A RESPONSABILIDADE CIVIL NO VAZAMENTO DE DADOS PESSOAIS SOB A PERSPECTIVA DA LEI GERAL DE PROTEÇÃO DE DADOS

Wellington de Carvalho (IC) e Murilo Rezende dos Santos (Orientador)

Apoio:PIBIC Mackpesquisa

RESUMO

O presente trabalho faz-se relevante, pois tem como foco demonstrar a importância do direito a proteção de Dados Pessoais, e como isso afeta a vida das pessoas, uma vez que ocorrendo o vazamento desses dados, os prejuízos são irreparáveis. Também estudar acerca da responsabilidade civil, bem como o direito à privacidade e seus amparos legais. Para tal, é importante trabalhar os conceitos que a Lei Geral de Proteção de Dados Pessoais traz na sua redação, assim como a evolução histórica da proteção destes dados, e os princípios que nortearam a criação da referida legislação. Utiliza-se o método científico qualitativo, fundado em estudos doutrinários e legal.

Palavras-chave: Responsabilidade Civil. Vazamento de Dados. Lei Geral de Proteção de Dados Pessoais. Direito à Privacidade. Princípios.

ABSTRACT

This work is relevant because it focuses on demonstrating the importance of the right to protection of Personal Data, and how this affects people's lives, since if this data is leaked, the losses are irreparable. Also study about the civil responsibility, as well as the right to privacy and its legal protection. To this end, it is important to work on the concepts that the General Law on Personal Data Protection brings in its wording, as well as the historical evolution of the protection of this data, and the principles that guided the creation of such legislation. The qualitative scientific method is used, based on doctrinal and legal studies.

Keywords: Civil liability. Data leak. General Law of Personal Data Protection. Right to Privacy. Principles.

1. INTRODUÇÃO

Com globalização e os avanços tecnológicos, a população se viu mais conectada do que nunca, estamos prestes a viver a chamada Quarta Revolução Industrial, pois vivemos em um mundo em que cada vez mais o real se confunde com o virtual.

E assim como qualquer avanço tecnológico, traz as suas vantagens e desvantagens, no qual uma das principais é garantir a privacidade dos usuários na rede, que se tornou uma tarefa difícil, visto que a cada acesso na internet se deixa um rastro, uma pegada.

Partindo deste pressuposto, é notória a importância da proteção dos dados que são coletados, assim como o direito dos usuários saberem para que fins estão sendo destinados e utilizados esses dados.

Nesse sentido, o presente artigo visa abordar um dos temas que vem cada vez mais preocupando a sociedade: a proteção de dados pessoais e a responsabilidade civil pelo vazamento destes dados.

Assim, com a aprovação da Lei Geral de Proteção de Dados brasileira, fica evidente a importância de se dar o adequado tratamento aos dados pessoais coletados cotidianamente. Além de que, a nova lei possui aplicação ampla e abrangente e que engloba grande parte das atividades empresariais.

Dessa forma, no primeiro momento cabe contextualizar, assim como trazer conceitos preliminares da legislação.

Num segundo momento, analisar a proteção de dados pessoais como um direito fundamental, no qual estão intimamente ligados com a intimidade e privacidade tutelados na Constituição Federal de 1988.

Posteriormente, será feito estudo acerca da Lei Geral de Proteção de Dados Pessoais, bem como identificar os princípios que deram ensejo a criação da referida legislação.

Por derradeiro, buscou-se trabalhar exclusivamente à análise da responsabilidade civil, sob a perspectiva da lei acerca do vazamento dos dados pessoais, do mesmo modo que, realizando um paralelo com o Código de Defesa do Consumidor.

2. A Sociedade da Informação

Ao longo dos anos, a sociedade teve diversas formas de organização social. Em cada época existiu um elemento chave que contribuiu para o seu pleno desenvolvimento, podendo destacar três grandes momentos ao longo dos anos.

No primeiro momento, na época agrícola, o que impulsionava a economia eram os produtos advindos da terra, por meio da agricultura.

Num segundo momento, constitui-se a sociedade industrial com a criação das máquinas a vapor e da eletricidade, que impulsionaram a produção fabril e consequentemente na formação das riquezas.

E por sua vez, o terceiro momento, é caracterizado pela sociedade pós-industrial, tendo como marco a Segunda Guerra Mundial. Essa sociedade já não é mais caracterizada pela produção, mas sim pelos serviços que poderiam ser prestados. Isto é, a prestação de serviços passava a moldar a economia.

No entanto, na atual sociedade o elemento chave para o desenvolvimento é o fenômeno da informação, substituindo os recursos que antigamente estruturavam as sociedades agrícola, industrial e pós-industrial.

Com a corrida tecnológica e ideológica travada entre os Estados Unidos e a União Soviética, no período da Guerra Fria, foram desenvolvidas muitas tecnologias, dentre as quais, uma que revolucionou o mundo, a chamada Internet, que possibilitou processar e transmitir informações em uma quantidade e velocidade jamais imaginável.

Nesse sentido, a internet mostra-se como um meio de difusão de informações, assim como se transformou em um forte instrumento de engajamento social:

> Um exemplo sintomático foram as manifestações de junho de 2013. Nelas, o exercício da cidadania foi revitalizado por um fluxo informacional – em especial das redes sociais – que conectou seus manifestantes, facilitando a organização e a disseminação dos protestos. Verificou-se, sobretudo, um novo instrumento de engajamento social. (BIONI, 2019, p. 4).

A partir dessa concepção, diante dos avanços e aperfeiçoamentos da tecnologia desenvolvida no século XX, podemos dizer que estamos vivendo na sociedade da informação, visto que, o elemento central que remodela a atual sociedade é justamente a informação.

2.1 Dados Pessoais

Seguindo as diretrizes acima, verifica-se que a Internet tem diversas utilidades, mas, no presente artigo, cabe analisar a obtenção ou mineração de dados pessoais.

Sem embargo, primeiramente, se faz necessário definir um conceito do que são dados pessoais. De acordo com a Lei Geral de Proteção de Dados Pessoais (Lei n° 13.709/2018), dado pessoal é a informação relacionada a pessoa natural identificada ou identificável, conforme denota-se do art. (art. 5º, I) da legislação.

Nota-se que a lei traz um conceito amplo e aberto, uma vez que, qualquer dado que isoladamente ou ligado a outro possa permitir a identificação de uma pessoa natural, pode ser considerado como dado pessoal, como por exemplo os dados cadastrais como profissão, dados de GPS, interesses e hábitos de consumo, entre outros.

Dentre os tipos de dados contidos nos incisos do art. 5° da Lei Geral de Proteção de Dados, estabelece que:

> Dado pessoal sensível (Art. 5º, II) - 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; (Proteção de Dados Pessoais, 2018).

Isto é, são aqueles dados relacionados a pessoa natural identificada ou identificável por meio do qual uma pessoa pode ser discriminada e, por tal motivo, devem ser considerados e tratados como dados sensíveis.

Quanto à diferença de dado pessoal e dado pessoal sensível:

> Os dados sensíveis são uma espécie de dados pessoais que compreendem uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade: discriminação. Quando se pensa em dados que exprimem a orientação sexual, religiosa, política, racial, estado de saúde ou filiação sindical, surge a preocupação em haver distinção ou diferenciação de uma pessoa por conta de tais aspectos da sua personalidade" (BIONI, 2019, p. 84).

Salienta-se, que dentre os conceitos estipulados pela lei, há uma espécie de dado que na verdade não é considerado como dado pessoal, e sim identificado como dado anonimizado ou que passam por um processo de anonimização, logo, não é considerado dado pessoals conforme a legislação descreve:

> Dado Anonimizado (art. 5º, III e XI) - dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. (Proteção de Dados Pessoais, 2018).

Com exposto acima, a anonimização consiste na utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, a uma determinada pessoa seja diretamente ou indiretamente.

Ademais, assim como o conceito amplo sobre os dados pessoais, a LGPD, apresenta as ações que são consideradas como tratamento de dados pessoais, como segue na forma da lei:

> Tratamento (art. 5º, X): 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. (Proteção de Dados Pessoais, 2018).

Posto isso, nota-se então que tratamento é toda operação relacionada a dados pessoais, desde o acesso até a exclusão desses dados.

Além disso, diante da lei o tratamento de dados é um rol exemplificativo e não taxativo, tendo em vista que a tecnologia evolui muito rápido e o direito não é capaz de acompanhar, logo, o legislador teve o cuidado de colocar um rol exemplificativo, pois se surgir algo novo a lei não ficará desatualizada.

Feitas essas ponderações, com o conhecimento dos dados pessoais "[...] a ciência mercadológica percebeu que a Internet poderia propiciar uma abordagem publicitária mais efetiva." (BIONI, 2019), dessa maneira tais dados passaram a serem utilizados de maneiras indevidas e muitas vezes sem o consentimento dos seus titulares.

Esse é um diagnóstico necessário, sem o qual não se poderia avançar na investigação do papel do consentimento na proteção dos dados pessoais, especialmente, por rivalizar com tal condição de passividade atribuída ao cidadão quanto ao fluxo de suas informações pessoais (BIONI, 2019).

3. Intimidade e Privacidade como um direito fundamental

Seguindo adiante, com os avanços da tecnologia, o constituinte brasileiro buscando evitar que a privacidade das pessoas seja violada, regula o fenômeno da informação na Constituição Federal de 1988, garantindo a livre manifestação do pensamento, o direito de resposta, o sigilo da fonte, o acesso à informação, bem como a inviolabilidade e da vida privada.

Sendo este direito fundamental, concretizado por meio de uma cláusula pétrea prevista no art. 5º, X, Constituição Federal.

> Dos Direitos e Deveres Individuais e Coletivos: Art. 5º - X: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação". (Constituição Federal, 1988).

Nesse sentido, não faria sentido excluir as situações em que a vida privada está sujeita a uma maior violação, como o caso do processamento de dados pessoais. Afinal, o tratamento de dados hoje configura-se uma ameaça muito mais grave à intimidade e à vida privada do cidadão do que os perigos que rodeavam na época em que foi criado esse direito.

De acordo com Laura Mendes (2019) "não há dúvidas de que a Constituição Federal protege o homem médio desses riscos, que raramente ocorrem na vida real, não haveria sentido em negar-lhe a proteção constitucional perante os bancos de dados, que constituem um risco constante e diário para todos os cidadãos".

Ocorre que, o bem jurídico protegido por esse direito é duplo, de um lado visando proteger a integridade moral da pessoa, e por outro as liberdades.

Insta ressaltar, que a privacidade é um dos direitos da personalidade, que também é

assegurada pelo Código Civil no artigo 21:

> Dos Direitos Da Personalidade: Art. 21 - "A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma. " (Código Civil, 2002).

Estendendo para o campo digital, Patricia Peck, afirma que cabe ao direito equilibrar as relações de interesse comercial e privacidade que os novos veículos de comunicação geram.

> Se, por um lado, cresce a cada dia o número de empresas que disputam os consumidores da Internet e, consequentemente, a publicidade virtual, com preenchimento de formulários e cadastros, por outro lado, cresce também o nível de conscientização dos consumidores quanto à possibilidade de aplicação do atual Código do Consumidor, que trata da matéria de utilização de informações de consumidores para fins comerciais, trazendo uma série de penalidades para quem as pratica" (PECK, 2019, p. 95-96).

Desse modo, o direito fundamental à proteção de dados engloba tanto um direito subjetivo de defesa do cidadão, assim como um dever de proteção estatal.

> Na dimensão subjetiva, a atribuição de um direito subjetivo ao cidadão acaba por delimitar uma esfera de liberdade individual que não pode sofrer intervenção do poder estatal ou privado. A dimensão objetiva representa a necessidade de concretização e delimitação desse direito por meio da ação estatal, a partir da qual surgem deveres de proteção do Estado para a garantia desse direito nas relações privadas. (MENDES, 2019, p. 176).

Assim, em síntese, pode-se considerer o direito à privacidade como um direito a personalidade, que tem como propósito resguardar a esfera privada e íntima, logo, garantindo o livre desenvolvimento psíquico da pessoa.

4. Lei Geral de Proteção de Dados Pessoais (n° 13.709/2018)

Com a globalização impulsionada pelos avanços tecnológicos, surge a necessidade de regulamentação da proteção de dados pessoais de forma mais consistente e consolidada, haja vista que a atual sociedade é lastreada por informações, em especial os dados.

Diante disso, houve a necessidade de resgatar e repactuar o compromisso das instituições com os indivíduos, cidadãos desta atual sociedade digital, no tocante à proteção e à garantia dos direitos humanos fundamentais, como o da privacidade, já celebrados desde a Declaração Universal dos Direitos Humanos (DUDH) de 1948. (PECK, 2019).

Sem embargo, o tema surgiu na União Europeia (UE), em especial com o partido The Greens, e se consolidou na promulgação do Regulamento Geral de Proteção de Dados Pessoais Europeu n. 679, aprovado em 27 de abril de 2016 (GDPR), com o objetivo de abordar a proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, conhecido pela expressão "free data flow". (PECK, 2019).

No Brasil, a Lei Geral de Proteção de Dados (Lei n°13.709/18) dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado.

Foi sancionada em agosto de 2018 com *vacatio legis* de 18 meses (fevereiro/2020). Porém, Michel Temer presidente interino na época editou a Medida Provisória n° 869/2018 (dezembro/2018) alterando a *vacatio legis* para 24 meses (agosto/2020). Na sequência, o Congresso sanciona a Lei n° 13.853/2019 (julho/2019), que acolhe a MP n° 859/2019, assim prorrogando a *vacatio legis* para 24 meses (agosto/2020).

Advém que, o presidente Jair Bolsonaro editou a MP n° 959/2020, estabelecendo a vigência da LGPD para maio de 2021. Portanto, em síntese, a lei está com a vigência temporária para maio/2021, mas para que esse prazo se torne definitivo, é necessário que Congresso converta a MP em lei.

Todavia, o Senado Federal aprovou no dia 26 de agosto de 2020 a medida provisória nº 959/2020 que adiava, em seu art. 4º, o início da vigência da Lei Geral de Proteção de Dados. Mas acontece, que o art. 4º, foi considerado prejudicado e, assim, o adiamento nele previsto não mais acontecerá.

Não obstante, a LGPD não entrará em vigor imediatamente, mas somente após sanção ou veto do restante do projeto de lei de conversão, nos exatos termos do § 12 do art. 62 da Constituição Federal:

> Art. 62 [...]
> § 12. Aprovado projeto de lei de conversão alterando o texto original da medida provisória, esta manter-se-á integralmente em vigor até que seja sancionado ou vetado o projeto."

Portanto, a Lei Geral de Proteção de Dados só entra em vigor após a sanção ou veto dos demais dispositivos da MP 959/2020.

A legislação tem abrangência nacional para qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica (público ou privado), independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

> Art. 3° [...]
> I - A operação de tratamento seja realizada no território nacional;
> II - A atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;
> III - Os dados pessoais objeto do tratamento tenham sido coletados no território nacional. (Proteção de Dados Pessoais, 2018).

Observa-se que o primeiro obstáculo das instituições tomadoras das informações de dados pessoais é estabelecer notadamente o seu papel e responsabilidade em relação a esses dados, vez que a lei determina os seguintes agentes:

> Art. 5° [...]
> VI - Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
> XIX - Autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. (Proteção de Dados Pessoais, 2018).

Diante disso, o papel das instituições poderá ser distinto de acordo com a informação e dado ao qual ela está tratando. Essa distinção se dá em razão à forma de obtenção do dado, sua utilização, a necessidade de autorização, entre outros.

Ademais, no caso de identificação de não conformidade em relação ao tratamento ou eventual violação de dados pessoais, as instituições poderão ser sancionadas por meio de advertência; multa simples de até 2% do faturamento (limitada à R$ 50 milhões); multa diária; publicitação da infração; e até, bloqueio/eliminação de dados pessoais referentes à infração.

Cabe ressaltar, que as violações aos dados pessoais poderão ocorrer tanto por ação, no caso da venda de dados por exemplo, como por omissão, que a título de exemplo ocorre com os ataques de hackers da tomadora da informação, havendo responsabilidade igualitária entre os dois casos.

Não obstante, com a criação da LGPD, pode-se dizer que o Brasil se encontra no mesmo patamar de 109 países do mundo que já possuem alguma legislação sobre o tema, considerando que atualmente a privacidade e os dados pessoais são uma preocupação global.

4.1 Princípios da Lei Geral de Proteção de Dados Pessoais

Com o mundo preocupado com o tratamento de dados, o Brasil, após anos do Projeto de Lei em trâmite decidiu, de uma vez, dedicar todos os esforços para a aprovação da Lei de Proteção de dados.

A legislação no seu artigo 6º traz um rol de princípios, no entanto, será dada maior ênfase aos princípios ligados à eventuais obrigações do controlador e do operador. Dentre os quais, os três principais princípios (finalidade, adequação e necessidade) são princípios “[...] que somados resultam no que se chama de mínimo essencial” (TEIXEIRA, ARMELIN, 2019).

Desse modo, todo tratamento de dados pessoais realizado com base nos princípios da finalidade, adequação e necessidade, dificilmente incidira em violações legais previstos na Lei Geral de Proteção de Dados Pessoais. (LOPES, TEIXEIRA, TAKADA, 2019).

Assim, o princípio da finalidade trata-se da adequação e da devida necessidade, isto é, a coleta de dados pessoais tem que ter uma determinada finalidade específica que justifique a sua coleta.

> [...] princípio da finalidade, que vincula o tratamento de dados pessoais à finalidade que motivou e justificou a sua coleta. A aplicação desse poderoso princípio tem como consequência a concretização de algumas das finalidades últimas da Lei, qual seja a consideração de que o tratamento de dados pessoais são indissociáveis de uma determinada função que sempre poderá ser avaliada, ou mesmo que dados pessoais, por estarem de certa forma "afetados" por uma finalidade, jamais poderão ser considerados como mera *res in commercium*. (MENDES, 2019, p. 05).

A adequação está ligada diretamente com o consentimento contextual, visando regular o correto fluxo informacional dos dados pessoais, isto é, busca-se por este princípio "[...] a compatibilidade do tratamento com as finalidades informadas ao titular" (Proteção de Dados, 2018, Art. 6º).

Destarte, os dados deverão ser utilizados apenas para as finalidades específicas para as quais foram coletados e devidamente informados aos titulares, além de que o tratamento não pode estar dissociado daquilo que o titular razoavelmente espera fornecê-lo.

No tocante a necessidade seria a "[...] limitação do tratamento ao mínimo necessário para a realização de suas finalidades" (Proteção de Dados, 2018, Art. 6º), assim:

> [...] depois de haver sido comunicado ao titular de dados para que seus dados estão sendo coletados, a utilização dos mesmos deve ser fiel ao que foi uma vez informado, e não apenas isso, mas também de forma restrita, de maneira que os dados só sejam usados dentro da estrita necessidade. (LOPES; TEIXEIRA; TAKADA; 2019, p. 278-279).

Dessa forma, o dado que é coletado tem que estar em conformidade com a necessidade daquilo que é preciso e devido para prestar o serviço, sempre em consonância com a mínima coleta, haja vista que muitas empresas ao primeiro momento coletam todos os tipos de dados possíveis, para depois ver se esses determinados dados são realmente relevantes e necessários.

5. A especial Responsabildiade Civil na LGPD

A responsabilidade civil constitui um dos institutos jurídicos mais complexos e relevantes, pois não se restringe tão somente no mundo jurídico, vez que, a responsabilidade primeiro se liga aos domínios da sociedade e tem como principal função reestabelecer o *status quo ante* ou punir o agente que causa dano a outrem.

No entanto, mesmo sem a entrada em vigor da Lei Geral de Proteção de Dados, se estabeleceu nos meios jurídicos um debate sobre o regime da responsabilidade civil adotado na novel disciplina protetiva dos dados pessoais.

Há aqueles que afirmam que a responsabilidade civil nesse contexto é subjetiva, vez que atrelada à análise da culpa dos agentes de tratamento por eventuais danos causados aos titulares dos dados pessoais. Mas por outro lado, há aqueles que entendem que a responsabilidade civil na LGPD adotou uma forma objetiva destinada à distribuição dos riscos inerentes à atividade de tratamento de dados.

Nesse liame, a coleta, gestão e armazenamento de dados estão sujeitos à responsabilidade objetiva, sendo um excelente exemplo as relações consumeristas, pois o próprio Código de Defesa do Consumidor exclui a necessidade da caracterização de culpa do agente, isso devido aos riscos que os consumidores são expostos.

Desse modo, caso se esteja diante de uma relação de consumo entre o titular e o terceiro que capta os dados, a responsabilidade objetiva é cristalina, quando há prestação de serviço. Não importando que se trate de uma transferência contratual ou clandestina de dados. Como institui o artigo 14 do Código de Defesa do Consumidor:

> Da Responsabilidade pelo Fato do Produto e do Serviço: Art. 14 - O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos. (Código de Defesa do Consumidor, 1990).

Nota-se que a responsabilidade objetiva é embasada na ideia de o consumidor ser vulnerável e hipossuficiente frente aos produtores e prestadores de serviços.

Do mesmo modo, tal fato justifica a exceção que o CDC faz aos profissionais liberais, dos quais serão responsabilizados subjetivamente (art. 14, §4º, Código de Defesa do Consumidor). A norma é justificada, visto que os profissionais liberais individuais, assim como os consumidores, estão muitas vezes em posição de vulnerabilidade ou hipossuficiência. (TARTUCE, 2018).

Assim, a legislação observa a vulnerabilidade e os riscos a que o consumidor é exposto, optando pela maior proteção ao consumidor, podendo dizer que como regra a responsabilidade objetiva, ao passo que a subjetiva seria uma exceção.

A LGPD dispõe um capítulo sobre o tema da responsabilidade, porém não traz nenhum dispositivo específico que indique qual é o regime a ser adotado. Não se tem uma regra expressa adotando o regime da responsabilidade objetiva e, tampouco, um dispositivo que indique precisamente que a responsabilidade tem como fundamento a culpa.

Desse modo, o mesmo raciocínio do CDC pode ser aplicado aos titulares dos dados pessoais, pois mesmo que a LGPD não explicite a natureza da responsabilidade civil, observa-se que deve ser objetiva, haja vista, que os titulares dos dados pessoais, sejam consumidores de fato ou por equiparação, são hipervulneráveis, tendo em vista que muitas vezes não sabem que seus dados estão sendo coletados, ou se sabem não tem consciência do real valor destes dados.

Portanto, para a reparação dos danos morais e materiais advindos da violação do direito fundamental à proteção de dados, faz-se necessária a aplicação de um sistema de responsabilidade objetiva e solidária (MENDES, 2019). Estabelecendo a responsabilidade objetiva como regra na LGPD.

O art. 42 da LGPD estabelece que o agente de tratamento que, na realização do tratamento de dados pessoais, causar dano a outrem, em violação à legislação, é obrigado a repará-lo. Não basta, por conseguinte, o desenvolvimento da atividade de tratamento causadora de um dano para se configurar a responsabilidade civil dos agentes de tratamento, pois essa responsabilidade pode ser atribuída tão somente quando o tratamento for considerado violador, isto é, quando for ilícito.

Frente à exigência do ilícito, também resta descartada uma responsabilidade civil objetiva centrada no risco como critério de imputação, seja qual risco for, da atividade, proveito, criado ou profissional.

Acerca disso, analisando os moldes do artigo 42 da LGPD, ao vincular a obrigação de reparação dos danos com o exercício do tratamento de dados pessoais, percebe-se que o legislador demonstra a opção pela objetividade da responsabilidade.

Assim, justifica-se a opção do legislador por um regime de responsabilidade objetiva no art. 42, vinculando a obrigação da reparação do dano ao exercício de atividade de tratamento de dados pessoais. (MENDES, 2019).

Em contrapartida, o artigo 43 da LGPD retrata as situações em que os agentes de tratamento (controladores e operadores), não serão responsabilizados, quando demonstrado que: i) não foi realizado o tratamento; ii) não houve ilícito ou; iii) o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros, nas quais são congêneres às descritas pelo artigo 12, §3° do CDC.

Sendo assim, pode se dizer que o que justifica a afinidade entre os dispositivos é o fato de que ambas as legislações destinam-se proteger o titular dos dados e o consumidor, tendo em vista a vulnerabilidade de cada um.

Ademais, a responsabilidade objetiva em ambos os diplomas, é outra prova de tal similaridade, assim como fundamenta a aplicação análoga do Código de Defesa do Consumidor.

Portanto, feitos estes ponderamentos, a aplicação do sistema de responsabilização objetiva é o mais adequado, vez que os titulares dos dados podem ser considerados hipervulneráveis. Além disso, devido a extrema importância dos dados pessoais, as atividades de processamento expõem a figura do titular à riscos, justificando ainda mais a proteção.

5.1 Responsabilidade dos Agentes de Tratamento de dados

A legislação introduz a figura dos agentes de tratamento, o qual é composto tanto o controlador, aquele que tem a decisão acerca do tratamento de dados, quanto o operador, aquele que efetua o tratamento, em nome e por conta do controlador. Na maioria dos casos, ambas as figuras podem se concentrar na mesma instituição.

Daí decorre o dever do operador e do controlador de "[...] manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse" (Proteção de Dados, 2018, art. 37).

O legislador no artigo 46, determinou a observância, pelos agentes de tratamento de medidas de segurança, técnicas e administrativas, para proteção dos dados pessoais.

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. (Proteção de Dados Pessoais, 2018).

Nesse contexto, a própria lei já imputa a responsabilidade aos agentes pela falta de segurança, no artigo 44 que define um dever geral de segurança aos agentes de tratamento, cuja violação geradora de danos a outrem ensejará a responsabilização civil.

> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: [...] Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano. (Proteção de Dados Pessoais, 2018).

Nesse cenário, a violação à legislação de proteção de dados pessoais (elemento essencial para a imputação da responsabilidade civil dos agentes de tratamento) pode ocorrer através de ilícitos específicos, caracterizados pela contrariedade a deveres expressamente estabelecidos em lei para o tratamento de dados, mas também por uma forma de ilícito geral, própria desse sistema protetivo.

Assim, ainda que se reconheça que a falta ao dever de segurança se aproxima da análise da culpa em sentido estrito, entendida como falta ao dever de cuidado, é necessário concluir que o regime de responsabilidade civil centrado no ilícito geral decorrente de um tratamento irregular define uma responsabilidade objetiva especial.

Ademais, é dever dos agentes de tratamento, garantir a segurança dos dados, mesmo após o término do tratamento:

> Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término. (Proteção de Dados Pessoais, 2018).

Em suma, os agentes têm as seguintes obrigações: observar os princípios e garantias do titular (art. 7, §6º); fazer registros das operações, principalmente quando estiverem atuando em legitimo interesse (art. 37); adotar medidas de segurança, técnicas e administrativas (art. 46) e assegurar os dados mesmo após o termino do tratamento (art. 47), sendo que o controlador ainda tem a obrigação de prestar informações ao titular (art. 18) e de comunicar a autoridade nacional acerca de eventual incidente (art. 48).

Além disso, o artigo 42 da LGPD, estabelece que:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei. [...] (Proteção de Dados Pessoais, 2018).

Acerca da responsabilidade solidária no âmbito da LGPD, tanto o controlador como o operador podem ser responsabilizados pelos danos causados, implicando em responsabilidade solidária entre eles perante os titulares de dados.

Segundo o art. 42, §1º, I, o operador só responderá solidariamente, quando vier a descumprir as obrigações da legislação de proteção de dados, ou quando não obedecer às ordens lícitas do controlador. Enquanto o controlador responderá solidariamente, na hipótese em que o tratamento que estava diretamente envolvido cause danos ao titular (art. 42, §1, II), ou seja, bastaria a sua participação para responsabilização.

Percebe-se que a responsabilidade aplicada ao operador é diferente da aplicada ao controlador, vez que é atrelado ao descumprimento dos preceitos legais ou do descumprimento de ordens, sendo caracterizado por alguns de “responsabilização sui generis” (TEIXEIRA; ARMELIN, 2019).

Sem prejuízo, no que concerne à responsabilidade, a existência de governança e de política de gestão de risco de dados terá substancial relevância para o fim de apuração de responsabilidades, pois os agentes de tratamento não serão responsabilizados quando provarem as hipóteses do artigo 43:

> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados;
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro. (Proteção de Dados Pessoais, 2018).

Por conseguinte, caso os agentes deixem de cumprir com as suas obrigações, poderão sofrer sanções administrativas, previstas nos artigos 52 e 53 da Lei Geral de Proteção de Dados.

Desse modo, em suma, havendo tratamento de dados pessoais, apenas quando o tratamento for ilícito (específico ou geral pela falta na segurança) e causar dano a outrem (titular dos dados ou terceiro), surge a responsabilidade civil do agente de tratamento.

Nesse sentido, a responsabilidade civil não adota a forma subjetiva centrada na culpa, nem a forma da responsabilidade civil objetiva centrada no risco, mas sim uma nova e especial forma de responsabilidade civil objetiva, centrada na garantia da segurança no tratamento de dados pessoais.

6. CONSIDERAÇÕES FINAIS

Observou-se ao longo do artigo que os dados pessoais ganharam grande relevância tanto no mercado, quanto na sociedade, podendo ser chamados de o “novo petróleo”, devido ao seu grande valor e relevância na atual sociedade. Da mesma forma, o ordenamento jurídico teve que se adaptar para resguardar os direitos desses titulares.

Diante disso, os dados pessoais podem ser considerados como peças de um grande quebra cabeça, que se montado, forma um perfil do titular e se agregado com outras fontes, poderá formar a identidade digital do titular.

A utilização destes dados pelas diferentes plataformas acaba se tornando um excelente instrumento para manipular as massas, assim como influenciar decisões. Fato que pode se

agravar no momento em que o usuário não tem noção de que seus dados estão sendo coletados, ou se sabe, não dá a devida importância, o que os tornam vulneráveis.

Destarte, visando aumentar a tutela sobre os dados pessoais, em 2018, foi aprovado a lei 13.709/2018, a Lei Geral de Proteção de Dados Pessoais que entrará em vigor em 2020. É um importante marco para a proteção de dados no ordenamento brasileiro, vez que era necessária uma lei específica para tratar de um tema bastante técnico.

Ademais, a nova lei, busca dar efetividade à garantia constitucional intimidade e vida privada, do sigilo de dados e correspondência, colocando em prática o limite imposto pelo poder constituinte ao sistema capitalista adotado, que nada mais é do que à dignidade da pessoa humana.

Acerca da responsabilidade dos controladores e operadores, as instituições/empresas que tratam dados no Brasil deverão se valer de todos os meios para salvaguardar seus interesses e observar o cumprimento das normas, bem como dos princípios trazidos pela LGPD.

Nessa esteira, é importante que os agentes de tratamento garantam seus direitos e obrigações por meio de contratos entre si, especificando claramente os procedimentos e responsabilidades de cada um no tratamento de dados, assim como as obrigações e responsabilidades nas hipóteses de contingência.

Em que pese, a legislação não cita expressamente o regime de responsabilidade civil a ser aplicada aos agentes de tratamento, porém, devido a vulnerabilidade do titular dos dados, é certo que seja objetiva.

Dessa forma, nota-se uma similaridade com o Código de Defesa do Consumidor, que em sua premissa assume a responsabilidade objetiva no intuito de defender o consumidor que está em posição de vulnerabilidade frente ao produtor e prestador de serviços, tanto que as causas de excludentes de responsabilidade dispostas em ambos os diplomas são análogas, o que justificaria a aplicação da responsabilidade objetiva em ambas as legislações.

Contudo, os agentes de tratamento de dados pessoais responderão de maneira diversas, o operador terá uma responsabilidade *sui generis*, dependendo da obediência das ordens lícitas do seu controlador e da observância dos preceitos estipulados pela lei. Já o controlador bastaria a sua participação direta no tratamento que gerou os danos, assim aproximando-se da responsabilidade objetiva.

Outrossim, no caso do descumprimento de alguma das obrigações impostas ao controlador e ao operador, também poderão ser aplicadas sanções em âmbito administrativo.

Por fim, no caso de incidente de vazamento de dados pessoais por omissão ou ação a responsabilidade atribuída aos agentes de tratamento baseia-se nos pontos expostos anteriormente, no entanto, frisa-se a impossibilidade da alegação de culpa exclusiva de terceiros, haja vista que a própria lei impõe como uma obrigação a manutenção da segurança dos bancos de dados.

7. REFERÊNCIAS

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

COTS, Márico; OLIVEIRA, Ricardo. *Lei geral de proteção de dados pessoais comentada*. São Paulo: Thomson Reuters Revista dos tribunais, 2018.

CÓDIGO CIVIL BRASILEIRO. *Lei Federal nº 10.406, de 10 de janeiro de 2002*. Brasília, Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm>. Acesso em: 10 fev. 2020.

CÓDIGO DE DEFESA DO CONSUMIDOR. *Lei Federal nº 8.078, de 11 de setembro de 1990*. Brasília, Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8078.htm>. Acesso em: 10 fev. 2020.

CONSTITUIÇÃO FEDERAL. *Lei Federal de 1998.* Brasília, Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 10 fev. 2020.

DIAS, Ronaldo Brêtas de Carvalho. *A responsabilidade civil do estado no direito brasileiro*. Boletim Técnico. Belo Horizonte: Escola Superior de Advocacia da OAB/MG, n.º 01. p. 11-38, jan./jun. 2004. p. 11.

DINIZ, Maria Helena. *Curso de Direito Civil Brasileiro. Responsabilidade Civil*. 32. Ed. Vol. 7. São Paulo: Saraiva, 2018.

DONEDA, Danilo. *A proteção dos dados pessoais como um direito fundamental*. Espaço Jurídico, São Paulo, v. 12, n. 2, p. 91-108, jul./dez. 2011.

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

DONEDA, Danilo; MENDES, Laura Schertel. *Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados*. Revista de Direito do Consumidor, v. 120, nov.-dez., 2018, p. 469-483.

DRESCH, Rafael. *A especial responsabilidade civil na Lei Geral de Proteção de Dados*. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/330019/a-especial-responsabilidade-civil-na-lei-geral-de-protecao-de-dados. Acesso em: 06 mar. 2020.

FARIAS, Cristiano Chaves de et al. *Curso de Direito Civil: Responsabilidade Civil*. Salvador: Juspodivm, 2014.

FARIAS, Cristiano Chaves de et al. *Novo Tratado de Responsabilidade Civil*. 3. ed. São Paulo: Saraiva, 2018.

FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. *Privacidade e Lei geral de proteção de dados pessoais*. Revista de Direito Brasileira, Florianópolis, v. 23, n. 9, p. 284-301, maio./ago. 2019.

GONÇALVES, Carlos Roberto. *Direito Civil Brasileiro: Responsabilidade Civil*. 14. ed São Paulo: Saraiva, 2019, v.4.

LEONARDI, Marcel. *Tutela e privacidade na Internet*. São Paulo: Saraiva, 2011.

LOPES, Alan Moreira (Coord.); TEIXEIRA, Tarcísio (Coord.); TAKADA, Thalles (Coord.). *Manual Jurídico da Inovação e das Startups.* Ed. 1. Vol. Único. Salvador: Editora Juspodvim, 2019.

MALDONADO, Viviane Nóbrega; GUTIERREZ, Andriei. *A estratégia brasileira para a transformação digital e as questões que dela emergem no que se refere à proteção de dados pessoais*. Revista dos Tribunais, São Paulo, v. 993, p.293-304, jul. 2018.

MALINOWSKI, Carmen Lucia Ambrosio de Oliveira; BONINI, Luci M. M.; LEME, Maria de Lourdes C. da S. Leme. *A lei geral de proteção de dados (LGPD): direito constitucional da dignidade da pessoa humana*. Revista do Curso de Direito do Centro Universitário Braz Cubas, São Paulo, v. 3, n. 2, p. 148-156, dez. 2019.

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 dos Tribunais, São Paulo, v. 120, p.555-587, dez. 2018.

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

MEZZAROBA, Orides; MONTEIRO, Cláudia Servilha. *Manual de Metodologia da Pesquisa no Direito.* 7. ed. São Paulo: Saraiva, 2017.

PARENTONI, Leonardo Netto. *Responsabilidade civil pela coleta, gestão e armazenamento de dados de outrem.* 2018. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=7969>. Acesso em: 10 mar. 2019.

PINHEIROS, Patricia Peck. *Direito Digital.* 6. ed. São Paulo: Saraiva, 2016.

PROTEÇÃO DE DADOS PESSOAIS. *Lei Federal nº 13.709, de 14 de setembro de 2018*. Brasília, Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 10 fev. 2020.

SANTOS, Fabíola Meira de Almeida; TALIBA, Rita. *Lei Geral de Proteção de Dados no Brasil e os possíveis impactos*. Revista dos Tribunais, São Paulo, v. 998, p.225- 239, dez. 2018.

TARTUCE, Flávio. *Manual de Responsabilidade Civil: volume único*. Versão digital. Rio de Janeiro: Forense; São Paulo: Método, 2018.

TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. *Lei Geral de Proteção de Dados Pessoais: comentado artigo por artigo.* Vol. Único. Salvador: Juspodvim, 2019.

VILHALBA, Isabela Moreira. *Vazamento de dados, internet e a responsabilidade das empresas.* 2018. Disponível em: <https://politica.estadao.com.br/blogs/fausto-macedo/vazamento-de-dados-internet-e-a-responsabilidade-das-empresas/>. Acesso em: 10 mar. 2019.

ZANDONAI, Amanda Closs; ARGILES, André Vátimo. *Incidente de segurança: O vazamento de dados de clientes do Banco Inter sob a perspectiva da Lei 13.709/2018.* Justiça & Sociedade, Porto Alegre, v. 4, n. 2, p. 273-314, set. 2019.

Contatos: wellington-carvalho@hotmail.com.br e murilo.santos@mackenzie.br