

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: UM NOVO DESAFIO PARA O VAREJO.

Lucas Souza dos Anjos¹

1. Introdução; 2. A lei geral de proteção de dados pessoais; 2.1. Aspectos gerais; 2.2. Princípios; 3. A transformação digital do setor varejista; 4. Novo desafio para o varejo; 5. A legitimação de processos; 6. Considerações finais; Referências bibliográficas.

RESUMO

Na era digital outro grande desafio se levanta para o mercado interno através de novas regulamentações, estas que colocam em xeque toda a ciência mercadológica até então desenvolvida. Ocorre que o desenvolvimento tecnológico trouxe nova roupagem aos antigos modelos de negócios, em especial ao varejo, que hoje possui como principal insumo informações pessoais. A possibilidade de coleta, organização, tratamento e armazenamento (*big data*) destes dados de maneira escalável já são possíveis, mas ordinariamente prevalece de forma promiscua e sem garantir a autodeterminação informacional dos titulares daquelas informações. Neste cenário que a Lei Geral de Proteção de Dados Pessoais (LGPD) surge e impõe novas regras, não somente para ampliar o rol de direitos dos titulares de dados pessoais, mas para viabilizar o desenvolvimento de novas atividades que, em virtude de sua natureza, não se submetem às leis setoriais vigentes. O presente estudo tem por escopo frisar a importância deste marco como ferramenta de legitimação de processos que dependem de informações pessoais, isto que se apresenta como um verdadeiro desafio à medida que novos ditames deverão ser observados para permitir a continuidade do modelo de negócio e não obstar inovações no setor.

Palavras Chaves: Varejo. Inovação. Dados Pessoais. Autodeterminação informacional

¹ Acadêmico de direito na Universidade São Judas Tadeu –SP.

ABSTRACT

In the digital age, another big challenge comes to the domestic market through new regulations that highlight all the marketing science developed. Technological development has brought a new aspect to the old business models, especially retail, which today has personal information as its main input. The possibility of collecting, organizing, processing and storing data in a scalable way is already possible, but ordinarily prevails indiscriminately and without guaranteeing the informational self-determination of the information holders. In this scenario, the General Law on Personal Data Protection (GLPDP) emerges and imposes new rules, not only to extend the rights of personal data holders, but also enables the development of new activities that, due to their nature, are not subject of the current sectoral laws. This study aims to emphasize the importance of this modality as a tool for legitimizing processes that depend on personal information and become a real challenge as new aspects will emerge to allow the continuity of the business model and not limit innovations in the sector.

Keywords: Retail. Innovation. Personal data. informational self-determination.

1. INTRODUÇÃO.

As novas condições impostas pela Lei Geral De Proteção De Dados Pessoais (LGPD) aos *players* do mercado no tocante ao tratamento de informações pessoais, em especial ao setor varejista, para a continuidade, promoção e inovações de seus negócios são os fatores que serviram para delimitar o objeto da pesquisa.

A justificativa principal da investigação se refere à transformação digital levada a efeito sobre o modelo tradicional varejista, que culminou na transmutação de processos do *off-line* para o *on-line* bem como a necessidade de personalizar cada vez mais a experiência do produto ou serviço ofertado, já que o consumidor está cada vez mais familiarizado com as novas ferramentas digitais, especialmente as redes sociais. Com isso, constata-se que a tônica de muitos negócios passa a ser a publicidade direcionada.

Outra constatação é que, diante desta perspectiva, o tratamento eficaz de informações pessoais passa a ser essencial para atividades relacionadas à estrutura organizacional da empresa, bem como para promover o seu próprio *core business*.

Diante deste quadro, a pesquisa se propõe a contextualizar a Lei Geral de Proteção de Dados Pessoais brasileira como um importante marco regulatório na defesa de direitos e garantias fundamentais dos cidadãos e a partir disso, investigar alguns dos possíveis caminhos para a adequação de processos que dependem de dados pessoais, sem que haja risco para o modelo de negócio adotado pelas empresas do setor, ou obste inovações.

Para melhor desenvolvimento do tema, o artigo científico foi estruturado de maneira que primeiro se abordam o contexto histórico de aprovação da Lei Geral de Proteção de Dados Pessoais, seus aspectos gerais, principais conceitos e alguns de seus princípios norteadores, estes que também impõem deveres às empresas.

Após, procurou-se destacar o papel ativo do consumidor no ciclo de produção de bens e formatação de serviços, bem como a identificação de três atividades eventualmente essenciais para empresas do setor varejista que dependem da coleta de informações pessoais.

Ao longo do percurso, constatou-se que a citada legislação trouxe um novo grande desafio para o varejo, e a partir disso cuidou a pesquisa de identificar meios para uma correta adequação à lei e a legitimação de seus processos.

2. A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS.

Em compasso com o cenário internacional, tramitou no Congresso Nacional brasileiro projeto² que desencadeou a Lei n.º 13.709/2018, sancionada em agosto de 2018³, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), que objetiva em síntese, reforçar direitos e garantias dos cidadãos⁴, enquanto pessoas físicas, que possuem informações pessoais em circulação no mercado bem como simplificar as regras para as empresas na era digital.

A mencionada regulação surge a partir de um contexto social familiarizado com as novas ferramentas digitais, cuja informação pessoal toma um lugar de destaque na concepção e aprimoramento de mecanismos de promoção e manutenção de negócios.

Com a aparente necessidade de se coletar cada vez mais informações, a criar indeterminados bancos de dados e promover o compartilhamento desses com uma indeterminada soma de parceiros comerciais, e estes com tantos outros, é de se imaginar a conseqüente potencial violação de direitos (diga-se, já garantidos legalmente⁵) das pessoas identificáveis por estes dados.

Imperioso destacar que o Brasil não está caminhando por terreno desconhecido, de maneira que se alinha ao comportamento global. Em meados do ano de 2019 cerca de 109 países já possuíam leis gerais de proteção de dados pessoais⁶, incluindo a Áustria, Bélgica, República Checa, Finlândia, Hungria, Irlanda, Itália, Suíça e Inglaterra. Não obstante, se vê como a principal fonte de inspiração para o direito doméstico os atuais⁷ instrumentos legislativos referendados pela União Europeia.

² Projeto de Lei da Câmara n.º 53 de 2018 (PL n.º 4060/2012, na Casa de origem), de iniciativa do Deputado Federal Milton Monti (PL/SP).

³ Projeto de Lei da Câmara n.º 53 de 2018 foi sancionada com Veto Parcial n.º 33/2018.

⁴ Art. 5º, inciso 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;”(BRASIL) Constituição da República Federativa do Brasil de 1988.

⁵ São algumas das leis setoriais de proteção de dados pessoais vigentes no ordenamento jurídico pátrio: (i) proteção dos dados pessoais dos consumidores: Código de Defesa do Consumidor (artigos 43 e 44); (b) proteção dos dados pessoais para fins de análise de crédito: Lei do Cadastro Positivo (Lei n.º 12.414/2011); (c) proteção dos dados no âmbito da transparência da Administração Pública: Lei de Acesso à Informação Pública (artigo 31 da Lei n.º 12.527/2011); (d) proteção de dados pessoais dos usuários de internet: Marco Civil da Internet (artigo 3º, incisos II e III, 7º a 17 da Lei n.º 12.965/2014).

⁶ DONEDA, Danilo, *Privacidade e Proteção de Dados Pessoais*, in: , Brasília: [s.n.], 2017.

⁷ A proteção de dados pessoais na União Europeia foi matéria de diversas regulamentações anteriores de sua legislação geral (GDPR). Citamos a Carta dos Direitos Fundamentais da EU (2000/C 364/01); Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, de 28.01.1981 e a Convenção Europeia dos Direitos do Homem (CEDH).

Apesar da promulgação da Convenção n 108⁸ pelo Conselho da Europa que entrou em vigor em 1985 e o fato de que desde 1997 aproximadamente 15 países membros do bloco europeu já possuíam legislação nacional com diretrizes compatíveis com a Convenção, o grau de proteção às informações pessoais não se deu de forma uniforme no continente.

Diante deste quadro a União Europeia editou a Diretiva 95/46/EC, aprovada em 1995, esta que foi um divisor de águas visto que cuidou de harmonizar as leis internas de cada país do bloco europeu sobre proteção de dados pessoais e com isso, assegurar certo grau de proteção comum, permitindo o livre fluxo de informações.

Atualmente, a Diretiva Europeia 95/46/EC foi substituída em 2016 pelo Regulamento Geral de Proteção de Dados Pessoais (*General Data Protection Regulation* ou *GDPR*)⁹, que entrou em vigor dois anos depois, em 25 de maio de 2018, que muito embora com a mesma finalidade de sua antecessora agrega os novos conceitos contemporâneos da internet, como *big data*, computação em nuvem, marketing comportamental, aplicativos, redes sociais e outros¹⁰.

Esta diretiva passou a ser diretamente aplicável a todos os membros da União Europeia e a vincular toda e qualquer organização que ofereça bens ou serviços no território europeu, mesmo que essas empresas tenham sede fora dela.

Trata-se, portanto, de um instrumento de grande importância na defesa dos direitos singulares no universo cada vez mais baseado em dados em face de violações de privacidade.

2.1. Aspectos gerais.

Alguns dos conceitos aprimorados pela nova regulação ou ali concebidos foram, em grande parte, fontes de inspiração ou ate mesmo incorporadas integralmente na Lei Geral de Proteção de Dados Pessoais brasileira, a exemplo do que será considerado um dado pessoal, dado pessoal sensível, formula mais rígida para se aperfeiçoar o consentimento, outras hipóteses que legitimam o próprio tratamento de dados, o direito ao esquecimento e a vinculação extraterritorial.

Se aproximar dos conceitos estampados no escopo da LGPD é essencial para, especialmente, compreender a extensão e os limites de sua atuação.

⁸Convention for the protection of individuals with regard to automatic processing of personal data.

⁹Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (General Data Protection Regulation).

¹⁰ FERREIRA, Ricardo *et al*, Entra em vigor o Regulamento Geral de Proteção de Dados da União Europeia, 2016.

A lei geral brasileira de proteção de dados formula o que venha a ser dado pessoal de forma expansionista, à medida que considera para tanto qualquer informação relacionada à pessoa natural identificada ou identificável, esta que é a titular dos dados. Para fins de informação, deve-se compreendê-la da maneira mais abrangente possível, desde nome, idade, endereço, até dados de geolocalização, perfis de compras, número do *Internet Protocol* (IP), histórico de compras, relativos a perfil comportamental, dentre outros.

Em apertada síntese, qualquer informação que possua qualidade de ser cogitada como um prolongamento da pessoa ali identificada ou passível de assim ser¹¹.

Norte outro, não escapa da ótica do legislador a necessidade de conceder proteção especial a determinada espécie de dado pessoal, em virtude de guardar em seu conteúdo certa carga de vulnerabilidade do titular, objetivando frear práticas discriminatórias. Estes são chamados de dados sensíveis, que, por exemplo, exprimem a orientação sexual, religiosa, política, referente à saúde ou à vida sexual¹².

Todo e qualquer acesso, desde a coleta, utilização ou eliminação é considerada para fins legais tratamento de dados pessoais¹³, e os agentes de tratamento são denominados de controlador, pessoa jurídica ou natural, de direito público ou privado, a quem competem às decisões referentes ao tratamento e operador, pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento dos dados em nome do controlador.

As companhias igualmente deverão indicar um responsável para atuar como canal de comunicação entre o controlador, os titulares e a Autoridade Nacional de Proteção de Dados (ANPD). Figura anglicana do *Data Protection Officer* (DPO) incorporada à LGPD como encarregado¹⁴, que pode ser assumido por uma pessoa natural ou jurídica.

O encarregado parte do pressuposto de ser uma das obrigações legais e possui um rol de tarefas que vão desde a prestar esclarecimentos e adotar providências quando deparado

¹¹ BIONI, Bruno Ricardo, **Proteção de dados pessoais: a função e os limites do consentimento**, Rio de Janeiro: Forense, 2019. p. 68. “Em outras palavras, um dado que não avoque tal qualidade não poderia ser cogitado como um prolongamento da pessoa por lhe faltar centro de imputação.”

¹² Art. 5º, inciso 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.”(BRASIL) Lei Geral de Proteção de Dados Pessoais (LGPD).

¹³ Art. 5º, inciso 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;”*Ibid.*

¹⁴ Art. 5º, inciso 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).”*Ibid.*

com reclamações e comunicações de titulares a promover o treinamento de funcionários que lidam com dados pessoais em suas responsabilidades¹⁵.

Respostas às perguntas sobre “o que fazer se algo der errado, incluindo uma violação de banco de dados interno”, “quais violações, resultantes de causas acidentais ou deliberadas devem ser relatadas à Autoridade Nacional de Proteção de Dados (ANPD)” ou ainda “quais violações a empresa deve informar as pessoas”, estarão em sua rotina.

Importante frisar que a lei em pauta versa também de dados anonimizados¹⁶, ou seja, informações relativas a uma pessoa natural não passível de ser identificada ou pseudonimizadas¹⁷. Mas não abrange tratamentos desencadeados por pessoa natural para fins exclusivamente pessoais¹⁸, jornalísticos, artísticos, literários ou acadêmicos¹⁹ ou de segurança pública, defesa nacional, segurança do Estado, atividade de investigação e repressão de infrações penais²⁰.

2.2. Princípios.

O ordenamento legislativo busca tutelar os mais diversos bens, estes considerados historicamente como relevantes para sociedade, com este intuito a lei geral de proteção de dados pessoais insere no arcabouço jurídico, com o fito de criar direitos e obrigações, tanto regras quanto novos mecanismos de orientação para o processo de interpretação destas (princípios)²¹.

Apesar da manifesta importância dos princípios em uma norma que busca centralizar os institutos para a proteção de dados pessoais, iremos nos debruçar sobre aqueles que não de guardar ainda um maior impacto na tomada de decisões do setor varejista brasileiro frente à compatibilização de seus modelos de negócio.

Como evidenciado anteriormente, há uma predisposição à coleta de dados desenfreada para abastecimento de quantos *Big Data* se apresentem necessários. Em direção

¹⁵ Art. 41, §2º, inciso III. “orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;” *Ibid.*

¹⁶ 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.” *Ibid.*

¹⁷ Art. 13, §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”. *Ibid.*

¹⁸ Art. 4º, inciso I. *Ibid.*

¹⁹ Art. 4º, inciso II. *Ibid.*

²⁰ Art. 4º, inciso III. *Ibid.*

²¹ DWORIN, Ronald, **Levando Os Direitos A Sério**, 3. ed. São Paulo: Martins Fontes, 2010. Pg. 39.

contrária a essa pseudonecessidade do mercado as empresas brasileiras devem se voltar para os princípios da finalidade e necessidade no tratamento de dados pessoais.

O princípio da finalidade ou especificação de propósitos²² proíbe o tratamento de dados para propósitos que não sejam legítimos, específicos, explícitos ou que não tenham sido informados ao titular. Ato contínuo veda o tratamento posterior dos dados pessoais coletados para finalidades incompatíveis com aquelas originais, informadas no momento da coleta.

Ao passo que o princípio da necessidade, ou minimização, orienta os agentes a não proceder com a coleta excessiva de dados não compatíveis com o propósito informado. Este comando legal pode ser visualizado de duas frentes, seja por oferecer um maior controle ao titular destes dados, visto que terá menos informações em fluxo²³, seja por reduzir riscos aos agentes de tratamento diante de eventual incidente de segurança.

Norte outro, as empresas terão de adequar os seus sistemas de coleta e especialmente de armazenamento de dados pessoais, tanto com a adoção de medidas técnicas e administrativas aptas a protegê-los quanto preveni-los de acessos não autorizados, situações acidentais ou ilícitas.

Isso porque os agentes de tratamento, sob pena de responsabilização, terão o dever de demonstrar a 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.

Por fim, hão de serem observados, com igual rigor, o princípio do livre acesso, transparência e o da não discriminação, com garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e duração do tratamento, bem como a atualidade de suas informações pessoais.

Observa-se que todos os princípios elencados na Lei Geral de Proteção de Dados Pessoais brasileira (LGPD) constituem não só uma orientação geral para interpretação das disposições nela positivadas, mas em si, criam novos deveres, ações positivas que deverão ser levadas a efeito pelas empresas.

A ordem prática que se extrai destas disposições mandamentais é a necessidade de se desenvolver, adequar ou aperfeiçoar as diferentes plataformas de coleta direta de informações pessoais, seja de cadastros de consumo, pelo acesso a *websites*, programas de fidelidade, contrato de trabalho além de suas políticas de privacidade.

²² MENDES, Laura Schertel, **transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo.**, Dissertação(Mestrado em Direito), Faculdade de Direito da Universidade de Brasília, Brasília, 2008. Pg. 47

²³ BIONI, **Proteção de dados pessoais: a função e os limites do consentimento.** Pg. 123

Para estar em conformidade, portanto, os registros devem, a um primeiro momento, de maneira precisa dispor sobre quais dados pessoais estão sendo coletados, para qual motivo, por quanto tempo pretende mantê-los e se há interesse em compartilhá-los.

Em um segundo momento, a minimização de informações pode ser referendada pela coleta de dados necessários para aquele motivo específico. Garantir que as pessoas saibam a diferença entre informações que precisam fornecer e as que são opcionais é uma possibilidade.

Pressupõe-se que a garantia do livre acesso, consubstanciada na possibilidade de a empresa dispor de meios para que os titulares exerçam seus direitos sobre seus dados que aquela possui em seu poder, é um dos grandes desafios a ser enfrentado.

Isto porque toda pessoa terá, a partir da entrada em vigor da mencionada lei, direito de ser informado sobre quais dados a empresa possui e o que faz com eles; de acesso, podendo inclusive solicitar uma cópia dos dados armazenados; direito de solicitar a correção e retificação de dados imprecisos ou desatualizados; de solicitar que a controlador exclua qualquer informação a ele relacionada; direito de solicitar a qualquer momento a portabilidade de dados, através da transferência eletrônica de dados para outra instituição; direito de solicitar a interrupção de uso daqueles dados dentre outros²⁴.

²⁴ Art. 18, incisos I-VIII. (BRASIL) Lei Geral de Proteção de Dados Pessoais (LGPD).

3. A TRANSFORMAÇÃO DIGITAL DO SETOR VAREJISTA.

A convergência digital levada a efeito sobre o modelo tradicional varejista pode ser percebida sob duas grandes dimensões, a primeira delas dialoga com situações externas, situa-se na relação de consumo, no próprio *core business*. Enquanto que outro grande âmbito igualmente afetado se estende pela estrutura organizacional interna da empresa que igualmente tiveram seus processos digitalizados e partem do tratamento de informações pessoais, como por exemplo, o setor de recursos humanos.

É notável que a transformação digital impôs mudanças significativas a empresas de diversos setores, e igualmente uma etapa a ser transposta seja pelo empresário de pequeno, médio ou grande porte. Estas que vão além da necessária transmutação de processos do *off-line* para o *on-line*, mas precisamente o modo como se relacionar com o consumidor.

A cultura digital está emancipada e se desenvolvendo a passos largos, e a partir disso, o consumidor está mais educado, exigente, conectado e com mais possibilidades de pesquisar, comparar preços e comprar *on-line*²⁵. Deve-se então encará-lo não mais um mero expectador de suas informações pessoais em rede, mas como um sujeito ativo no ciclo de consumo, o consumidor então não apenas consome, também produz o bem de consumo (*prosumer*)²⁶.

Isto que se confirma à medida que o consumo e o seu processo de produção passam a serem resultantes, cada vez mais, de recomendações que as pessoas fazem em seus canais particulares de opiniões a partir de suas redes, especialmente pela *web*, com seus *websites*, *blogs*, redes sociais (*facebook*, *instagram*, *twitter*, *linkedIn*, *youtube...*)²⁷ etc., resultantes de suas experiências diretas com o produto ou serviço. Ainda assim, estas que escolhem se tal experiência é ou não digna de indicação²⁸.

²⁵ PORTUGAL, Filipe; ARAÚJO, Fernando, Os desafios do varejo na era digital – recap Fórum e-commerce Brasil 2016, 2016. “Com a mudança de cultura do consumidor, que está mais educado, mais exigente, mais conectado e com mais possibilidades de pesquisar, comparar preços e comprar online, as soluções digitais se tornaram fundamentais para que as empresas estejam engajadas com os clientes de diferentes maneiras.”

²⁶ BIONI, **Proteção de dados pessoais: a função e os limites do consentimento**. Pg. 15: “O consumidor deixa, portanto, de ter uma posição meramente passiva no ciclo do consumo. Ele passa a ter uma participação ativa, que condiciona a própria confecção, distribuição e, em última análise, a segmentação do bem de consumo, transformando-se na figura do *prosumer*. O consumidor não apenas consome (*consumption*), mas, também, produz o bem de consumo (*production*): *prosumer*.”

²⁷ TORRES, Claudio, **A bíblia do marketing digital**, São Paulo: Novatec, 2009. Pg. 24: “Novas tecnologias e aplicações, como os blogs, as ferramentas de busca, os fóruns, as redes sociais e tantas outras aplicações on-line foram utilizadas pelos internautas para, literalmente, assumir o controle, a produção e o consumo da informação, atividades antes restritas aos grandes portais”

²⁸ CARLOS, Piazza, Como será o futuro do varejo?, 2016. “Quando se faz uma análise destas vertentes todas, chega-se à conclusão que a base futura de relacionamento, portanto, de consumo, está muito delegada às

Assim, o produto ou serviço que chega ao final do ciclo foi de certa forma, construído a partir das informações prestigiadas pelos consumidores²⁹. Este papel ativo, portanto, dá uma nova atribuição positiva aos consumidores enquanto produtores de bens de consumo³⁰.

O diagnóstico dessa perspectiva é que para se alcançar o consumidor da era digital é preciso se afastar do modelo tradicional e personalizar cada vez mais a experiência com o produto ou serviço ofertado. Em decorrência disso pode-se falar que a publicidade direcionada tornou-se a tônica de muitos modelos de negócios. Por outro lado, para atingir este objetivo o tratamento eficaz de informações pessoais torna-se cada vez mais imprescindível.

A outra dimensão da crescente transformação em decorrência do avanço da tecnologia é aquele relacionado à estrutura organizacional da empresa. Desde o setor responsável pelos recursos humanos ao de TI (tecnologia da informação), a tônica de uso de dados pessoais está presente e ganha potência na digitalização de processos.

As empresas possuem um interesse legítimo em resguardar os seus segredos comerciais, propriedade intelectual e informações sensíveis, aqui também compreendidos tanto bancos de dados quanto informações disponíveis na rede de computadores de empregados.

Em virtude da assunção dos riscos da atividade econômica desenvolvida, permite-se que o empregador³¹ se utilize de mecanismos de monitoramento de atividades de computadores com o intuito de melhorar a produtividade dos funcionários, gerir riscos, investigar fraudes e até mesmo combater condutas dissonantes do ofício.

O monitoramento de funcionários através de software já é uma realidade, permitindo ao empregador, por meio de coleta de dados, saber quanto tempo foi despendido em jogos casuais e socialização, além de acessar o registro de teclas pressionadas, monitoramento de tráfego de rede, *key-logger* e capturas de tela.

Recomendações Que As Pessoas Fazem A Partir Do Centro De Conexão De Suas Redes, Diretamente E São Elas Que Pontuam Se Uma Experiência É Digna Ou Não De Ser Colocada Para Suas Redes.”

²⁹ Matos, Karla Cristina Da Costa E Silva, **O Valor Econômico Das Relações De Consumo**, 1. Ed. São Paulo: Almedina Br, 2012. Pg. 131-149.

³⁰ Lisboa, Roberto Senise. Prefácio. *Ibid.* Pg. 16: “O Acesso À Informação, Como Direito Fundamental E Direito Básico Dos Consumidores, Transforma-Os Em *Prosumers*, Ou Seja, Participantes Ativos Na Própria Confecção, Distribuição, Aquisição E Descarte De Produtos E Serviços Colocados No Mercado Pelos Fornecedores”.

³¹ Art. 2º. Brasil, Decreto-Lei Nº 5.452, De 1º De Maio De 1943. Aprova A Consolidação Das Leis Do Trabalho.

Lado outro, há algum tempo se discute em ações na justiça do trabalho acerca da possível violação da intimidade e privacidade de empregados em detrimento da utilização ostensiva de câmeras de vigilância³².

Muito embora já esteja em nosso cotidiano o acionamento das empresas por empregados demandando reparação moral em decorrência de influências nocivas carregadas por esta vigilância em um grau mais elevado, relembramos que imagens capturadas são dados pessoais para fins da Lei Geral de Proteção de Dados. Desta forma, acredita-se que temas como este poderão ser (re)apreciados sob uma nova roupagem com a entrada em vigor da referida norma, o que propositalmente reforça o dever de adequação das companhias.

Processos de checagem de informações em currículos de candidatos a vagas de emprego igualmente merecem uma atenção especial, isto porque a consultoria de risco, ou "*background check*", seja prestada por uma empresa terceirizada ou realizada pelo próprio empregador, consubstancia-se primordialmente na coleta, compartilhamento e mineração de dados pessoais para embasar a tomada de decisões.

Este tipo de checagem já é rotina nas grandes companhias e tende a se expandir para os médios e pequenos negócios, à medida que os meios deixam de ser integralmente manuais e a busca passa a ser via inteligência artificial em grandes bancos de dados, o que diminui expressivamente o custo por candidato.

Além disso, a necessidade de tal serviço se confirma à proporção que, em virtude da exigência cada vez maior do mercado em obter mão de obra qualificada, as pessoas tendem a “exagerar” ao fornecer suas informações pessoais, especialmente no tocante a titulação acadêmica, habilidades, atividades sob sua responsabilidade no trabalho anterior, conhecimento em línguas estrangeiras e etc.

Ocorre que as consultas que compõem "*background check*" vão desde telefonemas a buscas pelo histórico financeiro do candidato, seus "*posts*" ofensivos nas redes sociais, situação jurídico-criminal e até mesmo filiações e participação política. Alguma das informações pessoais, portanto, que a LGPD classifica como dados pessoais sensíveis, alvos de maior proteção e hipóteses de legitimação do tratamento menos concessivas.

³² REIS, Ricardo, Tecnologias de controle criam novas situações de dano moral, 2012.

4. NOVO DESAFIO PARA O VAREJO.

Os processos em análise de maneira alguma esgotam as atividades empresariais em que está presente o embate principiológico entre o exercício do poder diretivo do empregador, seus legítimos interesses e o direito à proteção dos dados pessoais de seus colaboradores.

O avanço tecnológico permitiu o incremento de novas tendências e formulas comercial, concebeu novos meios para o aperfeiçoamento de ferramentas de promoção de serviços e produção de bens, não bastasse, revestiu toda a estrutura organizacional das empresas digitalizando processos a partir do tratamento eficaz de dados pessoais, com o intuito de não só otimizar, mas prevenir riscos e fraudes.

Na esteira desta constante, consoante a mudança estática do consumidor para um papel ativo na economia da produção e o reconhecimento de que as informações pessoas são um prolongamento da própria personalidade, intimidade e privacidade, surgem, em um movimento global, leis que em ultima instância objetivam impor ao mercado uma nova cultura.

O respeito à privacidade e a autodeterminação informativa, a liberdade de expressão, de informação, de comunicação e de opinião³³, a transparência dos processos de tratamento de dados pessoais, a realização destes para propósitos específicos e informados aos titulares, a coleta do mínimo necessário para a consecução das atividades, a prevenção da ocorrência de danos em detrimento do tratamento de dados e, especialmente, a não utilização de dados pessoais para fins discriminatórios, ilícitos ou abusivos³⁴ fazem parte desta nova cultura.

Não obstante, o desafio colocado para as empresas, em especial as do setor varejista, este que está em constante escalada digital, é de como legitimar legalmente o tratamento de dados pessoais, tão essencial para os processos em curso, não colocando em risco o seu modelo de negócio ou obstruindo a inovação.

³³ Art. 4º. (BRASIL) Lei Geral de Proteção de Dados Pessoais (LGPD).

³⁴ Art. 6º. *Ibid.*

5. A LEGITIMAÇÃO DE PROCESSOS.

Para a finalidade de permitir o tratamento de dados pessoais a LGPD trouxe um rol consideravelmente abrangente, neste constam dez hipóteses de permissão³⁵, ou bases legais. A exceção está em caso de tratamento de dados pessoais sensíveis, de menores ou para fins de transferência internacional. Dentre as bases legais, para fins de exemplificar modos de adequação dos processos revisitados neste estudo, destacam-se o consentimento do titular e os legítimos interesses do controlador.

Ainda na esteira das regulamentações setoriais que conversam com esta temática, por exemplo, o Marco Civil da Internet, a base legal por excelência para o tratamento de dados pessoais é o consentimento do titular.

O consentimento se traduz na manifestação do titular do dado pessoal em concordar com a coleta deste para um tratamento específico³⁶. Muito embora não fora prescrito em lei de que forma deve se obter esta manifestação, para que este ato não seja posteriormente considerado nulo e o tratamento a partir dele não se torne ilegal, os agentes de tratamento devem se atentar para alguns requisitos.

É preciso, portanto, adequar qualquer que seja o meio de obtenção do consentimento, seja por escrito como, por exemplo, em um contrato de prestação de serviço, ficha de cadastro ou consumo, termo de privacidade ou digital, a fim de ali conter todas as informações necessárias sobre o tratamento de dados, de forma clara e ostensiva.

As informações que a legislação considera necessárias dizem respeito a finalidade do tratamento, duração do tratamento (importante se estabelecer um ciclo de vida para o dado pessoal coletado), identificação do controlador, se este dado irá ser compartilhado e caso positivo, para qual destinatário e sua finalidade e por fim, a menção explícita de todos os direitos do titular elencados no art. 18 da LGPD³⁷.

Observa-se que os requisitos acima vão ao encontro de tornar tal manifestação de vontade inequívoca, informada e transparente. Lado outro, tão importante quanto, e talvez ainda mais desafiador, será a de garantir que este consentimento se deu por uma manifestação livre.

Ao dizer que a manifestação deve ser livre encara-se a questão da possível assimetria da relação existente entre o controlador e o titular. Poderá ocorrer que em certo

³⁵ Art. 7º. *Ibid.*

³⁶ Art. 5º inciso XII. *Ibid.*

³⁷ Art. 18. *Ibid.*

contexto o titular pode estar em uma posição de subordinação para com o controlador, como por exemplo, precisar fornecer seus dados pessoais para participar de um processo seletivo para uma vaga de emprego, ter acesso a determinado produto ou serviço ou ainda permitir que haja um monitoramento excessivo de sua atividade laboral. Destarte que para análise do preenchimento deste requisito será quase sempre necessário realizar uma análise casuística³⁸.

Apesar de o consentimento ainda ser a base legal de maior destaque e que, pelo menos a princípio, tem o potencial de legitimar inúmeros processos que pendem de tratamento de dados pessoais, é evidente que há situações vinculadas a interesses das empresas que fugiriam da aplicação seja do consentimento ou das demais bases legais, como por exemplo, a execução de um contrato, exercício regular de direitos em processo judicial, para proteção da vida, tutela da saúde, dentre outros³⁹.

No intuito de suprir situações não embarcadas pelo consentimento, especialmente, na esteira do regulamento europeu de proteção de dados pessoais (GPDR), a LGPD incluiu no rol de bases legais o legítimo interesse, tal hipótese seria então mais flexível. Procurou-se ainda, a luz da experiência europeia⁴⁰, estatuir certos limites para sua utilização, a fim de não ser uma espécie de “carta branca” autorizadora de qualquer tipo de tratamento de dados.

O legítimo interesse é uma das hipóteses legais que autorizam a coleta, armazenamento, mineração ou a transferência de dados pessoais. A rigor, deve ser utilizado de maneira subsidiária às demais bases legais específicas e surge para atender interesses não do titular, mas do controlador ou de terceiro⁴¹.

Tratamentos que detenham uma finalidade legítima do controlador ou de terceiro considerado a partir de situações concretas, aqui incluindo o apoio e promoção das atividades da empresa, podem ser por aqui legitimados. Em contrapartida, todas as medidas técnicas e administrativas ao alcance devem ser tomadas para garantir a transparência deste tratamento, inclusive pondo à disposição do titular meios para fazer valerem seus direitos (informação, retificação, portabilidade...), bem como utilizar somente os dados pessoais estritamente necessários e respeitando as legítimas expectativas dos titulares.

³⁸ BIONI, **Proteção de dados pessoais: a função e os limites do consentimento**. Pg. 198.

³⁹ *Ibid.* Pg. 249 – “em muitas situações, seria: a) desnecessário coletar novo consentimento para outros usos (implícitos) dentro de uma relação já preestabelecida com o titular; ou b) quando terceiros: b.1) não tivessem meios para obter tal tipo de autorização; ou b.2) esse tipo de interação inviabilizaria o próprio tratamento dos dados.”

⁴⁰ Menciona-se o *Article 29 Working Party*, órgão de aconselhamento composto de representantes de todas as autoridades de proteção de dados pessoais dos países-membros da União Europeia. Foi substituído pelo *European Data Protection Board* quando da vigência da GDPR.

⁴¹ Art. 7, inciso IX. (BRASIL) Lei Geral de Proteção de Dados Pessoais (LGPD).

Veja-se que toda a adjetivação trazida pela LGPD em volta desta base legal, “finalidades legítimas”, “situações concretas”, “legítimas expectativas” está repleta de conceitos um tanto quanto vagos. Sendo assim, estamos diante de conceitos jurídicos indeterminados que a princípio, correm o risco de serem interpretados como uma verdadeira “carta branca”, apta a legitimar todas aquelas situações que fogem da aplicação das demais bases legais.

Fora mencionado anteriormente que a LGPD teve como principal inspiração as regulamentações do bloco europeu, sendo a principal delas a recente GDPR. É desta última que fora importado o legítimo interesse ainda ao longo das consultas públicas do então anteprojeto de lei de proteção de dados, e em atenção a experiência europeia já um tanto quanto consolidada sobre este tema, igualmente importou-se para o ordenamento brasileiro as regras de aplicação desta base legal⁴².

As regras para a aplicação do legítimo interesse consistem em um verdadeiro teste de proporcionalidade que se busca balancear os direitos dos titulares garantidos pela ordem jurídica em detrimento de um interesse legítimo do controlador ou de terceiro. Tal teste, composto de quatro etapas e que deve ser necessariamente documentado, parte de uma interpretação sistêmica de vários dispositivos da LGPD⁴³.

O teste de proporcionalidade do qual o controlador deverá se valer para se submeter ao legítimo interesse deve ser documentado e apresentar as seguintes verificações, compatibilizar o interesse com uma finalidade legítima, esta que deve representar um real benefício, não ser ilegal e compreendida a partir de uma situação concreta⁴⁴; a segunda etapa diz respeito necessidade de se legitimar o tratamento por esta base legal e não outra, bem como de garantir que serão coletadas apenas informações pessoais estritamente necessários⁴⁵ (princípio da minimização).

O balanceamento propriamente dito entre os interesses comerciais, como por exemplo, na (re) utilização de dados pessoais para outra finalidade diversa daquela que originou a coleta (caso em que a coleta fora legitimada pelo consentimento ou outra base legal) e a proteção de direitos fundamentais do titular, enquanto transparência, acesso, correção e outros, assim como os possíveis impactos negativos decorrentes da utilização de

⁴²BIONI, **Proteção de dados pessoais: a função e os limites do consentimento**. Pg. 250: “*Mutatis mutandis* foi o que se sucedeu no Brasil. Ao longo das consultas públicas e do debate legislativo da lei geral brasileira de proteção de dados, chegou-se ao denominador comum em torno da necessidade de se prever critérios para a aplicação do legítimo interesse.”

⁴³ *Ibid.* Pg. 253.

⁴⁴ Art. 10, *caput*, inciso I. (BRASIL) Lei Geral de Proteção de Dados Pessoais (LGPD).

⁴⁵ Art. 10, §1º. *Ibid.*

dados sensíveis ou ainda possíveis de acarretar tratamentos discriminatórios, deverá ser posto em xeque na terceira fase do teste⁴⁶.

Por fim, transpostas as primeiras fases e estando a balança tendendo a estar equilibrada, no relatório deverá ainda conter de maneira precisa os meios técnicos e administrativos criados ou reforçados para garantir a mitigação de riscos ao titular dos dados e transparência do tratamento⁴⁷.

Feito este estudo sobre a forma de como deve ser o consentimento, bem como os requisitos para a utilização do legítimo interesse, poder-se-á então ao colocar uma lupa sobre cada processo em que há tratamento de dados pessoais, em poucos passos, atribuir uma base legal apta a legitimá-lo sem maiores dificuldades.

No tocante a promoção de publicidade direcionada, aquela em que é viabilizada por meio da (re) utilização de informações pessoais já constantes no banco de dados do controlador, coletadas pelo consentimento ou outra base legal para distinta finalidade (por exemplo, dado coletado por meio de uma ficha de cadastro para a finalidade de execução da prestação do serviço ali contratado), pode-se dizer que em muitos casos obter um novo consentimento seria inviável, e, portanto, a princípio este processo poderá ser legitimado pelo legítimo interesse.

Tal postura se mantém, ao nosso olhar, quando diante do interesse do controlador em monitorar o comportamento on-line de seus funcionários a título de melhorar a produtividades destes e gerir riscos, como até mesmo a vazão de informações pessoais em rede. Diferente não ocorre com a vigilância do ambiente de trabalho.

Tais processos mencionados acima podem não se justificarem pelo consentimento em virtude de existir uma relação de submissão entre o titular do dado, o empregado, e o controlador. No entanto, as luz dos princípios, direitos e garantias dos titulares garantidos pela LGPD, é recomendável que na realização do teste de proporcionalidade busque-se evitar meios invasivos, ostensivos e desproporcionais à finalidade perquirida.

Ato contínuo, no que concerne a utilização de “*background-check*”, seja pelo controlador ou a seu pedido por uma empresa terceirizada o legítimo interesse igualmente se mostra mais razoável, haja vista que a uma evidente subordinação entre o candidato e o possível empregador, relação esta que pode ser óbice ao consentimento não adquirido de forma livre.

⁴⁶ Art. 7º, inciso IX e art. 10, inciso II. *Ibid.*

⁴⁷ Art. 10, §§2º e 3º. *Ibid.*

Foram então revistas quatro situações, vividas diariamente por inúmeros agentes econômicos que exploram as mais diversas atividades, em especial pelo setor varejista, que foram criadas, desenvolvidas ou até transformadas em razão da utilização de dados pessoais, e destes necessitam, cada vez mais, para sua manutenção.

Lado outro as bases legais do consentimento e legítimo interesse foram destacadas, o consentimento foi amplamente revisto pela nova legislação, reformando-o para lhe tornar mais transparente e disposto a permitir que o titular do dado pessoal tenha chances reais de fazer valerem os seus direitos, e o legítimo interesse por se tratar de um conceito juridicamente aberto necessita de criterioso olhar ao passo que a partir do momento em que eleito para legitimar algum tratamento, diversas obrigações surgem para o controlador.

6. CONSIDERAÇÕES FINAIS.

Em suma, o avanço tecnológico culminou na digitalização de processos, embasando-os em novas tecnologias que surgem a partir de um contexto social no qual a informação pessoal é o seu principal insumo. A partir disso, as empresas devem estar em compasso com a cultura do digital para alcançar o consumidor, que está mais conectado, exigente e detentor de ferramentas digitais de controle de preços.

Enquanto que cabe aos *players* do mercado encarar o consumidor sob outra ótica, à medida que este deixou de ser um mero expectador para ter um papel cada vez mais ativo no ciclo de produção dos próprios bens ou serviços que usufrui. Isto porque, hoje, dados pessoais são o insumo necessário para a própria concepção e aprimoramento de bens e serviços.

É neste cenário que surgem as novas regulamentações para, ainda que reconhecendo as necessidades do mercado, ampliar o rol de direitos e garantias das pessoas que possuem seus dados em rede, com a finalidade de lhes garantirem o próprio direito de autodeterminação informacional⁴⁸.

Desta forma, o desafio aqui colocado para as empresas é de como legitimar legalmente seus processos que dependem do tratamento de dados pessoais, não colocando em risco o seu modelo de negócio ou impedindo inovações.

Retrocede-se às regras do marco regulatório da Lei Geral de Proteção de Dados Pessoais para inicialmente compreender o seu escopo de aplicação, a necessidade de se distinguir as diferentes categorias de dado pessoal e as pessoas envolvidas diretamente com o tratamento, merecendo atenção especial o *DPO - Data Protection Officer*, pessoa natural ou jurídica que lhe será atribuído o papel de incorporar à rotina da empresa as boas práticas em relação à proteção de dados e atuar como canal de comunicação entre o controlador, os titulares e a Autoridade Nacional de Proteção de Dados.

Ao longo deste percurso foram realçados alguns dos princípios norteadores de toda a legislação, entre eles o princípio da finalidade, necessidade ou minimização, livre acesso e transparência do processo de tratamento de dados pessoais.

Ao passo que se passou a analisar detidamente alguns processos levados a cabo pelas empresas, em especial do setor varejista, que de algum modo dependem da utilização de informações pessoais, bem como as possíveis bases legais eventualmente mais propensas a

⁴⁸ DONEDA, Danilo, **Da privacidade à proteção dos dados pessoais**, Rio de Janeiro: Renovar, 2006.

legitima-los, como os citados consentimento e legítimo interesse do controlador ou de terceiro.

Ao final desta trajetória busca-se fixar a tese de que o principal desafio da era digital para o setor varejista é justamente adequar-se a este novo marco regulatório da proteção de dados pessoais, à vista da interconexão necessária existente dos processos, internos ou externos, com o tratamento eficaz de dados pessoais, sejam de clientes, empregados, fornecedores, parceiros, enfim, 'de informações pessoais.

A legislação em apreço, que está em período de vacância, se propôs a estatuir normas gerais que extrapolam as leis setoriais já vigentes sobre a proteção de dados pessoais, de modo que o debate sobre os seus significativos impactos nos mais diversos setores do mercado brasileiro está em plena efervescência e de modo algum se limitam a finalidade deste estudo.

Também pelo seu caráter regulatório geral, espera-se que a Autoridade Nacional de Proteção de Dados tenha um papel fundamental no sentido de introduzir os *players* do mercado (incluindo os consumidores) nesta nova cultura. Haja vista que estão no seu escopo de atribuições desde a emissão de pareceres à responsabilização administrativa dos agentes de tratamento em sanções que podem alcançar multa de até 2% (dois por cento) do faturamento da empresa, limitada a R\$ 50.000.000,00 (cinquenta milhões de reais), por infração.

REFERÊNCIAS BIBLIOGRÁFICAS.

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

BRASIL. DECRETO-LEI Nº 5.452, de 1º de maio de 1943. **Aprova a Consolidação das Leis do Trabalho**. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm>. Acesso em: 26 out. 2019.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 22 out. 2019.

BRASIL. **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: 22 out. 2019.

CARLOS, Piazza. **Como será o futuro do varejo?** 2016. Disponível em: <<https://www.linkedin.com/pulse/como-será-o-futuro-do-varejo-carlos-alberto-piazza-timoiaria>>. Acesso em: 22 out. 2019.

Convention for the protection of individuals with regard to automatic processing of personal data. Disponível em: <<https://rm.coe.int/1680078b37>>. Acesso em: 22 out. 2019.

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

DONEDA, Danilo. **Privacidade e Proteção de Dados Pessoais**. In: Brasília: [s.n.], 2017. Disponível em: <<https://www.cgu.gov.br/sobre/institucional/eventos/anos-anteriores/2017/5-anos-da-lei-de-acesso/arquivos/mesa-3-danilo-doneda.pdf>>. Acesso em: 26 jul. 2019.

DWORKIN, Ronald. **Levando Os Direitos A Sério**. 3. ed. São Paulo: Martins Fontes, 2010.

FERREIRA, Ricardo; BRANCHER, Paulo; TALIBERTI, Camila; *et al.* **Entra em vigor o Regulamento Geral de Proteção de Dados da União Europeia**. 2016. Disponível em: <<https://www.migalhas.com.br/dePeso/16,MI281042,81042-Entra+em+vigor+o+Regulamento+Geral+de+Protecao+de+Dados+da+Uniao>>. Acesso em: 27 jul. 2019.

MATOS, Karla Cristina da Costa e Silva. **O valor econômico das relações de consumo**. 1. ed. São Paulo: Almedina Br, 2012.

MENDES, Laura Schertel. **Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo**. Dissertação(Mestrado em Direito), Faculdade de Direito da Universidade de Brasília, Brasília, 2008.

PORTUGAL, Filipe; ARAÚJO, Fernando. **Os desafios do varejo na era digital – recap Fórum e-commerce Brasil 2016**. 2016. Disponível em: <<https://blog.euromonitor.com/os-desafios-varejo-na-era-digital-recap-forum-e-commerce-brasil-2016/>>. Acesso em: 22 out. 2019.

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (General Data Protection Regulation). Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679>>. Acesso em: 27 jul. 2019.

REIS, Ricardo. **Tecnologias de controle criam novas situações de dano moral**. 2012. Disponível em: <http://www.tst.jus.br/materias-especiais/-/asset_publisher/89Dk/content/id/2435588>. Acesso em: 26 out. 2019.

TORRES, Claudio. **A bíblia do marketing digital**. São Paulo: Novatec, 2009.