dar fiel atendimento aos princípios previstos nos incisos do artigo 6º, em especial quanto à *finalidade* (I), *adequação* (II), *necessidade* (III) e *transparência* (VI).

A transparência talvez seja justamente a tônica da norma, uma vez que a partir do desenvolvimento deste princípio as partes envolvidas estarão em um patamar informacional equivalente. Neste sentido, DONEDA (2010, p. 84) esclarece que para salvaguarda das informações pessoais, estas deverão ser submetidas "através de uma política de privacidade clara e precisa e do recurso a outros meios que garantam que sua inscrição não se efetive sem o real conhecimento das suas consequências".[29]

Para traçar um paralelo, os Termos de Uso e Políticas de Privacidade, embora, como visto, ostentem a natureza instrumental própria dos contratos de adesão, são documentos que muito se assemelham a uma 'Carta de Intenções', por meio dos quais se estabelecem premissas acerca dos interesses, direitos, obrigações e demais regras consideradas necessárias para reger uma relação superficial entre as partes, que em muitos casos se limita ao acesso de

29 Op. cit., p. 84.

determinado site, plataforma, aplicativo, etc., adequando tais interesses às balizas legais.

Estas intenções devem refletir fielmente aquilo que se pretende dar e, sobretudo, receber acesso, mormente considerando que tais documentos em regra são concebidos de forma unilateral pela parte que oferece os serviços ou detém a titularidade do ambiente em que a coleta e o tratamento de dados pessoais virá a ocorrer, valendo destacar que os Termos de Uso e Políticas de Privacidade, serão o principal instrumento de comunicação e de registro entre as partes dos moldes da relação entre elas estabelecida, vinculando-os a seus termos.

A título meramente exemplificativo, elencam-se, aqui, algumas disposições possíveis de serem estabelecidas nos Termos de Uso e Políticas de Privacidade como: direitos e deveres dos usuários e clientes; regras para utilização de serviços como *sites*, plataformas, aplicativos, etc., inclusive com relação à proteção de propriedade intelectual sobre conteúdos veiculados pelas partes; responsabilidade e limites de responsabilização, entre outras questões a serem pensadas casuisticamente, de acordo com os interesses envolvidos na consecução da atividade empresarial, que deverão nortear a elaboração dos referidos documentos.

Mais especificamente quanto à privacidade no tratamento de dados, é essencial, por exigência da LGPD, especificar quais serão os dados tratados – cujo tratamento

deve se limitar aos dados mínimos necessários –; qual será a finalidade do tratamento, por qual prazo os dados serão tratados e o de que forma será realizada a eliminação dos dados quando do alcance da finalidade proposta, ou do exaurimento do prazo previsto (art. 15, I e II, LGDP); e qual serão os meios disponíveis para que o titular dos dados (art. 5º, V, LGPD) possa exercer o direito de livre acesso aos dados tratados (art. 9º).

Além disso, tão importante quanto dar ao titular dos dados informações precisas a respeito dos pontos acima elencados – e aqui reside um dos grandes desafios para as empresas, sobretudo aquelas que exploram comercialmente os dados que tratam – é justificar o tratamento dos dados através da subsunção do caso concreto às hipóteses legais previstas no artigo 7º da Lei.

A política de privacidade deve dar ciência ao titular dos dados pessoais de que o tratamento de seus dados apenas será realizado em razão de alguma das hipóteses legais previstas nos incisos do artigo 7º, da LGPD.

Em linhas gerais, a LGPD apresenta dez hipóteses que autorizam o tratamento de dados pessoais, fugindo dos objetivos deste breve estudo tecer considerações mais aprofundadas a respeito de cada uma delas. Contudo, dado o tema a que ora nos debruçamos, mais apropriado do que esta abordagem é estabelecer a *necessidade*, em si, de liame entre os Termos de Uso e Políticas de Privacidade e algumas das hipóteses legais.

Sem embargo, abre-se exceção para tecer breves considerações a respeito da especial hipótese legal quanto ao consentimento (art. 7º, I, LGPD), instituto que, na concepção de CAVALCANTI e SANTOS "tem importante papel na autodeterminação informativa, controle e liberdade do titular em relação aos seus dados, configurando-se elemento central para a proteção de dados pessoais".[30]

O consentimento é, notoriamente, uma das principais e mais utilizada das hipóteses, embora seja considerada justamente a mais frágil delas, em razão da possibilidade de sua revogação pelo titular e da possibilidade de considerar-se nula a aquiescência do titular em caso de abuso ou se obtido mediante informações incompletas ou de teor enganoso (arts. 8º, § 5º e 9º, § 1º, LGPD).

A Lei traz em seu artigo 5º todo um rol de definições, conceituando, em seu inciso XII, o 'consentimento' como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada", cuja descrição se demonstra relevante por carregar densa carga principiológica, sobretudo no aspecto da autodeterminação informativa, um dos fundamentos da LGPD (art. 2º, II).

É também exigência legal que a obtenção do consentimento para tratamento de dados pessoais seja realizada por escrito ou *"por outro meio que demonstre a manifestação de vontade do titular"* (art. 8º, § 1º), com cláusula em

30 Op. cit., p. 359.

destaque, cabendo ao controlador o ônus da prova quanto à regularidade do consentimento obtido (art. 8º, § 2º). FRAZÃO (2018), sustenta que o consentimento é *qualificado*, ao afirmar que

> "(...) a manifestação de vontade precisa ser (i) livre e inequívoca, (ii) formada mediante o conhecimento de todas as informações necessárias para tal, o que inclui a finalidade do tratamento de dados, e (iii) restrita às finalidades específicas e determinadas que foram informadas ao titular dos dados."[31]

Cabe atentar ao fato de que o consentimento se torna ainda mais qualificado, quando se pretende o tratamento de dados pessoais sensíveis (art. 11, I) e de menores de idade, caso em que o consentimento deverá ser manifestado por um dos pais ou responsável legal pelo menor (art.14, § 1º).

Com base nestas considerações, conclui-se que esta nova cultura imposta – de maneira ainda mais ostensiva – pela LGPD visa à efetiva proteção, em sentido material, da privacidade dos titulares de dados pessoais e traz grande impacto sobre a atividade empresarial, demandando adequações operacionais no tratamento de dados, mas também providências jurídicas para que as 'regras do jogo' sejam claras e estejam compreendidas e aceitas pelos envolvidos, a fim de prevenir a ocorrência de danos e prejuízos aos

31 FRAZÃO, Ana. **Nova LGPD: a importância do consentimento para o tratamento dos dados pessoais**; disponível em https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-a-importancia-do-consentimento-para-o-tratamento-dos-dados-pessoais-12092018; acesso em 31/10/2018.

usuários e à sociedade em geral, bem como às próprias empresas que realizarem o tratamento de dados pessoais.

Para efetivamente prevenir a ocorrência de danos e prejuízos, importante analisar as funções do controlador e do operador de dados.

4. A figura do Data Protection Officer (DPO)

Uma das obrigações impostas pela LGPD é a necessidade dos controladores de dados pessoais, sejam eles entes públicos ou privados, terem que indicar um encarregado (DPO - *Data Protection Officer*), pessoa natural ou jurídica, que deverá ser o profissional responsável pela proteção dos dados tratados e atuará como intermediador da comunicação entre o controlador e os titulares e a autoridade nacional[32].

A identidade do encarregado e a forma de comunicação deverão ser publicadas no site do controlador de maneira clara e objetiva, com a finalidade de facilitar requisições e comunicados dos titulares dos dados e da autoridade nacional.

Inicialmente as atividades do encarregado consistirão em receber reclamações e requisições dos titulares de dados, interagir com autoridade nacional de proteção de

32 BRASIL. **Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 2 de novembro 2018.

dados, orientar os funcionários e prestadores de serviços a respeito de boas práticas, bem como adotar as providências necessárias de proteção dos dados tratados.

Desta forma, é fundamental que o encarregado tenha conhecimento, e possa acompanhar e se envolver com todos os fluxos de processos realizados dentro da empresa controladora, bem como auxiliar diretamente no desenvolvimento de produtos e serviços, na elaboração de termos de consentimento, no processo de anonimização dos dados armazenados em bancos de dados, entre outros, de maneira que possa supervisionar todas as práticas de tratamento de dados, e certificar se estão em *compliance* com a Lei Geral de Proteção de Dados.[33]

Para isso, será de suma importância que o encarregado desempenhe suas funções com autonomia e imparcialidade dentro das organizações, podendo ele interferir nos processos internos, e sugerir mudanças e adequações, mesmo que isso afete economicamente a empresa, tendo em vista que sua motivação principal deve ser a de fazer com que a empresa cumpra as normas impostas pela legislação[34].

---

33 MARCONDES, Juliana. **Quem é o Data ProtectionOfficer?**. Disponível em: <http://www.plmj.com/xms/files/2017_PDF/junho/Quem_e_o_Data_Protection_Officer.pdf>. Acesso em: 2 de novembro 2018.

34 LEORATTI, Alexandre. **Nova lei de dados cria carreira no Direito com salários de até R$ 50 mil**. Disponível em: <https://www.jota.info/carreira/dados-dpo-carreira-direito-salarios-23102018>. Acesso em: 2 de Novembro de 2018.

Além disso, a autoridade de proteção de dados, poderá através de normas complementares incluir novas atribuições ao encarregado, bem como definir sobre as hipóteses de dispensa da necessidade de sua indicação, conforme o tamanho e a natureza da empresa, bem como o volume de tratamento de dados.

Em linhas gerais, o encarregado pela proteção de dados dentro das empresas controladoras, deverá ser um profissional, com expertise em legislação de proteção de dados, tecnologia da informação em especial criptografia, e gestão de processos, que desempenhará um papel muito importante dentro das empresas a partir da vigência da Lei Geral de Proteção de Dados, e deverá estar capacitado para agir em prol do cumprimento da lei.

5. Conclusão

Diante da universalidade de dados pessoais existentes no mundo virtual, e das novas consequências impactantes na sociedade, foi necessário a criação de legislações específicas sobre o tema. Nesse panorama, a Lei Geral de Proteção de Dados, Lei n.º 13.709/2018, foi promulgada no Brasil.

Com isso surgiram novos desafios, especialmente para quem manuseia dados pessoais, a exemplo das empresas privadas. Diante disso, surge a importância do presente estudo, que vem com o intuito de encontrar soluções práticas para a adequação à nova legislação por parte das pessoas jurídicas de direito privado.

Inicialmente, foi apresentada a ideia de *Compliance* como meio de garantir a correta aplicação da nova legislação. Para a instituição do Programa de Integridade, além da observância dos princípios que protegem direitos fundamentais, é necessário ter boa governança corporativa, fazer a correta gestão dos riscos, possuir uma boa estrutura tecnológica de segurança da informação e capacitar adequadamente as equipes de funcionários.

Em seguida, restou demonstrada a importância das funções dos Termos de Uso e Políticas de Privacidade, que possuem como finalidade informar sobre a utilização dos dados pessoais, de forma clara e transparente. Apesar de possuírem natureza instrumental de contratos, os Termos de Uso e Políticas de Privacidade se mostram como uma "Carta de Intenções", acerca da coleta e manipulação dos dados pessoais do usuário. Diante disso, foi verificada a importância do consentimento do titular dos dados pessoais para a sua proteção.

Por fim, foi analisada a figura obrigatória do *Data Protection Officer*, que recai sobre o encarregado. Este será sempre pessoa física, responsável pela proteção dos dados pessoais, atuando também como intermediador entre o controlador e os titulares e a autoridade nacional.

Muitos desafios vão surgir para as empresas privadas que manipulam dados pessoais com a futura vigência da Lei Geral de Proteção de Dados. Contudo, os primeiros passos de proteção já se mostram perceptíveis. E, tendo em

vista a proximidade da vigência da nova lei, a atuação para a conformidade deve ser imediata.

Referências bibliográficas

BARROS, Augusto Paes de. **Gestão de Risco.**In CABRAL, Carlos; CAPRINO, Willian (org.). Trilhas em Segurança da Informação, Caminhos e Ideias para a Proteção de Dados. Rio de Janeiro: Brasport, 2015.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 2 de novembro 2018.

CAVALCANTI, Natália Peppi; SANTOS, Luiza Mendonça da Silva Belo.**A Lei Geral de Proteção de Dados do Brasil na era do Big Data.** *In* Tecnologia Jurídica & Direito Digital - II Congresso Internacional de Direito, Governo e Tecnologia. 2018.

DONEDA, Danilo. **Proteção de dados pessoais nas relações de consumo: para além da informação creditícia**. Brasília: SDE/DPDC. 2010.

FRANÇA, T. C.; FARIA, F. F.; RANGEL, F. M.; FARIAS, C. M.; OLIVEIRA, J..**Big Social Data: Princípios sobre coleta, tratamento e análise de dados sociais.** Artigo publicado nos anais do XXIX Simpósio Brasileiro de Banco de Dados (SBBD) 2014. Curi-

tiba. 2014, p. 8. Disponível em: http://www.inf.ufpr.br/sbbdsbsc2014/sbbd/proceedings/artigos/pdfs/127.pdf. Acesso em: 29/10/2018.

FRAZÃO, Ana. **Nova LGPD: principais repercussões para a atividade empresarial**, 2018.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: 31/10/2018.

FREITAS, Cinthia Obladen de Almendra; PAMPLONA, Danielle Anne. **A complexa relação entre negócios e direitos humanos: as violações dos direitos de personalidade por meio de Tracking e Profiling em serviços online.** 2018.

LEORATTI, Alexandre. **Nova lei de dados cria carreira no Direito com salários de até R$ 50 mil**. Disponível em: <https://www.jota.info/carreira/dados-dpo-carreira-direito-salarios-23102018>. Acesso em: 2 de Novembro de 2018.

MAGRANI, Eduardo. **Democracia conectada: a internet como ferramenta de engajamento político-democrático**. Curitiba: Juruá. 2014.

MARCONDES, Juliana. **Quem é o Data Protection Officer?**. Disponível em: <http://www.plmj.com/xms/files/2017_PDF/junho/Quem_e_o_Data_Protection_Officer.pdf>. Acesso em: 2/11/2018.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental.** São Paulo: Saraiva, 2014.

RIBEIRO, Márcia Carla Pereira; GALESKI JUNIOR, Irineu. **Teoria geral dos contratos: contratos empresariais e análise econômica**. 2ª ed. São Paulo: Editora Revista dos Tribunais. 2015.

SILVA, Felipe. **Gestão de Identidades e Acessos.**In CABRAL, Carlos; CAPRINO, Willian (org.). Trilhas em Segurança da Informação, Caminhos e Ideias para a Proteção de Dados. Rio de Janeiro: Brasport, 2015.

VENOSA, Sílvio de Salvo. **Direito civil: teoria geral das obrigações e teoria geral dos contratos.** 14ª ed. São Paulo: Atlas. 2014.

VERÍSSIMO, Carla. **Compliance: incentivo à adoção de medidas anticorrupção**. São Paulo: Saraiva, 2017.