Insper

LLC de Direito Empresarial

Gabriela Gonçalves Sanchez

A incidência da Lei Geral de Proteção de Dados nas relações consumeristas celebradas entre as incorporadoras e compradores.

São Paulo

2021

Gabriela Gonçalves Sanchez

A incidência da Lei Geral de Proteção de Dados nas relações consumeristas celebradas entre as incorporadoras e compradores.

TCC apresentado ao programa de LLC de Direito Empresarial como requisito parcial para a obtenção do título de pós-graduada em Direito Empresarial.

Orientadora: Profa. Pamela Gabrielle Romeu Gomes Roque

São Paulo

2021

Sanchez, Gabriela Gonçalves.
A incidência da Lei Geral de Proteção de Dados nas relações consumeristas celebradas entre as incorporadoras e compradores. Gabriela Gonçalves Sanchez – São Paulo, 2021.
30 folhas.

TCC – Insper, 2021.
Orientadora: Profa. Pamela Gabrielle Romeu Gomes Roque

1. Incorporadoras. 2. Incorporação Imobiliária. 3. Lei Geral de Proteção de Dados. 4. Relação de Consumo.

Resumo

Em face da urgente necessidade de adequação das incorporadoras à vigente Lei Geral de Proteção de Dados, o presente trabalho aborda os principais dispositivos da referida lei, incluindo o estudo sobre os agentes de tratamento responsáveis pelos dados pessoais tratados pelas incorporadoras e a responsabilização destas.

Palavras-chave: Incorporadoras. Incorporação Imobiliária. Lei Geral de Proteção de Dados. Relação de Consumo.

Abstract

Given the urgent need for real estate developers to adapt to the current Brazilian General Personal Data Protection Law, the present paper addresses its main provisions, including the analysis of the processing agents responsible for the personal data processed by the real estate developers and their responsibility.

Keyword: Incorporation Companies. Real Estate Development. Brazilian General Personal Data Protection Law. Consumer Relationship.

Sumário

1. INTRODUÇÃO 6

2. PREVISÕES LEGAIS 10

2.1. Dados Pessoais, Titular dos Dados Pessoais e Tratamento dos Dados Pessoais 10

2.2. Controlador e Operador dos Dados Pessoais 10

2.3. Violação de Dados Pessoais 13

2.4. Responsabilidade dos Agentes de Tratamento 16

3. INCORPORADORAS 19

3.1. Caso Cyrela 19

3.2. Situações Hipotéticas e a Incidência da LGPD 21

4. CONCLUSÃO 25

1. INTRODUÇÃO

Como bem pontuado pela autora Laura Schertel Mendes[1], a disciplina da proteção dos dados pessoais surge como uma possibilidade de tutelar a personalidade do indivíduo contra os potenciais riscos a serem causados pelo tratamento dos dados pessoais, cuja função não é a proteger os dados pessoais em si, mas sim a pessoa titular destes. Isso porque o valor das informações não reside apenas na capacidade de armazenamento de grande volume dados, mas, principalmente na possibilidade de obtenção de novos elementos informativos sobre os titulares, a partir do tratamento desses dados inicialmente obtidos.

Não é de hoje que os dados pessoais de clientes ou parceiros são utilizados indiscriminadamente para a realização de negociações, contratos, permutas, sem que as respectivas pessoas que deles se utilizam tenham qualquer preocupação acerca da relevância, finalidade e possibilidade de utilização de tais informações. Isto porque, é sabido que, por meio de determinadas informações combinadas, é possível identificar uma pessoa (caracterizando-se, portanto, como dado pessoal). E esta pessoa, por sua vez, tem o direito de não querer que seus dados sejam acessados, o que caracterizaria uma violação de seus direitos. Por isso, somado ao fato de que a utilização de dados pessoais se mostra cada vez mais importante tanto no cenário econômico quanto político, e observados o desenvolvimento tecnológico e democratização da internet, mais do que uma possibilidade, tornou-se uma necessidade a regulamentação de tais dados pessoais observada a potencialização do uso indevido e/ou não autorizado dos dados pessoais.

Um exemplo amplamente divulgado pela mídia foi o Facebook e Cambridge Analytica, ocorrido em 2018, sendo inclusive objeto do documentário Privacidade Hackeada (*The Great Hack*)[2]. Neste caso, foi identificado o compartilhamento indevido de dados pessoais de titulares que utilizavam o aplicativo do Facebook *This is your digital life*, visando atender com interesses eleitorais. Era apresentado um questionário aos usuários do aplicativo vinculado ao Facebook para análise de sua personalidade; tais informações seriam colhidas supostamente para fins acadêmicos, e, para tanto, os usuários que cooperassem com a pesquisa seriam remunerados com determinada quantia em dinheiro. Porém, a finalidade da coleta dos dados pessoais foi

---

[1] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo. Saraiva, 2014. (Série IDP: linha pesquisa acadêmica). p. 32 e 33.
[2] NOUJAIM, Jehane; AMER, Karim (Diretores). Privacidade Hackeada (The Great Hack). Estados Unidos da América, 2019. 113 min. Netflix.

desvirtuada: antes que o usuário respondesse tal questionário, o aplicativo podia acessar os dados pessoais, sendo possível que a empresa Cambridge Analytica analisasse o perfil psicográfico dos eleitores americanos e, por meio de anúncios, pudesse ser possível manipular o resultado das eleições, colocando em risco inclusive a instituição democrática do país A polêmica atingiu diretamente o Facebook, que teria ciência do compartilhamento indevido de tais dados com a Cambridge Analytica há pelos menos 2 anos, mas que não teria tomado qualquer providência para resguardar os direitos dos titulares dos dados pessoais[3].

A proteção de dados pessoais, portanto, representa uma preocupação mundial que já vinha sendo tutelada por grande parte dos países e, cada vez mais, tornando-se como requisito para a concretização de negócios entre players globais.

Em nosso país, infelizmente as pessoas ainda não têm o hábito de zelar pelos próprios dados pessoais, tampouco dos alheios, por não ter ciência do valor agregado em tais informações. A recorrente solicitação de fornecimento de dados pessoais (tais como nome completo, números de documentos pessoais como RG e CPF, biometria) deve ser urgentemente revista, visando assegurar a mudança de visão e somente se trabalhar com aqueles efetivamente necessários para a finalidade almejada, com a devida sem qualquer fundamentação e transparência ao seu titular. Por exemplo, o fornecimento de CPF para realizarmos uma compra na farmácia visando um desconto, o fornecimento de CPF para que seja possível efetuar uma troca de um presente no shopping center, a apresentação de documentos pessoais e fornecimento da biometria para acesso a um prédio comercial, entre outras inúmeras situações que estamos vivenciando regularmente nos dias atuais necessitariam ser revistas ou, ao menos, informadas aos titulares de tais dados. Esses dados são efetivamente necessários para a finalidade pretendida? Em caso positivo, o responsável que trata tais dados tem conhecimento suficiente para a realização de um tratamento adequado? É razoável que as pessoas forneçam tais dados como condição para realização de um negócio?

Assim, a grande maioria dos países vem tentando encontrar formas de regulamentar tais questões. Danilo Doneda[4] observa que o perfil atual da proteção de dados está fortemente ligado

---

[3] OTTO, Samira; SOUTO, Gabriel Araújo; DE FARIAS, Gabreille de Graça. Caso Facebook e Cambridge Analytica: O GDPR e a Nova Lei Brasileira (13.709/2018). Revista de Direito e as Novas Tecnologias, v. 4/2019. Julho/Setembro 2019. Disponível em: https://revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad6adc60000017a2b3d69d57793bb32&docguid=I445e33a0bfde11e98308010000000000&hitguid=I445e33a0bfde11e98308010000000000&spos=1&epos=1&td=38&context=5&crumb-action=append&crumb-label=Documento&isDocFG=true&isFromMultiSumm=true&startChunk=1&endChunk=1. Acesso em: 20/06/2021. (Paginação da versão eletrônica difere da versão impressa).

[4] BIONI, Bruno. Panorama Histórico da Proteção de Dados Pessoais, em BIONI, Bruno (Coordenador Executivo); MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES Jr, Otavio Luiz

aos marcos regulatórios europeus, que por sua vez são resultado de uma dinâmica de influências mútuas entre diversos sistemas jurídicos locais e dos Estados Unidos.

Em 25 de maio de 2018, entrou em vigor na Europa o Regulamento Geral de Proteção de Dados, ou a General Data Privacy Regulation (GDPR), enquanto no Brasil, a Lei 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados (LGPD), somente passou a vigorar em 2020. Laura Mendes e Bruno Bioni[5] comentam ser inegável a influência do regulamento europeu de proteção de dados pessoais sobre a LGPD, e, ainda que se verifiquem diferenças substanciais em tais regimes jurídicos, há semelhanças no tocante aos princípios que devem tangenciar a proteção de dados, a previsão de consolidação dos direitos dos titulares desde sua origem até o acesso, notificação, retificação e cancelamento de dados.

Importa destacar que, no Brasil, antes da LGPD, os dados pessoais já encontravam proteção em alguns diplomas, sejam eles a Constituição Federal, o Código de Defesa do Consumidor, o Código Civil, a Lei do Cadastro Positivo, o Marco Civil da Internet e o Decreto nº 8.771/2016. Contudo, foi a partir da promulgação da LGPD, que foi amplamente discutida pela sociedade, e de fato introduziu a proteção sobre o tratamento dos dados pessoais de uma forma mais extensa e com maior profundidade se comparado com os diplomas que a antecederam. Complementarmente, a autora Patrícia Peck Pinheiro[6] sustenta que o surgimento da LGPD se relaciona com a necessidade de atualização do arcabouço regulatório nacional frente aos impactos socioeconômicos trazidos com a revolução tecnológica. A principal finalidade do dispositivo legal, conforme previsto no artigo 1º, é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, sendo este o titular dos dados pessoais.

(Coordenadores). Tratado de Proteção de Dados Pessoais. Rio de Janeiro. Forense, 2021. p. 24, Localização 485 (kindle).

[5] MENDES Laura Schertel; BIONI Bruno R. O regulamento europeu de proteção de dados pessoais e a Lei Geral de Proteção de Dados brasileira: mapeando convergências na direção de um nível de equivalência. Revista de Direito do Consumidor. v. 124, p. 157-180. Julho/Agosto, 2019. Disponível em https://revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad82d9b0000017807d83217c335c036&docguid=I050bb350b78f11e987cc010000000000&hitguid=I050bb350b78f11e987cc010000000000&spos=2&epos=2&td=1701&context=106&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1. Acesso em 28/02/2021. (Paginação da versão eletrônica difere da versão impressa).

[6] PINHEIRO, Patricia Peck Garrido. Nova lei brasileira de proteção de dados pessoais (LGPD) e o impacto nas instituições públicas e privadas. Revista dos Tribunais. v. 1000, p. 309-323. Fevereiro, 2019. Disponível em: https://revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad82d9b0000017807ddcaa3a8d849a7&docguid=I5371afa01e0511e9a1ed010000000000&hitguid=I5371afa01e0511e9a1ed010000000000&spos=1&epos=1&td=1&context=180&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1. Acesso em 28/02/2021. (Paginação da versão eletrônica difere da versão impressa).

Trazendo a questão para a problemática diretamente ligada às incorporadoras, atualmente, vivenciamos a falta de controle que as incorporadoras possuem sobre o fluxo de informações e dados pessoais que estas têm acesso, por exemplo, quando ocorre (a) a venda de um imóvel intermediada por um corretor de imóveis, que por consequência, tem acesso aos dados pessoais dos compradores; (b) a entrega dos dados pessoais dos efetivos compradores para administradora do condomínio; (c) o vazamento de dados pessoais dos efetivos compradores, para interessados em realizar vendas relacionadas ao imóvel recém adquirido, dentre outras situações que serão analisadas no presente trabalho à luz da legislação vigente, doutrina e jurisprudência.

Dessa forma, verifica-se a urgente necessidade de adequação destas empresas aos principais objetivos previstos na LGPD, especialmente no tocante ao seu artigo 2º, quais sejam a proteção dos direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade natural, tendo em vista a quantidade de dados pessoais tratados pelas incorporadoras, cuja grande monta se relaciona com *leads* (potenciais adquirentes dos imóveis) ou efetivos compradores de seus imóveis ofertados, sendo, em sua grande maioria, pessoas físicas consideradas consumidores e, portanto, titulares dos dados pessoais a serem tutelados pela LGPD.

2. PREVISÕES LEGAIS

2.1. Dados Pessoais, Titular dos Dados Pessoais e Tratamento dos Dados Pessoais

A LGPD, em seu artigo 5º, inciso I, conceitua dado pessoal como "informação relacionada a pessoa natural identificada ou identificável", e, o inciso V caracteriza o titular de tais dados como "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento". É de suma importância ressaltar que atualmente não existem dados irrelevantes, tendo em vista que os dados pessoais são projeções diretas da personalidade e devem assim ser considerados, conforme apresentado por Laura Mendes e Danilo Doneda[7]. Importante ressaltar que a proteção prevista na LGPD se limita às pessoas naturais, não sendo, aplicável às pessoas jurídicas.

O tratamento, por sua vez, está definido no artigo 5º, inciso X da referida lei, consistindo nas operações envolvendo dados pessoais, que podem ser realizadas por meio de acesso, coleta, produção, recepção, classificação, utilização, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Quando restar caracterizada qualquer de tais condutas, o particular e o ente público devem sempre observar a regulamentação legal atinente à proteção de dados.

2.2. Controlador e Operador dos Dados Pessoais

Um dos maiores desafios a ser verificado pelas incorporadoras será verificar de que forma deve lidar com os dados pessoais a que tiver acesso, na medida em que as empresas do setor tangenciarão, no exercício de suas atividades econômicas, diferentes posições como agentes de tratamento de dados, o controlador e o operador previstos na LGPD, a depender da situação fática.

---

[7] MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova lei de proteção de dados (lei 13.709/2018): o novo paradigma da proteção de dados no brasil. Revista de Direito do Consumidor. v. 120, p. 555-587. Novembro/Dezembro, 2018. Disponível em: https://revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad82d9a0000017807d90fb5443c635d&docguid=I875dcd60f7ab11e89be5010000000000&hitguid=I875dcd60f7ab11e89be5010000000000&spos=9&epos=9&td=13&context=128&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1. Acesso em: 28/02/2021. (Paginação da versão eletrônica difere da versão impressa).

Enquanto o controlador é definido na LGPD como "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais", o operador caracteriza-se como "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador", que, em conjunto, são considerados pela lei como agentes de tratamento.

A GDPR, prevê, semelhantemente à LGPD, uma diferenciação dos institutos dos responsáveis pelos tratamentos de dados pessoais, sendo o *controller* a pessoa que determina os fins e os meios de tratamento de dados pessoais, enquanto o *processor* é a pessoa que trata os dados em nome do *controller*. Adicionalmente aos conceitos de *controller* e *processor*, o *European Data Protection Board – EDPB*, prevê em um de seus *guidelines*[8] que os conceitos de controlador e operador são funcionais, visando alocar responsabilidades de acordo com os papéis reais das partes.

Partindo da definição prevista pela LGPD, verificamos que a diferenciação da caracterização de tais institutos dar-se-á, principalmente, pelo fato de que o controlador tem o poder de realizar decisões referentes ao tratamento de dados pessoais e por definir a finalidade deste tratamento, enquanto o operador simplesmente realizará o tratamento de dados em nome do controlador e conforme a finalidade por este delimitada. Na teoria, a diferenciação nos parece um tanto quanto simples. Contudo, na prática, a definição torna-se um tanto complexa, considerando o dinamismo das atividades e diretrizes de tratamento dos dados pessoais.

Além disso, a LGPD apresenta a definição de encarregado, que embora não seja um agente de tratamento de dados, tem papel importante na relação e troca de informações entre o controlador, os titulares dos dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD).

Neste aspecto, recentemente em 28 de maio de 2021, a ANPD publicou o Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado ("Guia")[9], com a finalidade de estabelecer as diretrizes não vinculantes aos agentes de tratamentos e explicar quem pode exercer a função de controlador, do operador e do

---

[8] Guidelines 07/2020 on the concepts of the controller and processor in the GDPR, p. 3: "*The concepts of controller, joint controller and processor are functional concepts in that they aim to allocate responsibilities according to the actual roles of the parties and autonomous concepts in the sense that they should be interpreted mainly according to EU data protection law*.". Disponível em: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-072020-concepts-controller-and_en. Acesso em: 30/06/2021.

[9] Autoridade Nacional de Proteção de Dados, Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-guia-orientativo-sobre-agentes-de-tratamento-e-encarregado. Acesso em: 30/06/2021.

encarregado, tendo em vista que o texto legal se limita à definição supramencionada e não estabelecia claramente os efeitos práticos de sua aplicação.

De acordo com o Guia, o papel de controlador pode ser decorrente de obrigações estipuladas em instrumentos legais e regulamentares ou em contrato firmado entre as partes. Ademais, extrai-se (a) que observado o texto legal, o tratamento não precisa ser realizado diretamente pelo controlador, pois o elemento distintivo é o poder da decisão, sendo possível que o operador realize o tratamento em nome do controlador, conforme disposto no artigo 5º, inciso VII e artigo 39 da LGPD; (b) a desnecessidade de que todas as decisões sejam tomadas pelo controlador, bastando apenas que este mantenha sob sua influência e controle as principais decisões, isto é, aquelas relativas aos elementos essenciais para o cumprimento da finalidade do tratamento; (c) a definição dos elementos decisórios que se caracterizam como "principais" ou "essenciais" devem permanecer sob o domínio do controlador, e dentre esses elementos decisórios principais, destaca-se a definição da finalidade do tratamento, que será sempre estabelecida pelo controlador, a quem compete, em conformidade com as disposições da LGPD, estipular os objetivos que justificam a realização do tratamento, bem como a sua respectiva base legal, e (d) além da finalidade, o controlador é o responsável por estabelecer outros elementos essenciais relativos ao tratamento, como, por exemplo, a definição da natureza dos dados pessoais tratados e da duração do tratamento, isto é, do período durante o qual será realizada a operação, incluindo o estabelecimento de prazo para a eliminação dos dados, a ser verificado no caso concreto.

Como mencionado acima, o operador é aquele que trata os dados em nome do controlador conforme a finalidade por este delimitada, podendo definir elementos "não essenciais" do tratamento. O Guia elenca exemplificativamente obrigações do operador, tais como: (i) seguir as instruções do controlador; (ii) firmar contratos que estabeleçam, dentre outros assuntos, o regime de atividades e responsabilidades com o controlador; (iii) dar ciência ao controlador em caso de contrato com suboperador.

Outro ponto relevante é que, em regra, os funcionários atuantes na função de subordinados da incorporadora, estes não são operadores, mas meros subordinados ao controlador. Não é incomum que o responsável administrativo da incorporadora decida pelo envio de dados pessoais da empresa para uma outra terceirizada que presta serviço para aquela primeira. Neste exemplo, a empresa contratante, no caso a incorporadora, é controladora dos dados, ainda que a decisão tenha sido tomada pelo seu funcionário: ou seja, por atuar sob o poder diretivo da empresa, não se caracteriza como agente de tratamento. No entanto, caso o

subordinado, neste caso, o responsável administrativo, exceda o que lhe é conferido, tratando os dados pessoais dos titulares de forma não condizente com a instrução ou com o melhor interesse da empresa, este poderá ser pessoalmente responsabilizado.

Uma possível forma de evitar a confusão entre os institutos de controlador e operador, e, consequentemente a responsabilização dos responsáveis pelo tratamento dos dados, é por meio de celebração de contrato que institua o objeto, a duração, a natureza e a finalidade do tratamento dos dados, os tipos de dados pessoais envolvidos e os direitos e obrigações e responsabilidades relacionados ao cumprimento da LGPD, sendo estabelecida a delimitação de cada agente de tratamento desde o início da relação contratual.

2.3. Violação de Dados Pessoais

Observada a legislação americana, Daniel J. Solve estabelece uma pirâmide de abuso na gestão de dados pessoais dividida em três níveis a ser utilizado como modelo, conforme previsto em tal ordenamento jurídico: (a) no topo encontramos o uso irregular de dados pessoais, abrangendo situações como roubo de identidade, fraude, *stalking*[10], marketing; (b) no centro, os vazamentos de dados pessoais, quando, por exemplo, a empresa vaza informações ou autoriza que estas sejam acessadas inapropriadamente, e (c) na base, a falta de segurança, na qual os dados pessoais não são vazados, mas a segurança da informação é de má qualidade[11]. Podemos utilizar como ilustração para este estudo de vazamento de dados a pirâmide criada por Solve para que possamos visualizar com mais facilidade onde se encaixa o vazamento de dados.

A GDPR conceitua em seu artigo 4º, item 12, a violação de dados pessoais como uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento[12].

A LGPD não traz uma definição de violação de dados pessoais como expressamente previsto na GDPR, contudo, determina em seus artigos 44 e 46, que o tratamento de dados

---

[10] Palavra da língua inglesa utilizada para definir perseguição, cuja conduta fora tipificada como crime com a publicação da Lei nº 14.132/2021, que incluiu o artigo 147-A no Código Penal.

[11] SOLVE, Daniel J. The new vulnerability: data security and personal information, p. 113 – 121. The George Washington University Law School. Public Law and Legal Theory Working Paper. Disponível em: http://ssrn.com/abstract=583483. Acesso em: 16/05/2021. Em Securting Privacy in the Internet Age, pp. 111 – 136 (Anupam Chander, Lauren Gelman & Margaret Jane Radin eds. 2008).

[12] General Data Privacy Regulation, de 25 de maio de 2018. Disponível em: https://gdpr.eu/tag/gdpr/. Acesso em: 30/06/2021. "*Article 4 – Definitions: (12) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*."

pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias previstas em lei. Previu-se, ainda, que os agentes de tratamento são obrigados a 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. Ricardo Oliveira pontua, neste contexto, que a LGPD traz critérios subjetivos de segurança do tratamento, tornando, dessa forma, as disposições resistentes ao longo do tempo[13]. Ainda que encontremos na lei a previsão expressa do princípio da segurança definido como a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, a reflexão trazida por Fabiano Menke e Guilherme Goulart é no sentido de que não é simples indicar o que seria uma medida apta, mas que, cuja especificação poderia vir a ser suprida com o artigo 46, § 1º da LGPD, caracterizando-se como guias e parâmetros propostos pela autoridade nacional[14].

A LGPD traz em seu artigo 50 a possibilidade de que os controladores e operadores de dados pessoais formulem, como descrito por Fabiano Menke e Guilherme Goulart, regras de boas práticas de segurança, e a previsão de um programa de governança em privacidade, conforme definido no parágrafo 2º, inciso I do mesmo artigo mencionado acima; o programa deverá levar em consideração as medidas técnicas e administrativas ou organizativas[15]. Importa dizer que tais medidas devem ser observadas desde a fase de concepção do produto ou serviço, até sua execução, nos termos do artigo 46, §2º da LGPD. Thomas Smedinghoff afirma que os controles de segurança devem abranger três tipos ou níveis de segurança: (a) medidas administrativas, seja por meio de políticas, procedimentos, ou outros meios que possibilitem a implementação e observação da LGPD; (b) medidas técnicas, que geralmente envolvem o uso

---

[13] OLIVEIRA, Ricardo Alexandre de. Vazamento de dados pessoais pós LGPD. Revista dos Tribunais. vol. 1025. ano 110. p. 365-370. São Paulo: Ed. RT, março 2021. Disponível em: https://revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad6adc60000017971b8358b995f7872&docguid=I8b2c2e0067fc11ebaf36e629f7103d22&hitguid=I8b2c2e0067fc11ebaf36e629f7103d22&spos=1&epos=1&td=14&context=34&crumb-action=append&crumb-label=Documento&isDocFG=true&isFromMultiSumm=true&startChunk=1&endChunk=1. Acesso em: 15/05/2021. (Paginação da versão eletrônica difere da versão impressa).

[14] MENKE, Fabiano, GOULART, Guilherme Damasio. Segurança da Informação e Vazamento de Dados, em BIONI, Bruno (Coordenador Executivo); MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES Jr, Otavio Luiz (Coordenadores). Tratado de Proteção de Dados Pessoais. Rio de Janeiro. Forense, 2021, p. 24, posição 489 (kindle).

[15] MENKE, Fabiano, GOULART, Guilherme Damasio. Segurança da Informação e Vazamento de Dados, em BIONI, Bruno (Coordenador Executivo); MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES Jr, Otavio Luiz (Coordenadores). Tratado de Proteção de Dados Pessoais. Rio de Janeiro. Forense, 2021, p. 24, posição 489 (kindle).

de *software* e sistema de segurança de dados instalados nos *softwares*, *hardwares* e dispositivos semelhantes como antivírus, senhas, cartões inteligentes, certificados biométricos, *firewalls*, para prevenir o acesso de hackers e *malware*, e além das medidas previstas na LGPD e (c) as medidas físicas, que se destinam a proteger os itens tangíveis que abrangem o sistema informático físico e a rede que armazena os dados, incluindo servidores, terminais que têm acesso ao sistema, dispositivos de armazenamento e afins[16].

A LGPD, em si, não conceitua o termo "incidente de segurança", mas podemos concluir que este é um evento decorrente da não observância do artigo 46 da referida lei, no qual as 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 não foram realizadas.

Os agentes de tratamento devem tratar os dados pessoais de seus clientes (ou potenciais clientes) desde o momento da coleta ou da recepção de dados pessoais, ou seja, momento anterior à realização de uma formalização de um contrato - envolvendo negociações, tratativas pré-contratuais, celebração de documentos não vinculantes entre as partes - até o momento posterior à execução do contrato - momento em que se armazenam ou se eliminam os dados pessoais que se encontram em posse da empresa em questão.

Assim dizendo, os dados pessoais não devem ser cuidados e observados apenas durante a vigência de uma contratação, mas sim durante todo o período em que o agente de tratamento, seja controlador ou operador, tratar tais dados. Assim, em havendo um incidente de segurança ocasionado pela incorporadora ou por algum terceiro que teve acesso a tais dados por seu intermédio, a empresa titular dos dados pessoais objetos do incidente deverá comprovar que adotou as medidas de segurança compatíveis e eficazes com a natureza das informações tratadas e que pretendeu fornecer a segurança que o titular poderia esperar.

Ademais, tal obrigação das incorporadoras reflete que a tutela dos dados pessoais extrapola as relações contratuais, já que, muitas vezes, um potencial comprador fornecerá seus dados e não concluirá o negócio de compra e venda de um imóvel. Não obstante, os dados pessoais deste indivíduo recebem a mesma proteção que os dados dos clientes das incorporadoras, tendo em vista que as normas jurídicas de proteção têm como objeto os dados

---

[16] SMEDINGHOFF, Thomas J. Information Security Law: *The Emerging Standard for Corporate Compliance. Cambridgeshire*: ITGP, 2008. p. 19-21. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=fWhyfJGM3kYC&oi=fnd&pg=PA1&dq=The+Emerging+Standard+for+Corporate+Compliance&ots=8IoXV3CFaG&sig=17IDflIRrXftF7-fEVTEd4IovnM#v=onepage&q&f=false. Acesso em: 15/06/2021.

pessoais tratados pelos agentes de tratamento, sem distinção da relação existente entre o controlador/operador e o titular dos dados.

2.4. Responsabilidade dos Agentes de Tratamento

O legislador determina a responsabilidade dos agentes de tratamento nos artigos 42 a 45 da LGPD, estabelecendo que o controlador ou operador que, em razão do exercício 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.

Ainda que a LGPD traga a previsão de responsabilidade solidária, em regra, as responsabilidades de cada um dos agentes de tratamento são distintas, devendo estas refletirem suas respectivas obrigações. Nos termos trazidos por Bruno Bioni e Daniel Dias, um dos objetivos da lei foi delimitar as obrigações dos agentes de tratamentos e, assim, fixar regime jurídico para sua responsabilização[17].

A responsabilização do controlador está diretamente relacionada com a determinação realizada por este dos elementos essenciais relativos ao tratamento de dados pessoais, incluindo a determinação da natureza dos dados pessoais tratados e a duração do tratamento. Por seu turno, ao operador compete atentar-se ao determinado pelo controlador, e atuar em tal esfera delimitada, sendo que, caso ocorra o descumprimento das obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, esse equiparar-se-á àquele, respondendo ambos solidariamente pelos danos causados. Importa ainda dizer que, conforme artigo 45 da LGPD, a responsabilização nas relações de consumo permanece sujeita às regras previstas na legislação pertinente, ou seja, a responsabilidade objetiva.

Uma vez caracterizadas infrações às normas previstas na legislação, o artigo 52 da LGPD prevê a aplicação de sanções como advertência com indicação de prazo para adoção de medidas corretivas, multas simples, multas diárias, publicização da infração, bloqueio ou eliminação de dados pessoais, suspensão do funcionamento de banco de dados ou do exercício do tratamento de dados ou proibição total do exercício de atividades relacionadas a tratamento de dados.

---

[17] BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. Civilistica.com. Rio de Janeiro, a. 9, n. 3, 2020. Disponível em: http://civilistica.com/responsabilidade-civil-na-protecao-de-dados-pessoais/. Acesso em: 28/02/2021. (Paginação da versão eletrônica difere da versão impressa).

As sanções previstas acima somente poderão ser aplicadas após instauração de respectivo procedimento administrativo, que conceda a oportunidade do exercício à ampla defesa dos responsáveis, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto, conforme determina o artigo 52, §1º da LGPD, considerando (a) a gravidade e a natureza das infrações e dos direitos pessoais afetados; (b) a boa-fé do infrator; (c) a vantagem auferida ou pretendida pelo infrator; (d) a condição econômica do infrator; (e) a reincidência; (f) o grau do dano; (g) a cooperação do infrator; (h) 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 parágrafo 2º do artigo 48 da LGPD; (i) a adoção de política de boas práticas e governança; (j) a pronta adoção de medidas corretivas e (k) a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Neste cenário, observa-se que o §2º do artigo 52 da LGPD busca excepcionar o princípio do *non bis idem* ao dispor que a sanção aplicada por violação às normas de proteção de dados não substitui as sanções administrativas previstas no Código de Defesa do Consumidor, cuja graduação de multa leva em conta alguns aspectos idênticos (gravidade da infração, vantagem auferida e condição econômica do autuado).

Muito embora este não seja o foco principal do trabalho, destaca-se que em casos de aplicações de multas pela ANPD e por qualquer dos órgãos da administração pública que atuem em defesa do consumidor em razão de danos causados pelo vazamento de dados, surgirão discussões sobre a possibilidade de subsistirem simultaneamente tais sanções. O conflito entre a aplicação de sanções por diferentes órgãos de defesa do consumidor já é enfrentado pelas empresas há muito tempo, o que levou à inclusão em 2020 do parágrafo único ao artigo 5º do Decreto nº 2.181/1997, atribuindo à Secretaria Nacional do Consumidor do Ministério da Justiça e Segurança Pública (SENACON) a competência de dirimir o conflito, considerada a competência federativa sobre a atividade econômica envolvida. Não obstante, a ANPD se trata de agência que possui autonomia técnica e decisória e não estará adstrita às decisões da SENACON, o que, certamente, integrará as discussões administrativas e judiciais em busca de anulação das sanções simultâneas aplicadas por danos causados ao consumidor em razão do inadequado tratamento dos dados pessoais. Essa discussão torna-se relevante para entendermos qual o grau de responsabilização de uma incorporadora em caso de violação de sigilo dos dados pessoais feita por um corretor em uma fase pré-contratual, por exemplo, ao passo que, caso

consideremos um corretor como um operador que atue em nome da incorporadora, esta também será responsável em tal incidente de violação.

Uma vez apresentados os conceitos previstos na LGPD, resta claro que é imprescindível que a incorporadora, seus funcionários e aqueles relacionados, tenham ciência e apliquem os dispositivos e requisitos da LGPD na rotina da empresa sob pena de serem responsabilizados nos termos acima expostos. A incorporadora deve tratar os dados pessoais de titulares sejam estes efetivos compradores do imóvel, ou meramente potenciais compradores, com a devida atenção e cuidado, zelando pela segurança e privacidade de tais dados nos termos da mencionada lei.

No momento atual, verificamos a relevância que os dados pessoais possuem, principalmente, a identificação de uma pessoa e seus interesses nunca foi tão visada por terceiros interessados e a futura tendência é só aumentar, pois tais informações podem ser utilizadas para fins rentáveis e o titular de dados acaba por ficar vulnerável. Por esse e outros motivos, verificaremos a seguir alguns exemplos e a incidência dos dispositivos da LGPD nas incorporadoras.

3. INCORPORADORAS

Notadamente, as incorporadoras são empresas que tratam diversos dados pessoais. Ao celebrar um contrato de compra e venda de um imóvel, por exemplo, a incorporadora inserirá em sua minuta padrão os dados do interessado, como nome completo, nacionalidade, profissão, estado civil, número de RG, número de inscrição no CPF, endereço residencial e, no caso das pessoas jurídicas, os dados pessoais dos representantes das partes contratantes. Todavia, é de se avaliar, que, além das pessoas celebrantes do presente contrato, diversos outros funcionários da empresa terão acesso a tal documento. Com a entrada em vigor da LGPD, deve ser um ponto de atenção a importância do tratamento adequado a tais dados.

Neste cenário, apresenta-se um exemplo de fácil ilustração: é necessário que todos os dados em questão (costumeiramente solicitados) constem no contrato? Se sim, seria possível limitar o acesso a apenas um certo grupo de funcionários, observados os princípios previstos na LGPD? De uma forma bem simplificada, é necessário determinar a esfera de atuação da incorporadora, se ela efetivamente atua como uma controladora dos dados, inclusive aqueles coletados por um corretor no caso de um contrato não celebrado, e a consequente responsabilização. Tal análise e adequação são imprescindíveis para que a incorporadora não seja injustamente responsabilizada em caso de um incidente de vazamento de dados pois, certamente será objeto de investigação por parte da ANPD ou de ações judiciais promovidas pelos titulares dos dados.

3.1. Caso Cyrela

Tem sido objeto de ação judicial o compartilhamento de dados de efetivo comprador de unidade autônoma de empreendimento imobiliário[18]. A ação foi proposta por referido comprador, pessoa física comprador de um imóvel, em face da construtora e incorporadora do empreendimento, Cyrela Brazil Reality S.A. Empreendimentos e Participações ("Cyrela"), narrando que esta deu origem ao vazamento de dados do comprador, como nome, endereço, profissão e estado civil, lhe causado danos de natureza extrapatrimonial, por ter sido constantemente contatado e assediado por contatos de empresas alheias à relação contratual

[18] SÃO PAULO, Brasil. Tribunal de Justiça do Estado de São Paulo. Responsabilização da Cyrela Empreendimentos S/A com fundamentos nos dispositivos da Lei Geral de Proteção de Dados. Magistrado: Tonia Yuka Koruku. São Paulo. Processo nº. 1080233-94.2019.8.26.0100. Acesso em: 30/06/2021.

consumerista celebrada entre as partes da ação. Muito provavelmente essa será a primeira de muitas ações judiciais envolvendo incorporadoras, tendo em vista a grande quantidade e variedade de dados pessoais tratados por estas.

O comprador do imóvel informou no processo que terceiros obtiveram acesso aos seus dados após o compromisso firmado com a Cyrela e deles dispuseram para uso comercial, sendo certo que inexistiu qualquer autorização do titular para repasse de seus dados a terceiros, nem de informações acerca de sua aquisição de imóvel residencial. Informou, ainda, que em todos os contatos travados pelos interessados, o empreendimento da Cyrela foi citado, de modo que esses terceiros tinham ciência da aquisição do imóvel, bem como dados financeiros do consumidor, e que a Cyrela teria repassado, vazado, vendido ou alugado os dados do comprador do imóvel aos terceiros para uso e exploração comercial sem a sua autorização. O consumidor, então, contatou a Cyrela sobre o vazamento de dados, requerendo à construtora e incorporadora a abstenção imediata de divulgação, repasse, venda, transmissão, de seus dados a terceiros. A Cyrela, por sua vez, apresentou respostas evasivas e o comprador continuou a receber contatos de empresas ou pessoas que tinham a informação sobre a compra do imóvel desta primeira

A sentença proferida em 29/09/2020 condena a Cyrela a se abster de repassar ou conceder a terceiros, a título gratuito ou oneroso, dados pessoais, financeiros ou sensíveis titularizados pelo autor, sob pena de multa de R$300,00 (trezentos reais) por contato indevido e ao pagamento de indenização a título de dano moral no importe de R$ 10.000,00 (dez mil reais), todavia o processo encontra-se em grau de recurso[19].

A referida decisão tem como principal fundamento a responsabilidade objetiva e solidária da Cyrela com relação aos dados coletados durante a comercialização de unidade em um de seus empreendimentos. Isto porque, a Excelentíssima Julgadora declarou a irrelevância dos mecanismos de proteção de dados investidos pela incorporadora, bem como afirmou ser desnecessária a aferição de culpa das demais empresas envolvidas por se tratar de uma relação consumerista[20].

---

[19] No momento de conclusão deste trabalho os Recursos de Apelação apresentados pelas partes não tinham sido julgados.

[20] "(...) Irrelevante se a ré possui mecanismos eficazes para a proteção de dados, seja porque se sujeita às normas consumeristas em relação à sua responsabilidade, bem como pelo fato de que houve utilização indevida dos dados do requerente em decorrência do contrato firmado entre as partes. Sendo a responsabilidade objetiva, não há suporte para se inquirir a existência de culpa ou a presença de suas modalidades (imperícia, negligência ou imprudência). Tampouco desnecessário aferir se outras pessoas físicas ou jurídicas participaram da ilicitude (como no caso de corretores de imóveis), porquanto todos que participam da cadeia produtiva respondem de forma solidária pelos danos causados (arts. 7º, parágrafo único, e 25, I, CDC). A própria testemunha da ré, Sr. Carlos Eduardo de Castro Pires, afirmou que não seria impossível que corretores compartilhassem dados dos clientes, bem como teria trabalhado como corretor em alguns empreendimentos da ré e que esta não teria treinamento que

Assim, tendo como entendimento a inexistência de excludentes de responsabilidade previstas no artigo 14, §3º do Código de Defesa do Consumidor, condenou-se a Cyrela pelos danos morais suportados pelo demandante em razão do não autorizado acesso aos seus dados pessoais, independentemente da demonstração de culpa da incorporadora.

Além disso, podemos concluir que a Cyrela foi enquadrada, ainda que tacitamente, como controladora dos dados pessoais da pessoa física que teve seus dados violados. Tal caracterização se verifica pelo poder de tomada de decisão ser da incorporadora e ser ela a responsável pela determinação dos elementos essenciais do tratamento. Não é possível concluir pela responsabilidade ou não da Cyrela no caso em questão a partir da análise dos fatos e documentos disponibilizados no âmbito do processo. Ocorre que, não é razoável que as incorporadoras sejam responsabilizadas integralmente pelo incidente de segurança caso não sejam as efetivas responsáveis pelo vazamento dos dados, como verificaremos a seguir.

3.2. Situações Hipotéticas e a Incidência da LGPD

Como citado acima, as incorporadoras celebram diversos contratos de compra e venda de imóveis. Os dados em que constam em tais contratos, quando firmados com uma pessoa física, são dados pessoais do comprador identificado, que é o titular destes. Uma vez que, sendo a incorporadora decide o destino de tais dados pessoais, enquadra-se como a controladora de tais dados e, em ocorrendo algum incidente, será responsabilizada a depender do caso em questão e das providências que a empresa já tiver tomado para proteger os dados pessoais por ela tratados.

Suponhamos que um corretor de imóveis, realizará a venda de um imóvel diretamente no *stand* de vendas de um empreendimento. Para que a venda seja efetivada, celebrar-se-á um contrato de compra e venda no qual constarão os dados do comprador, necessários à qualificação da parte contratante. O corretor, então, coletará os dados pessoais e realizará o preenchimento dos campos necessários. O procedimento parece um tanto quanto simples, mas caso o processo de tratamento que se segue à tal coleta não estiver bem sedimentado, justificado e baseado em determinada finalidade, proporcionalidade e transparência, dentre outros, pode ser considerado como é um risco em potencial para eventual incidente de violação de dados.

---

abordasse sigilo de dados (fls. 798/801). (...)" (Tribunal de Justiça de São Paulo. 13ª Vara Cível. Juíza Exma. Dra. Tonia Yuka Koroku. DJe em 01/10/2020).

Nesse caso, o corretor de imóveis não é funcionário da incorporadora, ou seja, não é efetivamente subordinado. Contudo, perante o titular de dados, as figuras do corretor de imóveis e a incorporadora atuam conjuntamente. Caso o corretor de imóveis aja de má fé e com intuito de beneficiar-se, este poderá fornecer os dados ali coletados para parceiros interessados em tais dados como arquitetos, lojas de eletrodomésticos, prestadores de serviços relacionados, entre outros. Este é um dos exemplos em que uma pessoa alheia à incorporadora recepciona os dados pessoais do titular, motivo pelo qual, a empresa responsável pelo empreendimento deve atentar-se a tais situações e municiar-se de formas a evitar tais ocorrências, sob pena de ser responsabilizada, pois indubitavelmente a incorporadora enquadra-se como controladora no caso em questão por ser a responsável pela tomada de decisões e determinadora dos elementos essenciais da contratação.

Como uma solução para evitar os compartilhamentos de dados ilegais acima descritos, a incorporadora deve implementar, em primeiro lugar, um treinamento tanto de seus funcionários quanto de terceiros contratados, que forem responsáveis pelo tratamento de dados pessoais de titulares que confiaram tais informações à empresa.

O treinamento deve ter como objetivo demonstrar que a divulgação dos dados pessoais, sem o consentimento do titular e/ou quando desnecessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados, não deve ser compartilhado sem.

Além de informar os funcionários, é indispensável que haja um mapeamento dos dados tratados pela incorporadora. Isto porque, se um titular decidir por exercer seus direitos, aqueles previstos no artigo 18 da LGPD, dos quais incluem a solicitação de confirmação da existência de tratamento de dados pessoais deste titular e acesso a tais dados, a controladora deverá imediatamente fornecer tais informações, e, no prazo de 15 (quinze) dias contados da data de requerimento, apresentar a declaração completa destes dados, conforme disposto no artigo 19 da LGPD. Principalmente pelo motivo exposto, é indispensável que a incorporadora realize o mapeamento dos dados controlados por ela.

Um outro exemplo, é a transferência de informações que a incorporadora deve fornecer à administradora do condomínio, após a finalização da obra e emitido o certificado de conclusão da obra (habite-se). A incorporadora é responsável pela entrega das unidades vendidas, e a administradora, que será a responsável pela gestão do condomínio, precisará do acesso às informações dos futuros moradores coletadas ou recepcionadas pela incorporadora. Positivamente, no exemplo em questão ambas serão controladoras dos dados pessoais dos

efetivos compradores, pois ambas necessitam de tais dados para atingir o objeto do contrato celebrado entre consumidor e incorporadora.

Uma possível solução, seria, desde o contrato de compra e venda, prever em determinada cláusula a necessidade de compartilhamento de dados específicos por parte da incorporadora com a administradora do condomínio, para que, caso venha a ocorrer algum incidente em momento posterior ao encerramento de tratamento dos dados pessoais pela incorporadora, esta última não venha a ser responsabilizada pela conduta da administradora. É possível argumentar que diante da existência de um documento que delimite o fim do exercício do tratamento da incorporadora e o início do tratamento da administradora do condomínio, eventual incidente de segurança seria responsabilidade integral da administradora e não da incorporadora, pois, em havendo a notificação, ciência e anuência do comprador sobre o procedimento, não há mais de se falar em responsabilização da incorporadora.

Além da referida previsão contratual, o ideal seria fazer constar no próprio contrato de compra e venda celebrado entre a incorporadora e o comprador, um anexo com modelo de uma declaração a ser assinada pelo comprador do imóvel ciência e anuência do compartilhamento de dados necessários para a execução do contrato, que tem como finalidade última a entrega da unidade sob administração do condomínio. Para melhor ilustrar, imagine, dentro da situação mencionada acima, que um porteiro contratado da administradora, que possua consigo a relação de condôminos para liberar ou não a entrada de pedestres de acordo com os registros, forneça tais dados a um terceiro interessado. Como seria possível evitar que tal situação ocorra?

Outro recurso aplicável, seria a automatização do sistema de entrada e saída de pedestres a partir do uso de biometria de todos e quaisquer condôminos e/ou inquilinos para livre acesso sem que o porteiro possua livre acesso a dados pessoais que não sejam indispensáveis para realização de seu trabalho. E, novamente, verificamos a necessidade criação de um fluxo de dados bem sedimentado e de um treinamento e instrução adequados dos funcionários para realização do tratamento de dados exclusivamente para a realização da finalidade almejada.

Um outro tema, é a contratação de uma agência de marketing para que seja desenvolvida uma estratégia publicitária com a finalidade de atingir um maior alcance a potenciais compradores, que, para atingir tal objetivo, passa a gerenciar a conta das redes sociais da empresa. Nessa situação, a incorporadora é a controladora dos dados pessoais, enquanto a agência de marketing é a operadora. Para realizar o objeto da contratação a empresa terá acesso a todos os potenciais compradores que possivelmente poderão ser atingidos por meio de redes sociais. Suponhamos que a incorporadora forneça à agência acesso a conta de seu Instagram, e,

consequentemente a todas e quaisquer mensagens privadas eventualmente enviadas pelos titulares de dados, podendo estas incluir dados pessoais. No caso em questão, ainda que a empresa de marketing tenha a possibilidade de acessar tais informações, esta deve se limitar à finalidade outorgada pela empresa contratante, sob pena de ser responsabilizada pela atuação excedente ao contratado nos termos da LGPD.

Por fim, uma última situação exemplificada na qual a LGPD deve ser aplicada: a contratação pela incorporadora de uma empresa responsável pelo *software Customer Relationship Management* ("CRM"), que é responsável pelo serviço digital que fornecerá para a incorporadora a plataforma que gerencia desde o momento da proposta efetuada pelo interessado, até a geração do contrato de compra e venda com todas as informações do comprador, incluindo as condições comerciais contratadas.

Neste caso, a incorporadora é a controladora dos dados que constam na plataforma, pois ela será responsável pela tomada de decisões e a empresa contratada deverá observar as delimitações impostas pela contratante. Como vimos anteriormente, neste caso, o ideal é que a empresa possua medidas técnicas, como senhas, antivírus, *firewall*, bem como medidas físicas, como a proteção do equipamento que armazena o software em questão, pois ela será responsável caso ocorra um vazamento de dados, sendo também, indispensável, o treinamento dos funcionários que tenham acesso aos dados pessoais dos titulares.

Diante dos diversos exemplos, verifica-se a urgente necessidade de a incorporadora estar ciente, aplicando a LGPD diariamente e providenciar uma adequação nos moldes de sua atuação efetiva sob pena poder vir a ser responsabilizada em casos cuja mitigação do risco mostra-se possível e pouco onerosa, ainda que não tenha dado ensejo a uma violação de quaisquer dos requisitos da referida lei.

4. CONCLUSÃO

Ante o exposto, resta claro que as incorporadoras devem se adequar à LGPD, implementando-as nos procedimentos de rotina da empresa, assim como demais políticas de governança corporativa. Os dados pessoais tratados devem ser devidamente tutelados pelas empresas e utilizados apenas com a finalidade pela qual o titular os concedeu, tendo em vista que estes podem proporcionar ainda a obtenção de novos elementos informativos sobre os titulares.

Como estamos vivenciando um momento no qual toda e qualquer informação pode vir a identificar um indivíduo e seus respectivos interesses, o titular não pode estar suscetível e vulnerável a ponto de perder o controle sobre suas próprias informações para finalidades desconhecidas ou até mesmo para terceiros. As incorporadoras, além de controlarem um número expressivo de dados pessoais, tinham como prática informal o compartilhamento indevido de dados com empresas terceiras, e, por esses motivos, muito provavelmente serão alvos de investigação da ANPD e de processos judiciais.

Conforme disposto no presente trabalho, a incorporadora deve adotar medidas jurídicas, administrativas, técnicas e físicas, nas mais diversas situações, que deverão ser aplicadas de acordo com cada caso concreto, a fim de resguardar os titulares dos dados, e como consequência direta, proteger a si própria proporcionando a mitigação de riscos caso eventualmente ocorra um incidente de segurança, seja esse originado pela própria incorporadora ou por terceiros a ela conexos de alguma das formas anteriormente citadas.

Por fim, podemos concluir a importância do presente tema para proteção tanto do titular de dados, quanto da incorporadora. É de suma importância que as incorporadoras utilizem a LGPD como um marco para uma revolução na cultura com relação à proteção de dados no Brasil.

LEVANTAMENTO BIBLIOGRÁFICO

BIONI, Bruno. *Panorama Histórico da Proteção de Dados Pessoais*, em BIONI, Bruno (Coordenador Executivo); MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES Jr, Otavio Luiz (Coordenadores). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro. Forense, 2021.

BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. Civilistica.com. Rio de Janeiro, a. 9, n. 3, 2020. Disponível em: http://civilistica.com/responsabilidade-civil-na-protecao-de-dados-pessoais/. Data de acesso: 28/02/2021. (Paginação da versão eletrônica difere da versão impressa).

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo. Saraiva, 2014. (Série IDP: linha pesquisa acadêmica).

MENDES Laura Schertel; BIONI Bruno R. O regulamento europeu de proteção de dados pessoais e a Lei Geral de Proteção de Dados brasileira: mapeando convergências na direção de um nível de equivalência. Revista de Direito do Consumidor. v. 124, p. 157-180. Julho/Agosto, 2019. Disponível em https://revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad82d9b0000017807d83217c335c036&docguid=I050bb350b78f11e987cc010000000000&hitguid=I050bb350b78f11e987cc010000000000&spos=2&epos=2&td=1701&context=106&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1. Acesso em 28/02/2021. (Paginação da versão eletrônica difere da versão impressa).

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova lei de proteção de dados (lei 13.709/2018): o novo paradigma da proteção de dados no brasil. Revista de Direito do Consumidor. v. 120, p. 555-587. Novembro/Dezembro, 2018. Disponível em: https://revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad82d9a00

00017807d90fb5443c635d&docguid=I875dcd60f7ab11e89be5010000000000&hitguid=I875dcd60f7ab11e89be5010000000000&spos=9&epos=9&td=13&context=128&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1. Acesso em: 28/02/2021. (Paginação da versão eletrônica difere da versão impressa).

MENKE, Fabiano, GOULART, Guilherme Damasio. *Segurança da Informação e Vazamento de Dados*, em BIONI, Bruno (Coordenador Executivo); MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES Jr, Otavio Luiz (Coordenadores). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro. Forense, 2021.

NOUJAIM, Jehane; AMER, Karim (Diretores). Privacidade Hackeada (*The Great Hack*). Estados Unidos da América, 2019. 113 min. Netflix.

OLIVEIRA, Ricardo Alexandre de. Vazamento de dados pessoais pós LGPD. Revista dos Tribunais. vol. 1025. ano 110. p. 365-370. São Paulo: Ed. RT, março 2021. Disponível em: https://revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad6adc60000017971b8358b995f7872&docguid=I8b2c2e0067fc11ebaf36e629f7103d22&hitguid=I8b2c2e0067fc11ebaf36e629f7103d22&spos=1&epos=1&td=14&context=34&crumb-action=append&crumb-label=Documento&isDocFG=true&isFromMultiSumm=true&startChunk=1&endChunk=1. . Acesso em: 15/05/2021. (Paginação da versão eletrônica difere da versão impressa).

OTTO, Samira; SOUTO, Gabriel Araújo; DE FARIAS, Gabreille de Graça. Caso Facebook e Cambridge Analytica: O GDPR e a Nova Lei Brasileira (13.709/2018). Revista de Direito e as Novas Tecnologias, v. 4/2019. Julho/Setembro 2019. Disponível em:
Acesso em: 20/06/2021. Disponível em: https://revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad6adc60000017a2b3d69d57793bb32&docguid=I445e33a0bfde11e98308010000000000&hitguid=I445e33a0bfde11e98308010000000000&spos=1&epos=1&td=38&context=5&crumb-action=append&crumb-label=Documento&isDocFG=true&isFromMultiSumm=true&startChunk=1&endChunk=1. Acesso em: 20/06/2021. (Paginação da versão eletrônica difere da versão impressa).

PINHEIRO, Patricia Peck Garrido. Nova lei brasileira de proteção de dados pessoais (LGPD) e o impacto nas instituições públicas e privadas. Revista dos Tribunais. v. 1000, p. 309-323. Fevereiro, 2019. Disponível em: https://revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad82d9b0000017807ddcaa3a8d849a7&docguid=I5371afa01e0511e9a1ed010000000000&hitguid=I5371afa01e0511e9a1ed010000000000&spos=1&epos=1&td=1&context=180&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1. Acesso em 28/02/2021. (Paginação da versão eletrônica difere da versão impressa).

SOLVE, Daniel J. The new vulnerability: data security and personal information. The George Washington University Law School. Public Law and Legal Theory Working Paper. Disponível em: http://ssrn.com/abstract=583483. Acesso em: 16/05/2021. Em Securting Privacy in the Internet Age, pp. 111 – 136 (Anupam Chander, Lauren Gelman & Margaret Jane Radin eds. 2008).

SMEDINGHOFF, Thomas J. Information Security Law: The Emerging Standard for Corporate Compliance. Cambridgeshire: ITGP, 2008. Acesso em: 15/06/2021. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=fWhyfJGM3kYC&oi=fnd&pg=PA1&dq=The+Emerging+Standard+for+Corporate+Compliance&ots=8IoXV3CFaG&sig=17IDflIRrXftF7-fEVTEd4IovnM#v=onepage&q&f=false

LEGISLAÇÃO E JURISPRUDÊNCIA

BRASIL. Autoridade Nacional de Proteção de Dados, Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Guia Orientativo Sobre Agentes de Tratamento e Encarregado. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-guia-orientativo-sobre-agentes-de-tratamento-e-encarregado. Acesso em: 30/06/2021.

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: 30/06/2021.

BRASIL. Código de Defesa do Consumidor. Lei nº 8.078, de 11 de setembro de 1990. Brasília, 11 de setembro de 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 30/06/2021.

BRASIL. Decreto nº 2.181 de 20 de março de 1997, Brasília, 20 de março de 1997 Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/d2181.htm. Acesso em: 30/06/2021.

EUROPA. *General Data Privacy Regulation*, de 25 de maio de 2018. Disponível em: https://gdpr.eu/tag/gdpr/. Acesso em: 30/06/2021.

EUROPA. *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*. Disponível em: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-072020-concepts-controller-and_en. Acesso em: 30/06/2021.

SÃO PAULO, Brasil. Tribunal de Justiça do Estado de São Paulo. Responsabilização da Cyrela Empreendimentos S/A com fundamentos nos dispositivos da Lei Geral de Proteção de Dados. Magistrado: Tonia Yuka Koruku. São Paulo. Processo nº. 1080233-94.2019.8.26.0100. Acesso em: 30/06/2021.