REVISTA ACADEMICA
Faculdade de Direito do Recife
Vol. 94 n. 01 – Anno CXXXI

O CONSENTIMENTO, OS DADOS SENSÍVEIS E A RESPONSABILIDADE CIVIL NA LGPD: UMA ANÁLISE À LUZ DOS CONTRATOS DE SEGURO

CONSENT, SENSITIVE DATA AND CIVIL RESPONSIBILITY: AN ANALYSIS IN THE LIGHT OS INSURANCE CONTRACTS

Recebimento em 13/07/2021
Aceito em 10/03/2022

Indyanara Cristina Pini[1]
http://orcid.org/0000-0003-0111-8118
indyanara.cp92@hotmail.com

RESUMO

Aborda-se no estudo, de início, a necessidade histórica da existência de legislações específicas para a regulamentação do tratamento de dados, sobretudo pelos movimentos mundiais decorrentes da globalização e informatização das relações sociais. Analise-se ainda as bases legais das legislações que regulamentam o tratamento de dados na atualidade, com enfoque específico a GDPR e a LGPD, sendo a primeira de origem Europeia e a segunda a atual legislação sobre o tema no Brasil, e, especificamente a figura do consentimento informado e da autodeterminação informativa como norteadores para o tratamento de dados, especialmente aqueles dispostos na legislação de natureza sensível. Busca-se com o estudo, demonstrar a importância e as previsões específicas do tratamento de dados sensíveis nas legislações, e, igualmente, a importância do consentimento informado para o compartilhamento destas informações nos contratos de seguro, visando evitar ao titular dos dados que o tratamento inadequado ou o vazamento das informações prestadas implique na sua exclusão ou dificulte a avença de outras situações contratuais. Neste cenário, analisa-se também a tutela dada pelas legislações em estudo para as situações de violação e a possibilidade de reparação civil ao titular do dado. Utilizando-se, do método dedutivo para demonstrar a previsão quanto a responsabilização civil e, igualmente, a sua aplicação, através das análises conjuntas da legislação brasileira e do direito comparado, amparando-se ainda em bibliografia sobre o tema, fundamenta-se o estudo.

PALAVRAS-CHAVE: contratos; dados sensíveis; consentimento; LGPD; GDPR.

ABSTRACT

It is approached in the study, from the beginning, the historical need for the existence of specific legislations for the regulation of data treatment, especially by world movements resulting from globalization and computerization of social relations. The legal bases of the legislations that regulate the treatment of data nowadays are also analyzed, with specific focus on the GDPR and the LGPD, the first being of European origin and the second the current legislation on the theme in Brazil, and specifically the figure of informed consent and informative self-determination as guidelines for the treatment of data, especially those provided for in legislation of a sensitive nature. The study seeks to demonstrate the importance and specific provisions of the treatment of sensitive data in the legislation, and the importance of informed consent for the sharing of this information in insurance contracts, in order to prevent the holder of the data that the inappropriate treatment or the leakage of the information provided implies in its exclusion or hinders the agreement of other contractual situations. In this scenario, we also analyze the protection provided

[1] Universidade Estadual de Londrina

Este obra está licenciada com uma Licença Creative Commons Atribuição 4.0 Internacional (CC BY 4.0).

https://doi.org/10.51359/2448-2307.2022.251044

by the legislations under study for situations of violation and the possibility of civil compensation to the holder of the data. The study is based on the deductive method to demonstrate the forecast as to civil liability and, equally, its application, through the joint analysis of Brazilian legislation and comparative law, further supported by bibliography on the theme.

KEYWORDS: contracts; sensitive data; consent; LGPD; GDPR.

1 INTRODUÇÃO

Encontra-se largamente refletido e difundido, nos sistemas legislativos ao redor de todo o mundo, incluindo o Brasil, o direito à privacidade, consagrado nos EUA no início do século XX, e, apesar de toda a revolução tecnológica que o mundo experienciou, minimizando fronteiras, aproximando pessoas e desnudando várias áreas da vida privada, ainda assim, existem espaços, condições e situações que são mantidas longe destes "palcos".

Contemplando esse direito precípuo do indivíduo, surgem os marcos regulamentadores para o tratamento de dados, tendo em vista que, desde o final da segunda guerra mundial, surgiu a preocupação voltada a tutela da propagação de questões mais íntimas do indivíduo frente a informatização da sociedade.

E, neste contexto, verifica-se sempre a importância e o reconhecimento da autodeterminação informativa do indivíduo em relação aos seus dados, de modo que possa tutelar aquilo que quer ou não compartilhar com o mundo, através de sistemas de tratamento de dados, notadamente, aqueles que dizem respeito às questões relacionadas a saúde.

Apesar da necessidade premente de legislação específica para garantir a incolumidade dos dados do cidadão, a proteção de dados no direito brasileiro não pode ser vista como matéria de vanguarda. Ao contrário. O conjunto normativo é recente, tendo as preocupações acerca da problemática se iniciado, de forma efetiva, no ano de 2010 e, a promulgação da LGPD, apesar disto, deu-se apenas 10 anos depois, já em 2020.

Não se olvida que, embora a Constituição Federal traga, em seu bojo, preocupações atinentes ao problema da informação, notadamente nos art. 5º, X, XII e LXXII, em muito se difere das preocupações mundiais acerca dos dados pessoais, que remontam ao fim da Segunda Guerra Mundial, e, no curso da evolução principiológica, alcançou quatro gerações.

Destaca-se que, ainda na segunda geração de leis de proteção de dados pessoais, o consentimento encontrou papel de protagonista no que diz respeito à proteção destes dados, sendo, portanto, transferido ao sujeito, *in casu*, titular dos dados, a responsabilidade de protegê-los, ao passo que, na terceira geração, buscou-se assegurar um controle ainda mais extensivo do sujeito aos seus dados, partindo-se não só da própria coleta, mas, acima de tudo, ao compartilhamento.

Em meio a tais panoramas, notadamente, fluxo de informações constantes, por meio de cadastros, disponibilização de dados de consumo e pessoais para formação de perfis, diuturnamente, exsurge a problemática em relação ao tratamento de todos estes dados e informações frente aos contratos de seguro, que, normalmente, já distinguem os indivíduos de acordo com o sexo, idade, localização e demais critérios subjetivos, pautados na Lei dos Grandes Números, não só para regular o custo, como também a viabilidade de contratação, e, como mencionado, no fluxo informacional, cuja possibilidade de tratamento de dados no campo da saúde é perfeitamente possível e concreta na atualidade, sem dúvidas, exsurge a preocupação sobre a utilização destes dados para, em conjunto com os demais fatores, dificultar ou encarecer ainda mais a contratação.

Nesta perspectiva, faz-se necessária uma análise da forma com que as leis que tutelam

Este obra está licenciada com uma Licença Creative Commons Atribuição 4.0 Internacional (CC BY 4.0).
https://doi.org/10.51359/2448-2307.2022.251044

a proteção de dados resguardam (ou não) tais informações dos indivíduos, e, a eventual licitude da utilização, nesta modalidade de contratos, e, igualmente, a possível responsabilização no tocante ao vazamento destes dados, de cunho sensível.

Frente a problemática mencionada, utilizando-se do método dedutivo, amparado em bibliografia nacional e estrangeria, e, nas análises da LGPD e da GDPR, será perfectibilizado o estudo neste trabalho.

2 A FIGURA DO CONSENTIMENTO NA LGPD E GDPR

A LGPD teve, indiscutivelmente, como fonte de inspiração a GDPR europeia, importando assim, em grande medida, o conteúdo, fundamentos e princípios, dentre outras características, e, foi marcada, acima de tudo, pela necessidade, em determinados casos, de privilegiar o consentimento do indivíduo que submeterá os seus dados a determinada categoria de tratamento.

Convém, ao adentrar no assunto do consentimento, destacar a evolução histórica da privacidade de dados no contexto global, sendo necessário discorrer que, a preocupação com referida tutela não é uma preocupação que data do século XXI, onde o fluxo de informações se tornou mais relevante, acessível e diário.

Contrariando a novel inovação legislativa nacional, ainda na década de 80, surge uma terceira geração de leis, que procurou sofisticar a tutela dos dados pessoais (...) proporcionando o efetivo exercício da autodeterminação informativa (DONEDA, 2011, p. 97).

Ainda nesta fase de leis, tem-se um marco normativo no tocante à privacidade de dados que foi a *privacy guidelines*, da OCDE (Organização para a Cooperação e Desenvolvimento Econômico), que vieram a influenciar mundialmente o desenvolvimento da proteção de dados pessoais, sendo, justamente, essa a finalidade intrínseca da OCDE como um organismo internacional multilateral (BIONI, 2021, p. 113-4).

Nesta esteira, verificou-se, justamente, que a noção do que era um tratamento de dados pessoais juro e lícito estava vinculado ao consentimento do indivíduo, e, muito embora no ano de 2013 as *guidelines* tenham sofrido um processo de revisão, as bases do consentimento foram mantidas (BIONI, 2021, p. 115).

A propósito, a GDPR (*General Data Protection Regulation*), a partir da norma n. 2016/679, segue justamente a linha do consentimento informado e protetivo ao cidadão em relação aos dados pessoais. Nesta dicção, o art. 6º, I, determina que a licitude do tratamento de dados está vinculado ao consentimento do titular.

Verifica-se, portanto que vários são os aspetos inovadores do RGPD face à Diretiva que vem revogar. Entre eles conta-se, desde logo, o alargamento do leque dos direitos dos titulares de dados. Nesta linha, o titular dos dados assume um papel central na coerência interna do sistema RGPD, podendo falar-se de um autêntico apoderamento dos titulares sobre os seus dados, sendo reforçados os direitos destes ao controle de seus dados (POÇAS, 2018, p. 226).

Também da LGPD, pode-se dizer que o consentimento no tocante ao tratamento de dados dos indivíduos assume papel de destaque, embora ainda esteja ao lado de outras bases legais, como preconizado no art. 7º, mas, nem por isso deixou de ser um vetor principal da lei. Isso porque, de uma análise detida dos princípios e a maneira pela qual a LGPD disseca o consentimento revela a preocupação e a carga participativa do indivíduo no fluxo de suas informações pessoais (BIONI, 2021, p. 127).

O objetivo da LGPD é a proteção dos dados pessoais dos indivíduos, com a finalidade de preservar a sua personalidade. Em última *ratio*, a LGPD visa à proteção dos direitos de personalidade dos indivíduos e das garantias constitucionais decorrentes (KLEE; NETO, 2019, p. 15).

Justamente com essa preocupação de tutela aos direitos da personalidade, a LGPD, em

Este obra está licenciada com uma Licença Creative Commons Atribuição 4.0 Internacional (CC BY 4.0).
https://doi.org/10.51359/2448-2307.2022.251044

seu art. 2º, II, prevê, como fundamento, o respeito à privacidade dos usuários, no tocante aos dados sensíveis e pessoais, e, igualmente, prevê também o consentimento informado para o compartilhamento destas informações.

O direito à proteção de dados angaria autonomia própria. É um novo direito da personalidade que não pode ser amarrado a uma categoria específica, em particular, o direito à privacidade. Ao contrário. Demanda-se uma necessária ampliação normativa, que clareie e não empole a sua tutela (BIONI, 2021, p. 95).

Entende-se, portanto, que o consentimento do titular para o tratamento de seus dados pessoais é um dos pontos mais sensíveis, não só da atualidade, como do curso do processo de proteção de dados, em cenário mundial, sendo, justamente, por meio dele a possibilidade de se estruturar e proteger direitos fundamentais (DONEDA, 2021, p. 296).

Considera-se que, mesmo em casos em que há a prevalência do consentimento para a tomada de decisão no tocante ao tratamento de dados, como disciplinado por Stéfano Rodotà (2008) é raro o cidadão ser capaz de perceber os riscos que corre ao fornecer seus dados, muito menos o potencial de tais informações pessoais para as organizações coletoras, diante da complexidade dos sistemas sofisticados de tratamento. Sem que haja a necessidade de consentimento, bastando apenas um aviso da coleta e disponibilização dos dados, resta mais do que evidente a vulnerabilidade a que o sujeito estará exposto.

Pode-se dizer que a "fé no consentimento prévio como redoma protetora da privacidade do titular é puramente teórica, e baseada na extrema confiança de que os controladores e operadores de dados irão respeitar todos os ditames da LGPD" (MOURA; ANDRADE, 2019, p. 124), já que, de início, não poderá estar seguro de que aquelas informações não serão, sob qualquer hipótese, compartilhadas com terceiros, tomando como verdadeira, exclusivamente, a responsabilidade do controlador para manter seguros os dados informados.

Sem adentrar às hipóteses em que o consentimento é dispensado, por se tratarem de exceção da legislação em estudo, é possível afirmar que, não só a base da LGPD, como de todo o histórico de tratamento de dados tem como pauta e princípio a figura do consentimento do titular de dados.

Mesmo porque, deve-se considerar que no atual cenário globalizado, frente às redes sociais e fluxo constante em navegadores, nos *www.* que se tem à disposição, as informações pessoais passaram a ser verdadeira moeda de troca, servindo de fomento econômico a toda à base da internet, derivando, também disto, a necessidade de se consentir para compartilhar as informações pessoais, de modo a reverter a possibilidade de que o cidadão se torne mera vitrine para o comércio, e não o contrário.

3 O ARMAZENAMENTO DE DADOS E DADOS: DEFINIÇÕES

É necessário, antes do prosseguimento às discussões também esclarecer, de início, o que são dados, e, igualmente, como funciona esse armazenamento, passível de violação, conforme as disposições traçadas pela LGPD.

O armazenamento de dados, por si, nada mais representa do que as informações pessoais que são arquivadas, tanto por entes públicos ou privados, ambos devidamente conceituados na LGPD, e, com as respectivas possibilidades de quais dados tratarem, que podem ser acessados em momento posterior ao cadastro.

Em virtude do avanço significativo das interações cibernéticas, como já mencionados, o que outrora não trazia qualquer risco aos cidadãos, nos tempos modernos, mostra-se como uma infinidade de informações capazes de garantir recompensas econômicas com a criação de perfis de consumo, a título de exemplo.

Este obra está licenciada com uma Licença Creative Commons Atribuição 4.0 Internacional (CC BY 4.0).
https://doi.org/10.51359/2448-2307.2022.251044

O conceito de banco de dados vem delineado no art. 5º, IV da LGPD, compreendendo o "conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico".

Os dados pessoais, por seu turno, também estão disciplinados no art. 5º, I e II, sendo basicamente as informações relacionadas a pessoa natural que está ou pode ser identificada a partir das informações. Os dados pessoais de natureza sensível serão abordados na sequência, pelos enfoques próprios necessários.

Conclui-se, portanto, que o armazenamento de dados nada mais é do que a hospedagem dos dados, que são nada mais que as informações pessoais dos indivíduos, em sistemas vinculados a órgãos e empresas públicas ou privadas, com possibilidade de traçar perfis e padrões de consumo e mesmo de comportamento dos cidadãos.

4 OS DADOS SENSÍVEIS

Para além das questões atinentes ao consentimento, e, sendo matéria indispensável para todo e qualquer dado que será submetido a tratamento, surge a problemática no tocante ao tratamento de dados sensíveis, cuja qualificação para enquadramento vem, devidamente preconizado, de forma expressa e em rol taxativo, tanto na GDPR como na LGPD.

E, frente a natureza do trabalho, forçoso analisar os meandros dos dados relativos à saúde, destacando, de início, que o tratamento de dados, conforme preceituado no art. 5º, inciso X, engloba a coleta, produção, classificação, arquivamento e eliminação, sendo que, em meio ao processo delineado, mostra-se possível eventual manipulação.

Na GDPR, os dados sensíveis são elencados no art. 9º, havendo expressa proibição do tratamento, e o rol elenca nesta categoria os dados pessoais que revelem a origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, filiação sindical, tratamento de dados genéticos, dados biométricos, dados relativos à saúde ou à vida sexual ou a orientação sexual de uma pessoa, trazendo ainda as hipóteses de exceção[2], resguardado ainda aos Estados-Membros, de acordo com o Considerando 10 e 51, eventuais acréscimos de especificidades em relação ao tratamento de dados genéticos, dados biométricos e relativos à saúde.

Na LGPD, sem maiores modificações, o art. 5º, inciso II, traz o rol, cujo entendimento é de que não se trata de rol taxativo, das categorias de dados pessoais sensíveis, que são, igualmente, 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, vida sexual, genético e biométrico[3].

---

[2] 1. É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.
2. O disposto no n.º 1 não se aplica se se verificar um dos seguintes casos:
(*omissis*)
3. Os dados pessoais referidos no n.º 1 podem ser tratados para os fins referidos no n.º 2, alínea h), se os dados forem tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional, nos termos do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade ao abrigo do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes.
4. Os Estados-Membros podem manter ou impor novas condições, incluindo limitações, no que respeita ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde.

[3] Art. 5º Para os fins desta Lei, considera-se:
(*omissis*)

Este obra está licenciada com uma Licença Creative Commons Atribuição 4.0 Internacional (CC BY 4.0).
https://doi.org/10.51359/2448-2307.2022.251044

De acordo com a LGPD, os dados pessoais sensíveis podem resultar em danos imediatos quando divulgados de forma indevida, por isso, requerem cuidados especiais e só podem ser solicitados para finalidades específicas, uma vez que poderão "implicar riscos e vulnerabilidades potencialmente mais gravosas aos direitos e liberdades fundamentais de titulares" (SALMEN, 2020, p. 249)

Pela natureza dos próprios dados considerados como sensíveis, já é possível vislumbrar que o objetivo da proteção especial a estes dados se dá com fulcro, principalmente, na dignidade humana, resguardando seus aspectos mais privados e não permitindo, por conseguinte, que qualquer tipo de preconceito ou discriminação, em decorrência destas particularidades seja possível.

E, afastando as críticas que, por vezes, gravitam ao redor da ponderação da legislação sob o auspício da dignidade humana, convém sempre refletir e reafirmar que a dignidade humana é um valor fundamental que se viu convertido em princípio jurídico de estatura constitucional, mostrando-se como fundamento dos direitos humanos, ideia símbolo do valor inerente à pessoa e da igualdade de todos, sem qualquer exclusão por gênero (BARROSO, 2010).

Não só para garantir o respeito as particularidades de cada indivíduo, a proteção especial desta categoria de dados também se mostra necessária, pois, segundo o estudo de Machado e Bioni (2016, p. 361) em relação aos CPF captados nas notas fiscais estaduais, conclui que "no conjunto dos estados onde existe o programa, a análise da transparência ativa das informações denota um cenário desolador. Não há qualquer tipo de informação sobre as políticas de proteção de dados pessoais adotados para garantir a privacidade do cidadão".

Mais uma vez, revolve-se a necessidade de assegurar estes dados, evitando qualquer tipo de discriminação, justamente sob a possibilidade de se ferir a dignidade inerente à pessoa, e, por qualquer razão, discriminá-la.

Frente a estes cenários de possibilidade de vazamentos, portanto, mostra-se inviável conceber o previsto no art. 5º, II da LGPD como rol taxativo de dados sensíveis, já que eles são definidos pelos efeitos potencialmente lesivos do seu tratamento. Justamente por isso, o próprio legislador reconhece que se aplicam as regras relativas ao tratamento de dados sensíveis aos dados pessoais que, posto não serem em si sensíveis, podem vir a revelar dados sensíveis (LGPD, art. 11, § 1º), servindo como exemplo aqueles decorrentes de geolocalização, hábitos de compras, preferências de filmes, históricos de pesquisas e afins, que, embora pareçam, a um primeiro olhar, inofensivos, mostram-se, em contexto amplo, capazes de criar perfis discriminatórios (KONDER, 2020).

Considerando, portanto, a possibilidade de se tratar, inclusive, dados relativos à saúde, entende-se que existe uma preocupação genuína na forma como os dados sensíveis devem ser tratados, que englobam, não só, as preocupações já delineadas como outras, a partir de pontos de vista específicos.

Deve-se visar a um tratamento limitado desses dados sensíveis, para evitar o seu eventual uso para propósitos que não atendam aos fundamentos republicanos do Estado Democrático de Direito (MULHOLLAND, 2018, p. 163).

Conclui-se, portanto, que os dados de natureza sensível, como bem explicitados em lei, serão todos aqueles que, de alguma forma, puderem não só identificar o cidadão, como e, principalmente, causar determinado tipo de segregação ou distinção, seja por qualquer das categorias nominadas, primando, sobretudo, pela dignidade humana, assegurando um tratamento justo e igualitário a qualquer pessoa.

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Este obra está licenciada com uma Licença Creative Commons Atribuição 4.0 Internacional (CC BY 4.0).

https://doi.org/10.51359/2448-2307.2022.251044

5 O TRATAMENTO DE DADOS PESSOAIS E AS REPERCUSSÕES NOS CONTRATOS DE SEGUROS SAÚDE: UMA ANÁLISE DA GDPR E DA LGPD

Para além das repercussões habituais do tratamento de dados, como já difundido, na formação de perfis comerciais, por exemplo, para ofertas de produtos e serviços por meio de publicidade, eletrônica ou física, incluindo redes de supermercado, farmácias e as mais diversas categorias de atacado e varejo, no campo dos contratos também se torna possível a aplicação do tratamento de dados para seleção de perfis.

Nos tempos hodiernos, o intercâmbio de dados é realizado para todo tipo de finalidade, e, por certo, as empresas privadas adquirem bancos de dados pessoais justamente no intento de garantirem assertividade no lançamento de produtos ou serviços, de modo que, é possível dizer que a complexidade do ser humano está se mostrando reduzida a determinado perfil comportamental, cuja origem advém do tratamento de dados.

Mesmo antes da entrada em vigor da LGPD, normas foram editadas e foram ainda instituídos critérios técnicos para compartilhamento de dados nos sistemas de saúde do país, incluindo o SUS, Saúde Suplementar e a Saúde Privada, posto que, "o compartilhamento de dados em saúde é essencial para reduzir os custos assistenciais, seja ao disponibilizar dados mínimos do paciente aos que integram a cadeia de assistência à saúde, seja para viabilizar um tratamento mais assertivo" (BONAFÉ, 2019, p. 47).

A Portaria de Consolidação nº. 01 de 28 de Setembro de 2017 instituiu regras para os sistemas de informação, regulamentando o uso de padrões, informações em saúde e de interoperabilidade entre os sistemas de informação do SUS e também os sistemas privados, permitindo, com isso, o compartilhamento de informações em saúde e, igualmente, de cooperação entre os profissionais de saúde e os estabelecimentos de saúde. Foram instituídos, em referida portaria, a instituição de sistemas de informação, criação e padronização de criação e padronização de codificação de dados, tornando célere o acesso a informações relevantes e fidedignas ao usuário de saúde.

Ato contínuo, destaca-se ainda que a Portaria estabeleceu que o sistema de informação permitirá identificar os usuários de saúde por meio do Sistema de Cartão Nacional de Saúde, cujos benefícios, permite: (i) a apuração do perfil epidemiológico dos usuários de acordo com seu domicílio residencial; (ii) a possibilidade de o usuário ter acesso aos seus dados de forma unificada; e (iii) a garantia de que os dados pessoais dos usuários sejam tratados de forma a respeitar os princípios constitucionais da intimidade, da integralidade das informações e da confidencialidade. Há possibilidade ainda de que essas informações e dados sejam compartilhadas entre entes federativos e demais órgãos que executem políticas públicas.

Imperioso destacar que, quando da publicação da LGPD, havia vedação expressa de compartilhamento de dados sensíveis referentes à saúde com objetivo de obter vantagem econômica, buscando evitar que houvesse a venda de dados, propriamente dita, rememorando que, poucos dias antes da edição da lei foram divulgados casos de venda de dados por drogarias, que, comumente realizam o cadastro de pessoas, por CPF, a fim de padronizar e perfilar o perfil de consumo, tendo, por consequência, acesso às medicações contínuas utilizadas pelos cadastrados, especialmente aquelas relacionadas a alguma comorbidade ou transtorno psiquiátrico.

Contudo, após a votação da MP nº. 869/2018, houve nova alteração na LGPD e, a partir daí a permissão para o compartilhamento de dados de saúde, com manifesto objetivo econômico, nas hipóteses de prestação de serviços de saúde, assistência farmacêutica e assistência à saúde.

Este cenário, no entanto, modifica relações, especialmente, aquelas relacionadas aos contratos de seguro, sendo certo que, o advento da LGPD, inicialmente, visa proteger os dados dos indivíduos, e, compartilhá-los e tratá-los, como visto, à medida em que se obtém autorização para tanto, sendo necessário destacar que o art. 11, § 5º, veda, inclusive, o tratamento de dados de saúde

Este obra está licenciada com uma Licença Creative Commons Atribuição 4.0 Internacional (CC BY 4.0).
https://doi.org/10.51359/2448-2307.2022.251044

para seleção de riscos.

A partir disto, indaga-se, frente a relação securitária, em que as informações pessoais se mostram necessárias para contratação, especialmente aquelas vinculadas à saúde, como e se será possível a manutenção do tratamento de dados dos indivíduos pelas empresas desta natureza.

Para a mensuração do risco a ser garantido, tem toda relevância a análise dos dados pessoais do segurado. Há íntima relação que se estabelece entre dados pessoais e risco coberto, na medida em que o conjunto de características subjetivas e comportamentais do segurado, definirá os riscos e as probabilidades do sinistro (MIRAGEM, 2020, p. 4).

Da análise da GDPR, constata-se, a partir da alínea b, do nº. 1 do art. 6º o reconhecimento da licitude do tratamento de dados quando seja necessário para executar um contrato em que o titular dos dados é parte, ou, para possíveis diligências pré-contratuais, a pedido do titular dos dados, destacando-se que, no tocante ao tratamento de dados de saúde, a licitude estará sedimentada na titularidade tanto dos dados tratados como da contratante. (POÇAS, 2018, p. 249).

Entende-se, portanto, que, se o indivíduo, voluntariamente, busca a contratação e, por consequência, tem interesse na execução do contrato em que há dependência de tratamento de dados pessoais, diante da ciência do cenário, não haverá meios de, simultaneamente, invocar a vedação legal e, ao mesmo tempo, exigir a contratação.

Cenário muito próximo ao que ocorre no Brasil, a partir da análise da LGPD, em que se possibilita o tratamento dos dados sensíveis, que, no presente estudo, vinculam-se àqueles de saúde, cujo amparo se dá no art. 5º, XII, 7º, V, 8º e 11, I.

> A legitimidade do tratamento de dados no seguro pressupõe a observância dos princípios que informam o tratamento de dados (art. 6º da LGPD), assim como dos direitos assegurados ao titular dos dados (arts. 17 e 18 da LGPD). A previsão desses direitos e princípios repercute no seguro, criando direitos ao segurado (titular dos dados) e deveres ao segurador (controlador dos dados) durante e após o término do tratamento, desde a fase de formação do contrato até as fases de execução e pós-contratual. Relativamente aos dados sensíveis, estes recebem uma proteção especial, com a delimitação mais estrita das condições do tratamento e a ampliação das garantias ao titular dos dados (art. 11 da LGPD) (MIRAGEM, 2020, p. 25).

Pode-se dizer, portanto, que a base contratual possibilitará o tratamento de dados sensíveis, tanto no contexto da GDPR como, igualmente, na LGPD, sendo necessário, no entanto, resguardar estes dados, de modo que, como lecionado por Bruno Bioni (2021, p. 216), questões de cunho genéticas, por exemplo, informadas em outros campos onde também se vinculam o tratamento de dados, não possibilitem uma recusa no ato da contratação ou mesmo à fixação de prêmios em patamares muito elevados, causando assim verdadeira *seleção eugênica* no mercado de consumo securitário.

Da mesma forma, é decisivo, no âmbito do seguro, precisar os critérios que permitam identificar o que seja o tratamento de dados discriminatório. A discriminação injusta poderá ser fundada em critério distintivo ilegítimo. E, neste aspecto, ao exigir que o tratamento se desenvolva para fins legítimos e se limite ao mínimo necessário, impõe-se uma racionalidade ao tratamento de dados, em que, o critério distintivo será legítimo e não discriminatório (MIRAGEM, 2020, p. 25).

Tratando-se os dados pessoais, contudo de verdadeira moeda de troca, e, havendo a previsão de angariação monetária em relação a eventuais transações, existe o risco de que determinadas empresas façam intercâmbio, a exemplo, de rede de farmácias com seguradoras de saúde, em que haverá vantagem tanto para aquele que mantém dados relacionados à saúde, em razão da aquisição pelo cidadão de remédios contínuos, e, sobretudo, o interesse e a submissão mais assertiva da seguradora em relação a sinistros, valores de prêmios e possibilidades de

Este obra está licenciada com uma Licença Creative Commons Atribuição 4.0 Internacional (CC BY 4.0).
https://doi.org/10.51359/2448-2307.2022.251044

ocorrência.

Não obstante, é real e noticiado que hackers acabam invadindo sistemas de armazenamento de dados e, inclusive, dão publicização ao que captam, não podendo ser descartado, portanto, eventual ataque a sistema e posterior venda de informações.

Tudo isso implicaria em verdadeira tragédia àqueles que buscam contratação de seguro saúde, mas que detém determinado tipo de enfermidade ou mesmo predisposição, que pode ser mapeada em perfis genéticos, e, certamente, ou o preço seria muito superior ao de um indivíduo sem outras predisposições ou doenças ou sequer seria aceito pela empresa.

E, justamente frente a estes riscos, é necessário que haja na LGPD, como também existe na GDPR, a possibilidade de responsabilização dos responsáveis pelo armazenamento e controle de dados, assegurando ao indivíduo maior segurança quando da aceitação de compartilhamento de dados.

6 A IMPLICAÇÃO DA RESPONSABILIDADE CIVIL FRENTE A UTILIZAÇÃO INADEQUADA DOS DADOS

Assim como a própria sociedade evolui e as relações se tornam mais complexas e amplas, também a figura da responsabilidade civil, frente às modificações, terá contornos distintos, mas, será preciso verificar o que, de fato, está se tutelando para exsurgir a obrigação. Aliás, torna-se necessário, inicialmente, encontrar o ponto fulcral da violação ocasionada, agora, na esfera digital, com eventual compartilhamento de dados sensíveis.

Partindo de um ensaio semântico, a partir de Ricoeur (1995, p. 33-34), pode-se dizer que a responsabilidade, definida, no sentido clássico do direito civil, traduz-se como "a obrigação de reparar danos que infringimos por nossa culpa e em certos casos determinados pela lei".

A teoria tradicional da responsabilidade civil garante, portanto, que, havendo dano a esfera alheia a obrigação de indenizar nasce, sobretudo, porque as investidas ilícitas ou antijurídicas no circuito de bens ou mesmo de valores alheios acabam por tirar da órbita o próprio fluxo das relações sociais, sendo a reação do direito o meio adequado para o reequilíbrio da ordem, motivo pelo qual, essa visão clássica da responsabilidade civil tem suas raízes a partir do princípio fundamental *neminem laedere* (BITTAR, 2015).

A partir daí, torna-se necessário encontrar as dimensões nucleares da pessoa humana, ainda que sem referência expressa legislativa, que merece a tutela jurídico-positiva, que foram atingidas pelo ato, no tocante aos fluxos digitais e tratamento de dados, para que se possa responsabilizar, concreta e corretamente, o violar.

Assim, e para feitos da convocação do instituto de responsabilidade civil, importa averiguar qual o concreto direito de personalidade, ou posição jurídica atingidos por quem procede ao tratamento de dados (MATOS, 2020, p. 65).

Como já sublinhado, os dados sensíveis estão intimamente ligados a própria dignidade humana, vinculando-se, no tocante aos dados de saúde, acima de tudo ao direito à igualdade, posto que, com a transmissão de determinados dados que apontem, por exemplo, a uma enfermidade, o serviço de seguro saúde ou sairá mais caro ao contratante ou sequer será disponibilizado.

> Como regra geral daí decorrente, pode-se dizer que, em todas as relações privadas nas quais venha a ocorrer u conflito entre uma situação jurídica subjetiva existencial e uma situação jurídica patrimonial, a primeira deverá prevalecer, obedecidos, assim, os princípios constitucionais que estabelecem a dignidade da pessoa humana como o valor cardeal do sistema (MORAES, 2009, p. 120)

A divulgação, portanto, de um dado de saúde que implique na negativa ou mesmo que dificulte o acesso do cidadão a determinado serviço no campo da saúde, ensejará a

Este obra está licenciada com uma Licença Creative Commons Atribuição 4.0 Internacional (CC BY 4.0).
https://doi.org/10.51359/2448-2307.2022.251044

responsabilização civil, cuja previsão, inclusive, existe na própria LGPD, não havendo necessidade de socorro ao Código Civil, por exemplo, para a efetiva configuração.

Vale ressaltar ainda, que o dano, nestes casos, causados aos cidadãos será de cunho moral, tendo em vista que referido dano se traduz, justamente, como a violação à dignidade (MORAES, 2009), que é justamente o campo tutelado em relação aos dados sensíveis.

Em relação a figura a ser responsabilizada, tem-se, em equivalência, tanto na LGPD como na GDPR, o operador e o controlador dos dados.

Tal como já acontecia com a anterior legislação europeia na matéria, confrontamo-nos novamente com as noções de *data controller* (responsável pelo tratamento de dados) e *data processor* (subcontratante). Logo, se o conceito de responsável pelo tratamento de dados traz a ideia de responsabilidade enquanto a assunção de um especial encargo, que implica deveres para resguardar dados alheios, o responsável pelo tratamento de dados, portanto, torna-se responsável no sentido da *liability*[4] em caso de violação (BARBOSA, 2018).

As figuras do controlador e do operador na LGPD estão delineadas nos artigos 37 a 40, sendo o controlador responsável pelo comando do operador, dando-lhe as normativas e instruções para realizar o tratamento de dados segundo a própria legislação.

Na GDPR, inspiração normativa para a LGPD brasileira, a responsabilidade dos operadores e controladores está delimitada no art. 82º, cuja disciplina assegura a qualquer pessoa que tenha sofrido danos materiais ou imateriais em razão de uma violação do regulamento tem direito ao percebimento de uma indenização do responsável, com o acréscimo nº. 2 de que qualquer responsável pelo tratamento de dados que esteja envolvido na lesão responderá pelos danos e o subcontratante só será responsabilizado se não tiver cumprido as obrigações impostas no regulamento.

> Esta responsabilidade pode ser afastada se o responsável pelo tratamento ou o subcontratante provar que não é responsável pelo evento que deu origem aos danos. Havendo mais do que um responsável pelo tratamento ou subcontratante, ou um responsável pelo tratamento e um subcontratante, que sejam responsáveis por danos causados pelo tratamento, cada um é responsável pela totalidade dos danos, prevendo-se no nº5 do artigo 82º a possibilidade de exercício do direito de regresso em relação à parte da indemnização correspondente à respetiva parte de responsabilidade pelo dano em conformidade com a regra estabelecida no nº 2 (BARBOSA, 2018, p. 162).

Inequívoco, portanto, que a GDPR consagrou a solidariedade obrigacional entre todos os corresponsáveis e, ao mesmo tempo, dá a impressão de inversão do ônus da prova a partir da constatação das violações às obrigações que foram impostas.

Dada a inspiração já mencionada, situação e tutela praticamente idêntica é também adotada no cenário legislativo brasileiro no tocante à responsabilização pelos danos que foram causados a terceiros em razão do tratamento e armazenamento de dados.

[4] Apresentam-se, aí, quatro sentidos para o termo *responsability*. A *role-responsability,* indicando que, se uma pessoa está investida num determinado cargo, lugar, estatuto, papel, fica adstrita a especiais deveres, alguns dos quais se prendem com a promoção do bem-estar dos outros ou a prossecução dos objetivos de uma dada organização; a *causal-responsability*, em cuja aceção o responsável se vem a identificar com o causador de um ato, pelo que não só os humanos, mas também as coisas, os animais ou os fenómenos não humanos podem ser considerados responsáveis (cf. p. 214); a *liability responsability*, que, ao contrário do sentido prévio, implica já uma assunção acerca do mérito da conduta, afastando-se do mecanicismo característico da visão da responsabilidade/causalidade, a implicar a responsabilidade como o desencadear de um efeito na realidade, tanto mais que a pessoa pode ser responsabilizada, neste sentido, pelos atos praticados por terceiros. H.L.A. HART, *Punishment and Responsability, Essays in the Philosophy of Law*, Oxford University Press, 1968, 210.

Este obra está licenciada com uma Licença Creative Commons Atribuição 4.0 Internacional (CC BY 4.0).
https://doi.org/10.51359/2448-2307.2022.251044

É no artigo 43 da LGPD que se encontra também as hipóteses de não responsabilização dos controladores e operadores, no tocante às relações privadas. A partir da leitura do referido artigo, torna-se possível identificar que, a legislação em questão tratou de aplicar as duas categorias a responsabilidade civil objetiva, uma vez que só será afastada a responsabilidade se comprovado o que disciplina os três incisos.

Verifica-se também ponto de encontro com a GDPR, ao passo que se vislumbra a responsabilidade solidária entre o controlador e o operador, e, inclusive, eventual direito regressivo.

Destaca-se ainda que o art. 45 da LGPD ressalva que para as hipóteses de violações decorrentes de relações de consumo, a responsabilização, bem como demais matérias pertinentes será aplicada de acordo com a legislação pertinente, que, *in casu*, será o Código de Defesa do Consumidor.

A figura objetiva da responsabilidade civil nestes casos é demasiadamente importante, já que, para o cidadão lesado pelo compartilhamento ou vazamento de seus dados e prejuízos advindos de tal fato seriam difíceis de comprovar, já que não existe uma forma de controle após o consentimento do tratamento de dados fornecidos em determinadas relações, havendo apenas a possibilidade de alterações e exclusões.

Ato contínuo, a responsabilização se mostra fundamental e necessária, pois, como visto, dados pessoais de cunho estritamente relacionados ao mais íntimo dos indivíduos são, muitas vezes, compartilhados, para determinados fins pré-estabelecidos e não se vislumbra qualquer cabimento em compartilhamento ou, pior, venda destes dados.

Não só isso, o eventual vazamento de dados pela inobservância de regras estabelecidas pela legislação ou mesmo pela falta de segurança adequada aos sistemas, igualmente, é de responsabilidade total do controlador e do operador, destacando-se a possibilidade de responsabilização como meio de assegurar o compromisso com o tratamento e segurança adequada dos dados.

Por fim, no tocante aos dados sensíveis, pelas complicações e consequências que o vazamento acarretará a vida e as relações negociais dos indivíduos afetados, e, por serem os dados que ferem, frontalmente, a dignidade da pessoa, mostra-se também adequada a responsabilização objetiva e, acima de tudo, a própria possibilidade de ingresso com ação reparatória.

7 CONSIDERAÇÕES FINAIS

A partir da observação simplista da sociedade contemporânea é bastante forçoso reconhecer que, cada dia mais e de forma intensificada, a sociedade tem se tornado governada por dados, e, o sujeito inserido neste contexto, dificilmente, poderá optar por viver alheio a esse tráfego de informações ou mesmo privado de qualquer interação eletrônica com fornecedores de bens e serviços. É justamente por esse motivo que a previsão de autodeterminação informativa, fundamento precípuo, inclusive, das leis que regulamentam os dados pessoais, mostra-se tão importante, sobretudo para proteger o titular dos dados da notável assimetria existente entre este e aqueles que realizam o respectivo tratamento, normalmente, empresas e grandes conglomerados econômicos.

Justamente para equilibrar esta assimetria tão evidente entre o titular e o responsável pelo tratamento dos dados é que a responsabilidade civil deste último deve ser, como de fato é, perfeitamente prevista nas legislações que regulamentam a proteção de dados, que, no Brasil é justamente a LGPD, ora tratada no estudo, especialmente no tocante aos dados cuja natureza contemplam o rol definido como sensível, a exemplo daqueles atrelados ao direito à saúde, liberdade de expressão e liberdade religiosa, já que, em caso de vazamento, inúmeras situações excludentes poderiam ser impostas ao seu titular.

Este obra está licenciada com uma Licença Creative Commons Atribuição 4.0 Internacional (CC BY 4.0).
https://doi.org/10.51359/2448-2307.2022.251044

É com base justamente nestes dados, na sua natureza e na possibilidade de danos que se buscou demonstrar que o tratamento de dados por parte de seguradoras, quando da formação e execução de um contrato de seguros, em verdade, não tomará por base banco de dados em que há a hospedagem de dados sensíveis dos indivíduos, sob pena de, a partir de análises, por exemplo, de histórico médico, religioso, medicamentoso e afins, coberturas contratuais serem negadas ou valores superiores ao comumente praticado serem cobrados do indivíduo a depender de seu possível perfil e maior ou menor risco de ocorrência do sinistro.

Como analisado, os dados sensíveis, tanto no contexto da GDPR como da LGPD, são tratados de forma totalmente privativa, sem qualquer possibilidade de cessão a terceiros, sem o consentimento e sem o conhecimento do titular, justamente para evitar práticas discriminatórias, a exemplo, da recusa da própria avença contratual.

Contudo, é de se observar que, diante de um cenário onde as informações de saúde são de suma importância para a avença contratual, de fato, não faz sentido que seja possibilitado ao contratante privar o contratado das informações, e, justamente, por força deste contrato que será avençado, possibilita-se, nos diplomas estudados, a submissão das informações ao tratamento de dados.

A base, portanto, do tratamento destes dados sensíveis, em paridade a todo o contexto legislativo é, sem dúvidas, o consentimento informado, e, igualmente, a previsão contratual da necessidade e tratamento dos dados ali fornecidos, possibilitando assim ao contratante, titular destes dados, ter a plena ciência da destinação e utilização das informações, a fim de evitar o vazamento destas e a imposição de situações, perante outras empresas ou contratos, de possível exclusão.

Nesta senda, torna-se de suma importância o exercício das funções do *data controller* (responsável pelo tratamento de dados) e *data processor* (subcontratante) quanto ao correto tratamento e armazenamento destes dados, destacando-se sempre que, a ingerência acarretará a responsabilização civil daquele que tiver em seu poder as informações, gerando ao titular, lesado pela irregularidade do tratamento ou vazamento das informações, o direito regular e devidamente previsto na LGPD de buscar a efetiva reparação aos danos sofridos, que, como mencionado no estudo, será, em regra, o dano moral, em virtude das esferas que são atingidas nas questões atinentes aos dados sensíveis.

REFERÊNCIAS

BARBOSA, Mafalda Miranda. Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil. **Revista online banca, bolsa e seguros**, Coimbra, n. 3, p. 147-217, 2018.

BARROSO, Luís Roberto. **A Dignidade da Pessoa Humana no Direito Constitucional Contemporâneo**: Natureza Jurídica, Conteúdos Mínimos e Critérios de Aplicação. 2010. Mimeografado. Versão provisória para debate público.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2021.

BITTAR, Carlos Alberto. **Reparação civil por danos morais**. 4. ed. São Paulo: Saraiva, 2015.

BODIN DE MORAES, Maria Celina. **Danos à pessoa humana**: uma leitura civil-constitucional dos danos morais. Rio de Janeiro: Renovar, 2009.

Este obra está licenciada com uma Licença Creative Commons Atribuição 4.0 Internacional (CC BY 4.0).

https://doi.org/10.51359/2448-2307.2022.251044

BONAFÉ, Lucas Alves da Silva *et al*. **LGPD na Saúde**. E-book 2019. Disponível em: https://lgpdesaude.com.br/. Acesso em: 05 jul. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 05/03/2022

CARVALHO, Gisele Primo; PEDRINI, Tainá Fernanda. Direito à privacidade na lei geral de proteção de dados pessoais. **Revista da ESMESC**, v. 26, n. 32, p. 363-382, 2019. Disponível em: https://revista.esmesc.org.br/re/article/view/217/186. Acesso em: 24 mar. 2021.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo. A Proteção da Privacidade e de Dados Pessoais no Brasil. **Revista Observatório Itaú Cultural**, São Paulo, n. 16, jan./jun. 2014. Disponível em: http://d3nv1jy4u7zmsc.cloudfront.net/wp-content/uploads/2014/06/OBSERVATORIO16_0.pdf. Acesso em: 28 mar. 2021.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço jurídico**, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: http://editora.unoesc.edu.br/index.php/espacojuridico/article/view/1315. Acesso em: 04 maio de 2021.

KLEE, Antonia Espíndola Longoni; PEREIRA NETO, Alexandre Nogueira. A lei geral de proteção de dados (LGPD): uma visão panorâmica. **Cadernos Adenauer**: Proteção de dados pessoais: privacidade versus avanço tecnológico Rio de Janeiro: Fundação Konrad Adenauer, outubro 2019. n. 3.

KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados e suas repercussões no Direito Brasileiro**. 2. ed. São Paulo: Revista dos Tribunais, 2020. Edição do Kindle.

MACHADO, Jorge; BIONI, Bruno Ricardo. A proteção de dados pessoais nos programas de Nota Fiscal: um estudo de caso do "Nota Fiscal Paulista. **LIINC em Revista**, Rio de Janeiro, v. 12, n. 2, p. 361, nov. 2016.

MATOS, Filipe Miguel Cruz de Albuquerque. O regulamento de proteção de dados pessoais (2016/679) no contexto dos desafios da actividade seguradora – o caso particular dos seguros saúde. **Revista online banca, bolsa e seguros**, Coimbra, n. 3, p. 217-302, 2018.

MIRAGEM, B. N. Bruno. O contrato de seguro e a lei geral de proteção de dados. **Revista dos Tribunais online**, São Paulo, v. 1018, p. 1-34, ago. 2020.

MOURA, Plínio Rebouças de; ANDRADE, Diogo de Calasans Melo. O direito de consentimento prévio do titular para o tratamento de dados pessoais no ciberespaço. **Revista de Direito, Governança e Novas Tecnologias**, Goiânia, v. 5, n. 1, p. 110-133, jan/jun. 2019.

Este obra está licenciada com uma Licença Creative Commons Atribuição 4.0 Internacional (CC BY 4.0).

https://doi.org/10.51359/2448-2307.2022.251044

MULHOLLAND, Caitlin. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, v. 19, p. 159-180, 2018.

PARLAMENTO EUROPEU. Jornal Oficial da União Europeia. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**, 27 de abril de 2016.

POÇAS, Luís. Problemas e dilemas do setor segurador: o RGPD e o tratamento de dados de saúde. **Revista online banca, bolsa e seguros**, Coimbra, n. 3, 2018, p. 217-302.

RODOTÀ, Stéfano. **A Vida na Sociedade da Vigilância**: A privacidade hoje. Rio de Janeiro: Renovar, 2008.

SALMEN, Caroline Salah. BELLE, Cathiani M. A proteção de dados sensíveis e as inovações da área da saúde. *In:* WACHOWICZ, Marcos (org). **Proteção de dados pessoais em perspectiva**: LGPD e RGPD na ótica do direito comparado. Curitiba: Gedai, UFPR 2020. p. 242-270.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, n. 5, p. 123-220, dez. 1890.

Este obra está licenciada com uma Licença Creative Commons Atribuição 4.0 Internacional (CC BY 4.0).

https://doi.org/10.51359/2448-2307.2022.251044