PONTIFÍCIA UNIVERSIDADE CATÓLICA DO PARANÁ
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
MESTRADO

MARIA CLAUDIA STANSKY

A PROTEÇÃO DE DADOS SOB O DOMÍNIO DO ESTADO E A RESPONSABILIDADE CIVIL DO PODER PÚBLICO

CURITIBA
2021

MARIA CLAUDIA STANSKY

A PROTEÇÃO DE DADOS SOB O DOMÍNIO DO ESTADO E A RESPONSABILIDADE CIVIL DO PODER PÚBLICO

Dissertação apresentada ao Programa de Pós-Graduação em Direito Área de concentração: Direito Socioambiental e Sustentabilidade, da Pontifícia Universidade Católica do Paraná, como requisito parcial à obtenção do título de mestre em Direito.

Orientador: Prof. Dr. Antônio Carlos Efing

CURITIBA

2021

Dados da Catalogação na Publicação
Pontifícia Universidade Católica do Paraná
Sistema Integrado de Bibliotecas – SIBI/PUCPR
Biblioteca Central
Edilene de Oliveira dos Santos CRB-9/1636

Stansky, Maria Claudia
S791p A proteção de dados sob o domínio do estado e a responsabilidade
2021 civil do poder público / Maria Claudia Stansky; orientador, Antônio Carlos Efing. -- 2021
129 f. : il. ; 30 cm

Dissertação (mestrado) – Pontifícia Universidade Católica do Paraná, Curitiba, 2021.
Bibliografia: f. 122-129

1. Defesa do consumidor. 2. Direito a privacidade. 3. Inovações tecnológicas. 4. Proteção de dados. 5. Responsabilidade do Estado. 6. Responsabilidade (Direito). I. Efing, Antônio Carlos. II. Pontifícia Universidade Católica do Paraná. Programa de Pós-Graduação em Direito. III. Título

Doris. 4. ed. – 342.5

MARIA CLAUDIA STANSKY

A PROTEÇÃO DE DADOS SOB O DOMÍNIO DO ESTADO E A RESPONSABILIDADE CIVIL DO PODER PÚBLICO

Dissertação apresentada ao Programa de Pós-Graduação em Direito Área de concentração: Direito Socioambiental e Sustentabilidade, da Pontifícia Universidade Católica do Paraná, como requisito parcial à obtenção do título de mestre em Direito.

COMISSÃO EXAMINADORA

_____

Prof. Dr. Antônio Carlos Efing

Pontifícia Universidade Católica do Paraná

_____

Prof. Dr. Sandro Mansur Gibran

Centro Universitário Curitiba

_____

Prof. Dr. Luiz Alberto Blanchet

Pontifícia Universidade Católica do Paraná

Curitiba, 25 de março de 2021.

À Isabella, minha amada filha.

AGRADECIMENTOS

Primeiramente, agradeço a Deus pela vida e por permitir concretizar meus sonhos. À Nossa Senhora Aparecida, minha protetora, que ilumina meu caminho.

Agradeço à toda minha amada família. Em especial, minha querida mãe, por ser minha fortaleza, por toda dedicação, cuidado e amor.

Agradeço meu marido, Thiago, pela família que construímos, por sempre estar ao meu lado, por compreender a minha ausência e aceitar as minhas escolhas.

Agradeço minha avó Iná, por ser a razão e o centro de tudo, pelas orações, lições de vida e apoio incondicional. Também, à minha tia Cleuza e meu tio José Luiz, pela torcida, imenso carinho e pelo suporte em todos os momentos.

Agradeço à Giovana Andretta, pela amizade sincera e pela parceria especial nos diversos os setores da vida.

Agradeço ao escritório Arruda Alvim, Aragão, Lins & Sato, pelo aprendizado nos últimos 14 anos, especialmente, ao meu chefe, Doutor Evaristo Aragão Santos, pelo exemplo de excelência na advocacia e pelo incentivo ao estudo ininterrupto.

Agradeço, também, à duas pessoas incríveis que tive o prazer de conhecer no curso do mestrado, que se tornaram amigos queridos e que levarei para vida toda: Hermelindo Chico e Lucas Troyan. Ambos foram meus parceiros durante as madrugadas de fichamentos e de dissertação, que tanto aliviaram os momentos de angústia, sempre com suas palavras positivas e de encorajamento. Obrigada, vocês dois foram fundamentais em todas as etapas.

Não posso deixar de agradecer meus colegas de sala de aula, com quem tive o prazer de conviver e dividir experiências: Ana Paula, Bruna, Daniel, Diego, Elisabete, Flávia e Guilherme. Agradeço, também, à Camila Purificação, competente e brilhante Professora Dra., que sempre me auxiliou nos assuntos acadêmicos com muito carinho.

Meu agradecimento especial ao meu orientador, Professor Doutor Antônio Carlos Efing, pela compreensão fora do comum em relação à esta pesquisa, pelas conversas produtivas e pelos ensinamentos em sala de aula, bem como pelo exemplo de como levar uma vida sustentável e ser uma pessoa melhor para o mundo.

Enfim, obrigada a todos que tornaram mais leve essa caminhada.

“*(...) o sucesso não é uma questão de nunca cair e nem mesmo de cair e se levantar repetidamente (...). O sucesso é mais do que a simples resiliência. É uma questão de usar essa queda para nos impelir na direção oposta. É uma questão de capitalizar os contratempos e as adversidades para nos tornarmos ainda mais felizes, ainda mais motivados e ainda mais bem-sucedidos. Não é simplesmente enfrentar as adversidades, mas encontrar as oportunidades que se escondem atrás delas”*.

(ACHOR, Shawn. O jeito Harvard de ser feliz, 2019. p. 134)

RESUMO

O estudo analisa a proteção de dados pessoais sob o domínio do Estado e como se dará a responsabilidade civil quando, em decorrência da violação aos direitos dos titulares de dados, ocasionar danos. A relevância da pesquisa reside na conscientização e ciência plena dos titulares de dados acerca de seus direitos, bem como dos deveres do Estado, buscando evitar o exacerbado controle e a invasão à esfera privada, opondo-se contra a vigilância extrema e ao uso indevido de dados pessoais. Utilizando o método dedutivo, a partir da análise de conteúdo da legislação vigente e material bibliográfico, a pesquisa tem como objetivo analisar a regulação jurídica para o tratamento de dados pelo Estado, demonstrando a necessidade de proteção de dados dos cidadãos e a utilização do instituto da responsabilidade civil para reparar danos decorrentes de violações às normas. Dentro do tema e hipóteses, o trabalho se divide em três capítulos. Em um primeiro momento, são traçadas a premissas básicas acerca da proteção de dados pessoais diante das inovações tecnológicas, analisando o direito fundamental à privacidade, a situação de panóptico digital da sociedade contemporânea, bem como a evolução legislativa e jurisprudencial referente à proteção de dados. Na sequência, efetivamente será analisado o tratamento de dados pessoais pelo Poder Público, o diálogo entre as fontes (em especial, o Código de Defesa do Consumidor), a existência de grandes bancos de dados em poder do Estado e os riscos do compartilhamento (quando ausente de finalidade específica e através de meros convênios). Ao final, em busca da efetividade da norma jurídica, passa-se ao estudo da responsabilidade civil, como forma de reparação da conduta violadora dos direitos dos titulares de dados pelo Estado. Para tanto, estuda-se a forma de responsabilidade do Estado, os elementos necessários para configuração dessa responsabilidade, suas excludentes e sugestões para dosimetria no momento da fixação da indenização. Conclui-se que o exercício dos direitos de proteção de dados em frente ao Estado, tendem a gerar a adoção de condutas condizentes com a Lei Geral de Proteção de Dados e as demais leis esparsas, de forma com que o Estado Democrático de Direito seja preservado, garantindo o respeito aos direitos humanos e garantias fundamentais, comportando-se de maneira sustentável no meio digital, em observância à estrita finalidade para coleta e tratamento dos dados, sob pena de reparar pelos danos causados.

Palavras-chave: Privacidade e novas tecnologias. Proteção de dados pessoais.

Estado e defesa do cidadão. Responsabilidade civil.

ABSTRACT

The study analyzes the protection of personal data under the control of the State and how civil liability will occur when, as a result of the violation of the rights of data subjects, damage is caused. The relevance of the research lies in the awareness and full recognition of data subjects about their rights, as well as the duties of the State, seeking to avoid exacerbated control and invasion into the private sphere, with opposition extreme surveillance, and the misuse of personal data. Using the deductive method, from the content analysis of the current legislation and bibliographic material, the research aims to analyze the legal regulation for data processing by the State, demonstrating the need for data protection for citizens and the use of the institute of civil liability to repair damages arising from violations of standards. Within the theme and hypotheses, the work is divided into three chapters. At first, basic premises are outlined about the protection of personal data in the face of technological innovations, analyzing the fundamental right to privacy, the digital panopticon situation of contemporary society, as well as the legislative and jurisprudential evolution regarding data protection. Sequentially, the treatment of personal data by the Public Power, the dialogue between the sources (in particular, the Consumer Protection Code), the existence of large databases held by the State and the risks of sharing (when absent of specific purpose and through mere agreements) will be analyzed. In the end, in search of the effectiveness of the legal norm, the study of civil liability begins, as a way of repairing the conduct that violates the rights of data subjects by the State. For that matter, the State's form of responsibility is studied, as well as the necessary elements for configuring this responsibility, its exclusions and suggestions for dosimetry when fixing the indemnity. It is concluded that the exercise of data protection rights in front of the State, tend to generate the adoption of conduct consistent with the General Data Protection Law and the other applicable sparse laws, so that the Democratic Rule of Law is preserved, guaranteeing respect for human rights and fundamental guarantees, behaving in a sustainable manner in the digital environment, in compliance with the strict purpose for collecting and processing data, under penalty of repairing the damages caused.

Key-words: Privacy and new technologies. Protection of personal data. State and citizen defense. Civil responsability.

LISTA DE ABREVIATURAS E SIGLAS

ADI	Ação Direta de Inconstitucionalidade
ANPD	Autoridade Nacional de Proteção de Dados
CC	Código Civil
CDC	Código de Defesa do Consumidor
CNJ	Conselho Nacional de Justiça
CPC	Código de Processo Civil
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados
RESP	Recurso Especial
STJ	Superior Tribunal de Justiça
STF	Supremo Tribunal Federal

LISTA DE FIGURAS

SUMÁRIO

1. INTRODUÇÃO

Na atualidade, dentro da sociedade capitalista global em que vivemos, a constante utilização de tecnologias da informação e comunicação produz uma quantidade incontável de dados, os quais se tornam relevantes economicamente a partir da vasta utilidade, seja dentro do mercado de consumo, seja como forma de controle. A circulação de informações é constante e dentre elas está a maior e mais valiosa moeda, que são os dados.

A internet e o mundo dos algoritmos invadiram e dominaram a vida das pessoas em todas as esferas, sendo de maior impacto perceptível na esfera profissional e social. É inegável que, em menos de uma década, essa conectividade constante e imediata assumiu um caráter de essencialidade. Contudo, muitos não notam que o Estado, também, tem se tornado cada vez mais digital, utilizando dados em todas as áreas de atuação, desde a segurança pública, até mesmo em um simples atendimento em um posto de saúde.

O Poder Público tem implementado mecanismos digitais, em muitos casos através de aplicativos, os quais os quais permitem a coleta de diversos dados dos usuários, com base na concordância aos termos de uso. Em regra, não há uma leitura atenta por parte do usuário ou, ainda, a compreensão é impossibilitada por aspectos técnicos e inelegíveis ao usuário comum. Nesse cenário, o Estado se tornou um dos maiores detentores de dados pessoais, especialmente, de dados sensíveis.

A célere criação de grandes bancos de dados estatais, acumulando um enorme e detalhado perfil dos cidadãos, não está atrelada com a necessária transparência. Com isso, a informação extraída com maior facilidade pelo uso da tecnologia, pode resultar em uma forma de controle desenfreado do Estado perante os cidadãos, a depender da maneira com que os dados serão manipulados.

A proteção desses dados paulatinamente tem tomado maior relevância, especialmente diante da falta de informação da grande maioria dos titulares de dados acerca de seus direitos. Não há dúvidas de que é necessária uma mudança de pensamento e postura para uma conscientização do titular de dados acerca de seus direitos, das gravidades do uso indevido e da justa reparação no caso de dano.

Dentro desse contexto, usando o método dedutivo e o procedimento monográfico de revisão bibliográfica, o presente estudo tem como objetivo analisar a regulação jurídica para o tratamento de dados pelo Estado, elencando a necessidade de proteção de dados dos cidadãos e a responsabilidade civil por violações.

Está vinculada a linha de pesquisa Estado, Sociedades, Povos e Meio Ambiente, pois procura definir e detalhar a atuação do Estado enquanto controlador de dados e apontar como a sociedade pode proteger seus dados obtidos, até mesmo, sem consentimento por força de exceções legais e da própria outorga que é dada ao Poder Público para consecução de políticas públicas. Trata de problema atual vivido pela sociedade dentro de um processo de evolução social e tecnológico.

A técnica de pesquisa adotada consiste na pesquisa a documentação indireta, pesquisa documental de fontes primárias e pesquisa bibliográfica de fontes secundárias (publicações, livros, etc). Foi realizada vasta pesquisa na legislação nacional, bem como no entendimento jurisprudencial existente contemporaneamente à pesquisa.

Com base nisso, a pesquisa tem por objetivos específicos analisar e compreender os deveres e obrigações do Estado na função de controlador de dados, bem como apontar qual é a forma de responsabilidade prevista na legislação para a violação dos deveres e obrigações por parte do Estado. Ainda, visa examinar a questão da observância à lei e aos princípios da Lei Geral de Proteção de Dados como requisito essencial para proteção de dados pessoais. Ainda, ingressando na parte da sociedade de risco global em que vivemos, analisará desde o panóptico digital, até os aspectos negativos da transparência total e do estado de vigilância.

Da mesma forma, a pesquisa busca demonstrar a necessidade de um diálogo entre as fontes, conjugando diversas leis sobre o tema, com enfoque principal no Código de Defesa do Consumidor.

Para o alcance dos objetivos traçados, o trabalho se divide em 3 capítulos.

O primeiro capítulo tratará das premissas necessárias para compreender a importância da proteção aos dados pessoais sob o domínio do Estado, analisando os pilares em que se sustenta. Para isso, como ainda não há emenda constitucional promulgada que elenque o direito à proteção de dados como um direito fundamental, a questão será abordada a partir da base que reside na proteção ao direito fundamental à privacidade, consagrado pela Constituição Federal.

Nesse tópico, demonstrará que, diante do intenso desenvolvimento tecnológico vivenciado nas últimas décadas, pode-se dizer que a perspectiva tradicional de proteção à privacidade se tornou ineficiente para as demandas da sociedade contemporânea. Por essa razão, perante as novas tecnologias, surgiram novos tipos

de violações à privacidade, de modo que se tornou necessária a existência de proteção específica e apropriada.

Ainda, no primeiro capítulo, será tratado o contexto tecnológico e informacional da sociedade contemporânea, o qual é analisado a partir da perspectiva de panóptico, criada no Sec. XVIII. Em síntese, aponta-se um cenário de vigilância extrema em que o vigiado não percebe a vigilância e seus perigos, exatamente, como a sociedade digital e informacional se comporta. O perigo maior dessa falta de percepção é o controle absoluto do Estado, intervindo em esferas da vida privada dos cidadãos e utilizando indevidamente os dados pessoais.

Na sequência, será demonstrada a evolução legislativa acerca da proteção de dados no Brasil, tendo como marco temporal a Constituição Federal de 1988. A pesquisa tratará de leis esparsas até chegar na Lei Geral de Proteção de Dados, a mais específica e atual sobre o tema.

As evoluções tocantes à proteção de dados do titular não se deram apenas na área legislativa. Na jurisprudência, o Supremo Tribunal Federal, aos poucos, também, foi alterando seu entendimento de forma a tutelar os dados como um direito dotado de relevância e autonomia.

O segundo capítulo serve como meio para se alcançar as hipóteses de responsabilidade civil do Estado envolvendo a violação de direitos inerentes à proteção de dados. Nele, será tratada a regulamentação acerca da forma de coleta, tratamento e armazenamento da dados pelo Poder Público. Em síntese, o capítulo visa definir de forma clara e direta a quais regras o Estado se submete ao agir como agente de tratamento de dados.

Além das disposições legais, serão tratadas as principais questões principiológicas dentro do tema. Ainda, será apontada como a teoria do diálogo das fontes pode ajudar na aplicação da nova Lei Geral de Proteção de Dados em consonância com as legislações já existentes no ordenamento jurídico, em especial, o Código de Defesa do Consumidor e a Lei de Acesso à Informação.

Ainda, serão abordados os riscos inerentes aos grandes bancos de dados em poder do Estado, bem como os recentes Decretos (nºs 10.046 e 10.047) que criaram cadastros de grande magnitude, nos quais, até mesmo, característimas biológicas dos cidadãos são armazadas. Tal coleta e armazenamento injusticado e sem finalidade apontam para dissonância dos Decretos com as normais da LGPD, o que também será objeto de análise. Também, será analisada a questão do compartilhamento de

dados em poder do Estado seja internamente entre seus órgãos, seja com a iniciativa privada, o que pode gerar graves riscos aos titulares de dados.

E, por fim, o terceiro e último capítulo, busca dar efetividade para todo o sistema de proteção de dados inserido na legislação, na medida em que estuda como se dará a resposta do ordenamento jurídico, em especial do Poder Judiciário, em punir e reparar as condutas que violarem os direitos dos titulares de dados.

A LGPD não aprofunda em seu texto a questão da responsabilidade civil e penal do Poder Público ao causar um dano ao titular de dados, apesar do título do da Seção I, do Capítulo IV, nada menciona acerca da responsabilidade propriamente dita. E, como não há pena de multa na esfera administrativa a ser imputada ao Poder Público, é muito provável, que a via judicial seja a grande sancionadora quando da ocorrência de danos.

Ainda, será abordada a forma de responsabilidade civil[1] a ser aplicada ao Estado, os elementos necessários para sua configuração diante de falhas no tratamento de dados, defendendo a modalidade objetiva, as hipóteses de excludentes da ilicitude.

Já se encaminhando para a parte final, será estudada a possibilidade de utilização da dosimetria prevista na LGPD no momento da quantificação do dano a ser reparado.

Dessa forma, o resultado esperado é que o presente estudo sirva para corroborar a importância da proteção de dados sob domínio do Estado, buscando evitar o exacerbado controle e a invasão à esfera privada dos cidadãos, protegendo-os de manipulações estatais e da vigilância extrema.

Espera-se a adoção de condutas em consonância as diretrizes estabelecidas pela LGPD e as demais leis esparsas, para que o Estado atue de forma legal e sustentável no meio digital. Porém, caso preenchidos os elementos necessários para responsabilização estatal, o dano deve ser reparado.

[1] Optou-se em utilizar o termo “responsabilidade civil”, porém, desde logo, destaca que há na doutrina de direito administrativo outros termos como “responsabilidade patrimonial extracontratual do Estado por comportamentos administrativos”, como defende Celso Antônio Bandeira de Mello.

2. PREMISSAS ACERCA DA PROTEÇÃO DE DADOS PESSOAIS

Para compreender a importância da proteção aos dados pessoais sob o domínio do Estado e a sua responsabilidade civil, imprescindível analisar seus pilares, em especial, a proteção ao direito fundamental à privacidade, consagrado pela Constituição Federal.

Igualmente, para se ter dimensão dos riscos existentes no tratamento de dados pessoais pelo Estado, especialmente, no uso como forma de controle, há que se analisar o contexto tecnológico, a situação do panóptico digital e a sociedade informacional.

O histórico legislativo acerca da proteção de dados no Brasil, também, é relevante para a presente pesquisa, já que demonstra a evolução do ordenamento jurídico na tutela do titular de dados.

Ocorre que, as evoluções tocantes à proteção de dados no Brasil, não se deram apenas na legislação. Na jurisprudência, é possível constatar que o Supremo Tribunal Federal, com o passar do tempo, também, aprimorou seu entendimento sobre a proteção de dados, ao reconhecê-la como um direito dotado de relevância e autonomia.

2.1. DIREITO FUNDAMENTAL À PRIVACIDADE E A PROTEÇÃO DE DADOS PESSOAIS

O direito fundamental à privacidade está previsto no artigo 5º, inciso X, da Constituição Federal, que dispõe expressamente que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.”

O direito à privacidade é conexo ao direito à vida e abarca todas as manifestações da esfera íntima, sendo considerado como o conjunto de informações que a pessoa natural pode decidir e manter ao seu controle, escolhendo como e para quem quer repassá-las.[2]

Tal direito “garante a proteção aos âmbitos mais imateriais, aos interesses espirituais da pessoa, configurando-se como um direito autônomo que adquire

[2] SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 37ª ed. São Paulo: Malheiros, 2014. p. 208.

substantividade própria.” De modo que configura o “direito de desfrutar a vida rechaçando expressamente qualquer conexão ou associação com os direitos de liberdade ou propriedade.”[3]

O artigo 21 do Código Civil, também confere tal proteção ao dispor que “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.”

Trata-se de um direito fundamental, inclusive figurando como limite à liberdade de expressão dos meios de comunicação, conforme se vislumbra no art. 220, §1º do texto constitucional.[4] Ou seja, a própria Constituição Federal admite a proteção especial de direitos mais sensíveis, como a privacidade, quando confrontados com outros direitos constitucionais, tal como a liberdade jornalística.[5]

Assim, sendo um direito fundamental, sua dimensão objetiva é caraterizada pelo direito de proteção do indivíduo em face de interferências indevidas do Estado ou terceiros, além do direito de liberdade pessoal em relação à sua vida privada com base em suas convicções, portanto, autodeterminação. Enquanto, a dimensão subjetiva consiste na eficácia irradiante dos direitos fundamentais, pela qual vincula a interpretação legislativa, bem como gera a proteção da privacidade nas relações privadas.[6]

Nesse sentido, Tércio Sampaio Ferraz Júnior conceitua privacidade como:[7]

> direito subjetivo fundamental, cujo titular é toda pessoa, física ou jurídica, brasileira ou estrangeira, residente ou em trânsito no país; cujo conteúdo é a faculdade de constranger os outros ao respeito e de resistir à violação do que lhe é próprio, isto é, das situações vitais que, por só a ele lhe dizerem respeito, deseja manter para si, ao abrigo de sua única e discricionária decisão; e cujo objeto é a integridade moral do titular.

Mendes e Branco conceituam-na da seguinte forma:[8]

---

[3] BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS; Cinthia Obladen de Almendra. **Proteção de dados e privacidade**: do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumen Juris, 2018. P. 65-66.

[4] SARMENTO, Daniel. Comentário ao Artigo 220. In: CANOTILHO, José Joaquim Gomes; MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; STRECK, Lenio Luiz. (Coords.). **Comentários à Constituição do Brasil**. São Paulo: Saraiva/Almedina, 2013. P. 2038.

[5] SILVA, Virgílio Afonso da. **Direitos fundamentais**: conteúdo essencial, restrições e eficácia. São Paulo: Malheiros, 2010. p. 118.

[6] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel Francisco. **Curso de direito constitucional**. 4. ed., ampl. São Paulo: Saraiva, 2015. P. 442.

[7] FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito, Universidade de São Paulo**, [S. l.], v. 88, p. 439-459, 1993. Disponível em: <https://www.revistas.usp.br/rfdusp/article/view/67231>. Acesso em: 15 dez. 2020.

[8] MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 10. ed., rev. e atual. São Paulo: Saraiva, 2015. P. 283.

> O direito à privacidade, em sentido mais estrito, conduz à pretensão do indivíduo de não ser foco da observação por terceiros, de não ter os seus assuntos, informações pessoais e características particulares expostas a terceiros ou ao público em geral.

Já Sarlet, Marinoni e Mitidiero destacam a necessidade do controle por parte dos indivíduos acerca das informações que lhe referem, além do direito de estar e permanecer só, de modo que conceituam o direito à vida privada como:[9]

> o **direito à privacidade** consiste num direito a ser **deixado em paz**, ou seja, na proteção de uma esfera autônoma da vida privada, na qual o indivíduo pode **desenvolver a sua individualidade**, inclusive e especialmente no sentido da **garantia de um espaço para seu recolhimento e reflexão**, sem que ele seja **compelido a determinados comportamentos socialmente esperados**. (sem grifos no original)

Apesar de haver posicionamentos doutrinários acerca da distinção entre privacidade e intimidade, no qual o primeiro se refere a preservação de informações pessoais em um aspecto mais geral incluindo relações profissionais, enquanto a segunda abarca condições mais íntimas e familiares, considerar-se-á uma unicidade entre os conceitos diante de sua estrita conexão que resulta no direito à vida privada.[10]

Nas palavras de Correia e Jesus, vida privada pode ser compreendida como aquela que: [11]

> Abrange aspectos particulares referentes a determinada pessoa, compreendendo o conjunto de situações e comportamentos individuais que não têm relação com a vida pública, que estão desta separados, e que estão estritamente ligados à vida individual e familiar da pessoa.

Em sentido contrário, Sampaio ressalta que no Brasil “usam-se intimidade e vida privada indistintamente”, contudo, defende que a partir da análise constitucional e internacional, há distinção entre as expressões e não podem ser empregadas como sinônimos, já que o direito à vida privada demanda de uma ampla compreensão sustentada na autonomia privada e liberdade para desenvolvimento da própria personalidade.[12]

---

[9] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel Francisco. **Curso de direito constitucional**. 4. ed., ampl. São Paulo: Saraiva, 2015. P. 441.

[10] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel Francisco. **Curso de direito constitucional**. 4. ed., ampl. São Paulo: Saraiva, 2015. P. 440.

[11] CORREIA, Pedro Miguel Alves Ribeiro; JESUS, Inês Oliveira Andrade de. O lugar do conceito de privacidade numa sociedade cada vez mais orwelliana. **Direito, Estado e Sociedade**, n. 43, p. 135-161, jul./dez., 2013. P. 149.

[12] SAMPAIO, José Adércio Leite. Comentário ao Artigo 5º, inciso X. In: CANOTILHO, José Joaquim Gomes; MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; STRECK, Lenio Luiz. (Coords.). **Comentários à Constituição do Brasil**. São Paulo: Saraiva/Almedina, 2013. P. 277.

Essas duas esferas ficam mais evidentes no conceito de Barroso, pelo qual a intimidade se refere às questões internas próprias do indivíduo, enquanto privacidade se vislumbra questões relacionadas ao círculo social mais próximo, em suas palavras:[13]

> A vida humana tem início e se desenvolve em sua primeira fase dentro de um espaço estritamente privado. Mesmo após tomar consciência de si mesmo, do outro e do mundo à sua volta, **todo indivíduo conserva**, pela vida afora, sua **intimidade personalíssima**: seus valores, sentimentos, desejos e frustrações. Este é um espaço inacessível da vida das pessoas e, normalmente, será indiferente ao Direito. Nele reina a psicologia, a psicanálise, a filosofia, a religião. Saindo de dentro de si, o homem conserva, ainda, um domínio reservado, o da sua **privacidade ou vida privada**: ali se estabelecem as relações de família (e outras, de afeto e de amizade), protegidas do mundo exterior pelo lar, pela casa, pelo domicílio. (sem grifos no original)

Ainda, Barroso ressalta que a ciência jurídica “interfere nessas relações, mas com o intuito de fortalecê-las e preservá-las. A intimidade e a vida privada formam o núcleo do espaço privado.”[14]

Destaca-se que a privacidade se caracteriza como uma necessidade do ser humano para preservar sua saúde mental, de modo que sua supressão ou violação acarreta a ausência de condições elementares para o desenvolvimento da livre personalidade e tentativas de auto superação.[15]

Nesse ponto, ressaltam Sarlet, Marinoni e Mitidiero que: “é líquido que a preservação de uma esfera da vida privada é essencial à própria saúde mental do ser humano e lhe assegura as condições para o livre desenvolvimento de sua personalidade.”[16]

Portanto, de forma sistematizada, Sampaio classifica o direito à vida privada em (a) direito de ser deixado em paz, ou seja, protege a revelação e disseminação de assuntos privados; (b) inviolabilidade do domicílio e objetos pessoais pelo Estado; e, (c) tomada de decisões de caráter pessoal e íntimo em face de intromissões

---

[13] BARROSO, Luís Roberto. **Curso de Direito Constitucional Contemporâneo:** os conceitos fundamentais e a construção do novo modelo. [Recurso Eletrônico], 7. ed., São Paulo: Saraiva Educação, 2018, não paginado.

[14] BARROSO, Luís Roberto. **Curso de Direito Constitucional Contemporâneo:** os conceitos fundamentais e a construção do novo modelo. [Recurso Eletrônico], 7. ed., São Paulo: Saraiva Educação, 2018, não paginado.

[15] MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 10. ed., rev. e atual. São Paulo: Saraiva, 2015. P. 280.

[16] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel Francisco. **Curso de direito constitucional**. 4. ed., ampl. São Paulo: Saraiva, 2015. P. 439.

indesejadas, especialmente em relação a esfera reservada dos indivíduos que compõe sua personalidade e intimidade.[17]

O direito à privacidade e/ou vida privada encontra proteção em todos os textos constitucionais brasileiros, porém, em proporções e contextos históricos distintos. Por exemplo, desde 1824, consta à inviolabilidade do domicílio e correspondências, a qual foi reproduzida nas demais constituições apesar de haver momentos com recorrentes violações em virtude de maior autoritarismo estatal, até lograr uma proteção mais ampla acerca da intimidade e vida privada em 1988, especialmente pelo momento político social de redemocratização do país.[18]

Nas palavras de Maurmo:[19]

> Em meio a tantas transformações, contudo, em maior ou menor escala, as constituições brasileiras sempre consagraram os direitos e as garantias individuais. A privacidade restou positivada, desde os primórdios, por meio da tutela à inviolabilidade do domicílio e das correspondências. Em 1988 a Constituição chamada de "cidadã" emerge após duas décadas de regime militar, e inaugura uma nova etapa na positivação dos direitos fundamentais, seguindo a tendência mundial.

O direito à privacidade identificado nos textos constitucionais brasileiros é reflexo do contexto internacional em que o cerne dos ordenamentos jurídicos era o patrimônio material, de modo que apenas havia proteção à privacidade quando relacionada com outros direitos. Contudo, a partir da consagração da dignidade da pessoa humana, a privacidade torna-se um direito autônomo, consolidando sua condição de direito humano e fundamental, acarretando a proteção autônoma à bens não materiais como intimidade, vida privada, honra e imagem.[20]

Com isso Maurmo, discorre que:[21]

> Na atual carta política, a **dignidade humana**, para além de **direito fundamental**, é erigida a **fundamento da República** (artigo 1º, III, da CF/1988), como núcleo básico e informador de todo ordenamento jurídico, que serve como critério e parâmetro de valoração na interpretação e compreensão que dá unidade ao sistema. No título que trata dos direitos e garantias fundamentais, o primeiro artigo é destinado aos direitos individuais e coletivos, e pela primeira vez a **privacidade surge positivada como**

---

[17] SAMPAIO, José Adércio Leite. Comentário ao Artigo 5º, inciso X. In: CANOTILHO, José Joaquim Gomes; MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; STRECK, Lenio Luiz. (Coords.). **Comentários à Constituição do Brasil**. São Paulo: Saraiva/Almedina, 2013. P. 276-277.
[18] MAURMO, Júlia Gomes Pereira. A tutela da privacidade nas constituições brasileiras. **Revista de Direito Constitucional e Internacional**, v. 101, p. 105-124, mai./jun., 2017. P. 113-114.
[19] MAURMO, Júlia Gomes Pereira. A tutela da privacidade nas constituições brasileiras. **Revista de Direito Constitucional e Internacional**, v. 101, p. 105-124, mai./jun., 2017. P. 108.
[20] MAURMO, Júlia Gomes Pereira. A tutela da privacidade nas constituições brasileiras. **Revista de Direito Constitucional e Internacional**, v. 101, p. 105-124, mai./jun., 2017. P. 105-106.
[21] MAURMO, Júlia Gomes Pereira. A tutela da privacidade nas constituições brasileiras. **Revista de Direito Constitucional e Internacional**, v. 101, p. 105-124, mai./jun., 2017. P. 113.

> **direito autônomo**, manifestada através de suas duas subespécies: a intimidade e a vida privada. (sem grifos no original)

Para se determinar o âmbito de proteção do direito à privacidade, se deve considerar a perspectiva material e não formal, já que ocasionaria numa proteção variável conforme a concepção do titular, enquanto se busca a proteção da vida pessoal conforme os usos e costumes da sociedade para se considerar o que não deve estar exposto ao Estado e terceiros, assegurando ao cidadão a vida digna.[22]

Acerca da relação entre privacidade e o Estado, defende Bruno Bioni que:[23]

> detém particular importância para o Estado democrático de direito, por garantir uma participação deliberativa e heterogênea entre os cidadãos em contraste às sociedades totalitárias. A privacidade não beneficia, portanto, somente o indivíduo, mas, colateralmente, a sociedade, revelando-se como um elemento constitutivo da própria vida em sociedade.

Com isso, verifica-se que a privacidade no contexto atual transcende a esfera individual tradicionalmente protegida, revelando uma função coletiva capaz de potencializar a participação democrática de forma livre, inclusive, inibindo perseguições ideológicas e políticas.

Em relação ao tema que será tratado nessa pesquisa, é imprescindível ressaltar que a privacidade está em constante risco perante as evoluções tecnológicas.

Não é de hoje o impacto causado pelas ferramentas de tecnologia da informação e comunicação na proteção e garantia do direito à vida privada. Constata-se a ocorrência de influências tecnológicas neste direito desde o desenvolvimento da fotografia em meados de 1890, a partir do emblemático e pioneiro artigo de Warren e Brandeis intitulado “The Right to Privacy”,[24] cujo qual é rememorado, dentre tantos

---

[22] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel Francisco. **Curso de direito constitucional**. 4. ed., ampl. São Paulo: Saraiva, 2015. P. 442.
[23] BIONI, Bruno Ricardo. Proteção de dados Pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. P. 2016.
[24] WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, vol. IV, n. 5, 1890.

outros, especialmente nas obras de Mendes e Branco,[25] Sartori[26] e, também, Boff, Fortes e Freitas.[27]

A referida obra tem relevância no aspecto doutrinário em decorrência da ruptura paradigmática entre o direito à privacidade e o direito à propriedade, de modo que defenderam a proteção do direito à privacidade de forma autônoma diante das ameaças ocasionadas pela fotografia e cobertura massiva de veículos de imprensa sob as atividades particulares dos cidadãos, cuja quais estavam desprovidas de interesse público para divulgação, portanto, violando os direitos da personalidade.

Diante do intenso desenvolvimento tecnológico vivenciado nas últimas décadas a perspectiva tradicional de proteção à privacidade se demonstra ineficiente, já que as novas tecnologias geram novos ambientes com potencial violação ao direito fundamental, cujo qual merece proteção apropriada, especialmente ao considerarmos o âmbito das tecnologias da informação e comunicação.

Nas palavras do Ministro do STJ Ricardo Villas Bôas Cueva, “o rápido desenvolvimento da informática multiplicou as possibilidades de invasão da intimidade.”[28]

No mesmo sentido, cabe mencionar as palavras de Maurmo:[29]

> O acelerado desenvolvimento **tecnológico** refletiu de maneira direta na vida das pessoas. Nesse passo, os conceitos de domicílio como asilo inviolável e de sigilo das correspondências passaram a ser **insuficientes para resguardar o indivíduo das novas possibilidades de incursão em sua vida íntima e privada**. (sem grifos no original)

Igualmente, afirma José Afonso da Silva:[30]

> O intenso desenvolvimento de complexa rede de fichários eletrônicos, especialmente de dados pessoais, constitui poderosa ameaça à privacidade das pessoas. O amplo sistema de informações computadorizadas gera um processo de esquadrinhamento das pessoas, que ficam com a sua individualidade inteiramente devassada. O perigo é tão maior quanto mais a utilização da informática facilita a interconexão de fichários com a

---

[25] MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 10. ed., rev. e atual. São Paulo: Saraiva, 2015. P. 282.

[26] SARTORI, Ellen Carina Mattias. Privacidade e Dados Pessoais: a proteção contratual da personalidade do consumidor na internet. **Revista de Direito Civil Contemporâneo**, v. 9, out./dez., p. 49-104, 2016, p. 57-58.

[27] BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS; Cinthia Obladen de Almendra. **Proteção de dados e privacidade**: do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumen Juris, 2018. P. 64.

[28] CUEVA, Ricardo Villas Bôas. A insuficiente proteção de dados pessoais no Brasil. **Revista de Direito Civil Contemporâneo**, v. 13, Out./Dez., 2017, p. 59-67.

[29] MAURMO, Júlia Gomes Pereira. A tutela da privacidade nas constituições brasileiras. **Revista de Direito Constitucional e Internacional**, v. 101, p. 105-124, mai./jun., 2017. P. 108.

[30] SILVA, Virgílio Afonso da. **Direitos fundamentais: conteúdo essencial, restrições e eficácia.** São Paulo: Malheiros, 2010. p. 211/212.

> possibilidade de formar grandes bancos de dados que desvendem a vida dos indivíduos, sem a sua autorização e até sem seu conhecimento.

Portanto, inegável que o desenvolvimento tecnológico viabiliza a “exponencial datificação das suas vidas, sendo estigmatizados e submetidos a uma série de decisões automatizadas, e por vezes práticas discriminatórias que afetam o livre desenvolvimento de sua personalidade.”[31]

O desenvolvimento tecnológico atual marcado pela constante utilização das ferramentas de tecnologia da informação e comunicação viabiliza o armazenamento e processamento eficiente e célere de dados pessoais, de modo que para efetiva proteção do direito à privacidade para além do tradicional direito de permanecer só, faz-se necessário a proteção dos dados pessoais e garantia da autodeterminação informativa no âmbito digital. [32]

Isso resulta no fenômeno denominado por Greenfield como Paradigma *Everyware*, o qual é composto pela (i) computação ubíqua, caracterizada pela onipresença natural e automática das tecnologias no cotidiano; (ii) computação pervasiva, que se refere a ausência de percepção da sociedade em relação à presença e funcionamento da tecnologia; e, (iii) inteligência ambiental, personalização dos serviços conforme a coleta de dados dos usuários para tornar as tecnologias proativas.[33]

Todos esses elementos compõem a 4º Revolução Industrial, abordado pioneiramente por Klaus Schwab, diante da modificação não apenas dos métodos utilizados para realizar as atividades socioeconômicas, mas principalmente por afetar a essência dos seres humanos, caracterizando um impacto sistêmico ocasionado pela velocidade, amplitude e profundidade com que as tecnologias afetam a sociedade atual.[34]

Ainda, no contexto da sociedade tecnológica, Sarlet, Marinoni e Mitidiero elencam que “estamos vivenciando o ‘fim da privacidade’, seja por conta da constante

---

[31] BIONI, Bruno Ricardo. **Proteção de dados Pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. P. 217.

[32] SARTORI, Ellen Carina Mattias. Privacidade e Dados Pessoais: a proteção contratual da personalidade do consumidor na internet. **Revista de Direito Civil Contemporâneo**, v. 9, out./dez., p. 49-104, 2016, p. 75.

[33] GREENFIELD, Adam. **Everyware**: The dawning age of ubiquitoues computing. AIGA: New Riders, 2006.

[34] BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS; Cinthia Obladen de Almendra. **Proteção de dados e privacidade**: do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumen Juris, 2018. P. 65-66.

e intensa autoexposição nas mídias sociais, na comunicação eletrônica em geral" especialmente pela "utilização de aplicativos diversos por meio dos quais permitimos o acesso a um conjunto de dados (informações pessoais de toda natureza)" além da "ampliação dos mecanismos de vigilância e monitoramento da vida individual e coletiva."[35]

Posto isso, inegável a preocupação e necessidade de proteção dos dados pessoais para garantia da privacidade dos cidadãos no ambiente tecnológico, já que são coletados constantemente na utilização massiva das tecnologias e refletem uma análise completa da personalidade de cada cidadão.

Conforme ressalta Bruno Bioni, os dados consistem em um "novo tipo de identidade" razão pela qual "tais dossiês digitais devem externar informações corretas para que seja fidedignamente projetada a identidade do titular daquelas informações." De modo que se "justifica dogmaticamente a inserção dos dados pessoais na categoria dos direitos da personalidade."[36]

Portanto, verifica-se que no contexto atual os dados pessoais são parcelas maiores ou menores do direito à privacidade de cada cidadão, nas palavras de Sartori "dados pessoais são a exteriorização da personalidade do indivíduo."[37] Cujo quais estão sob iminente possibilidade de violação pela constante utilização de mecanismos tecnológicos que coletam, armazenam e processam dados de forma célere, e, por vezes, sem o devido conhecimento e consentimento de seu titular.

Por essa razão, é que se pode dizer que **"**o Direito é um dos elementos que, juntamente com o desenvolvimento tecnológico, poderá contribuir com o fortalecimento do direito fundamental à privacidade."[38]

Apesar do direito à privacidade não contemplar a possibilidade de renúncia pelo titular, já que consiste em um direito fundamental, poderá ser objeto de autolimitação a partir do consentimento do titular, desde que, não viole o núcleo essencial da

---

[35] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel Francisco. **Curso de direito constitucional**. [Recurso Eletrônico] 7. ed., São Paulo: Saraiva Educação, 2018. Não paginado.
[36] BIONI, Bruno Ricardo. **Proteção de dados Pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. P. 137-138.
[37] SARTORI, Ellen Carina Mattias. Privacidade e Dados Pessoais: a proteção contratual da personalidade do consumidor na internet. **Revista de Direito Civil Contemporâneo**, v. 9, out./dez., p. 49-104, 2016, p. 76.
[38] BOFF, Salete Oro; FORTES, Vinícius Borges. FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade:** do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumen Juris, 2018. p. 109.

dignidade humana, de modo que possibilite o controle sobre os dados e informações de sua titularidade ou referência.[39]

Dessa forma, não se pode olvidar que o "direito subjetivo à privacidade, além de ser um direito fundamental, é um direito especial de personalidade, geral, intransmissível, irrenunciável e imprescritível", deve ser tido como "em princípio, indisponível, o seu titular pode consentir numa certa limitação", de modo que "teremos, pois, uma limitação voluntária ao direito."[40]

Nesse sentido, imprescindível destacar as palavras de Sampaio ao tratar do conteúdo de proteção do direito à privacidade:[41]

> Está o controle de informações emitidas e recebidas, juridicamente relevantes, desdobrado em um conjunto de faculdades atribuídas ao seu titular de, em gênero, seletividade dos *inputs* e *outputs* de informação. [...] O direito a intimidade concede um poder ao indivíduo para controlar a circulação de informações a seu respeito. As informações que se encontram protegidas são aquelas de caráter "privado", "particular" ou "pessoal".

Portanto, nesse contexto de proteção de dados, o direito à privacidade concede ao indivíduo a possibilidade de inserir, alterar e excluir informações armazenadas por terceiros, considerando o exercício de seu direito fundamental. Da mesma forma, no que tange à titularidade dos dados, o direito à privacidade possibilita o indivíduo selecionar criteriosamente o conjunto de informações que compõe sua esfera reservada, bem como a quem disponibilizará o acesso.

A problemática atual se agrava diante da quantidade de dados que são coletados diariamente enquanto o usuário utiliza tecnologias da informação e comunicação, a ponto de desconhecer todas as informações que disponibilizou, ou seja, "o indivíduo não tem controle sobre o fluxo dos seus dados, não tem acesso aos dados, não escolhe os próprios filtros, as decisões que são tomadas a seu respeito podem estar equivocadas."[42]

---

[39] MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 10. ed., rev. e atual. São Paulo: Saraiva, 2015. P. 284-286.

[40] CORREIA, Pedro Miguel Alves Ribeiro; JESUS, Inês Oliveira Andrade de. O lugar do conceito de privacidade numa sociedade cada vez mais orwelliana. **Direito, Estado e Sociedade**, n. 43, p. 135-161, jul./dez., 2013. P. 149.

[41] SAMPAIO, José Adércio Leite. Comentário ao Artigo 5º, inciso X. In: CANOTILHO, José Joaquim Gomes; MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; STRECK, Lenio Luiz. (Coords.). **Comentários à Constituição do Brasil**. São Paulo: Saraiva/Almedina, 2013. P. 282.

[42] SARTORI, Ellen Carina Mattias. Privacidade e Dados Pessoais: a proteção contratual da personalidade do consumidor na internet. **Revista de Direito Civil Contemporâneo**, v. 9, out./dez., p. 49-104, 2016, p. 57.

Diante do aspecto social e coletivo ocasionado pelo direito à privacidade, essencial para aprimorar e preservar a democracia. Nesse ponto, Sartori discorre sobre os riscos vivenciados pela constante coleta e armazenamento dos dados pessoais para além da perspectiva individual:[43]

> **violações ao direito à privacidade podem ser apenas a ponta do iceberg**, porquanto os **perigos da coleta e processamento de dados vão muito além da vida privada individual**, pois nossas "cópias virtuais" ou data doublés circulam livremente pela internet e, embora sejam cada vez mais alimentados por nós mesmos e tenham cada vez mais efeitos concretos em nossas vidas, "(...) **temos paulatinamente menos controle sobre os dados que são coletados e sobre as maneiras que eles são manipulados**." (sem grifos no original)

Em decorrência disso, surge a necessidade de reconhecer o direito fundamental à proteção de dados pessoais, que incide a todo e qualquer dado pessoal, independentemente do local e do modo como é armazenado. Sua proteção tem relevância porque na atualidade há facilidade de acesso, transmissão e manipulação de tais dados, potencializando violações ao direito fundamental.[44]

Assim, de maneira cada vez mais evidente, a proteção aos dados pessoais está assumindo a condição de direito fundamental de forma independente à violação de outros direitos fundamentais.

Inclusive, há em trâmite no Senado a proposta de Emenda à Constituição nº 17/2019, que visa incluir no artigo 5º da Constituição a proteção de dados pessoais entre os direitos fundamentais do cidadão, bem como fixar a competência da União para legislar sobre a matéria, alterando, também, o artigo 22 do texto constitucional.

Em resumo, a proteção de dados pessoais como direito fundamental contempla as seguintes esferas de proteção:[45]

> (a) o direito ao acesso e ao conhecimento dos dados pessoais existentes em registros (bancos de dados) públicos ou privados; (b) o direito ao não conhecimento, tratamento e utilização e difusão de determinados dados pessoais pelo Estado ou por terceiros, aqui incluído um direito de sigilo quanto aos dados pessoais; (c) o direito ao conhecimento da identidade dos responsáveis pela coleta, armazenamento, tratamento e utilização dos dados; (d) o direito ao conhecimento da finalidade da coleta e da eventual utilização dos dados; (e) o direito à retificação e, a depender do caso, à exclusão de dados pessoais armazenados em bancos de dados.

---

[43] SARTORI, Ellen Carina Mattias. Privacidade e Dados Pessoais: a proteção contratual da personalidade do consumidor na internet. **Revista de Direito Civil Contemporâneo**, v. 9, out./dez., p. 49-104, 2016, p. 56.

[44] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel Francisco. **Curso de direito constitucional**. 4. ed., ampl. São Paulo: Saraiva, 2015. P. 464-465.

[45] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel Francisco. **Curso de direito constitucional**. 4. ed., ampl. São Paulo: Saraiva, 2015. P. 466.

Seja a proteção de dados um direito fundamental independente ou não, tem-se que além da conexão com o direito à privacidade, há ligação direta com o direito da dignidade da pessoa humana que se revela “como um direito bastante sensível, tanto mais sensível quanto mais a sua restrição afeta a intimidade e pode implicar violação da dignidade da pessoa humana.”[46]

Portanto, ao considerar a proteção de dados pessoais como direito fundamental propriamente dito ou, ao menos, como elemento indispensável para garantir o direito à privacidade, deve-se buscar sua máxima efetividade, especialmente, diante da vulnerabilidade dos usuários e consumidores que utilizam as novas tecnologias da comunicação e informação, visto que os danos são imensuráveis tanto na perspectiva individual acerca da personalidade, quanto na perspectiva coletiva acerca dos riscos à liberdade e democracia.

Conforme será abordado nos tópicos seguintes, o direito constitucional e fundamental à privacidade, foi reiterado no artigo 17 da LGPD, bem como seus princípios conexos. Assim, em se tratando de proteção dos dados, os direitos fundamentais deverão ser utilizados como escudo protetor dos cidadãos, especialmente, em face do Estado, que atua em permanente de vigilância.

2.2. PANÓPTICO DIGITAL, ESTADO DE VIGILÂNCIA E ESTADO INFORMACIONAL

O filósofo e jurista inglês Jeremy Benthan utilizou o termo “panóptico”, em 1786, para designar uma penitenciária com estrutura arquitetônica bastante peculiar, a qual permitiria que apenas um vigilante observasse todos os prisioneiros, sem que estes pudessem saber se estavam ou não observados. Além de entender pela segurança e economia do local (baixo custo de vigilantes), acreditava que o medo e o receio levariam os prisioneiros a adotarem uma boa conduta.[47]

Apesar do projeto não ter sido executado, serviu de base para algumas reflexões acerca da teoria do Poder (controle e vigilância), já que a sua essência

---

[46] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel Francisco. **Curso de direito constitucional**. 4. ed., ampl. São Paulo: Saraiva, 2015. P. 467.
[47] BENTHAM. Jeremias. **O Panóptico.** TADEU, Tomaz. (Org.). 2ª ed. Belo Horizonte: Autêntica Editora, 2008. p. 19-29.

consistia “na centralidade da situação do inspetor, combinada com os dispositivos mais bem conhecidos e eficazes para ver sem ser visto.”[48]

Séculos mais tarde, Michel Foucault, ao analisar a estrutura de um panóptico em sua obra “vigiar e punir”, apontou como principal efeito dela decorrente, o fato de que “induzir no detento um estado consciente e permanente de visibilidade que assegura o funcionamento automático do poder.”[49]

No entendimento do referido filósofo moderno:[50]

> Fazer com que a vigilância seja permanente em seus efeitos, mesmo se é descontínua em sua ação; que a perfeição do poder tenda a tornar inútil a atualidade de seu exercício; que esse aparelho arquitetural seja uma máquina de criar e sustentar uma relação de poder independente daquele que o exerce; enfim, que os detentos se encontrem presos numa situação de poder de que eles mesmos são os portadores. Para isso, é ao mesmo tempo excessivo e muito pouco que o prisioneiro seja observado sem cessar por um vigia: muito pouco, pois o essencial é que ele se saiba vigiado; excessivo, porque ele não tem necessidade de sê-lo efetivamente.

Assim, “o Panóptico funciona como uma espécie de laboratório de poder. Graças a seus mecanismos de observação, ganha em eficácia e em capacidade de penetração no comportamento dos homens.”[51]

Dessa forma, pode-se dizer que Foucault via na estrutura do panóptico um instrumento e vetor de poder,[52] uma figura de tecnologia política, aplicável a todo tipo de estabelecimento (escolas, hospitais, fábricas, etc) e em cada uma de suas aplicações “permite aperfeiçoar o exercício do poder.”[53]

Apesar do decurso do tempo, as análises dos filósofos demonstram similaridade ao contexto atual, sendo relevantes para compreensão da temática apresentada.

Isso porque o século XXI trouxe um novo tipo de panóptico, o digital, em que os indivíduos, ligados em redes, são vigiados na grande maioria das vezes sem ter consciência e, ainda, contribuem ativamente e de forma pessoal com seus dados na

---

[48] BENTHAM. Jeremias. **O Panóptico.** TADEU, Tomaz. (Org.). 2ª ed. Belo Horizonte: Autêntica Editora, 2008. p. 28.
[49] FOCAULT. Michel. **Vigiar e punir**: nascimento da prisão. Tradução de Lígia M. Pondé Vassalo. Rio de Janeiro: Vozes, 1999. p. 224.
[50] FOCAULT. Michel. **Vigiar e punir**: nascimento da prisão. Tradução de Lígia M. Pondé Vassalo. Rio de Janeiro: Vozes, 1999. p. 224.
[51] FOCAULT. Michel. **Vigiar e punir**: nascimento da prisão. Tradução de Lígia M. Pondé Vassalo. Rio de Janeiro: Vozes, 1999. p. 228.
[52] FOCAULT. Michel. **Vigiar e punir**: nascimento da prisão. Tradução de Lígia M. Pondé Vassalo. Rio de Janeiro: Vozes, 1999. p. 34.
[53] FOCAULT. Michel. **Vigiar e punir**: nascimento da prisão. Tradução de Lígia M. Pondé Vassalo. Rio de Janeiro: Vozes, 1999. p. 229.

edificação e manutenção da “transparência” e “vigilância”, expondo-se e desnudando a si mesmos, expondo-se ao mercado panóptico.[54]

Hoje, em decorrência do panóptico digital, verifica-se uma vigilância constante e imperceptível para os cidadãos, a partir da captação e processamento de dados na utilização de tecnologias da informação e comunicação.[55]

Com isso, caracteriza-se a denominada sociedade da informação, oriunda do desenvolvimento tecnológico, na qual se possibilita a utilização massiva de equipamentos eletrônicos, os quais geram inúmeros dados que, por sua vez, estão interligados pelas ferramentas de internet das coisas, possibilitando o exercício de uma vigilância mais invasiva e acessível.[56]

Essas benesses tecnológicas com interfaces atrativas e supostamente gratuitas são na realidade mecanismos de autocontrole e disciplina, dos quais a sociedade não consegue se desvencilhar diante de suas facilidades, mesmo que para isso precise renunciar completamente à sua privacidade e direitos inerentes aos seus dados pessoais.[57]

Pode-se dizer, portanto, que a vigilância agora está voltada à coleta e uso da informação, não mais em uma cela de penitenciária. A informação, extraída de maneira muito mais fácil através do uso da tecnologia pelos cidadãos, passa a ser utilizada como forma de controle.

No mundo digital as pessoas têm a falsa sensação de liberdade, mas na verdade são subordinadas ao panóptico, são ao mesmo tempo agressores e vítimas.[58] Nesse cenário digital, os próprios usuários se colocaram na condição de vigiados, deixando de proteger sua esfera privada e alimentando a sociedade da transparência.

Contudo, a sociedade atual não nota que seu exibicionismo e voyeurismo alimentam o controle. E, para Byung-Chul Han, “onde impera a transparência não há espaço para confiança. Ela a destrói.”[59]

---

[54] HAN, Byung-Chul. **A sociedade da transparência.** Lisboa: Relógio D' Água, 2014.
[55] HAN, Byung-Chul. **A sociedade da transparência.** Lisboa: Relógio D' Água, 2014. p. 108.
[56] BRITO, Carlos; HERRASTI, Santiago Narváez. Medir y acotar la vigilancia estatal para no perder derechos. IN: BIANCHI, Matías (comp.) **Recuperar la política**: Agendas de Innovación Política en América Latina. Assuntos del Sur – Democracia en Red. Buenos Aires, 2017. P. 301-302.
[57] FERREIRA, Rubens da Silva. A Sociedade da Informação como Sociedade de Disciplina, Vigilância e Controle. **Información, cultura y sociedad**. n. 31, pp. 109-119. Diciembre, 2014. P. 116-117.
[58] HAN, Byung-Chul. **A sociedade da transparência.** Lisboa: Relógio D' Água, 2014a. p. 116.
[59] HAN, Byung-Chul. **A sociedade da transparência.** Lisboa: Relógio D' Água, 2014a. p. 111.

E, esse “estado de vigilância”, sempre foi algo inerente ao Estado, *“*o Estado cria e consome informações. E, quanto maior e mais complexo, o Estado aumenta a necessidade de obter informação.”[60]

Com as novas tecnologias da informação e comunicação, surgem paulatinamente novas formas de vigilância, por vezes, de formas obscuras e dissimuladas.

Para Sandra Braman, o processo de informatização gera problemas adicionais no estudo do poder e *“*muitas expressões de poder são difíceis de perceber porque os efeitos demoram tanto antes de serem reconhecíveis, como com danos genéticos.” Conclui que “pode não haver meios evidentes para os sentidos humanos perceberem o exercício do poder, como com novas formas de vigilância.”[61]

E, obviamente, quanto menos perceptível essa condição de vigilância, maior o poder do controlador dos dados sobre as pessoas.

Dentro desse cenário, está a computação ubíqua, caracterizada pela integração das máquinas com os seres humanos a ponto de serem invisíveis e naturais para o desempenho das atividades ordinárias, bem como a computação pervasiva, em que os instrumentos tecnológicos estão difundidos de forma imperceptível e natural aos objetos e ambientes.[62]

Portanto, o “panóptico eletrônico” ou “digital” resta configurado na medida em que ferramentas de tecnologia de informação e comunicação poderão ser utilizadas pelo controlador de dados – no caso deste trabalho, representado pelo Estado – para obter informações e exercer controle sob os cidadãos, que através de atividades cotidianas permitem a formação de “base de dados, que se constituem em mecanismos para a identificação e controle de padrões, da forma mais discreta, automática e não intrusiva possível, pois os dados e os ‘valores ’pessoais são fornecidos de forma voluntária pelos usuários.”[63]

---

[60] BOFF, Salete Oro; FORTES, Vinícius Borges. FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade:** do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumen Juris, 2018. p. 17.

[61] BRAMAN, Sandra. **Change of state**: information, policy and power. Cambrige: The MIT Press, 2006. p. 24.

[62] BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS; Cinthia Obladen de Almendra. **Proteção de dados e privacidade**: do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumen Juris, 2018. P. 133-136.

[63] BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS; Cinthia Obladen de Almendra. **Proteção de dados e privacidade**: do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumen Juris, 2018. P. 21-28.

Essa vigilância tem por base mecanismos muito sofisticados de dataficação, "pelos quais os mercados e os Estados recolhem e acumulam terabytes de dados para depois organizá-los, analisá-los e aplicá-los a usos ainda não tão bem conhecidos pela população mundial."[64] Isso se torna extremamente relevante porque essa captura e processamento dos dados, além de muito velozes, podem ocorrer sem o consentimento livre e consciente dos cidadãos, que em sua grande maioria são leigos quanto aos riscos da manipulação e controle indevidos desses dados.[65]

Dessa forma, assim como em todos os setores, o uso das tecnologias da informação e da comunicação, obviamente, têm impacto também no Estado, que passa a ser informacional, utilizando e controlando essas informações para o exercício de seu poder. É o chamado "poder informacional", que é capaz de moldar os comportamentos humanos e, inclusive, de manipular as bases informacionais dos demais poderes[66] (instrumental, estrutural e simbólico), alterando a sua forma de exercício e a natureza de seus efeitos, na análise de Braman, tem-se:[67]

> Poder Instrumental: que molda comportamentos humanos manipulando o mundo material através da força física; Poder Estrutural: que molda comportamentos humanos manipulando o mundo social através de regras e instituições. Poder Simbólico: que molda comportamentos humanos manipulando os mundos materiais, sociais e simbólicos através de ideias, palavras e imagens. Poder Informativo: que molda comportamentos humanos manipulando as bases informacionais do poder instrumental, estrutural e simbólico.

Com isso, inovação tecnológica e política se unem criando grandes sistemas de informações sobre os cidadãos, os quais podem ser utilizados desde a implantação de políticas públicas, uma forma positiva de aplicação das informações (extraídas através dos dados), como, até mesmo, um instrumento de manipulação e poder.

E, é nesse ponto, que surgem novos desafios da sociedade contemporânea e futura. Primeiro, descobrir em que medida essa total transparência perante o Estado Informacional, como um controlador dos dados, não será utilizada de forma negativa, como ferramenta de controle absoluto e vigilância extrema do cidadão.

---

[64] FERREIRA, Rubens da Silva. A Sociedade da Informação como Sociedade de Disciplina, Vigilância e Controle. **Información, cultura y sociedad**. n. 31, pp. 109-119. Diciembre, 2014. P. 116.
[65] FERREIRA, Rubens da Silva. A Sociedade da Informação como Sociedade de Disciplina, Vigilância e Controle. **Información, cultura y sociedad**. n. 31, pp. 109-119. Diciembre, 2014. p. 116.
[66] BRAMAN, Sandra. **Change of state**: information, policy and power. Cambrige: The MIT Press, 2006. P. 26-27.
[67] BRAMAN, Sandra. **Change of state**: information, policy and power. Cambrige: The MIT Press, 2006. P. 25.

Nesse sentido, Brito e Herrasti afirmam que, via de regra, os mecanismos estatais de vigilância resultam na supressão de parcelas significativas da privacidade dos cidadãos, em razão da necessidade de proporcionar maior segurança, que leva à ignorar a intrínseca relação deste direito com a manutenção do regime democrático. Para eles, o exercício da cidadania e dos direitos políticos relacionados a manifestação de opiniões e mobilizações sociais, ficam restringidos em um ambiente de vigilância e controle.[68]

Outro grande desafio, reside na responsabilização do Estado por eventual conduta ilícita ao manipular essas informações, especialmente, quando gerar um dano para uma pessoa física ou para própria coletividade, sendo esta a principal controversa que se pretende responder no último capítulo da presente pesquisa.

É preciso evitar justamente o cenário de um panóptico, em que o guarda a todos vigia sem ser notado, enquanto não há qualquer forma de controle ou vigilância sob o guarda. Por analogia, no contexto digital, o Estado figura como o guarda, cujo qual não pode deter o poder absoluto, sob pena de instauração de um regime totalitário, capaz de ensejar violações à direitos humanos que demoraram séculos para ser conquistados.

Pode-se dizer, então, que “disciplina, vigilância e controle são as três facetas de uma realidade que marca um novo cenário de lutas em conformação na sociedade contemporânea.”[69]

Nesse novo cenário, “as forças em tensão agora se organizam por meio do volume de dados, de informações e de conhecimentos que Estado, mercado e sociedade civil são capazes de mobilizar em torno da defesa de seus interesses.”[70]

Aplicando a teoria do poder de Michel Foucault, tem-se que “as relações de poder sempre trazem consigo movimentos de resistência que transformam a história e produzem novas realidades, novos sujeitos.”[71]

---

[68] BRITO, Carlos; HERRASTI, Santiago Narváez. Medir y acotar la vigilancia estatal para no perder derechos. IN: BIANCHI, Matías (comp.) **Recuperar la política**: Agendas de Innovación Política en América Latina. Assuntos del Sur – Democracia en Red. Buenos Aires, 2017. P. 298-299.
[69] FERREIRA, Rubens da Silva. A Sociedade da Informação como Sociedade de Disciplina, Vigilância e Controle. **Información, cultura y sociedad**. n. 31, pp. 109-119. Diciembre, 2014. P. 118.
[70] FERREIRA, Rubens da Silva. A Sociedade da Informação como Sociedade de Disciplina, Vigilância e Controle. **Información, cultura y sociedad**. n. 31, pp. 109-119. Diciembre, 2014. P. 118.
[71] FERREIRA, Rubens da Silva. A Sociedade da Informação como Sociedade de Disciplina, Vigilância e Controle. **Información, cultura y sociedad**. n. 31, pp. 109-119. Diciembre, 2014. P. 118.

É notória a dificuldade de se encontrar um limite para o Poder Público utilizar as informações que poderão ser obtidas e tratadas mesmo sem o consentimento do titular de dados.[72]

Para Basu “existe um limite para o que pode ser corrigido pelo estado e, também, não está claro que queremos que o estado esteja tão envolvido em nossas vidas cotidianas.”[73]

Analisando o contexto atual, denota-se a presença dessa nova relação de poder através do uso dos dados, resta saber em que medida os sujeitos estão preparados para se mobilizarem e lutarem na defesa de seus interesses. Obviamente, para que isso ocorra, os sujeitos devem estar cientes da forma com que seus dados são manipulados e os riscos envolvidos, precisam sair do panóptico e compreender a situação de vigilância e controle a qual estão expostos, sem isso, não haverá resistência.

A Lei Geral de Proteção de Dados, além de seu caráter jurídico, surge como um alerta para sociedade em geral, da importância e dos riscos do uso de dados, capaz de conscientizar os sujeitos titulares de dados de que é muito mais do que um mero “*accept*”, que deve haver preocupação e cuidado.

Por fim, sobre esse mundo tecnológico, globalizado, informacional e de certo modo desconhecido em que vivemos, importante ressaltar as palavras de Morin e Kern:[74]

> Ao mesmo tempo que a consciência da finitude, podemos doravante ter uma consciência de nossa inconsciência e um conhecimento de nossa ignorância: podemos saber doravante que estamos na aventura desconhecida. Acreditamos, confiando numa pseudo-ciência, que conhecíamos o sentido da história humana. Mas, desde a aurora da humanidade, desde a aurora dos tempos históricos, estávamos já numa aventura desconhecida, e nela estamos mais que nunca.

Nessa aventura desconhecida em que vivemos, só resta pesquisar e adotar mecanismos de defesa, a fim de que ao menos os direitos fundamentais sejam preservados diante dessa avalanche tecnológica.

---

[72] Artigo 7º da LGPD: Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] § 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização. § 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.
[73] BASU. Kaushik. **The Republic of Beliefs**. Princeton University Press, 2018. P.180-181.
[74] MORIN, Edgar; KERN, Anne Brigitte. **Terra-pátria.** Porto Alegre: Sulina, 2003. p.164.

2.3. PROTEÇÃO DE DADOS NO BRASIL E SUA REGULAMENTAÇÃO

Conforme já analisado no primeiro capítulo, nas últimas décadas, a tecnologia evoluiu em grandes níveis e, de forma muitas vezes imperceptível, incorporou-se ao cotidiano das pessoas.

Qualquer empresa ou organização, em diferentes dimensões, trabalham com o uso de dados de seus clientes. Da mesma forma o Estado, que tem sua atuação justamente voltada para o desenvolvimento [75] .Até mesmo as relações sociais passaram a ser intermediadas pela tecnologia, transformando tudo em um grande conglomerado de “dados”, denominado como *Big Data*.

Essas inovações tecnológicas, obviamente, trouxeram impactos à sociedade, que se tornou informacional e de transparência, incumbindo ao Estado regular tais interferências e os conflitos de interesses ocasionados, adequando de forma gradual a legislação ao progresso tecnológico.

No Brasil, após a promulgação da Constituição Federal de 1988,[76] além do próprio conteúdo da Constituição, algumas leis esparsas começaram a tutelar de forma específica alguns aspectos das relações jurídicas que envolviam dados pessoais.[77]

Primeiro, importante destacar o *Habeas Data*, previsto no artigo 5º, inciso LXXII, da CF, que se trata de uma ação constitucional que serve “como um instrumento para requisição das informações pessoais em posse do poder público.” Apesar de sua criação em 1988 estar intimamente ligada aos atos de repressão decorrentes do regime militar e não propositalmente à proteção de dados pessoais – que já estavam em evolução em países da Europa e nos Estados Unidos –, após sua regulamentação pela Lei 9.507/1997, acabou por assegurar ao cidadão o direito de acessar e retificar seus dados pessoais em banco de dados de entidades governamentais ou de caráter público.[78]

---

[75] BLANCHET, Luiz Alberto. **Administração Pública, Ética e Desenvolvimento**. 3ª Edição. Curitiba: Juruá, 2020.p. 9.

[76] Será adotado como marco temporal a Constituição Federal de 1988, portanto, leis anteriores não serão analisadas.

[77] RODRIGUES, Lucas Troyan; STANSKY, Maria Claudia. A Proteção de Dados Pessoais sob Domínio do Estado no Brasil. In: VEIGA, Fabio da Silva.; LEVATE, Luiz Gustavo; GOMES, Marcelo Kokke. (Org.). **Novos Métodos Disruptivos no Direito**. 1ed.Porto: Instituto Iberoamericano de Estudos Jurídicos e Escola de Direito Dom Helder, 2020, v. 1, p. 823-833.

[78] BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia**, elaboração Danilo Doneda. – Brasília: SDE/DPDC, 2010. P. 50-51.

Em 1990, com a promulgação do Código de Defesa do Consumidor (Lei nº 8.078), por meio de seu artigo 43 dispunha sobre o direito de livre acesso do consumidor aos dados arquivados sobre ele.

Frise-se, desde já, que o referido artigo do CDC abrange toda variedade de informações passíveis de registro, seja em bancos de dados, seja em simples cadastros, sendo eles informatizados ou não, estando de forma organizada ou precária, ou seja, é aplicável a qualquer tipo de armazenamento de informações.[79]

Além da Lei nº 8.078/1990 (CDC) outorgar ao consumidor pleno acesso às informações sobre ele contidas nos bancos de dados (conforme previsto no artigo 43, *caput*), ainda impede a divulgação de informações negativas sobre o consumidor se decorrido o prazo de cinco anos, conforme redação do §1º do dispositivo mencionado. Não bastasse isso, no §3º, a legislação permite ao consumidor pleitear a correção de informações errôneas que lhe fazem referência, o que deverá ser feito no prazo de 5 dias. Já o § 5º, do mesmo art. 43, dispõe que ao prescrever a cobrança do débito, devem ser baixadas as informações junto aos cadastros e bancos de dados.[80]

Inegável que, desde o início, a legislação consumerista demonstrava preocupação com a proteção de dados pessoais dos consumidores que obteve maior proteção pela edição de outras normas, tais como: a Portaria nº 5/2002 da SDE/MJ, que trata da abusividade das cláusulas que autorizam o envio de dados dos consumidores sem consentimento prévio; o Decreto nº 6523/2008, que versa sobre o Sigilo dos dados pessoais do serviço de SAC e a Lei nº 13.460/2017, referente à participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública.

Dentro do ordenamento jurídico, outras leis, também, trataram dos direitos dos titulares de dados, por exemplo, Lei nº 9.296/1996 (Lei da interceptação telefônica), Lei nº 9.472/1997 (Lei geral de Telecomunicações), Lei nº 9.507/1997 (*Habeas Data*), Lei nº 9.983/2000 (crime de inserção de dados falsos) e Lei Complementar nº 105/2001 (sigilo das operações financeiras).

---

[79] EFING, Antônio Carlos, **Fundamentos do Direito das Relações de Consumo**, 4ª Edição - Revista, Ampliada e Atualizada, Juruá Editora, 2020, p. 299.
[80] EFING, Antônio Carlos, **Fundamentos do Direito das Relações de Consumo**, 4ª Edição - Revista, Ampliada e Atualizada, Juruá Editora, 2020. P. 302.

Após, em 2002, o Código Civil dispôs de forma detida as questões inerentes aos direitos da personalidade, de especial importância para tutela, ainda que genérica, do titular de dados.

Em 2011, criou-se a Lei do Acesso a Informação (12.527/2011), que trouxe de forma mais direta a tutela de direitos dentro do ambiente da Internet, regulamentando o acesso à informações já previstos nos seguintes artigos: 5º, XXXIII, 37, §3º, II e 216, §2º, da Constituição Federal. O artigo 24 da referida lei vincula de forma expressa a necessidade de observância de seus dispositivos pela União, Estados, Distrito Federal e Municípios, bem como órgãos públicos da administração direta e indireta[81]. O escopo da Lei está previsto no artigo 3º, o qual dispõe que:

> Art. 3º Os procedimentos previstos nesta Lei destinam-se a assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com os princípios básicos da administração pública e com as seguintes diretrizes:
> I - observância da publicidade como preceito geral e do sigilo como exceção;
> II - divulgação de informações de interesse público, independentemente de solicitações;
> III - utilização de meios de comunicação viabilizados pela tecnologia da informação;
> IV - fomento ao desenvolvimento da cultura de transparência na administração pública;
> V - desenvolvimento do controle social da administração pública.

Ainda, nota-se que o artigo 6º, inc. II, da Lei de Acesso a Informação, já trazia a previsão acerca da proteção da informação por parte dos órgãos e entidades do Poder Público. Do mesmo modo, o artigo 25, dispõe que "é dever do Estado controlar o acesso e a divulgação de informações sigilosas produzidas por seus órgãos e entidades, assegurando a sua proteção."

O tratamento dos dados, também, logrou destaque na referida legislação, conforme artigo 31.[82] A questão da responsabilidade foi abordada de forma detida nos

---

[81] BOFF, Salete Oro; FORTES, Vinícius Borges. FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade:** do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumen Juris, 2018. p.90-91.

[82] Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.
§ 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:
I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e
II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.

artigos 32, 33 e 34,[83] os quais serão analisados neste trabalho quando pontuadas as sanções passíveis ao Estado em razão do vazamento de dados.

---

§ 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido.
§ 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias:
I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;
II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;
III - ao cumprimento de ordem judicial;
IV - à defesa de direitos humanos; ou
V - à proteção do interesse público e geral preponderante.
§ 4º A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância.
§ 5º Regulamento disporá sobre os procedimentos para tratamento de informação pessoal.

[83] Art. 32. Constituem condutas ilícitas que ensejam responsabilidade do agente público ou militar:
I - recusar-se a fornecer informação requerida nos termos desta Lei, retardar deliberadamente o seu fornecimento ou fornecê-la intencionalmente de forma incorreta, incompleta ou imprecisa;
II - utilizar indevidamente, bem como subtrair, destruir, inutilizar, desfigurar, alterar ou ocultar, total ou parcialmente, informação que se encontre sob sua guarda ou a que tenha acesso ou conhecimento em razão do exercício das atribuições de cargo, emprego ou função pública;
III - agir com dolo ou má-fé na análise das solicitações de acesso à informação;
IV - divulgar ou permitir a divulgação ou acessar ou permitir acesso indevido à informação sigilosa ou informação pessoal;
V - impor sigilo à informação para obter proveito pessoal ou de terceiro, ou para fins de ocultação de ato ilegal cometido por si ou por outrem;
VI - ocultar da revisão de autoridade superior competente informação sigilosa para beneficiar a si ou a outrem, ou em prejuízo de terceiros; e
VII - destruir ou subtrair, por qualquer meio, documentos concernentes a possíveis violações de direitos humanos por parte de agentes do Estado.
§ 1º Atendido o princípio do contraditório, da ampla defesa e do devido processo legal, as condutas descritas no **caput** serão consideradas:
I - para fins dos regulamentos disciplinares das Forças Armadas, transgressões militares médias ou graves, segundo os critérios neles estabelecidos, desde que não tipificadas em lei como crime ou contravenção penal; ou
II - para fins do disposto na Lei nº 8.112, de 11 de dezembro de 1990, e suas alterações, infrações administrativas, que deverão ser apenadas, no mínimo, com suspensão, segundo os critérios nela estabelecidos.
§ 2º Pelas condutas descritas no **caput,** poderá o militar ou agente público responder, também, por improbidade administrativa, conforme o disposto nas Leis nºs 1.079, de 10 de abril de 1950, e 8.429, de 2 de junho de 1992.
Art. 33. A pessoa física ou entidade privada que detiver informações em virtude de vínculo de qualquer natureza com o poder público e deixar de observar o disposto nesta Lei estará sujeita às seguintes sanções:
I - advertência;
II - multa;
III - rescisão do vínculo com o poder público;
IV - suspensão temporária de participar em licitação e impedimento de contratar com a administração pública por prazo não superior a 2 (dois) anos; e
V - declaração de inidoneidade para licitar ou contratar com a administração pública, até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade.
§ 1º As sanções previstas nos incisos I, III e IV poderão ser aplicadas juntamente com a do inciso II, assegurado o direito de defesa do interessado, no respectivo processo, no prazo de 10 (dez) dias.

Dessa forma, a Lei de Acesso à Informação é, sem sombra de dúvidas, um importante instrumento de proteção ao direito fundamental à privacidade.

Prosseguindo, no mesmo ano (2011), criou-se a Lei nº 12.414/2011, que introduziu o chamado Cadastro Positivo, a qual trata dos históricos de adimplementos de créditos de pessoas físicas e jurídicas. A referida Lei foi, recentemente (abril de 2019), alterada pela Lei Complementar nº 166, que tornou automática a adesão ao cadastro, de modo que se faz necessário solicitar a exclusão dos dados, enquanto anteriormente a solicitação se destinava para inclusão.

Assim, a Lei do Cadastro Positivo "fez com que se tornasse a normativa que refletisse com maior intensidade, em seu tempo, um modelo de proteção de dados pessoais – ainda que restrita ao seu âmbito, referente aos históricos de crédito."[84]

Na esfera penal, a Lei nº 12.737/2012, popularmente denominada de Carolina Dieckmann, que acrescentou os artigos 154-A, 154-B, 266 e 298 ao Código Penal, tipificando como crime a invasão de aparelhos eletrônicos para o alcance de dados ou, ainda, instalar vulnerabilidades nos dispositivos para fins ilícitos.

Em 2013, regulando o comércio eletrônico, surgiu o Decreto nº 7662/2013, que em seu artigo 4º, inciso VII, determina ao fornecedor a utilização de mecanismos de segurança eficazes para pagamento e tratamento de dados do consumidor.

De grande relevância para o presente estudo, tem-se a criação da Lei 12.965/2014 (Marco Civil da Internet) e o Decreto nº 8.771/2016 (regulador do Marco Civil da Internet), que estabelecem princípios, direitos e deveres para o uso da internet no Brasil, trazendo uma abordagem muito mais voltada para proteção aos registros e aos dados pessoais, em busca da segurança do cidadão no âmbito das relações concretizadas pela internet.

---

§ 2º A reabilitação referida no inciso V será autorizada somente quando o interessado efetivar o ressarcimento ao órgão ou entidade dos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso IV.
§ 3º A aplicação da sanção prevista no inciso V é de competência exclusiva da autoridade máxima do órgão ou entidade pública, facultada a defesa do interessado, no respectivo processo, no prazo de 10 (dez) dias da abertura de vista.
Art. 34. Os órgãos e entidades públicas respondem diretamente pelos danos causados em decorrência da divulgação não autorizada ou utilização indevida de informações sigilosas ou informações pessoais, cabendo a apuração de responsabilidade funcional nos casos de dolo ou culpa, assegurado o respectivo direito de regresso.
Parágrafo único. O disposto neste artigo aplica-se à pessoa física ou entidade privada que, em virtude de vínculo de qualquer natureza com órgãos ou entidades, tenha acesso a informação sigilosa ou pessoal e a submeta a tratamento indevido.

[84] DONEDA, Danilo. Princípios e proteção de dados pessoais. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira. (Coords.). **Direito & Internet III**: Marco Civil de Internet – Tomo I. Quartier Latin, 2015. P. 381.

Posto isso, pode-se dizer que:[85]

> Todas as normas desembocam na figura do usuário para que ele, uma vez cientificado a respeito do fluxo de seus dados pessoais, possa controlá-lo através de seu consentimento. Essa perspectiva de controle perpassa desde a fase de coleta e compartilhamento de seus dados com terceiros ao direito de deletá-los junto a prestador de serviços e produtos de internet ao término da relação.

Apesar dessa nítida proteção do usuário, conferida pelas leis acima expostas, não havia legislação para compilar as disposições já existentes, muito menos capaz de abarcar forma geral todo tipo de coleta, tratamento e uso de dados pessoais. Como se pode notar, todas as leis anteriormente mencionadas encontravam algum tipo de limitação diante das suas especificidades.

Enquanto isso, no cenário internacional, diversos outros países elaboraram uma legislação específica para o controle e proteção de dados como, por exemplo, a União Europeia (1995, reformulada em 2016), o Chile (1999), a Argentina (2000) e o México (2010).

No Brasil, inspirado no modelo Europeu (GDPR), aprovou-se a Lei nº 13.709/2018, cuja qual entrou em vigor em 18 de setembro de 2020, após muito tumulto legislativo,[86] além da pandemia do COVID-19. A LGPD (Lei Geral de Proteção de Dados) surge como principal legislação acerca do tema, visando a proteção dos direitos fundamentais de liberdade e privacidade, bem como do livre desenvolvimento da personalidade da pessoa natural, conforme dispõe seu artigo 1º.

Referida Lei por si só traz um senso de responsabilidade dos agentes de tratamento (operador e o controlador) de dados pessoais, seja ele pessoa natural ou jurídica, de direito público ou privado.

---

[85] BIONI, Bruno R. **Autodeterminação informacional:** Paradigmas inconclusos entre os direitos da personalidade, regulação dos bancos de dados eletrônicos e a arquitetura da internet. Dissertação de Mestrado. Faculdade de Direito da Universidade de São Paulo, 2016. P. 161.

[86] A Lei 13.709/2018 foi aprovada em 14/08/2018, na sua redação havia previsão de *vacatio legis* de 18 meses, ou seja, entraria em vigor em fevereiro de 2020. Em 08/07/2019, aprovou-se a Lei nº 13.853/2019, que criou a Autoridade Nacional de Proteção de Dados e alterou a entrada em vigor para agosto de 2020. Porém, em 03/04/2020, através do PL 1.179, alterou-se a entrada plena em vigor para janeiro de 2021, sendo que as sanções administrativas ficariam apenas para agosto de 2021. Com a pandemia do COVID-19, o Presidente editou a MP nº959/20, determinando que os artigos da LGPD entrariam em vigor em maio de 2021. Em 12/06/2020, a Lei nº 14.010/2020 é sancionada e fixa que as punições administrativas para as empresas somente ocorrerão em agosto de 2021. Na data de 25/08/2020, a Câmara aprovou a MP nº959/20, que determinava a entrada em vigor da LGPD para janeiro de 2021 e as penalidades para agosto de 2021. Ao ser enviada ao Senado, o artigo 4º da referida MP foi excluído, retrocedendo à data original, qual seja, agosto de 2020, com penalidades em agosto de 2021. O Decreto nº 10.474 surge para detalhar a estrutura e o quadro funcional da Agência Nacional de Proteção de Dados. Em 17/09/2020, houve a sanção da Presidência, fazendo com que a entrada em vigor efetiva da LGPD em 18/09/2020.

A LGPD traz a exigência de mais transparência das relações existentes na sociedade digital, exige a aplicação de técnicas e mecanismos que garantam a proteção dos dados pessoais.

A nova legislação coloca em foco a vontade do titular dos dados, apontando o consentimento como uma das bases para o tratamento de dados pessoais. O consentimento serve como instrumento de proteção do titular de dados, resguardando e tutelando seu direito fundamental à privacidade. Nesse ponto, tanto a LGDP quanto a GDPR trazem em seus dispositivos a exigência do consentimento como exigência para que o tratamento de dados seja lícito.[87] De igual forma, ambas as legislações permitem a revogação do consentimento a qualquer tempo pelo titular.

Em que pese a relevância do tema, a questão do consentimento do titular de dados será tratada no decorrer do capítulo 2.

Ademais, com a entrada da lei em vigor, os setores público e privado, na função de controladores de dados, deverão manter procedimentos de governança, gestão e controle, de forma a garantir a proteção dos dados.

Inegável a importância da LGPD, que apesar de seu surgimento tardio (se ponderado o avanço tecnológico das duas últimas décadas e a necessidade de proteção e regulamentação das práticas de coleta, tratamento e uso de dados pessoais), traz um cenário de segurança e clareza aos envolvidos, tanto controladores passam a saber a quais regras devem se submeter, quanto os titulares passam a visualizar e defender seus direitos frente a eventuais abusos.

A relevância da lei pode ser notada até mesmo por fatos corriqueiros da vida dos cidadãos, considerando que não é necessário refletir muito para recordar do último contato indesejado de empresa com a qual nunca se teve contato e não possui interesse em suas atividades. Resta buscar a origem desse contato, como a empresa conseguiu os dados, caso tenha sido de forma ilícita, deverá ser punida.

A LGPD naturalmente traz impactos sociais e econômicos e, obviamente, jurídicos, já que o ambiente digital e as regras do jogo foram alteradas, sendo que na esfera civil o grande desafio residirá na forma de como eventuais danos e descumprimentos legais serão tratados, aqui em especial, como o Estado será responsabilizado quando provocar danos oriundos de dados pessoais que estavam sob a sua custódia.

---

[87] Resguardas as exceções legais.

2.4. ENTENDIMENTO DO SUPREMO TRIBUNAL FEDERAL SOBRE PRIVACIDADE E PROTEÇÃO DE DADOS

Conforme apresentado acima, no Brasil, a Lei Geral de Proteção de Dados é muito recente, nem mesmo a Autoridade Nacional de Proteção de Dados (ANPD) estava formada no momento em que entrou em vigor. Aliás, a nomeação dos diretores da ANPD ocorreu recentemente, em 06 de novembro de 2020.[88]

De acordo com o teor da própria LGPD a atuação da ANPD é de extrema importância, tanto pelo seu caráter fiscalizador como sancionador. É a partir da atuação dessa autoridade que os controladores de dados pautarão suas condutas. Apesar da lei dispor sobre os deveres incumbidos aos controladores de dados, sabe-se que a forma com que a lei será cumprida depende da fiscalização e do controle pela autoridade competente.

Contudo, ainda que a ANPD exerça papel relevante, é notório que o Brasil é um País litigioso, seja pela via individual ou pela via coletiva, a judicialização das lides possui alto percentual, diferente de outros países como Europa e Estados Unidos, em que além do sistema judiciário distinto, possuem o costume prévio de mediação e arbitragem.

Basta um simples olhar nos números levantados pelo CNJ,[89] no ano de 2019, para se ter uma ideia da quantidade anual de novas demandas no Poder Judiciário, apenas em matéria de direito civil e de direito do consumidor, foram mais de 17 milhões de casos novos. Em casos de responsabilidade civil da Administração Pública foram mais de 200 mil casos, em 2019.[90]

Portanto, em breve, pode-se dizer que o Judiciário irá se deparar com um número crescente de demandas envolvendo proteção de dados, com base nas disposições contidas na legislação.

---

[88] BRASIL. Presidência da República. **Autoridade Nacional de Proteção de Dados contribui para a segurança jurídica de cidadãos**. 2020. Disponível em: <https://www.gov.br/casacivil/pt-br/assuntos/noticias/2020/novembro/autoridade-nacional-de-protecao-de-dados-contribui-para-a-seguranca-juridica-de-cidadaos-1>. Acesso em: 28.12.2020.

[89] BRASIL. Conselho Nacional de Justiça. **Justiça em Números – 2019**. Disponível em: <https://paineis.cnj.jus.br/QvAJAXZfc/opendoc.htm?document=qvw_l%2FPainelCNJ.qvw&host=QVS%40neodimio03&anonymous=true&sheet=shResumoDespFT>. Acesso em: 28.12.2020.

[90] BRASIL. Conselho Nacional de Justiça. **Justiça em Números – 2019**. Disponível em: <https://paineis.cnj.jus.br/QvAJAXZfc/opendoc.htm?document=qvw_l%2FPainelCNJ.qvw&host=QVS%40neodimio03&anonymous=true&sheet=shResumoDespFT>. Acesso em: 28.12.2020.

Aliás, nesse ponto, importante destacar a constatação trazida pelo site europeu POLICO[91] de que mesmo na Europa, em que há menor tendência de judicialização das lides, já se nota uma migração das discussões envolvendo dados pessoais da via administrativa ao Poder Judiciário.

Na referida reportagem, aponta-se para o fato relevante de que na Europa "grupos de consumidores e ativistas que desejam ver suas reclamações GDPR resolvidas em tempo hábil estão cada vez mais se voltando para os resultados do sistema judiciário europeu" para eles além da solução mais rápida, "ir ao tribunal lhes dá muito mais controle sobre o caso, bem como a capacidade de abrir um precedente legal assim que o veredicto for proferido."[92] Aqui no Brasil, muito provavelmente, não será diferente.

Com a entrada em vigor da LGPD discussões envolvendo proteção de dados tendem a ser mais comuns no Judiciário e, aos poucos, com a capacitação dos Julgadores e a maior pesquisa doutrinária sobre o tema, logo surgirão alguns precedentes, inclusive, vinculantes sobre a matéria.

Não quer dizer que a questão de dados nunca foi enfrentada, inclusive, em 2020 houve grande alteração de entendimento jurisprudencial no Supremo Tribunal Federal em relação a temática, cujo qual será analisado posteriormente.

Analisando alguns julgamentos importantes do STF acerca da proteção de dados, anteriores à 2020, nota-se que o entendimento da Corte era de que o compartilhamento e uso de dados pelo Estado não importava em violação à privacidade, aliás nem vislumbrava a necessidade da proteção dos dados de forma autônoma.

Em acórdão publicado em 2006, o STF ao julgar o Recurso Extraordinário nº418.416/SC, discutiu a condenação do Réu com base em prova obtida por meio ilícito, no caso, a inviolabilidade dos dados decorrentes da extensão dos efeitos de uma busca e apreensão de computadores de um empresário, que permitiu o acesso dos dados para outros órgãos (Receita Federal e INSS), para além da autoridade policial que apreendeu o bem.

---

[91] MANANCOURT, Vicent. Have a GDPR complaint? Skip the regulator and take it to court. **Politico**. 2020. Disponível em:<https://www.politico.eu/article/have-a-gdpr-complaint-skip-the-regulator-and-take-it-to-court/>. Acesso em 28.12.2020.

[92] MANANCOURT, Vicent. Have a GDPR complaint? Skip the regulator and take it to court. **Politico**. 2020. Disponível em:<https://www.politico.eu/article/have-a-gdpr-complaint-skip-the-regulator-and-take-it-to-court/>. Acesso em 28.12.2020.

A parte ré, recorrente, alegava que o mandado de busca e apreensão visava apenas os equipamentos de informática, o que não autorizaria a decodificação dos registros armazenados no computador apreendido. A tese voltada para a proteção dos dados existentes no computador foi refutada.

O acórdão foi assim ementado:[93]

> I. Decisão judicial: fundamentação: alegação de omissão de análise de teses relevantes da Defesa: recurso extraordinário: descabimento. Além da falta do indispensável prequestionamento (Súmulas 282 e 356), não há violação dos art. 5º, LIV e LV, nem do art. 93, IX, da Constituição, que não exige o exame pormenorizado de cada uma das alegações ou provas apresentadas pelas partes, nem que sejam corretos os fundamentos da decisão; exige, apenas, que a decisão esteja motivada, e a sentença e o acórdão recorrido não descumpriram esse requisito (v.g., RE 140.370, 1ª T., 20.4.93, Pertence, DJ 21.5.93; AI 242.237 - AgR, 1ª T., 27.6.00, Pertence, DJ 22.9.00). II. Quebra de sigilo bancário: prejudicadas as alegações referentes ao decreto que a determinou, dado que a sentença e o acórdão não se referiram a qualquer prova resultante da quebra do sigilo bancário, tanto mais que, dado o deferimento parcial de mandado de segurança, houve a devolução da documentação respectiva. III. Decreto de busca e apreensão: validade. 1. Decreto específico, que somente permitiu que as autoridades encarregadas da diligência selecionassem objetos, dentre aqueles especificados na decisão e na sede das duas empresas nela indicadas, e que fossem "interessantes à investigação" que, no caso, tinha pertinência com a prática do crime pelo qual foi efetivamente condenado o recorrente. 2. Ademais não se demonstrou que as instâncias de mérito tenham invocado prova não contida no objeto da medida judicial, nem tenham valorado qualquer dado resultante da extensão dos efeitos da decisão determinante da busca e apreensão, para que a Receita Federal e a "Fiscalização do INSS" também tivessem acesso aos documentos apreendidos, para fins de investigação e cooperação na persecução criminal, "observado o sigilo imposto ao feito". IV - Proteção constitucional ao sigilo das comunicações de dados - art. 5º, XVII, da CF: ausência de violação, no caso. 1. Impertinência à hipótese da invocação da AP 307 (Pleno, 13.12.94, Galvão, DJU 13.10.95), em que a tese da inviolabilidade absoluta de dados de computador não pode ser tomada como consagrada pelo Colegiado, dada a interferência, naquele caso, de outra razão suficiente para a exclusão da prova questionada - o ter sido o microcomputador apreendido sem ordem judicial e a consequente ofensa da garantia da inviolabilidade do domicílio da empresa – este segundo fundamento bastante, sim, aceito por votação unânime, à luz do art. 5º, XI, da Lei Fundamental. 2. **Na espécie, ao contrário, não se questiona que a apreensão dos computadores da empresa do recorrente se fez regularmente, na conformidade e em cumprimento de mandado judicial. 3. Não há violação ao art. 5. XII, da Constituição que conforme se acentuou na sentença, não se aplica ao caso, pois não houve "quebra de sigilo das comunicações de dados (interceptações das comunicações), mas sim apreensão de base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial". 2. A proteção a que se refere o art. 5º, XII, da Constituição, é da comunicação 'de dados 'e não dos dados em si mesmos, ainda que armazenados em computador.** (...). (sem grifos no original)

[93] BRASIL. Supremo Tribunal de Justiça. **Recurso Extraordinário nº 418.416**. Relator: Min. Sepúlveda Pertence. Tribunal Pleno. Julgado em 10/05/2006. Disponível em:< http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=395790>. Acesso em 28.12.2020.

Apesar de ter lavrado voto divergente quanto à condenação, o Ministro Marco Aurélio concordou com o entendimento do Relator em relação aos dados, nesse ponto, surpreende a seguinte frase: “Comungo inteiramente com a afirmação dos colegas de não haver, no caso, a proteção a dados armazenados.”[94]

Quanto ao compartilhamento indevido de dados, nota-se que o Ministro Ricardo Lewandowski destacou em seu voto o desconforto e sua opinião de desaprovação da conduta. Afirmou que “penso ter havido um extravasamento indevido dos dados de um processo penal que possuía objeto específico.”[95] Em que pese tenha demonstrado preocupação em relação ao compartilhamento de dados apreendidos em um processo sigiloso para outros órgãos da Administração Pública, o Ministro acompanhou o voto do Relator.

Outro caso emblemático, ocorreu em 2016, quando o STF julgou o Recurso Extraordinário nº 601.314/SP, com Repercussão Geral, consolidado no Tema 225, da Corte.

Em síntese, no referido julgamento, autorizou a transferência de dados acerca de movimentações financeiras ao Fisco sem ordem judicial. O processo era de relatoria do Ministro Edson Fachin e foi assim ementado:

> RECURSO EXTRAORDINÁRIO. REPERCUSSÃO GERAL. DIREITO TRIBUTÁRIO. DIREITO AO SIGILO BANCÁRIO. DEVER DE PAGAR IMPOSTOS. REQUISIÇÃO DE INFORMAÇÃO DA RECEITA FEDERAL ÀS INSTITUIÇÕES FINANCEIRAS. ART. 6º DA LEI COMPLEMENTAR 105/01. MECANISMOS FISCALIZATÓRIOS. APURAÇÃO DE CRÉDITOS RELATIVOS A TRIBUTOS DISTINTOS DA CPMF. PRINCÍPIO DA IRRETROATIVIDADE DA NORMA TRIBUTÁRIA. LEI 10.174/01. 1. O litígio constitucional posto se traduz em um confronto entre o direito ao sigilo bancário e o dever de pagar tributos, ambos referidos a um mesmo cidadão e de caráter constituinte no que se refere à comunidade política, à luz da finalidade precípua da tributação de realizar a igualdade em seu duplo compromisso, a autonomia individual e o autogoverno coletivo. 2. Do ponto de vista da autonomia individual, o sigilo bancário é uma das expressões do direito de personalidade que se traduz em ter suas atividades e informações bancárias livres de ingerências ou ofensas, qualificadas como arbitrárias ou ilegais, de quem quer que seja, inclusive do Estado ou da própria instituição financeira. 3. Entende-se que a igualdade é satisfeita no plano do autogoverno coletivo por meio do pagamento de tributos, na medida da capacidade contributiva do contribuinte, por sua vez vinculado a um Estado soberano comprometido com a satisfação das necessidades coletivas de seu Povo. 4. Verifica-se que o Poder Legislativo não desbordou dos parâmetros

[94] BRASIL. Supremo Tribunal de Justiça. **Recurso Extraordinário nº 418.416**. Relator: Min. Sepúlveda Pertence. Tribunal Pleno. Julgado em 10/05/2006. Disponível em:< http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=395790>. Acesso em 28.12.2020. P. 1317.

[95] BRASIL. Supremo Tribunal de Justiça. **Recurso Extraordinário nº 418.416**. Relator: Min. Sepúlveda Pertence. Tribunal Pleno. Julgado em 10/05/2006. Disponível em:< http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=395790>. Acesso em 28.12.2020. P. 1296.

> constitucionais, ao exercer sua relativa liberdade de conformação da ordem jurídica, na medida em que estabeleceu requisitos objetivos para a requisição de informação pela Administração Tributária às instituições financeiras, assim como manteve o sigilo dos dados a respeito das transações financeiras do contribuinte, observando-se um translado do dever de sigilo da esfera bancária para a fiscal. 5. A alteração na ordem jurídica promovida pela Lei 10.174/01 não atrai a aplicação do princípio da irretroatividade das leis tributárias, uma vez que aquela se encerra na atribuição de competência administrativa à Secretaria da Receita Federal, o que evidencia o caráter instrumental da norma em questão. Aplica-se, portanto, o artigo 144, §1º, do Código Tributário Nacional. 6. Fixação de tese em relação ao item "a" do Tema 225 da sistemática da repercussão geral: "**O art. 6º da Lei Complementar 105/01 não ofende o direito ao sigilo bancário, pois realiza a igualdade em relação aos cidadãos, por meio do princípio da capacidade contributiva, bem como estabelece requisitos objetivos e o translado do dever de sigilo da esfera bancária para a fiscal".** 7. Fixação de tese em relação ao item "b" do Tema 225 da sistemática da repercussão geral: "**A Lei 10.174/01 não atrai a aplicação do princípio da irretroatividade das leis tributárias, tendo em vista o caráter instrumental da norma, nos termos do artigo 144, §1º, do CTN**". 8. Recurso extraordinário a que se nega provimento. (grifo no original)

O acórdão foi prolatado por maioria de votos, vencidos os Ministros Marco Aurélio e Celso de Mello, que entenderam pela inconstitucionalidade do envio e compartilhamento de dados.

Nas palavras do Ministro Marco Aurélio, analisando o caso concreto, afirmou que a pretensão de acesso aos dados pela Receita Federal diretamente de Instituições Financeiras "vulnera a privacidade do cidadão, irmã gêmea da dignidade, concluir-se que é possível ter-se a quebra do sigilo de dados bancários de forma linear, mediante comunicações automáticas." [96] Por essa razão, discordou do compartilhamento, entendendo que seria possível apenas quando "consideradas as finalidades previstas na cláusula final do inciso XII do art. 5º, investigação criminal ou instrução criminal e a Receita não atua fazendo as vezes do Ministério Público."[97]

Em dezembro de 2019, mais um caso importante envolvendo compartilhamento de dados da Receita Federal com o Ministério Público, também foi

---

[96] BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 601.314.** Relator: Min. Edson Fachin. Tribunal Pleno. Julgado em 24/02/2016. Disponível em: <redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=11668355>. Acesso em: 28.12.2020. P. 118.

[97] BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 601.314.** Relator: Min. Edson Fachin. Tribunal Pleno. Julgado em 24/02/2016. Disponível em: <redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=11668355>. Acesso em: 28.12.2020. P. 123.

julgado sob o regime de Repercussão Geral, que gerou o Tema 990 do da Corte,[98] o qual possui a seguinte ementa:

> Repercussão geral. Tema 990. Constitucional. Processual Penal. Compartilhamento dos Relatórios de inteligência financeira da UIF e da íntegra do procedimento fiscalizatório da Receita Federal do Brasil com os órgãos de persecução penal para fins criminais. Desnecessidade de prévia autorização judicial. Constitucionalidade reconhecida. Recurso ao qual se dá provimento para restabelecer a sentença condenatória de 1º grau. Revogada a liminar de suspensão nacional (art. 1.035, § 5º, do CPC). Fixação das seguintes teses: 1. É constitucional o compartilhamento dos relatórios de inteligência financeira da UIF e da íntegra do procedimento fiscalizatório da Receita Federal do Brasil - em que se define o lançamento do tributo - com os órgãos de persecução penal para fins criminais sem prévia autorização judicial, devendo ser resguardado o sigilo das informações em procedimentos formalmente instaurados e sujeitos a posterior controle jurisdicional; 2. O compartilhamento pela UIF e pela RFB referido no item anterior deve ser feito unicamente por meio de comunicações formais, com garantia de sigilo, certificação do destinatário e estabelecimento de instrumentos efetivos de apuração e correção de eventuais desvios.

Novamente, restaram vencidos os Ministros Marco Aurélio e Celso de Mello. A tese fixada, seguiu, mais uma vez, a linha favorável ao acesso e compartilhamento de dados pelos órgãos do Poder Público, sem prévia autorização judicial.

Dessa forma, nos três julgados acima citados, é possível concluir que o STF, ao menos a maioria de seus membros, tinha uma visão bem liberal quanto ao acesso do Estado aos dados dos cidadãos.

Contudo, em recente julgamento, ocorrido em maio de 2020, o STF apresentou uma nova reflexão sobre o tema, ao julgar a Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6.387/DF.

Em resumo, no contexto da notória pandemia do Covid-19, através da Medida Provisória nº 954/2020, autorizou-se o compartilhamento de dados de 100% dos cadastros das empresas de telefonia fixa e móvel com a Fundação Instituto Brasileiro de Geografia e Estatística (IBGE). A justificativa seria a impossibilidade de entrevistas presenciais em razão do cenário de pandemia.

O Autor da Ação Direta de Inconstitucionalidade é o Conselho Federal da Ordem dos Advogados do Brasil, que em síntese, alegou que a MP: [99]

---

[98] BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 1.055.941.** Relator: Min. Dias Toffoli. Tribunal Pleno. Julgado em 04/12/2019. Disponível em: <http://www.stf.jus.br/portal/diarioJustica/verDiarioProcesso.asp?numDj=243&dataPublicacaoDj=06/10/2020&incidente=5213056&codCapitulo=5&numMateria=168&codMateria=1>. Acesso em 28.12.2020.

[99] BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 6.387.** Relatora: Min. Rosa Weber. Julgado em 07/05/2020. Disponível em: < http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629>. Acesso em 02.01.2021. P. 6

> **a)** viola dados sigilosos, inclusive o telefônico, de todos os brasileiros; **b)** tem como finalidade informada, de modo genérico e impreciso, a produção de estatística oficial mediante a realização de entrevistas não presenciais no âmbito de pesquisas domiciliares; **c)** estabelece a guarda dos dados disponibilizados no âmbito da Fundação IBGE, sem definir procedimentos de controle pelo Judiciário, pelo Ministério Público ou por órgãos da sociedade civil; **d)** não apresenta com precisão a modalidade, a frequência e o objetivo das pesquisas a serem realizadas; **e)** não aponta razões justificadoras da urgência e da relevância da medida; **f)** não apresenta razões que justifiquem a necessidade do compartilhamento dos dados para a pesquisa estatística; **g)** silencia sobre a adoção de mecanismo de segurança para reduzir o risco de acesso e uso indevidos; e **h)** ao prever a elaboração de relatório de impacto após o uso dos dados, e não previamente ao compartilhamento, impede a efetiva avaliação dos riscos.

A medida cautelar foi deferida para o fim de suspender a eficácia da Medida Provisória e foi assim ementada:[100]

> **MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA Nº 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. *FUMUS BONI JURIS*. *PERICULUM IN MORA*. DEFERIMENTO.** 1. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais. **2.** Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, *caput*), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados. **3.** O Regulamento Sanitário Internacional (RSI 2005) adotado no âmbito da Organização Mundial de Saúde exige, quando essencial o tratamento de dados pessoais para a avaliação e o manejo de um risco para a saúde pública, a garantia de que os dados pessoais manipulados sejam "adequados, relevantes e não excessivos em relação a esse propósito" e "conservados apenas pelo tempo necessário." (artigo 45, § 2º, alíneas "b" e "d"). **4.** Consideradas a necessidade, a adequação e a proporcionalidade da medida, não emerge da Medida Provisória nº 954/2020, nos moldes em que editada, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia. **5.** Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP nº 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF), na dimensão substantiva, por não oferecer condições de avaliação quanto à sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades. **6.** Ao não apresentar mecanismo técnico ou administrativo apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização

[100] BRASIL. Supremo Tribunal Federal. **Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6.387**. Relatora Min. Rosa Weber. Julgado em 24.02.2020. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf>. Acesso em 28.12.20.

> indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados, a MP nº 954/2020 descumpre as exigências que exsurgem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros. **7.** Mostra-se excessiva a conservação de dados pessoais coletados, pelo ente público, por trinta dias após a decretação do fim da situação de emergência de saúde pública, tempo manifestamente excedente ao estritamente necessário para o atendimento da sua finalidade declarada. **8.** Agrava a ausência de garantias de tratamento adequado e seguro dos dados compartilhados a circunstância de que, embora aprovada, ainda não vigora a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), definidora dos critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais. O fragilizado ambiente protetivo impõe cuidadoso escrutínio sobre medidas como a implementada na MP nº 954/2020. **9.** O cenário de urgência decorrente da crise sanitária deflagrada pela pandemia global da COVID-19 e a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento não podem ser invocadas como pretextos para justificar investidas visando ao enfraquecimento de direitos e atropelo de garantias fundamentais consagradas na Constituição. **10.** *Fumus boni juris* e *periculum in mora* demonstrados. Deferimento da medida cautelar para suspender a eficácia da Medida Provisória nº 954/2020, a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel. 11. Medida cautelar referendada.

O voto da Ministra Relatora Rosa Weber evidencia a existência de desproporcionalidade do compartilhamento com o fim almejado. No caso concreto, haveria colheita de mais dados do que o necessário, inclusive pontou-se que o compartilhamento de duas centenas de milhões de números de telefone seria desproporcional levando em consideração as amostras utilizadas pelo IBGE em anos anteriores. A Relatora registrou no voto que sequer haveria previsão ou garantia do uso e tratamento dos dados de forma segura, inexistindo na MP qualquer previsão acerca dos cuidados mínimos com os dados, não apontando anonimização ou pseudonimização.

Para o STF, “a capacidade do indivíduo de autodeterminar seus dados pessoais é parcela fundamental do seu direito de desenvolver livremente sua personalidade”, [101] portanto, a atividade relativa ao tratamento e uso de dados pessoais deve ter limites, especialmente, porque os direitos da personalidade merecem integral proteção. Assim, o cenário de pandemia não pode servir de pretexto para se cometer abusos aos direitos fundamentais dos cidadãos.

---

[101] BRASIL. Supremo Tribunal Federal. **Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6.387**. Relatora Min. Rosa Weber. Julgado em 24.02.2020. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf>. Acesso em 28.12.20.

Com base nos votos devidamente fundamentados em doutrina nacional e estrangeira, o STF, por maioria de votos (vencido apenas o Ministro Marco Aurélio), consignou que o conteúdo da MP 954/2020 “vai de encontro ao direito de privacidade, à autodeterminação informativa, à inviolabilidade da intimidade dos consumidores”, bem como, acaba por ferir “os princípios da ordem econômica, da defesa do consumidor, do livre desenvolvimento da personalidade e da dignidade, bem como o exercício da cidadania quanto às pessoas naturais.”[102]

Portanto, pode-se dizer que assim como a legislação pátria evoluiu ao proteger os dados pessoais dos cidadãos, nota-se que o entendimento do STF também evoluiu e tende a evoluir mais com a vigência da LGPD, ao menos, espera-se.

[102] BRASIL. Supremo Tribunal Federal. **Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6.387**. Relatora Min. Rosa Weber. Julgado em 24.02.2020. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf>. Acesso em 28.12.20. P. 89.

3. TRATAMENTO DE DADOS PELO ESTADO

Para a presente pesquisa, a fim de se chegar na responsabilidade civil decorrente da violação de normas e direitos acerca do tratamento de dados pelo Poder Público, torna-se imprescindível analisar, primeiramente, como está atualmente regulamentada a forma de coletar e tratar dados pelo Poder Público.

Isso porque a responsabilidade existirá se tais normais forem violadas. Assim, cabível tratar das disposições legais e principiológicas existentes nas principais legislações do ordenamento jurídico específicas para o tratamento de dados pelo Estado. Bem como, demonstrar como a LGPD pode dialogar com o CDC e com a LAI.

Os riscos desse tratamento residem, principalmente, na existência de grandes bancos de dados em poder do Estado, que coletam inúmeros dados e estão sujeitos à compartilhamentos, que acabam por desvirtuar a finalidade da coleta.

Dessa forma, o capítulo se destina a definir de forma clara e direta quais são as regras a que se submete o Poder Público ao agir como controlador de dados pessoais.

3.1. Tratamento de dados pessoais pelo Poder Público

A LGPD em seus artigos 1º[103] e 3º[104] prevê expressamente sua aplicação para as pessoas jurídicas de direito público. Além disso, dedicou um capítulo todo (Capítulo IV) para regular o tratamento de dados pelo Poder Público.

Conforme exposto no primeiro capítulo dessa pesquisa, o armazenamento de dados pelo Poder Público está intrinsecamente ligado ao exercício de suas atividades

[103] Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

[104] Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

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; ou

III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

e serve, também, como norte para elaboração de políticas públicas e como forma de controle. Inegável que essa relação jurídica entre Estado e titulares de dados pessoais é marcada pela assimetria do poder.

Nas palavras de Fernando Antonio Tasso:[105]

> O tratamento de dados pessoais é um aspecto da execução das políticas públicas que mereceu da LGPD regulamentação específica decorrente do reconhecimento de que a massificação das relações travadas entre o Estado e os cidadãos, marcada pela voracidade na coleta de dados, tratados de forma não padronizada e, tampouco, transparente, redunda no risco de o Estado violar direitos e garantias fundamentais do titular.

Não bastasse isso, os dados que estão sob o controle do Estado, em sua grande maioria, podem ser considerados como de "caráter sensível", que nos termos do artigo 5º da LGPD são aqueles que contêm:[106]

> 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.

Isso porque desde prontuários de postos de saúde municipais, até grandes bancos de dados como os de órgãos federais, por exemplo, do Instituto Nacional do Seguro Social e a Receita Federal, manipulam dados com informações detidas e extremamente sensíveis dos cidadãos, assim, são dados que devem ser protegidos, inclusive em face do próprio Estado.

O artigo 7º da LGPD autoriza de forma expressa o tratamento de dados pela administração pública em seus incisos III e IV, os quais demonstram duas situações em que a Administração Pública tem interesse no tratamento. O inciso III prevê que a Administração Pública pode tratar e compartilhar dados "necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei". Já o inciso IV, aponta para possiblidade de tratamento para estudos realizados por órgão de pesquisa, com a obrigatoriedade de privilegiar a anonimização dos dados.

Nesse ponto, é inegável que a "execução de políticas públicas é, portanto, a principal e indubitavelmente a melhor justificativa para que o setor público realize

---

[105] TASSO, Fernando Antonio. Do tratamento de dados pessoais pelo Poder Público. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord). **LGPD**: Lei Geral de Proteção de dados comentada. São Paulo: Thomson Reuters Brasil, 2019. p. 246.

[106] Art. 5º, inc. II, da LGPD.

qualquer tipo de tratamento de dados.” Justamente por se tratar de um conceito aberto, acaba conferindo amplitude para a manipulação dos dados pessoais pelo Setor Público, já que, como se viu no capítulo 1, a consecução de políticas públicas é inerente à própria existência do Estado.[107]

Assim, Feigelson e Siqueira, discorrem que:[108]

> as entidades públicas, ao encontro do disposto, também estão subordinadas às previsões da LGPD quando da execução de políticas públicas – tais como campanha de vacinação, epidemia, regular controle do padrão de qualidade do ensino público etc. Assim, devem documentar e identificar o fundamento da licitude do tratamento e a finalidade a que se destina. Além disso, deve restar claro que os dados são necessários ao exercício da autoridade pública ou de funções de interesse público, justamente como uma forma de mitigar o abuso do Estado diante da privacidade e direitos dos cidadãos.

Portanto, analisando a LGPD, é possível afirmar que, apesar das pessoas jurídicas de Direito Público deterem legitimidade para coleta e tratamento de dados com fundamento na finalidade pública para concretizar o interesse público, não estão desobrigadas de atuarem em conformidade com as normas e princípios da Lei.[109]

Em relação ao consentimento, considerada a principal base legal para o tratamento de dados,[110] prevista no artigo 7º, inciso I, da LGPD, está conceituada no artigo 5º, inciso XII, que dispõe que consentimento consiste na “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.”

Dessa forma, “consentimento é o meio pelo qual o titular de dados pessoais tem para determinar o nível de proteção e fluxo de seus dados, dando sua anuência para que ocorra o tratamento de suas informações.” Para ter validade, deve ser “livre, específico e informado.”[111]

Quanto à exigência de consentimento para o tratamento de dados pelo Poder Público, não se nota abordagem específica pela doutrina, de modo que este instituto não logra protagonismo como nas relações privadas, já que o maior percentual de

---

[107] ROSSO, Angela Maria. LGPD E SETOR PÚBLICO: aspectos gerais e desafios. **Migalhas**. 2019. Disponível em: <https://migalhas.uol.com.br/depeso/300585/lgpd-e-setor-publico--aspectos-gerais-e-desafios>. Acesso em: 02.01.2021.

[108] FEIGELSON, Bruno. SIQUEIRA, Antonio. **Comentários à Lei Geral de Proteção de dados.** São Paulo: Thompson Reuters Brasil, 2019. p. 66-67.

[109] Princípios gerais da LGPD dispostos no Artigo 6º, cujo quais consistem em: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e da responsabilização.

[110] Com base no Artigo 7º da LGPD, verifica-se que existem 10 bases.

[111] FEIGELSON, Bruno; SIQUEIRA, Antonio. **Comentários à Lei Geral de Proteção de dados.** São Paulo: Thompson Reuters Brasil, 2019. p. 60.

dados utilizados pelos agentes e órgãos estatais encontra respaldo em políticas públicas e no ordenamento jurídico, conforme previsto nos artigos 7 e 11 da LGPD.

Por outro lado, alguns países como Estônia e Dinamarca possuem uma plataforma nacional para obtenção do consentimento do cidadão quanto ao uso específico de seus dados pelos órgãos públicos, possibilitando o autocontrole de quem e por qual razão necessita armazenar, acessar e utilizar tais informações.[112]

Embora o consentimento apareça de forma menos intensa em relação ao Poder Público, nota-se a existência de hipótese legal e de casos concretos em que se faz necessário colher o consentimento. Por exemplo: nas medidas instituídas para restituição do ICMS, há poder de escolha pelo titular de dados, tais como Nota Paraná; nas hipóteses do artigo 47, quando do compartilhamento de dados entre a administração pública e algum ente privado – novamente, com exceção daqueles necessários para execução da atividade pública e das hipóteses previstas nos artigos 11 e 26.[113]

O ideal é que mesmo perante o Estado, o titular de dados tenha plena ciência da forma como seus dados pessoais estão sendo tratados e que sempre haja máxima transparência nessa utilização.

Partindo para o Capítulo IV, específico para o Poder Público, tem-se no artigo 23 da LGPD quem são as pessoas jurídicas de direito público interno que estão sujeitas às suas regras. Para tanto, traz como referência o artigo 1º, § único, da Lei de Acesso à Informação (Lei nº 12.527/2001), confira-se:

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

Cabe, então, verificar quem são os integrantes da Administração Pública que estão sujeitos à LGPD, conforme remissão a Lei de Acesso à Informação:

> Art. 1º Esta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal.
> Parágrafo único. Subordinam-se ao regime desta Lei:

---

[112] GROSSMANN, Luís Osvaldo. **LGPD**: governo terá plataforma de consentimento e monitoramento do uso de dados, 2019. Disponível em:<https://www.lgpdbrasil.com.br/lgpd-governo-tera-plataforma-de-consentimento-e-monitoramento-do-uso-de-dados/>. Acesso em 02.01.2020.

[113] ROSSO, Angela Maria. LGPD E SETOR PÚBLICO: aspectos gerais e desafios. **Migalhas**. 2019. Disponível em: <https://migalhas.uol.com.br/depeso/300585/lgpd-e-setor-publico--aspectos-gerais-e-desafios>. Acesso em: 02.01.2021.

> I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;
> II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

Além dos entes e órgãos elencados no dispositivo de lei supracitado, os §§ 4º e 5º da LGPD acrescentam ao referido rol os seguintes sujeitos:

> § 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.
> § 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo.

Dentro desse contexto, imprescindível destacar que as empresas públicas e sociedades de economias mistas, as quais exploram atividade econômica nos termos do artigo 173, § 1º da Constituição Federal,[114] receberam regime diferenciado pela LGPD.

Nos termos do artigo 24,[115] o tratamento por tais entes dependerá da atividade que exercerá. Isto é, quando estiverem atuando em regime de concorrência, terão o mesmo tratamento dado às pessoas jurídicas de direito privado. Porém, quando estiverem operacionalizando políticas públicas e no seu âmbito de execução, estão subordinadas as regras do Capítulo IV da LGPD destinada ao tratamento de dados pelo Poder Público (§ único do art. 24).

Na prática, espera-se que haja “clara segregação do banco de dados de tais empresas, com controles internos e externos, a fim de que não haja aproveitamento

---

[114] Art. 173. Ressalvados os casos previstos nesta Constituição, a exploração direta de atividade econômica pelo Estado só será permitida quando necessária aos imperativos da segurança nacional ou a relevante interesse coletivo, conforme definidos em lei.
§ 1º A lei estabelecerá o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias que explorem atividade econômica de produção ou comercialização de bens ou de prestação de serviços, dispondo sobre:
I - sua função social e formas de fiscalização pelo Estado e pela sociedade;
II - a sujeição ao regime jurídico próprio das empresas privadas, inclusive quanto aos direitos e obrigações civis, comerciais, trabalhistas e tributários;
III - licitação e contratação de obras, serviços, compras e alienações, observados os princípios da administração pública;
IV - a constituição e o funcionamento dos conselhos de administração e fiscal, com a participação de acionistas minoritários;
V - os mandatos, a avaliação de desempenho e a responsabilidade dos administradores.

[115] Art. 24. As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.
Parágrafo único. As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos deste Capítulo.

indevido de vantagens dedicadas aos órgãos públicos", já que perseguem o lucro tanto para o Estado, como para seus acionistas particulares.[116]

Ainda sobre o sujeito passivo da norma destinada ao Poder Público, cabe destacar que a LGPD dispôs de forma expressa que se aplicam aos serviços notariais e de registro, de caráter privado, pois o exercício de suas funções decorre via delegação estatal (art. 23, §4º).

Assim, fixados quem são os sujeitos destinatários da norma, cabe agora analisar os principais pontos que permeiam o tratamento de dados pelo Poder Público.

Prosseguindo na análise do artigo 23, da LGPD, o tratamento de dados pelas pessoas acima detalhadas, deverá ter como fundamento: o atendimento de sua finalidade pública, a busca do interesse público e de executar as competências legais, cumprindo com as atribuições legais do serviço público. Ou seja, em atendimento aos princípios da finalidade e adequação, "tais operações devem visar a finalidade pública, com o objetivo de satisfazer o interesse público."[117]

Isso porque *"*a defesa do interesse público corresponde ao próprio fim do Estado. O Estado tem que defender os interesses da coletividade. Tem que atuar no sentido de favorecer o bem-estar social." Sem dúvida, *"*negar a existência desse princípio é negar o próprio papel do Estado."[118]

Para Celso Antônio Bandeira de Mello, o alcance do interesse público é dever do Estado Democrático de Direito no exercício da função pública[119] e, ainda, define que:[120]

> Ao se pensar em interesse público, pensa-se, habitualmente, em uma categoria *contraposta à de interesse privado, individual,* isto é, ao interesse pessoal de cada um. Acerta-se em dizer que se constitui no *interesse do todo,* ou seja, do *próprio conjunto social,* assim como acerta-se também em sublinhar que não se confunde com a somatória dos interesses individuais, peculiares de cada qual. Dizer isto, entretanto, é dizer muito pouco para compreender-se verdadeiramente o que é interesse público. [...] é que existe, de um lado, o interesse individual, particular, atinente às conveniências de cada um no que concerne aos assuntos de sua vida particular - interesse, este, que é o da pessoa ou grupo de pessoas singularmente consideradas-, e que, de par com isto, existe também o interesse igualmente pessoal destas

[116] COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada**. 2ª ed. São Paulo: Thompson Reuters Brasil, 2019. p. 143.
[117] FEIGELSON, Bruno. SIQUEIRA, Antonio. **Comentários à Lei Geral de Proteção de dados.** São Paulo: Thompson Reuters Brasil, 2019. p. 138.
[118] PIETRO, Maria Syilvia Zanella Di. **Direito Administrativo**. 31ª ed. Rio de Janeiro: Forense, 2018. p. 85.
[119] MELLO. Celso Antônio Bandeira de. **Curso de Direito Administrativo**. 32ª ed. São Paulo: Malheiros, 2015. p. 29.
[120] MELLO. Celso Antônio Bandeira de. **Curso de Direito Administrativo**. 32ª ed. São Paulo: Malheiros, 2015. p. 59-62.

> mesmas pessoas ou grupos, mas que comparecem enquanto partícipes de uma coletividade maior na qual estão inseridos, tal como nela estiveram os que os precederam e nela estarão os que virão a sucedê-los nas gerações futuras. Pois bem, é este último interesse o que nomeamos de interesse do todo ou interesse público. [...] o interesse público deve ser conceituado como o interesse resultante do conjunto dos interesses que os indivíduos pessoalmente têm quando considerados em sua qualidade de membros da Sociedade e pelo simples fato de o serem.

Nas palavras de Luiz Alberto Blanchet, “interesse público é todo aquele que compete ao Estado atender direta ou indiretamente”, tal conceito afasta “qualquer interferência ideológica excludente a preservar a segurança jurídica”.[121]

Portanto, o princípio da finalidade “exige que o ato seja praticado sempre com finalidade pública” que é atendida quando:[122]

> o Poder Público executar o tratamento de dados pessoais dos administrados, pessoas naturais, nos estritos termos da lei para execução de políticas públicas previstas na norma, zelando pela proteção de dados pessoais da pessoa natural e pela garantia de seus direitos personalíssimos.

Nesse ponto, não há como escapar de mencionar o princípio da supremacia do interesse público, que é a base de praticamente todas as funções do Estado, estando presente nos quatro tipos de funções administrativas, quais sejam: serviço público, fomento, polícia administrativa e intervenção.[123] Fato é que para o exercício dessas quatro funções, o Poder Público tem cada vez mais se utilizado de dados dos cidadãos, o que reforça ainda mais a necessidade de controle da finalidade desses dados, cuja qual deve estar voltada ao interesse público, como já dito.

Ademais, impossível deixar de resgatar nesse ponto, a discussão do Capítulo I, em relação ao controle e poder do Estado, pois a relação jurídica estabelecida entre o Poder Público e o titular de dados pessoais, inevitavelmente, é marcada pela assimetria do poder. Basicamente, por duas razões principais, a primeira “em decorrência da natureza jurídica do ente estatal que atua com poder de império, dotado de poderes para a consecução de seus deveres”, a segunda pela “circunstância objetiva de que o ente estatal detém grande quantidade de dados

---

[121] BLANCHET, Luiz Alberto. **Administração Pública, Ética e Desenvolvimento**. 3ª Edição. Curitiba: Juruá, 2020.p. 31.
[122] TASSO, Fernando Antonio. Do tratamento de dados pessoais pelo Poder Público. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord). **LGPD**: Lei Geral de Proteção de dados comentada. São Paulo: Thomson Reuters Brasil, 2019. p. 251.
[123] PIETRO, Maria Syilvia Zanella Di. **Direito Administrativo**. 31ª ed. Rio de Janeiro: Forense, 2018. p. 84.

pessoais em seus bancos de dados, como insumo ou subproduto do desempenho de sua atividade."[124]

Dessa forma, como as relações que envolvem dados travadas entre os cidadãos e o Estado é marcada pela coleta voraz e a ampla utilização dos dados, necessariamente precisa ser protegida e, para que isso ocorra, deve ser pautada na transparência (sempre que possível) e deve garantir direitos fundamentais do titular de dados.

Seguindo na análise do artigo 23, o inciso primeiro, aponta as seguintes condições para o tratamento de dados pelo Poder Público: a) informar as hipóteses, dentro do exercício de suas atribuições; b) informações claras e atualizadas sobre a previsão legal, finalidade e a forma para execução das atividades. Ou seja, "o órgão público deve deixar claro em quais situações – e para quais finalidades – os dados pessoais serão coletados, classificados e utilizados."[125]

Ainda, o inciso primeiro prevê que as informações acima mencionadas devem constar em veículos de fácil acesso ao titular de dados, preferencialmente, em seus sítios eletrônicos, sem a exclusão dos meios analógicos. Nesse ponto, cabível o diálogo das fontes, considerando que a Lei de Acesso à Informação já regula o direito fundamental do cidadão de obter junto aos órgãos Públicos as informações cadastradas em seu nome, nos termos do seu artigo 8º, que dispõe:

> Art. 8º É dever dos órgãos e entidades públicas promover, independentemente de requerimentos, a divulgação em local de fácil acesso, no âmbito de suas competências, de informações de interesse coletivo ou geral por eles produzidas ou custodiadas.
> § 1º Na divulgação das informações a que se refere o caput, deverão constar, no mínimo:
> I - registro das competências e estrutura organizacional, endereços e telefones das respectivas unidades e horários de atendimento ao público;
> II - registros de quaisquer repasses ou transferências de recursos financeiros;
> III - registros das despesas;
> IV - informações concernentes a procedimentos licitatórios, inclusive os respectivos editais e resultados, bem como a todos os contratos celebrados;
> V - dados gerais para o acompanhamento de programas, ações, projetos e obras de órgãos e entidades; e
> VI - respostas a perguntas mais frequentes da sociedade.
> § 2º Para cumprimento do disposto no caput, os órgãos e entidades públicas deverão utilizar todos os meios e instrumentos legítimos de que dispuserem, sendo obrigatória a divulgação em sítios oficiais da rede mundial de computadores (internet).

---

[124] TASSO, Fernando Antonio. Do tratamento de dados pessoais pelo Poder Público. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord). **LGPD**: Lei Geral de Proteção de dados comentada. São Paulo: Thomson Reuters Brasil, 2019. p. 245.

[125] LEVIN, Alexandre. Tratamento de dados pelo Poder Público – particularidades previstas na LGPD (Lei 13.709/2018). In: DAL POZZO, Augusto Neves E MARTINS, Ricardo Marcondes (coords.). **LGPD & Administração Pública**. São Paulo: Thomson Reuters Brasil, 2020. p. 240.

> § 3º Os sítios de que trata o § 2º deverão, na forma de regulamento, atender, entre outros, aos seguintes requisitos:
> I - conter ferramenta de pesquisa de conteúdo que permita o acesso à informação de forma objetiva, transparente, clara e em linguagem de fácil compreensão;
> II - possibilitar a gravação de relatórios em diversos formatos eletrônicos, inclusive abertos e não proprietários, tais como planilhas e texto, de modo a facilitar a análise das informações;
> III - possibilitar o acesso automatizado por sistemas externos em formatos abertos, estruturados e legíveis por máquina;
> IV - divulgar em detalhes os formatos utilizados para estruturação da informação;
> V - garantir a autenticidade e a integridade das informações disponíveis para acesso;
> VI - manter atualizadas as informações disponíveis para acesso;
> VII - indicar local e instruções que permitam ao interessado comunicar-se, por via eletrônica ou telefônica, com o órgão ou entidade detentora do sítio; e
> VIII - adotar as medidas necessárias para garantir a acessibilidade de conteúdo para pessoas com deficiência, nos termos do art. 17 da Lei nº 10.098, de 19 de dezembro de 2000, e do art. 9º da Convenção sobre os Direitos das Pessoas com Deficiência, aprovada pelo Decreto Legislativo nº 186, de 9 de julho de 2008.
> § 4º Os Municípios com população de até 10.000 (dez mil) habitantes ficam dispensados da divulgação obrigatória na internet a que se refere o § 2º , mantida a obrigatoriedade de divulgação, em tempo real, de informações relativas à execução orçamentária e financeira, nos critérios e prazos previstos no art. 73-B da Lei Complementar nº 101, de 4 de maio de 2000 (Lei de Responsabilidade Fiscal).

Como se viu acima, o §3º do artigo 8º da Lei de Acesso à Informação já descreve como deverá ser realizada a divulgação do conteúdo em sítios oficiais, que certamente se aplica para a apontar a forma de coleta, tratamento e uso dos dados.

No âmbito do Poder Judiciário, o Conselho Nacional de Justiça (CNJ), através da Resolução nº 215/2015, em seu artigo 6º, § 4º, também, dispõe acerca da forma da disponibilização da informação através dos sítios eletrônicos. Da mesma forma, a Recomendação nº 73 do CNJ,[126] indica as medidas necessárias para adequação do Poder Judiciário à LGPD, apontando, dentre as várias recomendações, a disponibilização em sítio eletrônico de informações nos termos da LGPD e de formulário para o exercício do direito do titular (art. 1º, inc. II, Recomendação 73, CNJ).

Assim, constata-se que tanto a LGPD quanto à LAI, tem como propósito "conferir ao Poder Público a mais concreta transparência de sua atividade, permitindo

[126] Há notícia de uma nova Resolução do CNJ aprovada que trata da LGPD, porém, ainda não foi publicada nos sítios oficiais até a data de 02.01.2021. Fonte: CNJ aprova resolução que padroniza adequação dos tribunais à LGPD. **Revista Consultor Jurídico**, 2020. Disponível em: <https://www.conjur.com.br/2020-dez-16/cnj-aprova-resolucao-padroniza-adequacao-tribunais-lgpd>. Acesso em 02.01.2021.

ao cidadão o acesso aos dados do próprio órgão consultado e, agora, às operações de tratamento de dados pessoais do indivíduo."[127]

Quando o Estado estiver tratando dados pessoais, o inciso terceiro do artigo 23 exige que seja indicado um encarregado, que irá atuar nos termos do artigo 39 da LGPD, seguindo as instruções do controlador e as normas sobre a matéria.

Além das disposições da própria LGPD, dispõe o parágrafo 1º, do art. 23, que a Agência Nacional de Proteção de Dados (ANPD) poderá criar novas regras sobre a publicidade das operações de tratamento. Já no parágrafo 2º reitera a observância à LAI.

Os prazos prescricionais, a forma de exercício do direito e o procedimento interno, conforme parágrafo 3º da LGPD, serão aqueles dispostos nas leis específicas do Habeas Data (Lei nº 3.507/1997), Lei Geral do Processo Administrativo (Lei nº 9.784/1999) e a LAI (Lei nº 12.527/2011).

A ANPD, ainda, nos termos dos artigos 29 e 30 da LGPD, poderá solicitar a realização de operações, informações e detalhes do tratamento de dados aos órgãos e entidades do Poder Público, bem como estabelecer normas complementares acerca das atividades de comunicação e do uso compartilhado dos dados pessoais. A questão do compartilhamento será tratada em tópico apartado, devido à sua relevância.

Posto isso, torna-se imprescindível destacar que, em alguns casos, poderá o ente público alegar a exceção prevista no artigo 4º, inc. III, da LGPD,[128] que versa sobre a inaplicabilidade da Lei para o caso de manejo de dados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão para fins penais.

---

[127] TASSO, Fernando Antonio. Do tratamento de dados pessoais pelo Poder Público. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord). **LGPD**: Lei Geral de Proteção de dados comentada. São Paulo: Thomson Reuters Brasil, 2019. p.253

[128] Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
[...]
III - realizado para fins exclusivos de:
a) segurança pública;
b) defesa nacional;
c) segurança do Estado; ou
d) atividades de investigação e repressão de infrações penais; ou
[...]
§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

Entretanto, tal inaplicabilidade não pode ser absoluta. Em primeiro lugar, porque o direito à privacidade é fundamental e decorre de norma constitucional, como exaustivamente tratado no primeiro capítulo. Em segundo lugar, porque, de acordo com o §1º do mesmo artigo 4º, os princípios gerais de proteção ao titular dos dados previstos nos artigos 6º, 17 e 18 são imperativos.

Ademais, a coleta, tratamento e uso de dados dos consumidores, deverão observar tanto os princípios a LGPD quanto os princípios do CDC, especialmente: o princípio da finalidade,[129] transparência, livre acesso, segurança, não discriminação e responsabilização.

Assim, ainda que a pessoa jurídica de direito público alegue a ocorrência das hipóteses previstas no artigo 4º, III da LGPD, o titular dos dados pode invocar seu direito de acesso, correção, anonimização e informações inadequadas.[130] Igualmente, o artigo 4º não poderá ser utilizado para justificar eventual abuso ou dano, pois a responsabilidade continuará intacta se seus atos violarem princípios e direitos fundamentais.

Aliás, o artigo 31 da Lei de acesso à informação (Lei 12.527/2011),[131] já prevê a exigência de conduta pautada no princípio da transparência e o respeito às liberdades e garantias individuais dos titulares de dados, a fim de evitar abusos.

---

[129] Previsto no artigo 6º, inciso I, da LGPD, o qual prevê que o tratamento de dados de ter "propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades", ou seja, deve ser respeitado o contexto da coleta e observado sem ampliações.

[130] FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thompson Reuters Brasil, 2019. p. 187.

[131] Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.
§ 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:
I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e
II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.
§ 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido.
§ 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias:
I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;
II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;
III - ao cumprimento de ordem judicial;

De acordo com a Lei de Acesso à Informação, até mesmo informações ultrassecretas possuem prazo limite de restrição de acesso, conforme dispõe o artigo 24:

> Art. 24. A informação em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, poderá ser classificada como ultrassecreta, secreta ou reservada.
> § 1º Os prazos máximos de restrição de acesso à informação, conforme a classificação prevista no caput, vigoram a partir da data de sua produção e são os seguintes:
> I - ultrassecreta: 25 (vinte e cinco) anos;
> II - secreta: 15 (quinze) anos; e
> III - reservada: 5 (cinco) anos.

Ou seja, até mesmo informações de sigilo absoluto um dia deverão ser divulgadas, ao que tudo indica, o acesso aos dados pessoais pelos titulares de dados deve seguir a mesma linha de raciocínio.

Fato é que sob os pretextos de sigilo e/ou de progresso, não é possível aceitar toda e qualquer manipulação de dados, em especial, por parte do Estado. Ainda mais dentro da sociedade de risco global em que vivemos, da assunção de riscos incalculáveis e efeitos imprevisíveis.[132]

Essa assunção de riscos não pode existir. A própria LGPD traz as disposições acerca de segurança, boas práticas e governança de dados, as quais inegavelmente devem ser observados pelo Poder Público, ou seja, deve atuar preventivamente, fomentando a cultura de proteção de dados e adotando medidas que assegurem a segurança dos dados em seu poder, nos termos da LGPD. Isso consequentemente, resultará na redução dos riscos.

Segundo o sítio eletrônico do Governo Federal isso já está sendo realizado. Afirma o site oficial que houve a disponibilização de um guia de boas práticas para adequação dos órgãos do Governo à LGPD; elaboração de um programa de governança em privacidade e a criação de inventários de dados pessoais, orientação nos termos de uso e políticas de privacidade vinculados à utilização de serviços

---

IV - à defesa de direitos humanos; ou
V - à proteção do interesse público e geral preponderante.
§ 4º A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância.
§ 5º Regulamento disporá sobre os procedimentos para tratamento de informação pessoal.

[132] FERREIRA, Heline Sivini. A dimensão ambiental da teoria da sociedade de risco. In: FERREIRA, Heline Sivini; Freitas, Cinthia Obladen de Almendra (orgs). **Direito Socioambiental e Sustentabilidade**: Estados, Sociedades e Meio Ambiente. Curitiba: Letra da Lei, 2016. p. 108-158.

públicos; bem como, orientações para o relatório de impacto de proteção de dados e auxílio no plano de resposta aos incidentes. Por fim, a transparência estaria sendo garantida pelo portal gov.br.[133]

Apesar das disposições legais e atuações institucionais internas, apenas com o decorrer do tempo será possível analisar em que medida o Poder Público está cumprindo as disposições da LGPD e como os dados de mais de 210 milhões de brasileiros estão sendo protegidos e tratados.

Nas palavras de Luiz Alberto Blanchet, é: [134]

> absolutamente indispensável para a boa condução da administração pública em direção ao desenvolvimento é o constante questionamento. Nenhuma boa solução pretérita tem o poder de ser boa para problemas a ela ulteriores, por mais semelhantes que sejam em relação ao problema anteriormente solucionado. Sequer problemas absolutamente idênticos requerem soluções idênticas, pois a identidade existe apenas em relação aos aspectos internos do problema, porém os fatores circunstantes seguramente terão evoluído serão diferentes. Dentre os fatores externos, destacam-se aspectos como a realidade do mercado, a situação da economia, as inovações tecnológicas, evolução das aspirações populares e alterações normativas.

Portanto, sendo as inovações tecnológicas um fator externo, deve o agente público atuar proativamente e antever soluções inteligentes, razão pela qual é manifesta a necessidade de contratações de pessoas capacitadas e com habilidades específicas no setor tecnológico, única forma de tornar eficiente a atuação do Estado nesse campo.[135]

3.2. DIÁLOGO DAS FONTES: O CÓDIGO DE DEFESA DO CONSUMIDOR E LGPD NA PROTEÇÃO DE DADOS CONTROLADOS PELO PODER PÚBLICO

A visão meramente hierárquica para solução de conflitos entre normas jurídicas foi superada pela necessidade de coordenação entre as leis dentro de um ordenamento jurídico, como forma de obter um sistema mais eficiente, coerente e justo.

---

[133] Brasil. Governo Digital. **Guias Operacionais para adequação à LGPD**. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd>. Acesso em: 02.01.2021.

[134] BLANCHET, Luiz Alberto. **Administração Pública, Ética e Desenvolvimento**. 3ª Edição. Curitiba: Juruá, 2020. p. 10.

[135] BLANCHET, Luiz Alberto. **Administração Pública, Ética e Desenvolvimento**. 3ª Edição. Curitiba: Juruá, 2020. p. 10.

A teoria de Erik Jayme, jurista alemão, intitulada como “diálogo das fontes” (*dialogue de sources*), busca harmonizar e coordenar as normas, como forma de priorizar e proteger direitos humanos. A intenção da doutrina é de trazer eficiência não só hierárquica, mas funcional ao sistema, dando-lhe coerência.[136]

Ao analisar tal teoria, Cláudia Lima Marques, aponta que há 3 tipos de diálogos possíveis entre duas leis da vida privada:[137]

> 1) na aplicação simultânea das duas leis, uma lei pode servir de base conceitual para a outra (*diálogo sistemático de coerência*), especialmente se uma lei é geral e a outra especial; se uma é a lei central do sistema[25] e a outra um micro-sistema específico,[26] não-completo materialmente, apenas com completude subjetiva de tutela de um grupo da sociedade. (...);
> 2) na aplicação coordenada das duas leis, uma lei pode complementar a aplicação da outra, a depender de seu campo de aplicação no caso concreto (*diálogo sistemático de complementariedade e subsidiariedade* em antinomias aparentes ou reais), a indicar a aplicação complementar tanto de suas normas, quanto de seus princípios, no que couber, no que for necessário ou subsidiariamente. (...);
> 3) há o diálogo das influências recíprocas sistemáticas, como no caso de uma possível redefinição do campo de aplicação de uma lei (...) ou como no caso da possível transposição das conquistas do *Richterrecht* (Direito dos Juízes) alcançadas em uma lei para a outra. É a influência do sistema especial no geral e do geral no especial, um diálogo de *double sens* (*diálogo de coordenação e adaptação sistemática*).

Ao final, conclui que “haveria o diálogo sistemático de coerência, o diálogo sistemático de complementariedade e subsidiariedade em antinomias e o diálogo de coordenação e adaptação sistemática.”[138]

Posto isso, na presente pesquisa, cabe aplicar tal teoria na convergência da nova Lei Geral de Proteção de Dados com o Código de Defesa do Consumidor, norma vigente há mais de 30 anos no ordenamento jurídico brasileiro. A legislação consumerista, “em razão, do corte horizontal nas mais diversas relações jurídicas, é significativo exemplo da necessidade de atual convivência com diversos outros diplomas.”[139]

---

[136] MARQUES, Claudia Lima**.** Diálogo Entre o Código de Defesa do Consumidor e o novo Código Civil – do “Diálogo Das Fontes” no Combate às Cláusulas Abusivas. **Revista de Direito do Consumidor**, vol. 45/2003, p. 71-99, Jan./Mar., 2003, p. 71-72.
[137] MARQUES, Claudia Lima**.** Diálogo Entre o Código de Defesa do Consumidor e o novo Código Civil – do “Diálogo Das Fontes” no Combate às Cláusulas Abusivas. **Revista de Direito do Consumidor**, vol. 45/2003, p. 71-99, Jan./Mar., 2003, p. 73-74.
[138] MARQUES, Claudia Lima**.** Diálogo Entre o Código de Defesa do Consumidor e o novo Código Civil – do “Diálogo Das Fontes” no Combate às Cláusulas Abusivas. **Revista de Direito do Consumidor**, vol. 45/2003, p. 71-99, Jan./Mar., 2003, p. 73-74.
[139] BESSA, Leonardo Roscoe Bessa. **Relação de Consumo e Aplicação do Código de Defesa do Consumidor**. 2ª ed. São Paulo: Revista dos Tribunais, 2009. p. 102.

A teoria do “diálogo das fontes”, tem sido frequentemente utilizada pelo Poder Judiciário para “indicar a aplicação simultânea do CDC com mais de uma lei geral ou especial, de forma ordenada e coerente com o valor constitucional de proteção do consumidor.”[140]

Apesar de concebido em um contexto diverso deste formado pelas tecnologias da informação e comunicação, o CDC é um diploma legislativo que contém princípios éticos aplicáveis à proteção de dados, tais como, transparência, boa-fé, proteção da segurança e dos interesses legítimos, prevenção, cooperação e equilíbrio. A legislação consumerista foi precursora ao disciplinar os bancos de dados e cadastros dos consumidores em seu artigo 43, conferindo o direito de autocontrole das informações pessoais pelo titular de dados.

Em princípio, não se nota nenhuma possibilidade de conflito entre a LGPD e o CDC, sendo plenamente viável o diálogo entre as duas fontes, aumentando a eficácia do sistema e da proteção do titular de dados, especialmente dentro de uma relação de consumo.

E, no caso, o CDC incluiu no artigo 22[141] as pessoas jurídicas de direito público como fornecedores, ou seja, reconhece o Estado como fornecedor, não havendo dúvidas quanto a aplicação da norma ao Poder Público. Ainda, nota-se a intenção do legislador voltada à aplicação do CDC aos serviços públicos nos artigos 4º, VII e 6º, X, do CDC.

Igualmente, a Lei nº 8.987/1995, que dispõe sobre o regime de concessão e permissão da prestação de serviços públicos, em seu artigo 7º dispõe:

> Art. 7º. Sem prejuízo do disposto na Lei no 8.078, de 11 de setembro de 1990, são direitos e obrigações dos usuários:
> I - receber serviço adequado;
> II - receber do poder concedente e da concessionária informações para a defesa de interesses individuais ou coletivos;
> III - obter e utilizar o serviço, com liberdade de escolha entre vários prestadores de serviços, quando for o caso, observadas as normas do poder concedente.
> IV - levar ao conhecimento do poder público e da concessionária as irregularidades de que tenham conhecimento, referentes ao serviço prestado;
> V - comunicar às autoridades competentes os atos ilícitos praticados pela concessionária na prestação do serviço;

---

[140] MARQUES, Claudia Lima. **Contratos Submetidos às Regras do Código de Defesa do Consumidor**. 8ª ed. São Paulo: Revista dos Tribunais, 2016. p. 673.

[141] Art. 22. Os órgãos públicos, por si ou suas empresas, concessionárias, permissionárias ou sob qualquer outra forma de empreendimento, são obrigados a fornecer serviços adequados, eficientes, seguros e, quanto aos essenciais, contínuos.
Parágrafo único. Nos casos de descumprimento, total ou parcial, das obrigações referidas neste artigo, serão as pessoas jurídicas compelidas a cumpri-las e a reparar os danos causados, na forma prevista neste código.

> VI - contribuir para a permanência das boas condições dos bens públicos através dos quais lhes são prestados os serviços.

Dessa forma, inegável o dever legal de observância ao CDC pelos órgãos públicos, através de suas empresas, concessionárias e/ou permissionárias ou de qualquer outra forma em que estiver prestando um serviço público.

Para Cláudia Lima Marques:[142]

> aplica-se o CDC, sempre que presente um consumidor, aos serviços públicos referentes ao fornecimento de água, energia elétrica, gás, telefonia, transportes públicos, rodovias e estradas com pedágio, financiamento, construção de moradias populares etc.

Nesse ponto, apesar de ser aplicável o CDC, deve-se apontar a ressalva legal que é confirmada pela jurisprudência do Superior Tribunal de Justiça, pela qual é possível a interrupção dos serviços, desde que, cumpridas as exigências de informação prévia e situação de inadimplência, nos termos do artigo 6º, § 3º, II, da Lei nº 8.987/1995.[143]

Assim, demonstrada a aplicabilidade do CDC aos serviços públicos e a LGDP ao Poder Público, como se viu no tópico anterior, ambas as legislações podem e devem ser aplicadas em conjunto no que tange à proteção de dados em poder do Estado.

Além das disposições expressas da LGPD em seus artigos 23 e seguintes, a Lei nº 13.460/2017, também, prevê mecanismos para participação, proteção e defesa dos direitos do usuário dos serviços públicos prestados direta ou indiretamente pela administração pública, podendo ser aplicada em casos concretos que envolvam o titular de dados, usuário do serviço público.

Os artigos 1º e 6º da referida Lei dispõem:

> Art. 1º Esta Lei estabelece normas básicas para participação, proteção e defesa dos direitos do usuário dos serviços públicos prestados direta ou indiretamente pela administração pública.
> § 1º O disposto nesta Lei aplica-se à administração pública direta e indireta da União, dos Estados, do Distrito Federal e dos Municípios, nos termos do inciso I do § 3º do art. 37 da Constituição Federal .
> § 2º A aplicação desta Lei não afasta a necessidade de cumprimento do disposto:
> I - em normas regulamentadoras específicas, quando se tratar de serviço ou atividade sujeitos a regulação ou supervisão; e
> II - na Lei nº 8.078, de 11 de setembro de 1990, quando caracterizada relação de consumo.

---

[142] MARQUES, Claudia Lima. **Contratos Submetidos às Regras do Código de Defesa do Consumidor**. 8ª ed. São Paulo: Revista dos Tribunais, 2016. P. 646.
[143] MARQUES, Claudia Lima. **Contratos Submetidos às Regras do Código de Defesa do Consumidor**. 8ª ed. São Paulo: Revista dos Tribunais, 2016. P. 646.

> § 3º Aplica-se subsidiariamente o disposto nesta Lei aos serviços públicos prestados por particular.
> [...]
> Art. 6º São direitos básicos do usuário:
> I - participação no acompanhamento da prestação e na avaliação dos serviços;
> II - obtenção e utilização dos serviços com liberdade de escolha entre os meios oferecidos e sem discriminação;
> III - acesso e obtenção de informações relativas à sua pessoa constantes de registros ou bancos de dados, observado o disposto no inciso X do caput do art. 5º da Constituição Federal e na Lei nº 12.527, de 18 de novembro de 2011 ;
> IV - proteção de suas informações pessoais, nos termos da Lei nº 12.527, de 18 de novembro de 2011 ;
> V - atuação integrada e sistêmica na expedição de atestados, certidões e documentos comprobatórios de regularidade; e
> VI - obtenção de informações precisas e de fácil acesso nos locais de prestação do serviço, assim como sua disponibilização na internet, especialmente sobre:
> a) horário de funcionamento das unidades administrativas;
> b) serviços prestados pelo órgão ou entidade, sua localização exata e a indicação do setor responsável pelo atendimento ao público;
> c) acesso ao agente público ou ao órgão encarregado de receber manifestações;
> d) situação da tramitação dos processos administrativos em que figure como interessado; e
> e) valor das taxas e tarifas cobradas pela prestação dos serviços, contendo informações para a compreensão exata da extensão do serviço prestado.

Assim, os usuários de serviços públicos prestados pela administração pública direta ou indireta, também, são considerados consumidores e têm seus dados tutelados pela Lei nº 13.460/2017, pela Lei nº 12.527/2011, pelo CDC e pela LGPD.

Da mesma forma, além dos princípios dispostos pela LGPD para proteção de dados, somam-se os princípios e garantias do CDC, especialmente, aqueles que tratam da proteção de dados dos consumidores, tais como: transparência, finalidade, acesso aos dados, possibilidade de retificação e cancelamento, proteção, segurança e limitação temporal.[144]

Primeiramente, quanto ao princípio da transparência, além do artigo 43, tem-se que o artigo 6º, inciso III, do CDC, também, prevê a necessidade de informação adequada, clara e precisa ao consumidor, o que significa que o fornecedor possui esse dever perante o consumidor antes da vigência da legislação de proteção de dados, portanto, obviamente, tal dever permanece quando o fornecedor coleta ou trata dados pessoais.

---

[144] MENDES, Laura Schertel Mendes. O direito básico do consumidor à proteção de dados pessoais. **Revista de Direito do Consumidor**, Vol. 95, p.53-75, set./out., 2014.

Nas palavras de Mendes:[145]

> o direito do consumidor de ser informado sobre: (i) quais os dados pessoais são tratados e para quais finalidades; (ii) se os dados pessoais são transmitidos para terceiros; (iii) para quais países os dados pessoais são transmitidos, se for o caso; (iv) qual é o período de conservação de dados; e (v) quais os mecanismos de segurança utilizados para garantir a segurança dos dados pessoais.

Em relação ao princípio da finalidade da coleta, que nada mais é do que o estrito uso do dado dentro do contexto em que foi coletado,[146] sem qualquer ampliação ou compartilhamento não consentido. Nesse ponto, é imprescindível ressaltar que o artigo 5º, inciso VII da Lei do Cadastro Positivo (nº 12.414/2011) já prevê a utilização dos dados "somente de acordo com a finalidade para a qual eles foram coletados."

Quanto à garantia de direito de acesso, retificação e cancelamento, como já visto acima, são resguardados pelo artigo 43, facultando ao consumidor titular de dados:[147]

> ter livre acesso aos seus dados (direito de acesso), deve poder corrigir dados equivocados e desatualizados (direito de retificação) e deve poder cancelar dados que foram armazenados e cujo consentimento tenha sido revogado por ele (direito de cancelamento).

No que tange à limitação temporal, o titular de dados poderá requerer a exclusão de informações negativas após o prazo de 5 anos, nos termos do artigo 43, § 1º, do CDC ou requerer a correção, conforme o artigo 43, § 3º, do CDC.

Ainda, imprescindível a ressalva feita pela LGPD em relação à aplicabilidade do CDC quando da violação de um direito do titular de dados:

> Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

Dessa forma, a aplicação em conjunto do CDC e da LGPD trará maior efetividade para as legislações, protegendo de forma ampla o titular dos dados, mesmo diante de uma relação englobando o Estado.

Nas palavras de Cláudia Lima Marques, o aplicador da lei deve "visar o diálogo das fontes, de forma a dar efeito útil a um grande número de normas, privilegiando as

---

[145] MENDES, Laura Schertel Mendes. O direito básico do consumidor à proteção de dados pessoais. **Revista de Direito do Consumidor**, Vol. 95, p.53-75, set./out., 2014.
[146] MENDES, Laura Schertel Mendes. O direito básico do consumidor à proteção de dados pessoais. **Revista de Direito do Consumidor**, Vol. 95, p.53-75, set./out., 2014.
[147] MENDES, Laura Schertel Mendes. O direito básico do consumidor à proteção de dados pessoais. **Revista de Direito do Consumidor**, Vol. 95, p.53-75, set./out., 2014.

normas narrativas, os valores constitucionais e, sobretudo, os direitos humanos."[148] Assim, em atenção aos ensinamentos de Erik Jayme, "o fio condutor, do direito na pós modernidade, do direito do século XXI, serão os direitos humanos."[149]

Ainda que não exista uma consolidação de que a proteção de dados deve ser considerada, de forma independente e uníssona, um direito fundamental, inegável sua vinculação direta com outros direitos fundamentais, bem como o fato de que o "diálogo" entre a LGPD e o CDC é extremamente necessário para assegurar máxima tutela ao titular de dados, especialmente, perante o Estado.

Portanto, verifica-se que o CDC e a LGPD, buscam o reequilíbrio da relação, o primeiro entre consumidor e fornecedor e a segunda entre titular de dados e controlador, reconhecendo a vulnerabilidade do consumidor e titular de dados pessoais.

3.3. GRANDES BANCOS DE DADOS EM PODER DO ESTADO

Desde a Pré-História, nota-se que o homem busca documentar objetos e fatos, como forma de produzir conhecimento. De acordo com Antônio Carlos Efing, no Egito antigo já era possível se notar a existência de cadastros:[150]

> Ao que tudo indica, a palavra cadastro tem origem ligada à função de censo, especialmente aquele relativo à orientação das autoridades administrativas no registro de proprietários de terra, e organização da cobrança de impostos deles, o que inclusive ocorria já no antigo Egito.

Igualmente, em Roma:[151]

> Ao que consta criado pelos romanos com o intuito exposto, o termo cadastro se difundiu e foi emprestado a "todo sistema de fichário, organizado pelos estabelecimentos públicos ou particulares, referente a qualquer assunto de seu interesse, seja econômico ou mesmo administrativo, inclusive aos cadastros bancários e de consumidores.

A partir do Século XIX, constata-se que o uso dos cadastros difundiu em resposta à necessidade de concessão de crédito, especialmente, na esfera do consumo, visto a expansão das concessões à desconhecidos, que implicava na necessidade de registro desses consumidores, como forma prevenção a hipótese de

---

[148] MARQUES, Claudia Lima. **Contratos Submetidos às Regras do Código de Defesa do Consumidor**. 8ª ed. São Paulo: Revista dos Tribunais, 2016. p. 673.
[149] MARQUES, Claudia Lima. **Contratos Submetidos às Regras do Código de Defesa do Consumidor**. 8ª ed. São Paulo: Revista dos Tribunais, 2016. p. 673.
[150] EFING, Antônio Carlos. **Banco de Dados e Cadastro de Consumidores**, São Paulo: Revista dos Tribunais, 2002. P. 20.
[151] EFING, Antônio Carlos. **Banco de Dados e Cadastro de Consumidores**, São Paulo: Revista dos Tribunais, 2002. P. 20.

inadimplemento (possibilitando a cobrança), bem como para servir de alerta em uma futura tentativa de concessão.[152]

Aos poucos tais cadastrados e bancos de dados foram acumulando cada vez mais dados e informações dos indivíduos, seja pelo Estado, seja por Instituições Privadas, especialmente as detentoras de crédito.

Na era da informação, com os grandes avanços na Engenharia, alargou-se a gama de ferramentas capazes de capturar, segregar e modelar dados, facilitando o controle e o acesso rápido aos dados contidos nos cadastros ou Banco de dados.

Segundo Antônio Carlos Efing, cadastros e banco de dados estariam englobados pelos denominados “arquivos de consumo”, contudo, diferenciam-se em diversos aspectos tais como: forma de coleta, organização dos dados, continuidade da coleta e divulgação, existência de requerimento para o cadastramento, extensão dos dados postos à disposição, função das informações obtidas e alcance da divulgação da informação.[153]

Em resumo, podem ser conceituados como:[154]

> [...] os bancos de dados de consumidores seriam sistemas de coleta aleatória de informações, normalmente arquivadas sem requerimento do consumidor, que dispõem de organização imediata, a atender necessidades latentes através de divulgação permanente de dados obrigatoriamente objetivos e não-valorativos, utilizando-se de divulgação a terceiros por motivos exclusivamente econômicos. Diferentemente disto, os cadastros de consumidores seriam sistemas de coleta individualizada de dados objetivos, sejam de consumo ou juízos de valor, obtidos normalmente por informação do próprio consumidor e com objetivo imediato relativo a operações de consumo presentes ou futuras, tendo provisoriedade subordinada aos interesses comerciais subjetivos do arquivista, e divulgação interna, o que demonstra a função secundária de seus arquivos.

Conforme apresentado no primeiro capítulo, a legislação consumerista, através dos artigos 43 e 44 do CDC, conferiu ao consumidor o pleno direito ao controle de suas informações em cadastros, dando-lhe autonomia e determinação para definir como será o uso de seus dados pessoais em cadastros e bancos de dados. Assim, “a racional do legislador foi alcançar todo e qualquer banco de dados que atinja o livre desenvolvimento da personalidade do consumidor.”[155]

---

[152] EFING, Antônio Carlos. **Banco de Dados e Cadastro de Consumidores**, São Paulo: Revista dos Tribunais, 2002. P. 22.
[153] EFING, Antônio Carlos. **Banco de Dados e Cadastro de Consumidores**, São Paulo: Revista dos Tribunais, 2002. p. 30-34.
[154] EFING, Antônio Carlos. **Banco de Dados e Cadastro de Consumidores.** São Paulo: Revista dos Tribunais, 2002. p. 36.
[155] BIONI, Bruno. **Proteção de dados Pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 127.

O CDC preza pela transparência dos fornecedores ao inserirem seus consumidores em cadastros e/ou bancos de dados, de forma que o consumidor possa acompanhar, intervir e discordar do uso de suas informações pessoais quando quiser.

De acordo com Bruno Bioni:[156]

> A referida transparência só tem razão de ser, porque o operador dos bancos de dados terá, simetricamente, os deveres de: i) garantir o seu acesso pelo consumidor (artigo 43, caput, do CDC); ii) a exatidão de tais informações; iii) que o banco de dados se restrinja para finalidades claras e verdadeiras e, por fim; seja observado o limite temporal de 05 (cinco) anos para armazenar informações negativas (artigo 43, §1°, do CDC). Por esse arranjo, o consumidor poderá demandar a imediata correção- cancelamento de uma informação errônea ou que tenha superado tal limite temporal (artigo 43, §3°, do CDC).

Com a edição da MP nº 518/2010, em 09/12/2010, deu-se início à formação de um novo Banco de Dados, com fins de concessão de crédito a pessoas naturais e jurídicas, indo além das informações acerca do inadimplemento que já existiam, apontando informações “positivas” da atuação do consumidor no mercado. O escopo da lei seria beneficiar os bons pagadores. Ou seja, ampliou a quantidade de informações dos consumidores que podem ser consultadas no momento da concessão do crédito.

Apesar das intensas críticas e debates, especialmente, sobre a discriminação oriunda da nova opção de consulta, a referida Medida Provisória foi convertida na Lei nº 12.414/2011.

Dessa forma, referida norma visa disciplinar a formação desse cadastro “positivo” – como foi comumente chamado – contendo informações e históricos de adimplemento para fins de concessão de crédito. Nas palavras de Bruno Bioni:[157]

> Essa nova peça legislativa setorial acabou por trazer, de uma forma original e mais sistematizada, a orientação de que o titular dos dados pessoais deve ter o direito de gerenciá-los. Nesse sentido, requer-se mais do que a simples comunicação da abertura do banco de dados, tal como fez a legislação consumerista. Exige-se o consentimento do titular dos dados pessoais que deve ser, a seu turno, informado e externado por meio de assinatura em um instrumento específico ou em cláusula apartada. Essa esfera de controle deve se prolongar, inclusive, para os casos de compartilhamento da base de dados com terceiros, hipótese na qual deverá haver um compartilhamento específico para tanto.

---

[156] BIONI, Bruno. **Proteção de dados Pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 127-128.

[157] BIONI, Bruno. **Proteção de dados Pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 129.

A Lei do Cadastro Positivo já prevê a autodeterminação informacional do consumidor, deixando-o no controle absoluto de suas informações pessoais. O artigo 3º prevê a vedação à coleta excessiva de dados e o artigo 5º, inciso VIII, proíbe a utilização dos dados pessoais para finalidades diversas da coleta. Ou seja, dentro das relações de consumo para fins de crédito, antes da vigência da LGPD já se vislumbrava a proteção dos consumidores perante os controladores dos dados.

A LGPD, em seu artigo 5º, IV, define como Banco de dados “conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico”.

Na seara de grandes Bancos de Dados e voltando-se para o Poder Público, é imprescindível ressaltar os dois Decretos editados no final do ano de 2019, que vão em sentido contrário as regras estabelecidas pela LGPD e pelo CDC, concedendo prerrogativas especiais ao Estado para uso de dados.

Tratam-se dos Decretos nºs 10.046 e 10.047, os quais demonstram que o Estado segue criando cadastros de grande magnitude, nos quais, até mesmo, caraterísticas biológicas dos cidadãos são armazenadas.

Por exemplo, o “Cadastro Base do Cidadão”, criado pelo Decreto nº 10.046, é composto de, no mínimo, de 12 atributos biográficos e cadastrais, os quais vão compor a base integradora, porém, de acordo com §2º do artigo 18, é possível a inserção de novos dados para a “consolidação inequívoca dos atributos biográficos, biométricos e cadastrais.”

Ou seja, dados completos dos cidadãos em posse do Estado e que sem o controle interno e da sociedade, possivelmente poderão ser utilizados de forma indiscriminada e indevida, causando danos aos seus titulares.

Fato é que a compatibilidade do Decreto nº10.046/2019 com a LGPD é totalmente questionável. Sua coleta excessiva de dados viola o princípio da necessidade, pois a coleta deve se restringir ao minimamente necessário para a finalidade pretendida, no caso da Lei, a própria finalidade é vaga e genérica, acarretando uma ampla coleta sem um fim determinado.

Há pelo menos 3 Projetos de Lei na Câmara dos Deputados que visam sustar os efeitos do Decreto nº 10.046/2019, são eles: 661/2019, 673/2019, 675/2019 (os dois últimos foram apensados ao primeiro). Veja-se parte das justificativas

extremamente relevantes e consistentes contidas nos Projetos de Lei, primeiramente o Projeto nº 661/2019:[158]

> [...] os motivos e as finalidades de compartilhamento das informações pessoais elencadas pelo Governo Federal são imprecisas. O texto aduz tão-somente uma previsão geral de compartilhamento total dos dados para prestação de serviços públicos ou execução de políticas públicas não definidas, carecendo de transparência para o cidadão. (...) o que se depreende do presente decreto é exatamente o oposto, a norma viola tanto o inciso X do artigo 5º da Constituição Federal, que tratou de proteger a privacidade do indivíduo, quanto a Lei Geral de Proteção de Dados, ao retirar do cidadão o poder sobre suas próprias informações. Destacamos, ainda, que a centralização dos dados pessoais que o governo deseja colocar em prática pode tornar tais dados bastante vulneráveis e provocar, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação de dados pessoais, ou até mesmo o acesso não autorizado. Atualmente, notícias sobre vazamento de dados e penalizações às empresas com consequências gravosas têm sido corriqueiras nos noticiários brasileiros.

Ainda, o Projeto nº 673/2019:[159]

> A confiança dos cidadãos é fundamental para assegurar a confiabilidade dos bancos de dados públicos. Entrementes, ao tentar orientar as atividades de coleta e processamento de dados pessoais por parte dos órgãos da Administração Pública, o Decreto aparenta desconsiderar a importância de mecanismos de transparência e controle e trata os dados pessoais como propriedade estatal. Aqui ressaltamos que é preciso oferecer meios para que o cidadão possa supervisionar e opinar acerca do tratamento de seus dados pessoais pelo poder público. O Decreto ainda vai na contramão do que as leis sobre a relação entre direito e tecnologia exigem em relação a governança. Tanto o Marco Civil da Internet (Lei n° 12.485, de 2014) quanto a LGPD apontam isso ao exaltar a participação e estruturas multissetoriais, como o Comitê Gestor da Internet (CGI.Br) e o Conselho Nacional de Proteção de Dados (CNPD).

Por fim, o Projeto nº675/2019:[160]

> Uma base de dados dessa dimensão pode-se tornar um instrumento perigoso sob a administração de uma gestão de viés autoritário ou que busca vigiar ou reprimir opositores. Para além disso, a centralização também traz problemas no tocante à segurança das informações dos cidadãos, que poderão ter verdadeiros dossiês sobre a sua vida privada. Diversos casos de vazamento por órgãos públicos evidenciam as limitações do armazenamento de informações importantes dos indivíduos. Uma base centralizada amplia os focos de vulnerabilidade para invasões e outros incidentes deste tipo. (...) incluem informações “sensíveis”, de cunho estritamente privado, como religião, orientação sexual, filiação a sindicatos, movimentos sociais, que podem ser utilizadas para controle político típico de regimes totalitários.

---

158 BRASIL. Câmara dos Deputados. **PDL 661/2019**. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1820623&filename=PDL+661/2019>. Acesso em 02.01.2021.

159 BRASIL. Câmara dos Deputados. **PDL 673/2019**. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1824299&filename=PDL+673/2019>. Acesso em 02.01.2021.

160 BRASIL. Câmara dos Deputados. **PDL 675/2019**. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1824574&filename=PDL+675/2019>. Acesso em 02.01.2021.

> A mesma incompatibilidade entre Decreto e a LGPD ocorre em relação ao inciso I do Art. 6º da LGPD, que apresenta o princípio da finalidade, segundo o qual "a realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades". Em contraponto, o decreto dispensa, para a efetivação de compartilhamento de dados entre os órgãos públicos, a existência de convênios, acordos de cooperação técnica ou instrumentos congêneres, o que vai de encontro ao art. 26 da LGPD. (...)
> Finalmente, além dos pontos apontados, o texto também desrespeita o inciso X do artigo 5º da Constituição, que incrementa a proteção aos direitos da personalidade ao dispor que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”. Isso porque o decreto não delimita a escala de coleta e tratamento de dados por parte do Estado.

Como se verifica, o Decreto nº 10.046/2019, nitidamente, extrapola o poder regulamentar do Poder Executivo, bem como é incompatível com dispositivos constitucionais e com a LGPD, capaz de gerar uma série de riscos aos titulares de dados pessoais.

Para se ter noção da quantidade de dados que são colhidos diariamente pelo Estado, em maio de 2018, o site Internet Lab, responsável por pesquisas em direito e tecnologia, publicou uma análise realizada em 13 aplicativos do Governo Brasileiro (Federal e Estadual) e demonstrou que esses aplicativos são capazes de coletar inúmeros dados dos cidadãos, o que faz, quase sempre, sem a percepção dos usuários, titulares dos dados.[161]

O escopo da pesquisa era:[162]

> Para fazer esse *ESPECIAL,* nós estudamos 13 aplicativos do governo, dentre eles bolsa família, caixa, CNH digital, Anatel, FGTS, Meu imposto de renda – oito da administração pública federal e cinco do estado de São Paulo – que consideramos que mais afetam cidadãos brasileiros cotidianamente por estarem relacionados a serviços especialmente relevantes ao dia-a-dia e à relação Estado-cidadão. Nosso objetivo era conhecer os tipos de dados que processam, as permissões que pedem, e, quando existente, conhecer suas políticas de privacidade em face dos direitos que possuímos hoje em vigor.

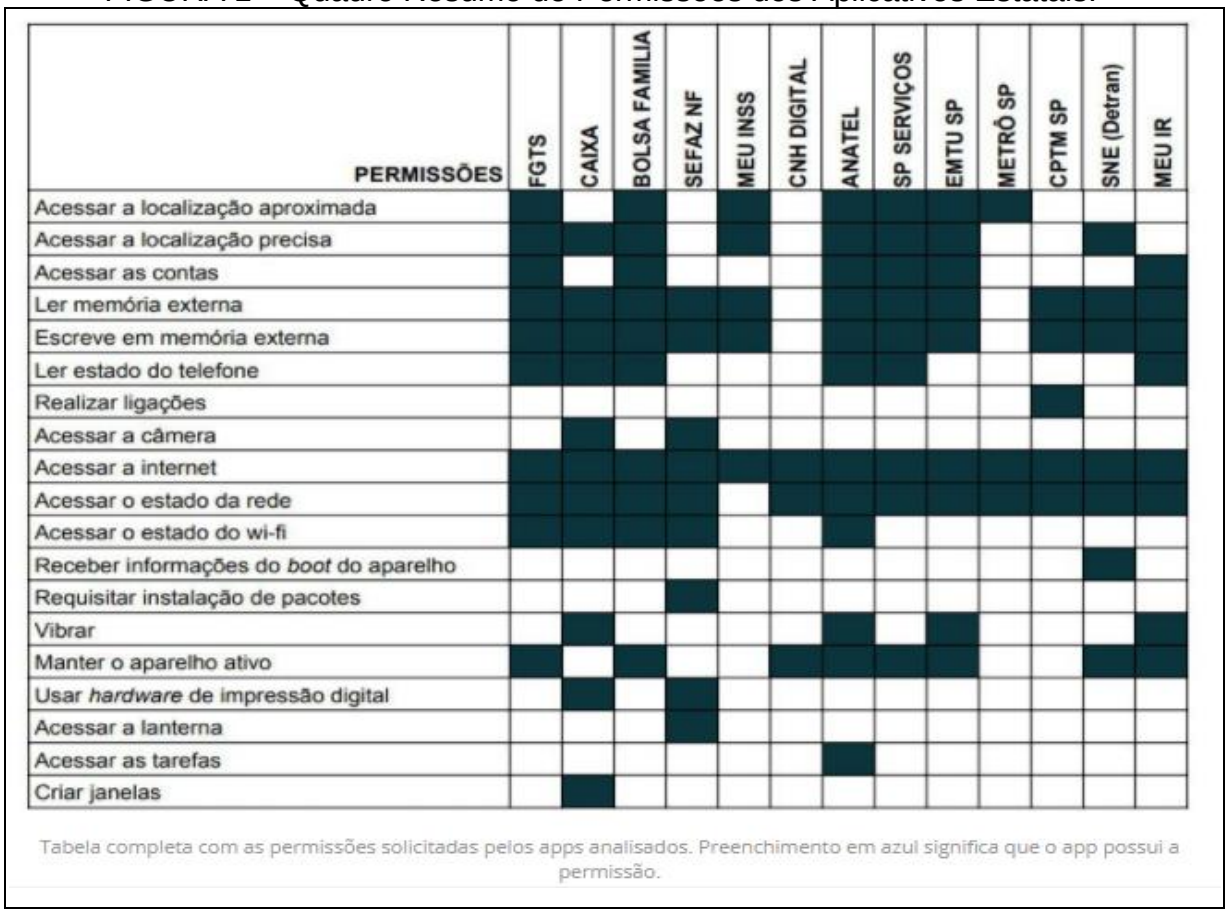
Ao final da pesquisa, apresentou-se um quadro resumo, no qual se vislumbra a grande quantidade de informações que o aplicativo, ao ser instalado pelo usuário, realiza a extração:

---

[161] ABREU, Jacqueline de Souza; LAGO, Lucas; MASSARO, Heloisa. Por que se preocupar com o que o Estado faz com nossos dados pessoais?. **Internet Lab**, 2018. Disponível em: <https://www.internetlab.org.br/pt/privacidade-e-vigilancia/especial-apps-do-governo/>. Acesso em 08.11.2020.

[162] ABREU, Jacqueline de Souza; LAGO, Lucas; MASSARO, Heloisa. Por que se preocupar com o que o Estado faz com nossos dados pessoais?. **Internet Lab**, 2018. Disponível em: <https://www.internetlab.org.br/pt/privacidade-e-vigilancia/especial-apps-do-governo/>. Acesso em 08.11.2020.

FIGURA 1 – Quadro Resumo de Permissões dos Aplicativos Estatais:



PERMISSÕES	FGTS	CAIXA	BOLSA FAMILIA	SEFAZ NF	MEU INSS	CNH DIGITAL	ANATEL	SP SERVIÇOS	EMTU SP	METRÔ SP	CPTM SP	SNE (Detran)	MEU IR
Acessar a localização aproximada	■		■		■		■	■	■	■			
Acessar a localização precisa	■	■	■		■		■	■	■			■	
Acessar as contas	■		■				■	■	■				■
Ler memória externa	■	■	■	■	■		■	■	■		■	■	■
Escreve em memória externa	■	■	■	■	■		■	■	■		■	■	■
Ler estado do telefone	■	■	■				■	■					■
Realizar ligações											■		
Acessar a câmera		■		■									
Acessar a internet	■	■	■	■	■	■	■	■	■	■	■	■	■
Acessar o estado da rede	■	■	■	■		■	■	■	■	■	■	■	■
Acessar o estado do wi-fi	■	■	■	■			■						
Receber informações do *boot* do aparelho												■	
Requisitar instalação de pacotes				■									
Vibrar		■					■		■				■
Manter o aparelho ativo	■		■			■	■	■	■			■	■
Usar *hardware* de impressão digital		■		■									
Acessar a lanterna				■									
Acessar as tarefas							■						
Criar janelas		■											

Tabela completa com as permissões solicitadas pelos apps analisados. Preenchimento em azul significa que o app possui a permissão.

FONTE: ABREU, Jacqueline de Souza; LAGO, Lucas; MASSARO, Heloisa. As “permissões” de acesso a dados em apps do governo. **Internet Lab**, 2018. Disponível em: <https://www.internetlab.org.br/pt/privacidade-e-vigilancia/especial-as-permissoes-de-acesso-dados-em-apps-do-governo/>. Acesso em 08.11.2020.

Ou seja, inegável que a grande maioria dos aplicativos são verdadeiros invasores da privacidade dos usuários. Ocorre que, tais usuários, na grande maioria das vezes, precisam do aplicativo para recebimento de seu benefício, consultas e obtenção de serviços públicos essenciais, de modo que são compelidos em aceitar os termos de uso que lhe são postos.

Por meio dos aplicativos é possível, até mesmo, extrair dados de geolocalização, porém a pesquisa concluiu que ao analisar os termos de uso “não fica claro para todos, pelo menos da perspectiva do usuário, para que isso seria necessário.” Nesse ponto, ressaltam os pesquisadores que “os aplicativos do Metrô de São Paulo e SP Serviços, que possuem essa permissão, não utilizam ela em nenhuma das funcionalidades acessíveis pelo usuário do aplicativo,” sem contar que

alguns dos aplicativos continuam buscando a localização do usuário mesmo sem qualquer permissão.[163]

É preciso avaliar em que medida o acesso à função “READ_PHONE_STATE” – que dá acesso ao “estado do celular” tais como: número, chamadas e lista de contatos – ocorre para real utilização do aplicativo ou se está havendo um abuso nesse acesso, capaz de violar a privacidade do usuário. De acordo com a pesquisa, apontou-se que alguns aplicativos, apesar de extremamente invasivos, sequer deixam claro essa “invasão” em sua política de privacidade, o que não poderia sequer ser admitido.[164]

Esse tipo de conduta é extremamente preocupante, vez que a sociedade deve rechaçar e combater a política simbólica, a qual se caracteriza por um processo em que as metas e medidas são anunciadas para alcançar resultados fictícios ou inexistentes. Trata-se de uma estratégia de dissimulação da verdade para manter um falso estado de normalidade. Os governos, por inúmeras vezes, utilizam-se de argumentos científicos como ferramenta política para o alcance de seus objetivos. Adequa-se o conhecimento científico ao que é politicamente desejável.[165]

Aplicando essa teoria aos aplicativos, tem-se a gravidade do uso do aplicativo com acessos obscuros e imperceptíveis aos usuários, um aproveitamento do uso do consentimento que se dá de forma ilegal, sem transparência e aproveitando da necessidade do uso do aplicativo pelo titular dos dados.

A grande questão é: em que medida as justificativas de aprimoramento e confiabilidade apresentadas pelo Poder Público[166] ao instituir as grandes bases de

---

[163] ABREU, Jacqueline de Souza; LAGO, Lucas; MASSARO, Heloisa. Por que se preocupar com o que o Estado faz com nossos dados pessoais?. **Internet Lab**, 2018. Disponível em: <https://www.internetlab.org.br/pt/privacidade-e-vigilancia/especial-apps-do-governo/>. Acesso em 08.11.2020.

[164] Nos aplicativos ANATEL Consumidor, CNH Digital, EMTU, Metrô SP, Nota Fiscal Paulista e DENATRAN não foi possível encontrar tal menção. IN: ABREU, Jacqueline de Souza; LAGO, Lucas; MASSARO, Heloisa. Por que se preocupar com o que o Estado faz com nossos dados pessoais?. **Internet Lab**, 2018. Disponível em: <https://www.internetlab.org.br/pt/privacidade-e-vigilancia/especial-apps-do-governo/>. Acesso em 08.11.2020.

[165] FERREIRA, Heline Sivini. A dimensão ambiental da teoria da sociedade de risco. In: FERREIRA, Heline Sivini; Freitas, Cinthia Obladen de Almendra (orgs). **Direito Socioambiental e Sustentabilidade**: Estados, Sociedades e Meio Ambiente. Curitiba: Letra da Lei, 2016. p. 108-158.

[166] Decreto nº 10.046: Art. 16. Fica instituído o Cadastro Base do Cidadão com a finalidade de:
I - aprimorar a gestão de políticas públicas;
II - aumentar a confiabilidade dos cadastros de cidadãos existentes na administração pública, por meio de mecanismos de manutenção da integridade das bases de dados para torná-las qualificadas e consistentes;

dados são de fato verdadeiras e necessárias ou se está diante de um exercício do poder de polícia abusivo utilizando-se da política simbólica?

Enfim, os grandes cadastros e bancos de dados do Estado já estão operantes, ainda que considerados ilegais por muitos, razão pela qual a adoção de medidas de controle dos dados pelos titulares – individuais ou coletivas – se apresentam extremamente necessárias.

Como se viu anteriormente, resta nítido que deve o Poder Público respeitar as bases legais da LGPD (consentimento, cumprimento de obrigação legal, execução de contrato, interesse legítimo, processo judicial, crédito, proteção à vida, tutela da saúde, pesquisa e política pública), razão pela qual qualquer incompatibilidade deve ser objeto de discordância.

3.4. COMPARTILHAMENTO

Considerando a vasta gama de dados em poder do Estado, além da preocupação com a forma de tratamento e uso, um dos principais perigos reside no compartilhamento desses dados, seja entre os próprios entes e órgãos, seja com pessoas jurídicas de direito privado.

Isso porque "modelos de governos tecnocratas, visando alcançar seus ideais de eficiência, enxergam no compartilhamento de bancos de dados um bem em si mesmo." Com isso, "mostra-se um perigoso caminho rumo ao intercâmbio de dados pessoais sem que se considerem contrapesos e salvaguardas."[167]

O compartilhamento é permitido pela LGPD, nos termos dos artigos 25 e 26:

> Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.
> Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

III - viabilizar a criação de meio unificado de identificação do cidadão para a prestação de serviços públicos;
IV - disponibilizar uma interface unificada de atualização cadastral, suportada por soluções tecnológicas interoperáveis das entidades e órgãos públicos participantes do cadastro;
V - facilitar o compartilhamento de dados cadastrais do cidadão entre os órgãos da administração pública; e
VI - realizar o cruzamento de informações das bases de dados cadastrais oficiais a partir do número de inscrição do cidadão no CPF.

[167] COPETTI, Rafael; CELLA, José Renato. A salvaguarda da privacidade e a autoridade nacional de proteção de dados. **Revista de direito, governança e novas Tecnologias**, v.5, n.1, p. 44-62, jan./jun., 2019, p. 45.

> § 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:
> I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);
> II - (VETADO);
> III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.
> IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou
> V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades.
> § 2º Os contratos e convênios de que trata o § 1º deste artigo deverão ser comunicados à autoridade nacional.

Dessa forma, nota-se que para LGPD o compartilhamento de dados pelo Poder Público é tido como regra, que inclusive prescinde de consentimento mesmo quando estiver tratando de dados sensíveis (art. 11, II, b, LGPD[168]).

O tratamento de dados pelo Poder Público e o uso compartilhado é expressamente autorizado pela LGPD quando visando a execução de uma política pública ou de um serviço público, respaldados em leis, regulamentos, convênios, contratos, qualquer tipo de instrumento (art. 7, III, LGPD). Ou seja, é ampla a possibilidade de compartilhamento de dados pela administração pública.

No compartilhamento de dados, conforme prevê o *caput* do artigo 26, da LGPD, consta expressamente a necessidade de observância aos princípios elencados no artigo 6º, da mesma lei, quais sejam: finalidade, adequação, necessidade, livre acesso, qualidade de dados, transparência, segurança, não discriminação, prevenção, responsabilização e prestação de contas.

No mesmo artigo 26, a LGPD traz em seus parágrafos a proibição de compartilhamento com entidades privadas, porém, elenca nos incisos algumas exceções como nos casos de: descentralização da atividade pública, dados de acesso público, previsão contratual, prevenção de fraudes e proteção do titular de dados. Nesses casos, seria prescindível o consentimento do titular, bem como desnecessário informar a ANPD, o que não está de acordo nem mesmo com os princípios da Lei.

---

[168] Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

Quando o compartilhamento se der entre os entes do Poder do Público e entes da iniciativa privada, haverá tanto a necessidade de consentimento – respeitadas as exceções do artigo 7º –, bem como prestar informações à ANPD, conforme dispõe o artigo 27 da LGPD:

> Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto:
> I - nas hipóteses de dispensa de consentimento previstas nesta Lei;
> II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; ou
> III - nas exceções constantes do § 1º do art. 26 desta Lei.
> Parágrafo único. A informação à autoridade nacional de que trata o caput deste artigo será objeto de regulamentação.

Contudo, as exceções dos incisos I, II e III, permitem o compartilhamento sem consentimento e sem informação à ANPD, o que nitidamente representa um risco aos titulares de dados, em especial, porque as hipóteses elencadas no § 1º do artigo 26, compreendem uma enorme gama de exceções à vedação, sendo uma delas a existência de previsão legal.

Aparentemente, a autorização legal poderia ser vista como de alta confiança jurídica, porém, na prática, não é o que tem ocorrido, com a publicação de Decretos pelo Poder Executivo que trazem dispositivos antagônicos à LGPD.

Em 2016, foi editado o Decreto nº 8.789, que dispunha sobre o compartilhamento de dados na administração pública federal. Contudo, tal Decreto foi revogado com a edição do Decreto nº 10.046/2019, que alterou de forma significativa os termos anteriormente dispostos sobre o tema.

Pode-se dizer que o atual Decreto (vigente) ampliou o compartilhamento de dados entre os órgãos e as entidades da administração pública federal direta, autárquica e fundacional e os demais Poderes da União, conforme as finalidades elencadas no artigo 1º:

> I - simplificar a oferta de serviços públicos;
> II - orientar e otimizar a formulação, a implementação, a avaliação e o monitoramento de políticas públicas;
> III - possibilitar a análise das condições de acesso e manutenção de benefícios sociais e fiscais;
> IV - promover a melhoria da qualidade e da fidedignidade dos dados custodiados pela administração pública federal; e
> V - aumentar a qualidade e a eficiência das operações internas da administração pública federal.

As exceções ao artigo primeiro seriam: o compartilhamento de dados com os conselhos de fiscalização de profissões regulamentadas e com o setor privado, bem

como os dados protegidos por sigilo fiscal geridos pela Receita Federal, conforme disposto na legislação.

As diretrizes para o compartilhamento estão previstas no artigo 3º do Decreto, que confirmam o amplo compartilhamento da informação para facilitar a execução de políticas públicas, devendo o ato observar os requisitos de segurança, de coleta e tratamento previstos na LGPD. Ainda, impõe assunção pelo recebedor dos dados de deveres de sigilo e auditoria e reforça a preservação da intimação e privacidade da pessoa natural.

O compartilhamento de dados entre os órgãos e entidades da Administração Pública é caracterizado por 3 níveis, [169] definidos de acordo com a sua confidencialidade: amplo, restrito e específico. Porém, o §7º deixa claro que o compartilhamento amplo deve ser priorizado.

Ocorre que, através do referido Decreto, ficou instituído o cadastro base do cidadão, que apresenta finalidades (previstas em seu artigo 16) [170] totalmente genéricas e que visam unicamente acumular grande número de dados para entes da administração pública, sem observar o princípio da necessidade.

A base integradora, além dos 12 atributos biográficos e cadastrais elencados no artigo 18, § 1º[171], poderá ser acrescida de outros dados que sequer especificados

---

[169] BRASIL. Governo Digital. **Compartilhamento de Dados**, 2019. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/compartilhamento-de-dados>. Acesso em 28.12.2020.

[170] Art. 16. Fica instituído o Cadastro Base do Cidadão com a finalidade de:
I - aprimorar a gestão de políticas públicas;
II - aumentar a confiabilidade dos cadastros de cidadãos existentes na administração pública, por meio de mecanismos de manutenção da integridade das bases de dados para torná-las qualificadas e consistentes;
III - viabilizar a criação de meio unificado de identificação do cidadão para a prestação de serviços públicos;
IV - disponibilizar uma interface unificada de atualização cadastral, suportada por soluções tecnológicas interoperáveis das entidades e órgãos públicos participantes do cadastro;
V - facilitar o compartilhamento de dados cadastrais do cidadão entre os órgãos da administração pública; e
VI - realizar o cruzamento de informações das bases de dados cadastrais oficiais a partir do número de inscrição do cidadão no CPF.

[171] Art. 18. A base integradora será, inicialmente, disponibilizada com os dados biográficos que constam da base temática do CPF.
§ 1º Os atributos biográficos e cadastrais que inicialmente comporão a base integradora serão, no mínimo, os seguintes:
I - número de inscrição no CPF;
II - situação cadastral no CPF;
III - nome completo;
IV - nome social;
V - data de nascimento;
VI - sexo;

no Decreto. Ou seja, deixa “em aberto” os dados que poderão ser inseridos na base e manipulados, o que vai totalmente contra aos princípios da LGPD.

Ainda, o Decreto cria um Comitê Central de Governança de Dados, ignorando completamente as atribuições e competências da ANPD.

A notável incompatibilidade do Decreto nº 10.046 com a LGPD é o fundamento principal dos projetos de lei que visam sustar seus efeitos. Veja-se alguns argumentos apontados em relação ao compartilhamento de dados no PDL 675/2019: [172]

> A norma se diz compatível com a Lei Geral de Proteção de Dados (LGPD - Lei n° 13.709/2018), principal legislação sobre o tema, aprovada em 2018 e que entrará em vigor em agosto de 2020. Entretanto, ao estabelecer regras para o compartilhamento de dados entre os órgãos da Administração Pública, o texto colide frontalmente com o disposto na lei, desconsiderando fundamentos como a autodeterminação informativa dos cidadãos (art. 2º, II) e o respeito aos direitos humanos, ao livre desenvolvimento da personalidade, à dignidade e ao exercício da cidadania pelas pessoas naturais (Art 2º, VII). Além disso, faz uso de terminologias completamente estranhas à LGPD, como "atributos biográficos" e "atributos biométricos."
> [...]
> Ao criar o Comitê Central de Governança de Dados, o decreto desconsidera a tradição brasileira de discussão de assuntos dedicados à Internet mediante ampla participação social, facilitada por mecanismos de participação multissetorial, como o Comitê Gestor da Internet (CGI.br) ou o recém-sancionado Conselho Nacional de Proteção de Dados e da privacidade (CNPD). Além de excluir a possibilidade de participação multissetorial e concentrar a participação no Comitê Central de Governança exclusivamente de entes da Administração Pública Federal, o decreto ainda concentra neste colegiado a resolução de controvérsias no compartilhamento de dados entre os órgãos e entidades públicas federais sem estabelecer critérios claros para a resolução de tais conflitos. Entende-se que algumas das competências atribuídas ao Comitê são conflitantes com as estabelecidas à Autoridade Nacional de Proteção de Dados no âmbito da Lei 13.709/2018. Por ser a autoridade, o órgão responsável por fornecer diretrizes e orientações a respeito de atividades de tratamento de dados em todo o território nacional e para os entes da Administração Pública, a atuação do comitê previsto no decreto deveria ser subsidiária às orientações formuladas pelo órgão central.

O compartilhamento de forma ampla, faz com que o dado coletado em um órgão público específico e, portanto, possivelmente, dotado de um consentimento específico, seja passível de ser consultado e/ou utilizado por diversos outros órgãos do Poder Público.

VII - filiação;
VIII - nacionalidade;
IX - naturalidade;
X - indicador de óbito;
XI - data de óbito, quando cabível; e
XII - data da inscrição ou da última alteração no CPF.

[172] BRASIL. Câmara dos Deputados. **PDL 675/2019**. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1824574&filename=PDL+675/2019>. Acesso em 28.12.2020.

Enfim, verifica-se que o Decreto, em desconformidade com a LGPD abriu brechas para o Poder Público, especialmente, ao permitir o indiscriminado compartilhamento de dados.

O artigo 25 da LAI, prevê que “é dever do Estado controlar o acesso e a divulgação de informações sigilosas produzidas por seus órgãos e entidades, assegurando a sua proteção”, porém, não há como garantir a existência de uma proteção quando o dado possui destino diverso da coleta.

Dessa forma, o fato de normas legais poderem ser facilmente editadas (autorizando o interesse do controlador/Estado), principalmente, pelo Poder Executivo, pode impactar de forma contundente na aplicação da LGPD frente ao Poder Público, já que a existência de previsão legal acaba por autorizar o compartilhamento sem o consentimento do titular de dados para finalidades diversas do momento da coleta.

4. RESPONSABILIDADE CIVIL DO ESTADO EM RAZÃO DA VIOLAÇÃO AOS DADOS SOB SEU DOMÍNIO

Conforme aduzido no capítulo anterior, o Poder Público é responsável pelos dados pessoais por ele coletados, tratados, utilizados e compartilhados.

O artigo 2º da LGPD[173], prevê como um dos 10 princípios nele elencados, o princípio da responsabilização, no qual "os agentes de tratamento deverão demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, inclusive da eficácia das medidas."[174].

Tal princípio foi inspirado na *Consideranda* nº 146 do Regulamento Geral de Proteção de Dados Europeu (GDPR), que dispõe:

> 146. O responsável pelo tratamento ou o subcontratante deverão reparar quaisquer danos de que alguém possa ser vítima em virtude de um tratamento que viole o presente regulamento responsável pelo tratamento. O responsável pelo tratamento ou o subcontratante pode ser exonerado da responsabilidade se provar que o facto que causou o dano não lhe é de modo algum imputável. O conceito de dano deverá ser interpretado em sentido lato à luz da jurisprudência do Tribunal de Justiça, de uma forma que reflita plenamente os objetivos do presente regulamento. Tal não prejudica os pedidos de indemnização por danos provocados pela violação de outras regras do direito da União ou dos Estados-Membros. Os tratamentos que violem o presente regulamento abrangem igualmente os que violem os atos delegados e de execução adotados nos termos do presente regulamento e o direito dos Estados-Membros que dê execução a regras do presente regulamento. Os titulares dos dados deverão ser integral e efetivamente indemnizados pelos danos que tenham sofrido. Sempre que os responsáveis pelo tratamento ou os subcontratantes estiverem envolvidos no mesmo tratamento, cada um deles deverá ser responsabilizado pela totalidade dos danos causados. Porém, se os processos forem associados a um mesmo processo judicial, em conformidade com o direito dos Estados-Membros, a indemnização poderá ser repartida em função da responsabilidade que caiba a cada responsável pelo tratamento ou subcontratante pelos danos causados em virtude do tratamento efetuado, na condição de ficar assegurada a indemnização integral e efetiva do titular dos dados pelos danos que tenha sofrido. Qualquer responsável pelo tratamento ou subcontratante que tenha pago uma indenização integral, pode posteriormente intentar uma ação de regresso contra outros responsáveis pelo tratamento ou subcontratantes envolvidos no mesmo tratamento. (Tradução Livre pela Autora)

---

[173] Desde já, cumpre ressaltar que são agentes de tratamento o controlador e o operador, nos termos da LGPD.

[174] FEIGELSON, Bruno. SIQUEIRA, Antonio. **Comentários à Lei Geral de Proteção de dados.** São Paulo: Thompson Reuters Brasil, 2019. P. 43-44.

Contudo, a LGPD não foi didática ao tratar da responsabilidade civil do Estado no caso de dano decorrente do tratamento de dados pessoais.

Em seus artigos 31 e 32, na Seção intitulada como “Responsabilidade”, limita-se a tratar de diretrizes genéricas para Autoridade Nacional de Proteção de Dados (ANDP):[175]

> Art. 31. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.
> Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

Ou seja, apesar do título, a Seção I do Capítulo IV, da LGPD, não dispõe de forma direta como se dará a responsabilidade civil e penal do ente de Direito Público ao infringir a lei, causando dano ao titular de dados.

O capítulo específico das sanções, Seção I do Capítulo VIII da LGPD, limita-se a prever as sanções administrativas decorrentes da violação aos direitos nela consagrados.

Veja-se as sanções previstas na LGPD, após regular processo administrativo, as quais estão listadas no artigo 52, da LGPD:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III - multa diária, observado o limite total a que se refere o inciso II;
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - eliminação dos dados pessoais a que se refere a infração;
> VII - (VETADO);
> VIII - (VETADO);
> IX - (VETADO).
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

[175] Entidade fiscalizadora nos termos dos artigos 55 e ss da LGPD.

Contudo, o parágrafo 3º do referido artigo, afasta expressamente os incisos que preveem a incidência de multa para o Poder Público:

> § 3º O disposto nos incisos I, IV, V, VI, X, XI e XII do **caput** deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011.

Portanto, o Poder Público não é punido com multa, bem como receberá penalidades mais brandas do que aquelas passíveis de aplicação às pessoas jurídicas de direito privado. De todo modo, "os agentes do Estado que derem causa à violação da LGPD estão sujeitos às cominações da Lei nº 8.112/1990 (Estatuto do Servidor Público Federal), da Lei nº 8.429/1992 (Lei de Improbidade Administrativa) e da Lei nº 12.527/2011 (Lei de Acesso à Informação)."[176]

Já as empresas públicas e sociedades de economia e todas as pessoas jurídicas de direito privado elencadas no rol do artigo 44 do Código Civil,[177] sujeitam-se à multa.[178]

A impossibilidade de imposição de multa ao Estado se justifica pelo próprio senso de coletividade, de não onerar o contribuinte em razão das falhas do Estado (a Administração Pública é sustentada pelos cidadãos através do recolhimento de impostos), porém, a falta de punição efetiva e sancionadora pode servir como estímulo para o não cumprimento da norma pelo Poder Público.

Norberto Bobbio define a sanção como "o expediente através do qual se busca, em um sistema normativo, salvaguardar a lei da erosão de ações contrárias", é,

---

[176] ZARDO, Francisco. As sanções administrativas de multa simples e multa diária na LGPD. In: DAL POZZO, Augusto Neves E MARTINS, Ricardo Marcondes (coords.). **LGPD & Administração Pública**. São Paulo: Thomson Reuters Brasil, 2020. p. 701.

[177] Art. 44. São pessoas jurídicas de direito privado:
I - as associações;
II - as sociedades;
III - as fundações.
IV - as organizações religiosas;
V - os partidos políticos.
VI - as empresas individuais de responsabilidade limitada.

[178] ZARDO, Francisco. As sanções administrativas de multa simples e multa diária na LGPD. In: DAL POZZO, Augusto Neves E MARTINS, Ricardo Marcondes (coords.). **LGPD & Administração Pública**. São Paulo: Thomson Reuters Brasil, 2020. p. 701.

portanto, “a reposta à violação.”[179] Assim, a sanção está relacionada à eficácia da norma.[180]

Para Hans Kelsen, “o estabelecimento de sanções se dá em aplicação do princípio da retribuição, decisivo para o convívio social”, como expressão máxima da Justiça da igualdade. Ou seja, se causar lesão, deverá ser punido (“deve ser-lhe causado um mal”), mas se causar o bem, será recompensado (“deve ser-lhe causado um bem”).[181]

Dessa forma, a ANPD, mesmo sendo um órgão da Administração Pública, precisará punir de forma efetiva o Poder Público quando da violação à proteção de dados pessoais, a fim de dar efetividade à norma.

Aliás, nesse ponto, importante resgatar a notícia mencionada no primeiro capítulo, do site europeu POLICO de que na Europa ocorreu um aumento das discussões envolvendo dados pessoais no Poder Judiciário, justamente em razão da morosidade e de ineficiência das penalidades administrativas.[182]

É bem provável que o Brasil siga o mesmo rumo, momento em que as indenizações arbitradas pelo Poder Judiciário quando da violação à proteção de dados pessoais assumirão papel de extrema relevância, já que serão as únicas capazes de punir financeiramente o Estado, fazendo-o adotar medidas efetivas de *compliance* e salvaguardas a fim de evitar a ocorrência do dano.

Na falta de disposições mais específicas para o Estado, no âmbito da responsabilidade civil[183], só resta aplicar a regra geral prevista na LGPD e as demais normas já existentes no ordenamento jurídico, aplicando o diálogo das fontes.

A LGPD, em seu capítulo VI, dispõe sobre a responsabilidade e o ressarcimento dos danos. Ainda que no referido capítulo não faça qualquer menção ao Poder Público, é evidente que possa ser aplicada já que é cláusula geral e está

---

[179] BOBBIO, Norberto. **Teoria da Norma Jurídica.** Trad. Fernando Pavan Baptista e Ariani Bueno Sudatti. São Paulo: EDIPRO, 2001. p. 153-154.
[180] BOBBIO, Norberto. **Teoria da Norma Jurídica.** Trad. Fernando Pavan Baptista e Ariani Bueno Sudatti. São Paulo: EDIPRO, 2001. p. 167.
[181] KELSEN, Hans. **Teoria Geral das Normas**. Trad. José Fiorentino Duarte. Porto Alegre: Fabris, 1986. p. 173.
[182] MANANCOURT, Vicent. Have a GDPR complaint? Skip the regulator and take it to court. **Politico**. 2020. Disponível em:<https://www.politico.eu/article/have-a-gdpr-complaint-skip-the-regulator-and-take-it-to-court/>. Acesso em 28.12.2020.
[183] Ressalta-se que Celso Antônio Bandeira de Mello utiliza o termo “responsabilidade patrimonial extracontratual do Estado”. MELLO. Celso Antônio Bandeira de. **Curso de Direito Administrativo**. 32ª ed. São Paulo: Malheiros, 2015. P. 1021. Por mera opção terminológica, neste trabalho será utilizado o termo “responsabilidade civil”.

voltada aos agentes de tratamento (controlador e operador). Confira-se o teor do artigo 42:

> 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.
> § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
> § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.
> § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Tratam-se de medidas para assegurar a efetiva reparação (§1º), além de apontar, dois tipos de relações jurídicas que trarão consequências na responsabilidade civil: “i) uma entre o controlador e operador; ii) outra entre os agentes de tratamento com o titular de dados.”[184]

Na primeira hipótese, a previsão legal acerca da solidariedade aponta para a necessidade de que, além do exercício das boas práticas estabelecidas em lei, os controladores saibam escolher bons operadores.[185] Em consonância com o artigo 932, III, do Código Civil, “o empregador ou comitente, por seus empregados, serviçais e prepostos, no exercício do trabalho que lhes competir, ou em razão dele.”

Ademais, a solidariedade é um grande fator para o exercício da segunda hipótese, já que auxilia na identificação do polo passivo da demanda.[186]

---

[184] TORCHIA, Bruno Martins. MACHADO, Tacianny Mayara Silva. A reponsabilidade subjetiva prevista ne lei geral de proteção de dados e a relação jurídica centre controlador e o encarregado de proteção de dados. In: DAL POZZO, Augusto Neves E MARTINS, Ricardo Marcondes (coords.). **LGPD & Administração Pública**. São Paulo: Thomson Reuters Brasil, 2020. P. 833.

[185] TORCHIA, Bruno Martins. MACHADO, Tacianny Mayara Silva. A reponsabilidade subjetiva prevista ne lei geral de proteção de dados e a relação jurídica centre controlador e o encarregado de proteção de dados. In: DAL POZZO, Augusto Neves E MARTINS, Ricardo Marcondes (coords.). **LGPD & Administração Pública**. São Paulo: Thomson Reuters Brasil, 2020. P. 836.

[186] TORCHIA, Bruno Martins. MACHADO, Tacianny Mayara Silva. A reponsabilidade subjetiva prevista ne lei geral de proteção de dados e a relação jurídica centre controlador e o encarregado de proteção de dados. In: DAL POZZO, Augusto Neves E MARTINS, Ricardo Marcondes (coords.). **LGPD & Administração Pública**. São Paulo: Thomson Reuters Brasil, 2020. P. 836.

O artigo 42, da LGPD, também, reforça a regra do Código de Processo Civil relativa à possibilidade de inversão do ônus da prova, que dependerá do caso concreto mediante análise da verossimilhança das alegações e hipossuficiência para fins de prova (§ 2º e artigo 373, § 1º do CPC).

No caso do Poder Público, conforme se verá no próximo tópico, este responde objetivamente pelos danos causados, hipótese em que, habitualmente, o ônus da prova é invertido. Porém, na prática, isso não exime o Autor da ação (titular dos dados ou seu representante no caso de tutela coletiva) de provar o fato constitutivo do direito.[187]

Diante do exposto, é inegável que "a responsabilidade civil em matéria de dados é primordial para o equilíbrio das relações dessa natureza, sobretudo quando envolvida a tecnologia"[188], especialmente, para dados pessoais tratados pelo Estado, a fim de se evitarem abusos diante da vulnerabilidade do cidadão nessa relação jurídica tão desigual.

4.1. DA RESPONSABILIDADE CIVIL OBJETIVA DO ESTADO ENQUANTO AGENTE DE TRATAMENTO DE DADOS PESSOAIS

Nos termos do artigo 37 da Constituição Federal, o Poder Público deve conduzir a sua atividade em estrita obediência aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência.

Assim, desrespeitados tais princípios e decorrendo dano de tal conduta, surge o dever de indenizar. O parágrafo 6º do referido artigo dispõe sobre a responsabilização:

> § 6º As pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa."

---

[187] AGRAVO INTERNO NO AGRAVO EM RECURSO ESPECIAL. CIVIL E PROCESSUAL CIVIL. DIREITO DO CONSUMIDOR. COMPRA E VENDA DE IMÓVEL. DEMORA NA BAIXA DE HIPOTECA. DANO MORAL. DECISÃO MONOCRÁTICA DO RELATOR. NULIDADE. INEXISTÊNCIA. NULIDADE DE JULGAMENTO. AUSÊNCIA DE PREQUESTIONAMENTO. SÚMULAS 282 E 356 DO STF. **INVERSÃO DO ÔNUS DA PROVA. NECESSIDADE DE COMPROVAÇÃO MÍNIMA DOS FATOS ALEGADOS. SÚMULA 83/STJ**. AGRAVO INTERNO DESPROVIDO. **3. "A jurisprudência desta Corte Superior se posiciona no sentido de que a inversão do ônus da prova não dispensa a comprovação mínima, pela parte autora, dos fatos constitutivos do seu direito"** (AgInt no Resp 1.717.781/RO, Rel. Ministro Marco Aurélio Bellizze, Terceira Turma, julgado em 05/06/2018, DJe de 15/06/2018).4. Agravo interno não provido. (AgInt no AREsp 862.624/RJ, Rel. Ministro Raul Araújo, Quarta Turma, julgado em 22/06/2020, DJe 01/07/2020).

[188] BRUNO, Marcos Gomes da Silva. Dos agentes de tratamento de dados pessoais. MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **LGPD**: Lei Geral de Proteção de dados comentada. São Paulo: Thomson Reuters Brasil, 2019. p. 319.

A doutrina e a jurisprudência, aplicando a Constituição Federal, reforçam que a responsabilidade mencionada no dispositivo de lei acima citado é objetiva[189].

Nas palavras de Alexandre de Moraes:

> A Constituição Federal prevê que as pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa. Assim, a responsabilidade civil das pessoas jurídicas de direito público e das pessoas jurídicas de direito privado prestadoras de serviço público baseia-se no risco administrativo, sendo objetiva. Essa responsabilidade objetiva exige a ocorrência dos seguintes requisitos: ocorrência do dano; ação ou omissão administrativa; existência de nexo causal entre o dano e a ação ou omissão administrativa e ausência de causa excludente da responsabilidade estatal.[190]

No mesmo sentido, afirma Celso Antônio Bandeira de Mello:[191]

> No que atina às condições para engajar responsabilidade do Estado, seu posto mais evoluído é a responsabilidade objetiva, a dizer, independente de culpa ou procedimento contrário ao Direito. Essa fronteira também já é território incorporado, em largo trecho, ao Direito contemporâneo. Aliás, no Brasil, doutrina e jurisprudência, preponderantemente, afirmam a responsabilidade objetiva do Estado como regra de nosso sistema, desde a Constituição de 1946 '(art. 194), passando pela Carta de 1967 (art. 105), pela Carta de 1969, dita Emenda 1 à "Constituição" de 1967 (art. 105), cujos dispositivos, no que a isto concerne, equivalem ao atual art. 37, § 6º.

A jurisprudência do STF, também, segue na mesma linha:[192, 193 e 194]

> AGRAVO REGIMENTAL EM RECURSO EXTRAORDINÁRIO COM AGRAVO. INTERPOSIÇÃO EM 03.07.2018. ILEGITIMIDADE PASSIVA DOS AGRAVADOS. INOVAÇÃO RECURSAL. ALEGAÇÃO DE SE TRATAR DE MATÉRIA DE ORDEM PÚBLICA. INADMISSIBILIDADE. RESPONSABILIDADE OBJETIVA DO ESTADO. REEXAME DE MATÉRIA FÁTICA. SÚMULA 279 DO STF. PRECEDENTES. 1(...). 2. A responsabilidade objetiva se aplica às pessoas jurídicas de direito público pelos atos comissivos e omissivos, a teor do art. 37, § 6º, do Texto

---

189 CAHALI, Yussef Said. **Responsabilidade Civil do Estado**. 5ª ed. São Paulo: Revista dos Tribunais, 2014. p. 30.

190 MORAES, Alexandre. **Direito Constitucional.** 33ª ed. São Paulo: Atlas, 2017. p. 281.

191 MELLO. Celso Antônio Bandeira de. **Curso de Direito Administrativo**. 32 ed. São Paulo: Malheiros, 2015. p. 1026-1027.

192 BRASIL. Supremo Tribunal Federal. **Agravo Regimental em Recurso Extraordinário nº 1137891**. Relator: Min. Edson Fachin, Segunda Turma. Julgado em 14/12/2018. Disponível em: < >. Acesso em 02.01.2021.

193 BRASIL. Supremo Tribunal Federal. **Agravo Regimental em Recurso Extraordinário nº 788009**. Relator: Min. DIAS TOFFOLI, Primeira Turma, julgado em 19/08/2014. Disponível em: < http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=6924973>. Acesso em 02.01.2021.

194 BRASIL. Supremo Tribunal Federal. **Agravo Regimental em Recurso Extraordinário nº 662563**. Relator: Min. Gilmar Mendes, Segunda Turma. Julgado em 20/03/2012. Disponível em: < http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=11879845>. Acesso em 02.01.2021.

> Constitucional. Precedentes. 3. O Tribunal de origem assentou a responsabilidade do Recorrente a partir da análise do contexto probatório dos autos e, para se chegar à conclusão diversa daquela a que chegou o juízo a quo, seria necessário o seu reexame, o que encontra óbice na Súmula 279 do STF. 4. Agravo regimental a que se nega provimento, com previsão de aplicação da multa prevista no art. 1.021, § 4º, do CPC.
>
> Agravo regimental no recurso extraordinário. Atividade notarial e de registro. Danos materiais. Responsabilidade objetiva do Estado. Possibilidade. Precedentes. 1. A Suprema Corte já assentou o entendimento de que o Estado responde objetivamente pelos danos causados a terceiros em decorrência da atividade notarial, cabendo direito de regresso contra o causador do dano em caso de dolo ou culpa, nos termos do art. 37, § 6º, da Constituição Federal. 2. Agravo regimental não provido.
>
> Agravo regimental em recurso extraordinário com agravo. 2. Morte de detento sob custódia da Administração Pública. Responsabilidade objetiva do Estado. Art. 37, § 6º, da Constituição Federal. Missão do Estado de zelar pela integridade física do preso. Precedentes do STF. 3. Discussão acerca da existência de culpa do Estado. Necessidade do reexame do conjunto fático-probatório. Súmula 279. 4. Agravo regimental a que se nega provimento.

Contudo, para casos específicos, o STF entende pela possibilidade de "abrandamento" dessa responsabilidade objetiva, confira-se:[195]

> CONSTITUCIONAL E ADMINISTRATIVO. RESPONSABILIDADE CIVIL DO ESTADO. ART. 37, § 6º, DA CONSTITUIÇÃO. PESSOA CONDENADA CRIMINALMENTE, FORAGIDA DO SISTEMA PRISIONAL. DANO CAUSADO A TERCEIROS. INEXISTÊNCIA DE NEXO CAUSAL ENTRE O ATO DA FUGA E A CONDUTA DANOSA. AUSÊNCIA DE DEVER DE INDENIZAR DO ESTADO. PROVIMENTO DO RECURSO EXTRAORDINÁRIO. 1. A responsabilidade civil das pessoas jurídicas de direito público e das pessoas jurídicas de direito privado prestadoras de serviço público baseia-se no risco administrativo, sendo objetiva, exige os seguintes requisitos: ocorrência do dano; ação ou omissão administrativa; existência de nexo causal entre o dano e a ação ou omissão administrativa e ausência de causa excludente da responsabilidade estatal. 2. **A jurisprudência desta CORTE, inclusive, entende ser objetiva a responsabilidade civil decorrente de omissão, seja das pessoas jurídicas de direito público ou das pessoas jurídicas de direito privado prestadoras de serviço público. 3. Entretanto, o princípio da responsabilidade objetiva não se reveste de caráter absoluto, eis que admite o abrandamento e, até mesmo, a exclusão da própria responsabilidade civil do Estado, nas hipóteses excepcionais configuradoras de situações liberatórias como o caso fortuito e a força maior ou evidências de ocorrência de culpa atribuível à própria vítima.** 4. A fuga de presidiário e o cometimento de crime, sem qualquer relação lógica com sua evasão, extirpa o elemento normativo, segundo o qual a responsabilidade civil só se estabelece em relação aos efeitos diretos e imediatos causados pela conduta do agente. **Nesse cenário, em que não há causalidade direta para fins de atribuição de responsabilidade civil extracontratual do Poder Público, não se apresentam os requisitos necessários para a imputação da responsabilidade objetiva prevista na Constituição Federal - em especial, como já citado, por ausência do**

---

[195] BRASIL. Supremo Tribunal Federal**. Recurso Extraordinário nº 608880**. Relator: MARCO AURÉLIO, Relator(a) p/ Acórdão: ALEXANDRE DE MORAES, Tribunal Pleno, julgado em 08/09/2020. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=753981868>. Acesso em 02.01.2021.

> **nexo causal.** 5. Recurso Extraordinário a que se dá provimento para julgar improcedentes os pedidos iniciais. Tema 362, fixada a seguinte tese de repercussão geral: "Nos termos do artigo 37, § 6º, da Constituição Federal, não se caracteriza a responsabilidade civil objetiva do Estado por danos decorrentes de crime praticado por pessoa foragida do sistema prisional, quando não demonstrado o nexo causal direto entre o momento da fuga e a conduta praticada."

Apesar da responsabilidade do Estado ser objetiva, eventual exercício de direito de regresso contra o causador do dano – agente ou servidor – é pautado na responsabilidade subjetiva. Ou seja, deve ser provado o dolo ou culpa em ação autônoma.

Portanto, partindo da premissa de que é indubitável a responsabilidade objetiva do Estado em se tratando de responsabilidade civil, não haveria razão para ser diferente quando essa responsabilidade decorrer de danos ocasionados durante a coleta, armazenamento e tratamento de dados.

Ademais, como visto no tópico 3.2, incide o CDC aos serviços prestados por órgãos públicos e suas empresas, concessionárias, permissionários ou outra forma de empreendimento (art. 22, CDC) e o CDC é a segunda norma mais importante em termos de responsabilidade civil (após o Código Civil).

No capítulo correspondente ao Poder Público e na Seção da responsabilidade (art. 42 e seguintes), a LGPD não indicou expressamente se a responsabilidade seria objetiva ou subjetiva, mas, ao interpretar a norma com as normas já existentes, resta claro que a responsabilidade pelos danos causados pelo Estado quando controlador de dados, será objetiva.

O que significa dizer que "a pessoa jurídica de direito público responde sempre, uma vez que se estabeleça nexo de causalidade entre o ato da Administração e o prejuízo sofrido". Dessa forma, "não há que cogitar se houve ou não culpa, para concluir pelo dever de reparação".[196]

A responsabilidade civil do Estado está fundada na "Teoria do Risco", na qual o Estado assume todos os riscos causados no desempenho de suas atividades. Ou seja, "a atividade do Estado não deve causar problemas ao particular, e, se assim o fizer, o particular merece ser indenizado pelo prejuízo."[197]

---

[196] PEREIRA, Caio Mário da Silva (atualizador Gustavo Tepedino). **Responsabilidade civil**. 11ª ed. Rio de Janeiro: Forense, 2016. p. 179-180.

[197] NERY, Rosa Maria de Andrade; NERY JÚNIOR, Nelson**. Instituições de Direito Civil**: volume II: Das obrigações, dos contratos e da responsabilidade civil. 2ª ed. São Paulo: Thompson Reuters Brasil, 2019. p. 432.

Assim, “quando uma pessoa sofre um ônus maior do que o suportado pelas demais, rompe-se o equilíbrio que necessariamente deve haver entre os encargos sociais, para reestabelecer esse equilíbrio, o Estado deve indenizar o prejudicado, utilizando recursos do erário.”[198]

De acordo com Maria Sylvia Zanella Di Pietro, na Teoria do Risco:[199]

> ideia de culpa é substituída pela de **nexo de causalidade** entre o funcionamento do serviço público e o prejuízo sofrido pelo administrado. É indiferente que o serviço público tenha funcionado bem ou mal, de forma regular ou irregular. Constituem pressupostos da responsabilidade objetiva do Estado: (a) que seja praticado um ato lícito ou ilícito, por agente público; (b) que esse ato cause **dano específico** (porque atinge apenas um ou alguns membros da coletividade) e **anormal** (porque supera os inconvenientes normais da vida em sociedade, decorrentes da atuação estatal); (c) que haja um nexo de causalidade entre o ato do agente público e o dano.
> É chamada teoria da **responsabilidade objetiva**, precisamente por prescindir da apreciação dos elementos subjetivos (culpa ou dolo); é também chamada **teoria do risco,** porque parte da ideia de que a atuação estatal envolve um risco de dano, que lhe é inerente.

Nesse contexto, o Estado, ao violar as normas da LGPD, além das sanções administrativas que poderão ser aplicadas pela Autoridade Nacional de Proteção de Dados – reforça-se aqui, que a essa autoridade é integrada por membros indicados e nomeados pelo Poder Executivo (com a aprovação do Poder Legislativo – Senado Federal), nos termos do artigo 55-D, §1º da LGPD -, nada impede do lesado, que suportou o dano decorrente da violação (ação ou omissão) ingresse no Poder Judiciário em busca da reparação do dano.

E, em se tratando de proteção de dados, os riscos são vários e iminentes, muito mais comum do que se pode imaginar.

De acordo com as análises do *Computer Securty Incident Response Team*, que em português significa Grupo de Resposta a Incidentes de Segurança, conhecido como CTIR GOV, que monitora as ocorrências de incidentes de segurança junto ao Governo Brasileiro, constata-se que de 2011 para 2020 houve um aumento considerável no número de eventos ligados ao vazamento de dados, de 20 casos em 2011 para 406 no ano de 2020.[200]

---

[198] PIETRO, Maria Sylvia Zanella Di. **Direito Administrativo**. [Recurso Eletrônico] 31ª ed. Rio de Janeiro: Forense, 2018. Não paginado.
[199] PIETRO, Maria Sylvia Zanella Di. **Direito Administrativo**. [Recurso Eletrônico] 31ª ed. Rio de Janeiro: Forense, 2018. Não paginado.
[200] BRASIL. Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo. **Incidentes**, 2020. Disponível em: <https://emnumeros.ctir.gov.br/incidentes/>. Acesso em 10.01.2020.

Referido Grupo é responsável por disponibilizar as “estatísticas resultantes do trabalho de detecção, triagem, análise e resposta a incidentes cibernéticos”[201] do Governo do Brasil.

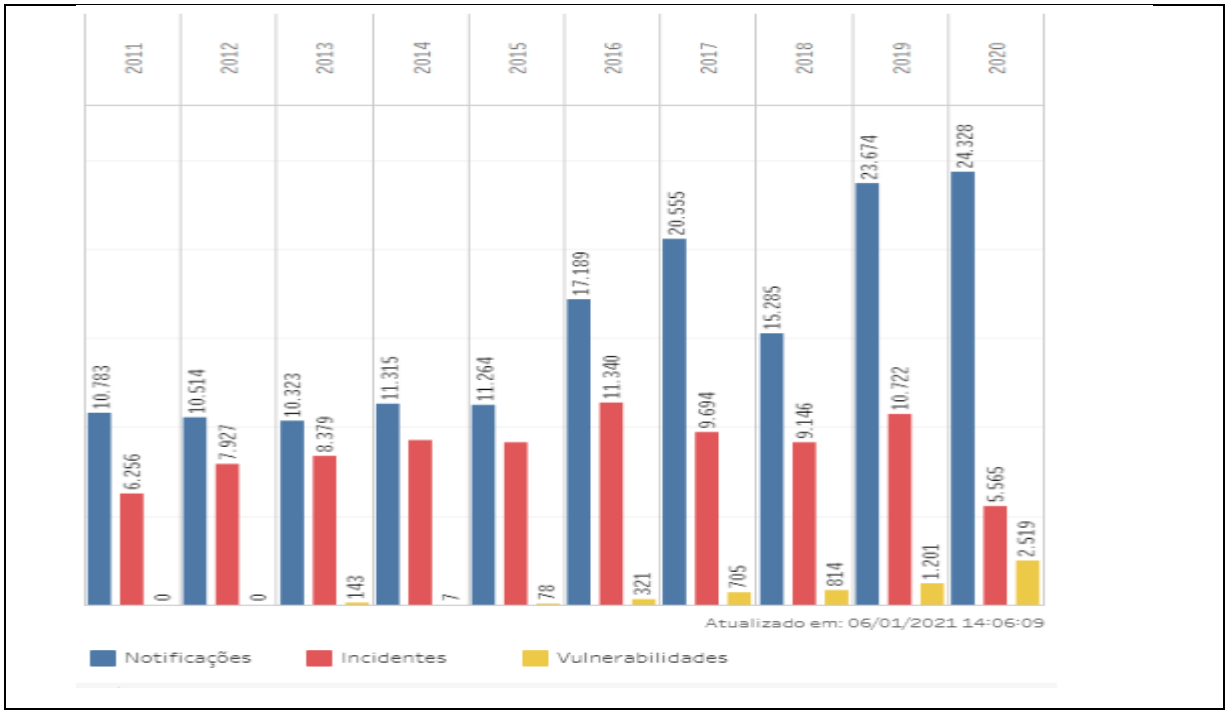
As apurações realizadas pelo CTIR Gov auxiliam na determinação de “tendências e padrões de atividades de ataques e para recomendar estratégias de prevenção adequadas.”[202] Além do mais, a CTIR Gov visa “disponibilizar essas estatísticas em um ambiente que simplifica o acesso e compreensão dos dados, utilizando-se de relatórios interativos e uma interface visual mais amigável.”[203]

Os incidentes ocorridos no País são colacionados e categorizados, o que permite apurar o número de eventos relacionados à segurança da informação, o que tem aumentado mesmo com a utilização de novas tecnologias e de mecanismos de segurança da informação, o que significa dizer que os dados que estão sob o controle do Estado estão em constante ameaça, como abusos, vazamentos e/ou fraudes.

Confira-se os gráficos abaixo que demonstram as estatísticas apuradas de notificações reportadas, incidentes e vulnerabilidades cibernéticos no Governo do Brasil desde 2011 até 2020:[204]

Figura 2 – Gráfico de Notificações e Incidentes do Governo Brasileiro:

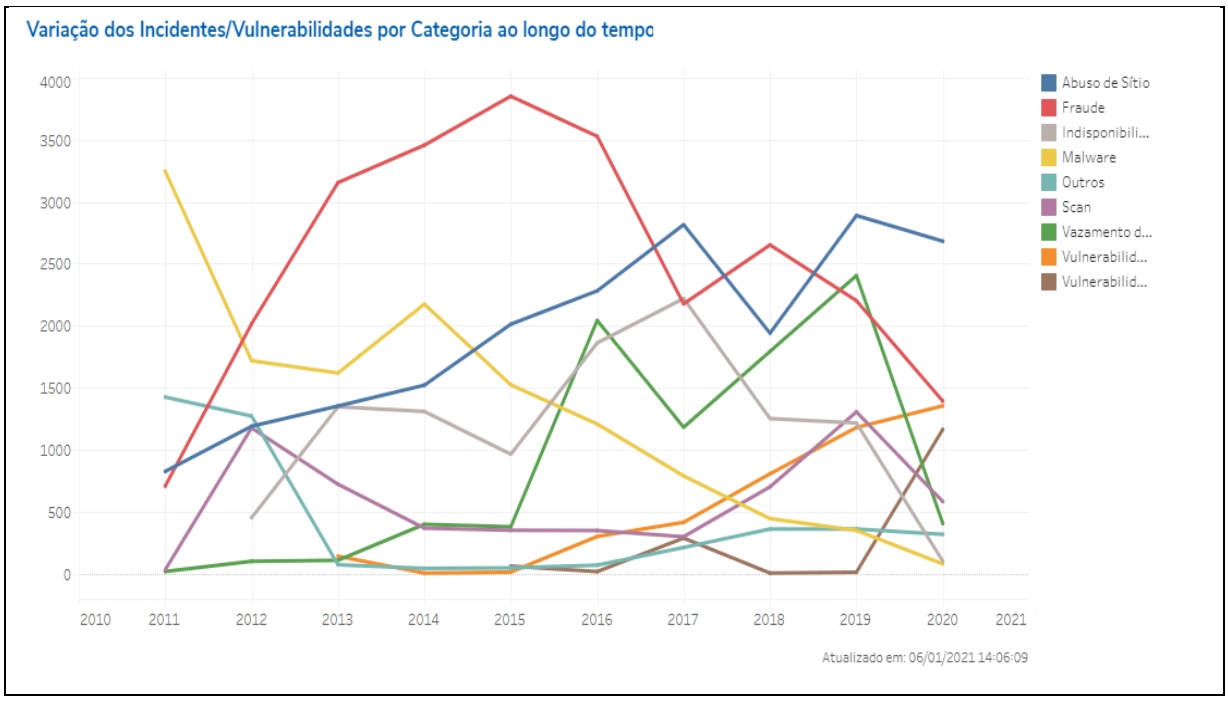
[201] BRASIL. Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo. **Sobre**, 2020. Disponível em: <https://www.ctir.gov.br/sobre/>. Acesso em 05.10.2020.
[202] BRASIL. Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo. **Estatísticas resultantes do trabalho de detecção, triagem, análise e resposta a incidentes cibernéticos**, 2020. Disponível em: <https://emnumeros.ctir.gov.br/>. Acesso em 05.10.2020.
[203] BRASIL. Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo. **Estatísticas resultantes do trabalho de detecção, triagem, análise e resposta a incidentes cibernéticos**, 2020. Disponível em: <https://emnumeros.ctir.gov.br/>. Acesso em 05.10.2020.
[204] BRASIL. Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo. **Estatísticas resultantes do trabalho de detecção, triagem, análise e resposta a incidentes cibernéticos**, 2020. Disponível em: <https://emnumeros.ctir.gov.br/>. Acesso em 05.10.2020.



FONTE: BRASIL. Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo. **Estatísticas resultantes do trabalho de detecção, triagem, análise e resposta a incidentes cibernéticos**, 2020. Disponível em: <https://emnumeros.ctir.gov.br/>. Acesso em 05.10.2020.

Ao detalhar os incidentes, os mesmos são divididos em 7 categorias (indisponibilidade, abuso de sítio, vazamento de informação, fraude, Scan, outros e Malware) que tiveram a seguinte variação ao longo dos últimos 9 anos:

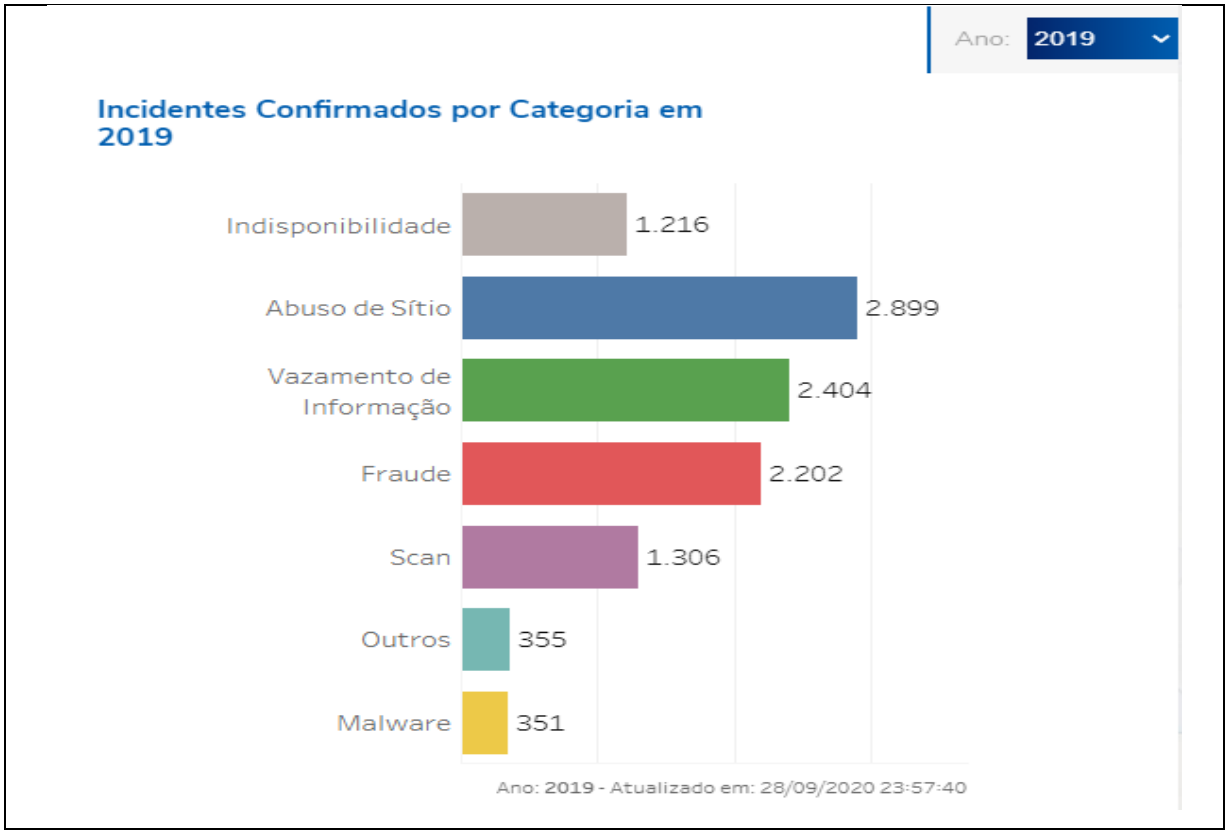
Figura 3 – Categoria dos Incidentes:



FONTE: BRASIL. Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo. **Estatísticas resultantes do trabalho de detecção, triagem, análise e resposta a incidentes cibernéticos**, 2020. Disponível em: <https://emnumeros.ctir.gov.br/>. Acesso em 05.10.2020.

Por exemplo, apenas em 2019, foram mais de 10.722 (dez mil setecentos e vinte e dois) incidentes ocorridos em face do Governo Brasileiro[205] os quais podem ser individualizados nas 7 categorias:

Figura 4 – Categoria dos Incidentes Ocorridos em 2019:



FONTE: BRASIL. Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo. **Incidentes**, 2020. Disponível em: <https://emnumeros.ctir.gov.br/incidentes/>. Acesso em 10.01.2020.

Na categoria de vazamento da informação, foram mais de 2.400 casos, porém, não se sabe dizer o que foi objeto do vazamento, se foi uma lista toda envolvendo diversos titulares de dados ou se cada vazamento corresponde à um único dado vazado.

[205] BRASIL. Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo. **Incidentes**, 2020. Disponível em: <https://emnumeros.ctir.gov.br/incidentes/>. Acesso em 10.01.2020.

Todas as 7 categorias são perigosas e são capazes de ensejar danos aos titulares de dados, especialmente o ataque do tipo *Malware* que decorre de:[206]

> software malicioso" (em inglês, malicious software) e se refere a um tipo de programa de computador desenvolvido para infectar o computador de um usuário legítimo e prejudicá-lo de diversas formas. O malware pode infectar computadores e dispositivos de várias maneiras, além de assumir diversas formas, entre elas vírus, worms, cavalos de Troia, spyware e outros. (...)

Trata-se de uma iniciativa criminosa, em que os criminosos bloqueiam o uso dos dados, tornando-os inacessíveis mediante pagamento de resgate ou não. Além do acesso aos dados, os criminosos podem utilizar os dados como produtos no mercado negro.[207]

No que tange aos efeitos do ataque há diferença técnica entre o *malware e o ransomware*, enquanto o ataque *malware* visa danificar ou desativar o sistema, o ataque *ransomware* se opera mediante a criptografia dos dados que somente após o pagamento do resgate tem sua chave de descodificação liberada.[208]

Aliás, recentemente, em 03/11/2020, o Superior Tribunal de Justiça – STJ sofreu um ataque *hacker,* considerado como "o pior ataque cibernético realizado contra a rede de tecnologia da informação de uma instituição pública brasileira."[209] Contudo, o Superior Tribunal de Justiça não confirmou se foi solicitado resgate pelos hackers, razão pela qual não há como se afirmar se o ataque foi da modalidade *malware* ou *ransomware*.

Em 2019, foram 351 incidentes decorrentes de ataques *malware* em sistemas do governo brasileiro, em 2020, foram 81 casos de ataque. Contudo, não se sabe qual a dimensão e proporção de dados coletados em cada um desses ataques.[210]

---

[206] KASPERSKI. **Aprenda sobre malware e como proteger todos os seus dispositivos contra eles**. Disponível em: <https://www.kaspersky.com.br/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it>. Acesso em 05/01/2021.

[207] KASPERSKI. **Aprenda sobre malware e como proteger todos os seus dispositivos contra eles**. Disponível em: <https://www.kaspersky.com.br/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it>. Acesso em 05/01/2021.

[208] CONVERGÊNCIA DIGITAL. **Ransomware e malware**: Entenda quais são as diferenças. 2017 Disponível em: <https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=45889&sid=18#:~:text=A%20diferen%C3%A7a%20entre%20um%20ransomware,%22Todos%20correm%20o%20risco>. Acesso em 10.10.2021.

[209] BRASIL. Superior Tribunal de Justiça. **STJ Notícias destaca reforço na segurança de informações digitais do tribunal após o ataque hacker**. 2020. Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/04122020-STJ-Noticias-destaca-reforco-na-seguranca-de-informacoes-digitais-do-tribunal-apos-o-ataque%E2%80%AFhacker.aspx>. Acesso em 10/01/2021.

[210] BRASIL. Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo. **Incidentes**, 2020. Disponível em: <https://emnumeros.ctir.gov.br/incidentes/>. Acesso em 10.01.2020.

Ainda que se tenha um sistema de *backup* e que o sistema possa ser prontamente reestabelecido – ou em poucos dias como ocorreu no caso do STJ,[211] importante investigar como se deu o acesso ao sistema e para onde foram enviados os dados, bem como dimensionar os prejuízos dele resultantes.

Caso tais dados extraídos indevidamente dos sistemas do Governo, causem danos ao titular dos dados, haverá necessidade de ampla análise e debate acerca da responsabilidade objetiva da administração pública em relação a eles.

A teoria que “mitiga” a responsabilidade objetiva e desloca a análise para o âmbito da causalidade tende a ser a mais adequada para casos envolvendo violação de dados pessoais em poder do Estado.

Tal teoria foi difundida por Yussef Said Cahali, que entende que seja qual for a subdivisão de nomenclatura acerca da responsabilidade objetiva, deve ser permitido o exame das excludentes da responsabilidade ou das causas concorrentes na verificação do dano.[212]

Já Hely Lopes Meirelles, na edição atualizada por José Emmanuel Burle Filho, aponta a existência de duas modalidades dentro da teoria do risco (enseja a responsabilidade objetiva), a do risco administrativo e a do risco integral:[213]

> a teoria do *risco administrativo,* embora dispense a prova da culpa da Administração, permite que o Poder Público demonstre a culpa da vítima para excluir ou atenuar a indenização. Isto porque o *risco administrativo* não se confunde com o *risco integral.* O *risco administrativo* não significa que a Administração deva indenizar sempre e em qualquer caso o dano suportado pelo particular; significa, apenas e tão somente, que a vítima fica dispensada da prova da culpa da Administração, mas esta poderá demonstrar a culpa total ou parcial do lesado no evento danoso, caso em que a Fazenda Pública se eximirá integral ou parcialmente da indenização.
> [...]
> *teoria do risco integral* é a modalidade extremada da doutrina do *risco administrativo,* abandonada na prática, por conduzir ao abuso e à iniquidade social. Por essa fórmula radical, a Administração ficaria obrigada a indenizar todo e qualquer dano suportado por terceiros, ainda que resultante de culpa ou dolo da vítima. Daí por que foi acoimada de "brutal", pelas graves consequências que haveria de produzir se aplicada na sua inteireza.

Maria Sylvia Zanella Di Pietro, coloca fim na discussão e afirma que:[214]

---

[211] Presidente do STJ diz que foi alertado sobre possibilidade de novo ataque hacker. **ESBRASIL**, 11 de novembro de 2020. Disponível em: <https://esbrasil.com.br/presidente-do-stj-diz-que-foi-alertado-sobre-possibilidade-de-novo-ataque-hacker/>.Acesso em 10/01/2021.

[212] CAHALI, Yussef Said. **Responsabilidade Civil do Estado**. 5ª ed. São Paulo: Revista dos Tribunais, 2014. p. 39.

[213] MEIRELLES, Hely Lopes; FILHO, José Emmanuel Burle. **Direito administrativo brasileiro**. 42ª ed. São Paulo: Malheiros, 2016. p. 781/782.

[214] PIETRO, Maria Sylvia Zanella Di. **Direito Administrativo**. 31ª ed. Rio de Janeiro: Forense, 2018. P. 892.

> não é demais repetir que as divergências são mais terminológicas, quanto à maneira de designar as teorias, do que de fundo. Todos parecem concordar em que se trata de responsabilidade **objetiva**, que implica averiguar se o dano teve como **causa** o funcionamento de um serviço público, sem interessar se foi regular ou não. Todos também parecem concordar em que algumas circunstâncias excluem ou diminuem a responsabilidade do Estado.

Marçal Justen Filho entende que há objetivação do elemento subjetivo, isto é, "não há responsabilidade civil objetiva do Estado, mas há presunção de culpabilidade derivada da existência de um dever de diligência especial."[215]

Dessa forma, ainda que incontroversa a incidência da responsabilidade objetiva do Estado sobre os dados pessoais sob sua guarda e controle, isso não implica em dizer que há responsabilidade integral e irrefutável, sendo plenamente possível a análise do caso concreto para constatação de eventuais excludentes da responsabilidade civil do Estado, o que será tratado no subtópico apartado.

Assim, apesar de não se cogitar a verificação de dolo ou culpa, será admissível a responsabilização do Estado "quando a ação ou omissão a ele imputável for antijurídica" [216] e não houver a incidência de nenhuma excludente capaz de romper o nexo causal.

Portanto, o Estado ao violar as regras da LGPD, da LAI e do CDC (em casos em que se aplica) ao coletar, tratar, armazenar e compartilhar dados e disso decorrer dano ao titular de dados, fatalmente, irá responder objetivamente seja por sua ação ou omissão.

Isso quer dizer que o Estado irá responder tanto pelos danos oriundos de condutas indevidas ao coletar, tratar, armazenar e compartilhar dados, como pela omissão de seu dever de diligência, deixando de implementar as diretrizes fixadas na LGPD ou ignorando os princípios e finalidades previstos nos artigos 6º e 23 da LGPD.

Nesse ponto, importante destacar que o STF já apresentou em alguns julgados o entendimento de que nos casos de omissão estatal ao dever se cautela, a responsabilidade seria subjetiva e não objetiva.[217]

---

[215] JUSTEN FILHO, Marçal, **Curso de direito administrativo**. 10 ed. São Paulo: Revista dos Tribunais, 2014. p. 1346.

[216] JUSTEN FILHO, Marçal. **Curso de direito administrativo**. 10 ed. São Paulo: Revista dos Tribunais, 2014. p. 1336.

[217] CONSTITUCIONAL. ADMINISTRATIVO. CIVIL. RESPONSABILIDADE CIVIL DO ESTADO. ATO OMISSIVO DO PODER PÚBLICO: DETENTO FERIDO POR OUTRO DETENTO. RESPONSABILIDADE SUBJETIVA: CULPA PUBLICIZADA: FALTA DO SERVIÇO. C.F., art. 37, § 6º. I. - Tratando-se de ato omissivo do poder público, a responsabilidade civil por esse ato é subjetiva, pelo que exige dolo ou culpa, em sentido estrito, esta numa de suas três vertentes -- a negligência, a imperícia ou a imprudência -- não sendo, entretanto, necessário individualizá-la, dado que pode ser

Ainda que, eventualmente, seja possível a propositura de ação regressiva em face do encarregado (art. 23, III, da LGPD), perante o titular de dados lesado, o Estado não poderá se furtar de indenizar, caso preenchidos os elementos da responsabilidade civil.

4.2. ELEMENTOS DA RESPONSABILIDADE CIVIL DO ESTADO NO TRATAMENTO DE DADOS

Definida a responsabilidade objetiva do Estado como controlador de dados, cabe analisar quais os elementos necessários no caso concreto passíveis de resultar na condenação do Estado quando cometer falhas na função de agente de tratamento de dados.

Nas palavras de Patrícia Peck, “a responsabilidade civil é um fenômeno social” e, “um dos principais pressupostos da responsabilidade civil é a existência de nexo causal entre o ato e o dano por ele produzido”. Assim, “muito mais importante que o ato ilícito que causou o dano é o fato de que esse dano deve ser ressarcido.”[218]

A LGPD, ao tratar da responsabilidade e do ressarcimento dos danos, prevê:

> 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:
> I - o modo pelo qual é realizado;
> II - o resultado e os riscos que razoavelmente dele se esperam;
> III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

---

atribuída ao serviço público, de forma genérica, a falta do serviço. II. - A falta do serviço -- faute du service dos franceses -- não dispensa o requisito da causalidade, vale dizer, do nexo de causalidade entre ação omissiva atribuída ao poder público e o dano causado a terceiro. III. - Detento ferido por outro detento: responsabilidade civil do Estado: ocorrência da falta do serviço, com a culpa genérica do serviço público, por isso que o Estado deve zelar pela integridade física do preso. IV. - RE conhecido e provido. (RE 382054, Relator(a): CARLOS VELLOSO, Segunda Turma, julgado em 03/08/2004, DJ 01-10-2004 PP-00029 EMENT VOL-02166-02 PP-00330 RT v. 94, n. 832, 2005, p. 157-164 RJADCOAS v. 62, 2005, p. 38-44 RTJ VOL 00192-01 PP-00356)

EMENTA DIREITO ADMINISTRATIVO. RESPONSABILIDADE CIVIL SUBJETIVA DO ESTADO. OMISSÃO. FALTA DE CONSERVAÇÃO E MANUTENÇÃO DE ÁREA PÚBLICA. INDENIZAÇÃO CARACTERIZADA. ANÁLISE DA OCORRÊNCIA DE EVENTUAL AFRONTA AOS PRECEITOS CONSTITUCIONAIS INVOCADOS NO APELO EXTREMO DEPENDENTE DA REELABORAÇÃO DA MOLDURA FÁTICA CONSTANTE NO ACÓRDÃO REGIONAL. SÚMULA 279/STF. PRECEDENTES. ACÓRDÃO RECORRIDO PUBLICADO EM 16.11.2009. Tendo o Tribunal de origem formado convencimento com espeque na prova produzida, conclusão em sentido diverso demandaria primeiramente o revolvimento do conjunto probatório, inviável em sede extraordinária (Súmula 279/STF). Agravo regimental conhecido e não provido. (AI 850063 AgR, Relator(a): ROSA WEBER, Primeira Turma, julgado em 10/09/2013, ACÓRDÃO ELETRÔNICO DJe-188 DIVULG 24-09-2013 PUBLIC 25-09-2013)

[218] PINHEIRO, Patrícia Peck. **Direito digital**. [recurso eletrônico]. 5ª ed. São Paulo: Saraiva, 2013. Não paginado.

> 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.

Dessa forma, nos termos da lei será considerado como tratamento irregular quando: i) estiver em desacordo com a lei; ii) não for seguro da forma esperada pelo titular, o que é totalmente relativo e pessoal.

As circunstâncias previstas nos incisos do referido dispositivo de lei, que exigem a análise da forma de tratamento, da ponderação dos resultados e riscos esperados na época em que a irregularidade ocorreu. Essa previsão é importante porque, obviamente, não se pode exigir a adoção de uma tecnologia que não estava disponível ao agente de tratamento quando da ocorrência do dano.

Apesar de parecer algo simples, Bruno Torchia e Tacianny Machado entendem que “a norma é de entendimento bastante complexo, pois ao mesmo tempo em que estabelece situações em que o tratamento é irregular, menciona em seu parágrafo único que só haverá dever de indenizar de houver dano.”[219]

Contudo, não há nada de diferente ou complexo em se exigir “dano”, pois o sistema brasileiro de responsabilidade civil sempre exigiu a ocorrência do dano para configurar o dever de indenizar.

Considera-se o dano um dos elementos da responsabilidade civil e, via de regra, a obrigação de reparar surgirá se estiverem presentes os requisitos previstos no art. 186 do Código Civil, a saber: (a) ato ilícito; (b) dano e (c) a relação de causalidade entre o dano e a conduta. A ausência de qualquer desses requisitos, impõe seja afastado o dever de indenizar (art. 927 do Código Civil).

Contudo, em se tratando de responsabilidade civil da administração pública, deve se seguir a Constituição Federal (art. 37, §6º) que adota a responsabilidade objetiva e a teoria do risco administrativo, apontando apenas 2 requisitos para caracterização do dever de indenizar, a existência do dano e do nexo de causalidade

Nesse sentido, Rosa Maria de Andrade Nery e Nelson Nery Júnior afirmam que para Administração Pública indenizar, devem estar presentes os seguintes requisitos:

---

[219] TORCHIA, Bruno Martins. MACHADO, Tacianny Mayara Silva. A reponsabilidade subjetiva prevista ne lei geral de proteção de dados e a relação jurídica centre controlador e o encarregado de proteção de dados. In: DAL POZZO, Augusto Neves E MARTINS, Ricardo Marcondes (coords.). **LGPD & Administração Pública**. São Paulo: Thomson Reuters Brasil, 2020. P. 837.

"(a) a existência do dano; (b) o nexo causal entre o fato da administração pública (comissivo ou omissivo) e o dano."[220] Ainda, aduzem que

> "Não há restrições dentro da organização do Estado quanto à imputação da responsabilidade civil objetiva prevista no CF 37 §6º. Basta que se trate de um ato que provenha de um órgão do Estado, ou tenha sido causado por alguém que trabalha em seu nome.
> E não é a licitude, ou não, do ato que irá determinar a incidência do dever de indenizar, mas a existência de prejuízo ao particular. Portanto, a administração não pode se furtar ao dever de indenizar apenas calcada no fato de que não cometeu ato ilícito" [221]

Conforme já demonstrado, considerando a existência de entendimento divergente tanto na doutrina como na jurisprudência de que a responsabilidade objetiva não seria adequada para atos omissivos da Administração Pública, importante analisar os 3 elementos da responsabilidade civil na esfera da proteção de dados, porque, de fato, não se sabe como se dará a aplicação nos Tribunais Pátrios.

Até mesmo porque, atos omissivos existirão, então, analisar a conduta ilícita é relevante para o caso de não se entender pela aplicação da teoria da responsabilidade objetiva.

No contexto de responsabilidade civil e proteção de dados, afirma Glenda Gonçalves Gondim:[222]

> A existência do direito a proteção dos dados pessoais importa dizer que nenhuma informação pode ser obtida à revelia do seu titular, seja desde a sua coleta, alteração de finalidade ou compartilhamento e, se assim ocorrer, entende-se como algo contrário ao ordenamento jurídico, por isso, indevidos. Assim, toda e qualquer utilização indevida, como a obtenção sem o devido controle do titular será considerada ilegal (acaso não exista exceção legal que previamente a regulamente) e poderá ocasionar a responsabilização civil, uma vez que será considerada como ato antijurídico (no seu sentido *lato*).

Apesar do consentimento ser uma das bases para o tratamento de dados, provavelmente a mais importante, quando o agente de tratamento é o Poder Público, é relativamente simples enquadrar a dispensa do consentimento nas exceções previstas na LGPD (por exemplo, execução de políticas públicas, persecução do interesse público).

---

[220] NERY, Rosa Maria de Andrade; NERY JÚNIOR, Nelson. **Instituições de direito civil:** direito das obrigações. Vol. II. São Paulo, Revista dos Tribunais, 2015. p. 404.
[221] NERY, Rosa Maria de Andrade. NERY JÚNIOR, Nelson. **Instituições de direito civil**: direito das obrigações, dos contratos e da responsabilidade civil. Vol. II. São Paulo, Thomson Reuters Brasil, 2019. p. 434.
[222] GONDIM, Glenda Gonçalves. Responsabilidade civil no uso indevido dos dados pessoais. In: AMORIM, José de Campos; VEIGA, Fabio da Silva.; AZEVEDO, Patrícia Anjos (Org.). **Desafios do Legaltech**. 1ed.Porto: Instituto Iberoamericano de Estudos Jurídicos, 2020. P. 78.

De todo modo, os demais dispositivos se aplicam, especialmente, os direitos e princípios elencados no artigo 6º, da LGPD: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas).

Assim, a atuação em desconformidade com esses princípios é capaz de configurar a inobservância à legislação prevista no artigo 44 da LGPD.

Da mesma forma, nota-se a existência de responsabilidade decorrente da omissão, pois no parágrafo único do artigo 44, fica muito claro que a falta da adoção de medidas se segurança de dados, também, implica na responsabilidade civil.

Cabe aqui uma ressalva quanto à forma de responsabilidade, pois nas palavras de Sérgio Cavalieri Filho:[223]

> Grandes são as divergências e dificuldades enfrentadas pela doutrina e jurisprudência para darem resposta a graves problemas decorrentes da omissão em sede de responsabilidade civil do Estado e outras áreas, Persiste, por exemplo, a controvérsia sobre a responsabilidade civil do Estado, se objetiva ou subjetiva, por não se fazer distinção entre omissão genérica e especifica.

Muito provavelmente, essa discussão acerca da aplicação da responsabilidade subjetiva em casos de condutas omissivas, irá ocorrer quando o agente de tratamento não adotar as medidas de segurança a que se refere o parágrafo único do artigo 44, que estão dispostas no artigo 46 da LGPD:

> 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.
> § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
> § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Portanto, os agentes de tratamento devem adotar as medidas de segurança, sejam elas técnicas ou administrativas para proteção dos dados pessoais, como um dever, caso contrário, estão passíveis de receber as punições administrativas e judiciais a respeito da sua conduta omissiva. O fato de que o Poder Público detinha

---

[223] CAVALIERI FILHO, Sergio. Responsabilidade por omissão. **Interesse Público – IP**, Belo Horizonte, ano 19, n. 104, p. 15-23, jul/ago. 2017.

meios de impedir a conduta lesiva e mesmo assim não o fez, conduz à uma responsabilidade objetiva, em que pese a existência de entendimento contrário.

A expectativa de segurança é relevante para configuração do nexo causal, já que "o atendimento dessa expectativa é fundamental para que o tratamento de dados seja regular."[224]

Assim, partindo-se do pressuposto de que a responsabilidade do Estado é objetiva, caberá a ele provar que agiu dentro da lei, no sentido de que não violou as normas da LGPD ou de que adotou todas as medidas de segurança nela exigidas, apontando eventuais causas de exclusão da responsabilidade.

Além das normas contidas na LGPD, deve-se ter em mente o diálogo das fontes, em que se coordena a previsão da LGPD com as demais normas do ordenamento jurídico, em especial, a Constituição Federal, o Código Civil e o CDC. Assim, não há razões para não se aplicar, também, os pressupostos comumente exigidos pelo direito público para se apurar a responsabilidade civil do Estado.

Acerca do tema, Nelson Nery Júnior e Rosa de Andrade Nery, afirmam que a Constituição Federal "só exige dois requisitos para a verificação do dever de indenizar: existência de dano (patrimonial ou moral) e o nexo de causalidade entre a conduta da administração e o dano." [225] Para eles, não é a ilicitude que determina o dever de indenizar, mas sim a existência do dano.[226]

Já Marçal Justen Filho, ao analisar a questão, afirma que a responsabilidade civil do Estado "depende de uma conduta estatal, seja comissiva, seja omissiva, que produza efeito danoso a terceiro."[227]

Como a LGDP em seu artigo 44 elencou as hipóteses de tratamento irregular, é possível concluir que a conduta comissiva ou omissa é um dos elementos da responsabilidade civil do Estado no tratamento de dados pessoais, que deve estar somado ao dano e entre eles deve existir nexo de causalidade.

---

[224] COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada**. 2ª ed. São Paulo: Thompson Reuters Brasil, 2019. P. 181.
[225] NERY, Rosa Maria de Andrade; NERY JÚNIOR, Nelson. **Instituições de Direito Civil**: volume II: Das obrigações, dos contratos e da responsabilidade civil. 2ª ed. São Paulo: Thompson Reuters Brasil, 2019. p. 433-434.
[226] NERY, Rosa Maria de Andrade; NERY JÚNIOR, Nelson. **Instituições de Direito Civil**: volume II: Das obrigações, dos contratos e da responsabilidade civil. 2ª ed. São Paulo: Thompson Reuters Brasil, 2019. p. 433-434.
[227] JUSTEN FILHO, Marçal, **Curso de direito administrativo**. 10 ed. São Paulo: Revista dos Tribunais, 2014. p. 1330-1331.

O dano, como pressuposto da responsabilidade civil:[228]

> no plano da reponsabilidade civil do Estado, em caso algum se pode prescindir do evento danoso: a só ilegalidade ou irregularidade do ato, que se verifique sem dano a terceiro, não pode produzir nenhuma responsabilidade, mas apenas, quando for o caso, a invalidade do ato.

Dessa forma, conforme ensina Yussef Cahali:[229]

> no caso de dano sofrido pelo particular em razão de dolo ou culpa do agente estatal, de deficiência ou falha do serviço público, de culpa anônima da Administração, da chamada *faute de servisse,* nasce a pretensão ressarcitória: a indenização, compreendendo os danos certos e não eventuais, atuais ou futuros, deve ser a mais completa possível, assimilando-se à responsabilidade civil do direito comum.

Assim, para confirmação da existência de um dano, deve necessariamente ter ocorrido a ofensa à um bem jurídico,[230] seja ele patrimonial ou não.

Celso Antônio Bandeira de Mello afirma que “para ser indenizável cumpre que o dano, ademais de incidente sobre um direito, seja certo, vale dizer, não apenas eventual, possível.”[231]

Em relação ao dano, mesmo aparentando ser de fácil identificação, também, será capaz de gerar controvérsia quando se está diante de dados pessoais, já que há casos em que é possível entender que o dano extrapatrimonial pode ser presumido.

Recentemente, o STJ, no julgamento do Recurso Especial nº 1.758.799/2019, entendeu que se presume a ocorrência do dano moral decorrente do compartilhamento ou comercialização de bancos de dados (do consumidor) sem que contar com a autorização expressa, dispensando a comprovação de prejuízos efetivos, diante da flagrante violação aos direitos de personalidade são evidentes. O caso concreto foi assim ementado:[232]

> RECURSO ESPECIAL. FUNDAMENTO NÃO IMPUGNADO. SÚM. 283/STF. AÇÃO DE COMPENSAÇÃO DE DANO MORAL. BANCO DE DADOS. COMPARTILHAMENTO DE INFORMAÇÕES PESSOAIS. DEVER DE INFORMAÇÃO. VIOLAÇÃO. DANO MORAL IN RE IPSA. JULGAMENTO: CPC/15. 1. Ação de compensação de dano moral ajuizada em 10/05/2013,

---

[228] CAHALI, Yussef Said. **Responsabilidade civil do Estado**, 5 ed. São Paulo: Revista dos Tribunais, 2014, p. 65.
[229] CAHALI, Yussef Said. **Responsabilidade civil do Estado**, 5 ed. São Paulo: Revista dos Tribunais, 2014, p. 66.
[230] PEREIRA, Caio Mário da Silva (atualizador Gustavo Tepedino). **Responsabilidade civil**. 11ª ed. Rio de Janeiro: Forense, 2016. P. 74
[231] MELLO. Celso Antônio Bandeira de. **Curso de Direito Administrativo**. 32ª ed. São Paulo: Malheiros, 2015. p.1050.
[232] BRASIL. Superior Tribunal de Justiça. **Recurso Especial nª 1.758.799-MG**. Relatora: Ministra Nancy Andrighi. Publicado em 19/11/2019. Disponível em: <https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1888267&num_registro=201700065219&data=20191119&formato=PDF>. Acesso em 12/01/2021.

> da qual foi extraído o presente recurso especial, interposto em 29/04/2016 e atribuído ao gabinete em 31/01/2017. 2. O propósito recursal é dizer sobre: (i) a ocorrência de inovação recursal nas razões da apelação interposta pelo recorrido; (ii) a caracterização do dano moral em decorrência da disponibilização/comercialização de dados pessoais do recorrido em banco de dados mantido pela recorrente. 3. A existência de fundamento não impugnado – quando suficiente para a manutenção das conclusões do acórdão recorrido – impede a apreciação do recurso especial (súm. 283/STF). 4. A hipótese dos autos é distinta daquela tratada no julgamento do REsp 1.419.697/RS (julgado em 12/11/2014, pela sistemática dos recursos repetitivos, DJe de 17/11/2014), em que a Segunda Seção decidiu que, no sistema credit scoring, não se pode exigir o prévio e expresso consentimento do consumidor avaliado, pois não constitui um cadastro ou banco de dados, mas um modelo estatístico. 5. A gestão do banco de dados impõe a estrita observância das exigências contidas nas respectivas normas de regência – CDC e Lei 12.414/2011 – dentre as quais se destaca o dever de informação, que tem como uma de suas vertentes o dever de comunicar por escrito ao consumidor a abertura de cadastro, ficha, registro e dados pessoais e de consumo, quando não solicitada por ele. 6. O consumidor tem o direito de tomar conhecimento de que informações a seu respeito estão sendo arquivadas/comercializadas por terceiro, sem a sua autorização, porque desse direito decorrem outros dois que lhe são assegurados pelo ordenamento jurídico: o direito de acesso aos dados armazenados e o direito à retificação das informações incorretas. 7. A inobservância dos deveres associados ao tratamento (que inclui a coleta, o armazenamento e a transferência a terceiros) dos dados do consumidor – dentre os quais se inclui o dever de informar – faz nascer para este a pretensão de indenização pelos danos causados e a de fazer cessar, imediatamente, a ofensa aos direitos da personalidade. 8. Em se tratando de compartilhamento das informações do consumidor pelos bancos de dados, prática essa autorizada pela Lei 12.414/2011 em seus arts. 4º, III, e 9º, deve ser observado o disposto no art. 5º, V, da Lei 12.414/2011, o qual prevê o direito do cadastrado ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais 9. O fato, por si só, de se tratarem de dados usualmente fornecidos pelos próprios consumidores quando da realização de qualquer compra no comércio, não afasta a responsabilidade do gestor do banco de dados, na medida em que, quando o consumidor o faz não está, implícita e automaticamente, autorizando o comerciante a divulgá-los no mercado; está apenas cumprindo as condições necessárias à concretização do respectivo negócio jurídico entabulado apenas entre as duas partes, confiando ao fornecedor a proteção de suas informações pessoais. 10. Do mesmo modo, o fato de alguém publicar em rede social uma informação de caráter pessoal não implica o consentimento, aos usuários que acessam o conteúdo, de utilização de seus dados para qualquer outra finalidade, ainda mais com fins lucrativos. 11. Hipótese em que se configura o dano moral in re ipsa. 12. Em virtude do exame do mérito, por meio do qual foram rejeitadas as teses sustentadas pela recorrente, fica prejudicada a análise da divergência jurisprudencial. 13. Recurso especial conhecido em parte e, nessa extensão, desprovido.

Do voto, é possível se extrair que “a inobservância dos deveres associados ao tratamento (que inclui a coleta, o armazenamento e a transferência a terceiros) dos dados do consumidor” é capaz de gerar o dever de indenizar. Houve falha no dever de informar, atualmente previsto no artigo 6º da LGPD e que é aplicável ao Estado.

Assim, ainda que o processo acima tenha como parte uma pessoa de direito privado, conclui-se que o entendimento se aplica ao Poder Público, ressalvadas as hipóteses de compartilhamento autorizadas já mencionadas no capítulo 3.4.

No mesmo sentido, o Tribunal Regional do Trabalho da 15ª Região, em um caso de acesso aos dados cadastrados junto à órgão público (Detran), também, entendeu pela presunção do dano moral e, ainda, apontou a necessidade do consentimento do titular de dados pessoais:[233]

> OBTENÇÃO DE INFORMAÇÕES DO TRABALHADOR JUNTO A CADASTROS INFORMATIZADOS SEM SUA EXPRESSA AUTORIZAÇÃO. DANO MORAL CARACTERIZADO. O mero acesso aos dados informatizados do cadastro mantido pelo DETRAN ou por qualquer outro órgão, sem a ciência e autorização específica do trabalhador, invade sua intimidade e causa prejuízo à sua honra, ensejando dano moral que deve ser reparado.

Não se sabe quais serão as exigências dos Tribunais Pátrios para configuração dos danos quando da violação aos dados, ainda mais diante da regra do compartilhamento amplo para o Poder Público, previsto tanto na LGPD quanto nos Decretos nºs 10.046 e 10.047.

Finalmente, para completar os 3 elementos essenciais da responsabilidade civil, sabe-se que não basta a existência de uma conduta ilícita e a ocorrência do dano, é preciso que haja uma relação entre elas, chamada de nexo causal. Ou seja, "é necessário que se estabeleça uma relação de causalidade entre a antijuridicidade da ação e o mal causado."[234]

O nexo de causalidade tem especial relevância em casos de responsabilidade objetiva, já que sendo irrelevante a conduta (se houve culpa ou não), é imprescindível analisar a ligação entre a conduta do agente com o dano suportado pela vítima.

A LGPD prevê a possibilidade de inversão do ônus da prova, assim como o CPC e o CDC, razão pela qual ao ser invertido o ônus, caberá ao Poder Público demonstrar que o dano não decorreu da conduta adotada pelo agente de tratamento, apontando as situações em que se tem o rompimento do nexo de causalidade, que serão detalhadas no próximo tópico abaixo.

---

[233] BRASIL. Tribunal Regional do Trabalho – Roraima. **Processo nº 410220145150044 SP 089934/2014** – PATR, Relator: MARIA INÊS CORREA DE CERQUEIRA CESAR TARGA, Data de Publicação: 28/11/2014.

[234] PEREIRA, Caio Mário da Silva (atualizador Gustavo Tepedino). **Responsabilidade civil**. 11ª ed. Rio de Janeiro: Forense, 2016. p. 105.

4.3. EXCLUDENTES DA RESPONSABILIDADE CIVIL DO ESTADO

A LGPD aponta as hipóteses em que será afastada a responsabilidade dos agentes de tratamento de dados, as quais estão previstas no 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; ou
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Basicamente, tratam-se de 3 excludentes da ilicitude. Na primeira hipótese, estará ausente a responsabilidade do agente de tratamento se ele comprovar que não realizou o tratamento que lhe foi imputado como irregular. Assim, "se não houve tratamento, não há nexo causal entre o dano e a ação ou omissão do agente"[235].

Na segunda hipótese prevista na LGPD, os agentes se eximirão do dever de indenizar caso tenha realizado o tratamento, mas comprova que o fez de acordo com as normais da LGPD e com o máximo de dever de cautela que lhe era exigido.

Nesse ponto, reside uma grande problemática tocante à anonimização dos dados, já que a partir dela os dados deixam de ser pessoais e não recebem a mesma tutela pela LGPD.

Nos termos do artigo 5º, XI, da LGPD, 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, direta ou indireta, a um indivíduo".

O artigo 12, da LGPD prevê:

> Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.
> § 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.
> § 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.
> § 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.

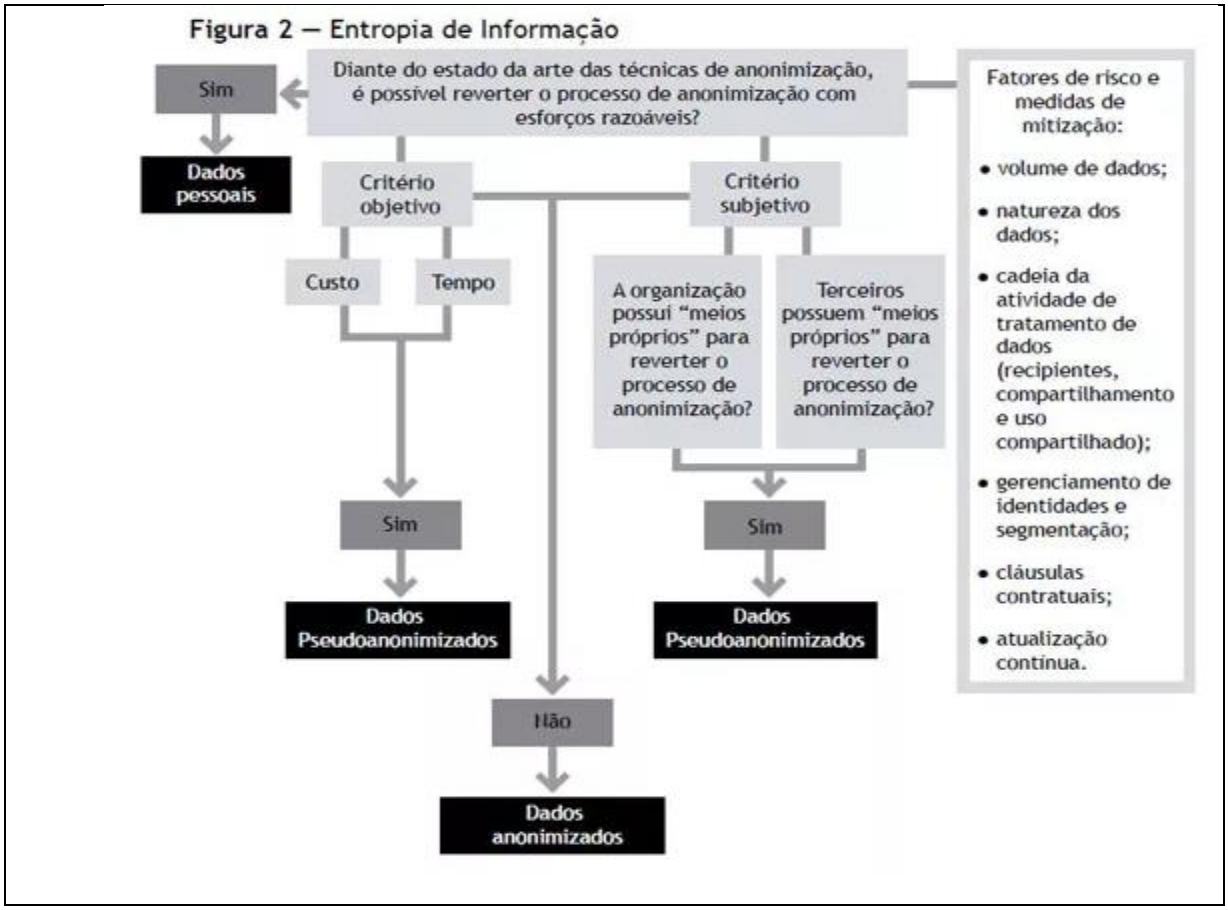
---

[235] COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada**. 2ª ed. São Paulo: Thompson Reuters Brasil, 2019. p. 178.

Dessa forma, por meio da anonimização, “no momento do tratamento, um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, sendo que os dados passam a formar um conjunto agregado de informações”[236], não podendo ser individualizadas. E, como a própria lei prevê, ocorrendo a reversão da técnica, os dados voltam a ser dados pessoais.

Assim, considerando as disposições do artigo 12, é possível se traçar o seguinte quadro resumo elaborado por Bruno Bioni:

Figura 5 – Entropia de Informação:



FONTE: BIONI, Bruno. Compreendendo o conceito de anonimização e dado anonimizado. **GEN Jurídico**. 2020. Disponível em: <https://genjuridico.jusbrasil.com.br/artigos/889500718/compreendendo-o-conceito-de-anonimizacao-e-dado-anonimizado>. Acesso em 10/01/2021.

O regulamento Europeu (GDPR) dispõe que:

> 26. Os princípios da proteção de dados deverão aplicar-se a qualquer informação relativa a uma pessoa singular identificada ou identificável. Os dados pessoais que tenham sido pseudonimizados, que possam ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares, deverão ser considerados informações sobre uma pessoa singular identificável. Para determinar se uma pessoa singular é

[236] FEIGELSON, Bruno. SIQUEIRA, Antonio. **Comentários à Lei Geral de Proteção de dados.** São Paulo: Thompson Reuters Brasil, 2019. P. 100-101.

> identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica. Os princípios da proteção de dados não deverão, pois, aplicar-se às informações anônimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anônimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anônimas, inclusive para fins estatísticos ou de investigação.

Ou seja, a GDPR, também, dispõe sobre o dado anonimizado não merecer proteção, mas a partir do momento em que ele possa vir a ser identificado deve ser protegido.[237]

O problema é que a legislação brasileira trata da proteção apenas dos dados pessoais, inclusive a redação do artigo 44 é exatamente nesse sentido e essa redação acaba por deixar de fora os dados pseudoanonimizados para fins de responsabilidade civil.

Na prática, importante será a atuação da ANPD no sentido de regulamentar esses padrões e técnicas de anonimização dos dados, evitando elevado grau de subjetividade na análise dos requisitos no caso concreto.

Na terceira e última hipótese, tem-se uma excludente bem comum no contexto de responsabilidade civil, que é a culpa exclusiva da vítima, no caso do titular de dados, ou de terceiro.

Para Marçal Justen Filho, “é evidente que, se o resultado danoso proveito de evento imputável exclusivamente ao próprio lesado ou de fato de terceiro ou pertinente ao mundo natural, não há responsabilidade do Estado.”[238]

A exceção da responsabilidade com base na culpa exclusiva da vítima se assemelha a hipótese prevista no artigo 14 do CDC. Assim, “é possível compreender, na análise de cada caso concreto, quando do titular dá causa ao dano, como pode

---

[237] BIONI, Bruno. Compreendendo o conceito de anonimização e dado anonimizado. **GEN Jurídico**. 2020. Disponível em: <https://genjuridico.jusbrasil.com.br/artigos/889500718/compreendendo-o-conceito-de-anonimizacao-e-dado-anonimizado>. Acesso em 10/01/2021.

[238] JUSTEN FILHO, Marçal, **Curso de Direito Administrativo**. 10 ed. São Paulo: Revista dos Tribunais, 2014. p. 1331.

ocorrer, por exemplo, quando fornece seus dados a sites flagrantemente falsos, ou quando não guarda em segurança seus documentos de identificação."[239]

A excludente da responsabilidade com base na culpa de terceiro, especialmente pelo ambiente virtual em que estão armazenados os dados, será frequentemente enfrentada pelos Tribunais pátrios, já que é cada vez mais comum a invasão por hackers aos sistemas.

Contudo, a mera situação de invasão e violação dos dados por conduta de um terceiro não é, por si só, capaz de afastar a responsabilidade. Isso porque, como se viu no tópico anterior, a LGPD prevê em seu artigo 46 uma série de medidas preventivas que devem ser adotadas pelos agentes de tratamento. Apenas após a comprovação de que todas as medidas de segurança foram adotadas é que se poderá admitir a isenção da responsabilidade.

Trata-se de uma tarefa árdua para os agentes de tratamento, pois diante dos avanços tecnológicos, seu trabalho exige constante atualização na prevenção de acidentes junto ao sistema de dados, protegendo-o. Nesse sentido, Marcos Gomes da Silva Bruno, afirma que:[240]

> Como é sabido, nenhum sistema é a prova de falhas ou vulnerabilidades, até porque a tecnologia de invasões evolui na mesma proporção (ou até mais rápido) que a tecnologia para defesa desses incidentes. Por conta disso, nunca se pode esperar uma absoluta segurança em sistemas informáticos.

Contudo, o STJ já entendeu que, ao aplicar o CDC, haveria responsabilidade de uma concessionária de serviço público em razão de danos decorrentes de um ataque *hacker*:[241]

> PROCESSUAL CIVIL E CONSUMIDOR. TELEFONIA. RESPONSABILIDADE SOLIDÁRIA ENTRE AS EMPRESAS FORNECEDORAS DE PRODUTOS E SERVIÇOS. EXISTÊNCIA DE SIMBIOSE. SISTEMA DE PABX. FALHA NA SEGURANÇA DAS LIGAÇÕES INTERNACIONAIS. RISCO DO NEGÓCIO. 1. Trata-se, na origem, de Ação Declaratória de Inexistência de Débito, cumulada com Consignação em Pagamento contra a Telefônica Brasil S.A., com o escopo de declarar a inexigibilidade da dívida referente a ligações internacionais constante das faturas telefônicas dos meses de outubro e novembro de 2014, nos respectivos valores de R$ 258.562, 47 (duzentos e cinquenta e oito mil e

[239] COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada**. 2ª ed. São Paulo: Thompson Reuters Brasil, 2019. p. 180.
[240] BRUNO, Marcos Gomes da Silva. Dos agentes de tratamento de dados pessoais. MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **LGPD**: Lei Geral de Proteção de dados comentada. São Paulo: Thomson Reuters Brasil, 2019. P. 325.
[241] BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1721669/SP**, Rel. Ministro Herman Benjamin, Segunda Turma, julgado em 17/04/2018, DJe 23/05/2018. Disponível em: <https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201800046115&dt_publicacao=23/05/2018>. Acesso em 12/01/2021.

> quinhentos e sessenta e dois reais e quarenta e sete centavos) e R$ 687.207, 55 (seiscentos e oitenta e sete mil e duzentos e sete reais e cinquenta e cinco centavos). 2. Consta dos autos que as partes celebraram contrato de consumo, cujo objeto é o fornecimento de linhas telefônicas, serviços especiais de voz, acesso digital, recurso móvel de longa distância DD e DDD e recurso internacional, local ou de complemento de chamada, para serem utilizadas em central telefônica - PABX, adquirida de terceira pessoa.
> 3. Conforme narrado, criminosos entraram no sistema PABX da empresa recorrente e realizaram ilicitamente diversas chamadas internacionais, apesar de esse serviço estar bloqueado pela operadora. 4. A interpretação do Tribunal de origem quanto à norma insculpida no art. 14 do CDC está incorreta, porquanto o serviço de telecomunicações prestado à recorrente mostrou-se defeituoso, uma vez que não ofereceu a segurança esperada pela empresa consumidora. 5. A responsabilidade pela reparação dos danos causados à recorrente não pode recair somente na empresa que forneceu o sistema PABX, mas também na operadora, que prestou o serviço de telefonia. Ademais, o conceito de terceiro utilizado pelo Tribunal bandeirante está totalmente equivocado, pois apenas pessoa totalmente estranha à relação de direito material pode receber esta denominação. Os Hackers que invadiram a central "obtiveram acesso ao sistema telefônico da vítima" e dispararam "milhares de ligações do aparelho" para números no exterior. 6. Não há dúvida de que a infração cometida utilizou as linhas telefônicas fornecidas pela recorrida, demonstrando que o seu sistema de segurança falhou na proteção ao cliente. Assim sendo, existe evidente solidariedade de todos os envolvidos na prestação dos serviços contratados, permitindo-se "o direito de regresso (na medida da participação na causação do evento lesivo) àquele que reparar os danos suportados pelo consumidor", REsp 1.378.284/PB, Relator o eminente Ministro Luis Felipe Salomão. 7. O risco do negócio é a contraparte do proveito econômico auferido pela empresa no fornecimento de produtos ou serviços aos consumidores. É o ônus a que o empresário se submete para a obtenção de seu bônus, que é o lucro. Por outro lado, encontra-se o consumidor, parte vulnerável na relação de consumo. 8. Os órgãos públicos e as suas empresas concessionárias são obrigadas a fornecer serviços adequados, eficientes e seguros aos consumidores em conformidade com o art. 22 do CDC.
> 9. Recurso Especial provido.

Isso porque o artigo 22, do CDC prevê:

> Art. 22. Os órgãos públicos, por si ou suas empresas, concessionárias, permissionárias ou sob qualquer outra forma de empreendimento, são obrigados a fornecer serviços adequados, eficientes, seguros e, quanto aos essenciais, contínuos.
> Parágrafo único. Nos casos de descumprimento, total ou parcial, das obrigações referidas neste artigo, serão as pessoas jurídicas compelidas a cumpri-las e a reparar os danos causados, na forma prevista neste código.

Ao que tudo indica, a tentativa de exclusão da responsabilidade com base no fato de terceiro será um trabalho árduo para os órgãos públicos, pois as exigências de segurança previstas no artigo 46 da LGPD, somadas à exigência de fornecimento de um serviço adequado, eficiente e seguro, levarão inevitavelmente a reparação dos causados.

Em sentido contrário, se restar comprovado que o Estado adotou todas as medidas cabíveis e possíveis para evitar o dano, defende Marçal Justen Filho que

“não se admite que um ato jurídico conforme ao direito, praticado pelo Estado de modo regular e perfeito, acarrete sua responsabilização civil – exceto quando essa for a opção explícita de uma lei.”[242]

4.4. A DOSIMETRIA PREVISTA NA LGPD COMO BASE PARA FIXAÇÃO DA INDENIZAÇÃO

O artigo 44 da LGPD deixa certo grau de subjetividade para o Magistrado avaliar as circunstâncias da responsabilidade civil. Ou seja, caberá ao Magistrado avaliar no caso concreto se estão presentes ou não os elementos ensejadores da responsabilidade civil e, em havendo os elementos, precisará definir como deve se dar a reparação do dano, quantificando-o de forma equitativa e condizente com o caso concreto.

O Código Civil dispõe em seu artigo 944 que “a indenização se mede pela extensão do dano.” Ainda, no parágrafo único prevê que “se houver excessiva desproporção entre a gravidade da culpa e o dano, poderá o juiz reduzir, equitativamente, a indenização.”

Fato é que “em qualquer hipótese, o montante da indenização não pode ser inferior ao prejuízo, em atenção ao princípio segundo o qual a reparação do dano há que ser integral.”[243] Nas palavras de Caio Mário da Silva, “há que se atentar para a gravidade da falta e as suas consequências, bem como para a natureza do dano.” [244]

Assim, por mais grave e dolosa que tenha sido a conduta do ofensor, o valor da indenização estará sempre atrelado à extensão do prejuízo à vítima, a teor do disposto no artigo 403, do Código Civil: “Ainda que a inexecução resulte de dolo do devedor, as perdas e danos só incluem os prejuízos efetivos e os lucros cessantes por efeito dela direto e imediato, sem prejuízo do disposto na lei processual.”

Dessa forma, a reparação do dano em valor superior ao prejuízo implica em enriquecimento sem causa, o que é vedado pelo artigo 884 do Código Civil.[245]

---

[242] JUSTEN FILHO, Marçal. **Curso de direito administrativo**. 10 ed. São Paulo: Revista dos Tribunais, 2014. p. 1337.
[243] PEREIRA, Caio Mário da Silva (atualizador Gustavo Tepedino). **Responsabilidade civil**. 11ª ed. Rio de Janeiro: Forense, 2016. P. 404.
[244] PEREIRA, Caio Mário da Silva (atualizador Gustavo Tepedino). **Responsabilidade civil**. 11ª ed. Rio de Janeiro: Forense, 2016. P. 404.
[245] Art. 884. Aquele que, sem justa causa, se enriquecer à custa de outrem, será obrigado a restituir o indevidamente auferido, feita a atualização dos valores monetários.

Importante lembrar que o CDC utiliza o princípio da reparação integral, elenca-o como direito básico do consumidor no art. 6º, inciso VI, o que significa dizer que a reparação deve ser a mais ampla e efetiva possível, abrangendo todos os danos causados ao consumidor de forma integral.

Via de regra, as demandas envolvendo a responsabilidade civil do Poder Público são essencialmente indenizatórias, já que a reparação do dano *in natura* é inconcebível na maioria dos casos (evita-se a paralisação dos serviços públicos e a destruição do que já foi realizado em prol da coletividade).[246]

No que tange ao dano material ou patrimonial, é aquele tradicionalmente estimável em dinheiro, representado por "toda a diminuição do patrimônio do credor, quer consistente na perda sofrida (*damnum ermergens*), quer num lucro de que haja sido privado (*lucrum cessans*)."[247]

Essa lesão ao patrimônio é apurada de maneira mais direta do que os danos imateriais, já que vinculada à prova concreta das despesas oriundas do ato ilícito, de forma quantificada e específica. O artigo 402 do Código Civil dispõe que: "Salvo as exceções expressamente previstas em lei, as perdas e danos devidas ao credor abrangem, além do que ele efetivamente perdeu, o que razoavelmente deixou de lucrar."

Já o dano moral é mais complexo, pois sua quantificação depende de uma série de critérios para se chegar ao arbitramento de um valor condizente com a reparação do dano.

Tanto é complexo que o STJ criou um método para a fixação do dano moral, chamado de método bifásico. Basicamente, é posto um valor básico para a reparação, o qual é analisado a partir do interesse jurídico do lesado e de um grupo de precedentes, que, após são analisadas as circunstâncias do caso concreto.[248]

Parágrafo único. Se o enriquecimento tiver por objeto coisa determinada, quem a recebeu é obrigado a restitui-la, e, se a coisa não mais subsistir, a restituição se fará pelo valor do bem na época em que foi exigido.

[246] CAHALI, Yussef Said. **Responsabilidade civil do Estado**, 5 ed. São Paulo: Revista dos Tribunais, 2014. p. 194-195.

[247] LOPES, Serpa. Curso de Direito Civil. *apud* FARIAS, Cristiano Chaves de. ROSENVALD, Nelson. **Curso de direito civil**: obrigações. 11 ed. Salvador: JusPodivm, 2017. p. 600-601.

[248] BRASIL. Superior Tribunal de Justiça. **O método bifásico para fixação de indenizações por dano moral**. 2018. Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias-antigas/2018/2018-10-21_06-56_O-metodo-bifasico-para-fixacao-de-indenizacoes-por-dano-moral.aspx>. Acesso em 19/01/2021.

Para o Ministro Paulo de Tarso Sanseverino: [249]

> A doutrina e a jurisprudência têm encontrado dificuldades para estabelecer quais são esses critérios razoavelmente objetivos a serem utilizados pelo juiz nessa operação de arbitramento da indenização por dano extrapatrimonial. Tentando proceder a uma sistematização dos critérios mais utilizados pela jurisprudência para o arbitramento da indenização por prejuízos extrapatrimoniais, destacam-se, atualmente, as circunstâncias do evento danoso e o interesse jurídico lesado.

A indenização, ainda, deve ter caráter pedagógico e sancionador para aquele que cometeu o dano (ou seu responsável).

Posto isso, resta saber como se quantificará um dano, especialmente o extrapatrimonial, quando tal dano decorrer de violação às normas de tratamento e armazenamentos de dados pessoais dispostas na LGPD.

Uma solução para o Magistrado nos casos que envolverem violação de dados pessoais, seria considerar as variáveis que já são mencionadas na LGPD quando da apuração da responsabilidade na via administrativa, pela ANPD, as quais podem, analogicamente, ser utilizadas para o arbitramento do valor da reparação.

A dosimetria prevista na LGPD está elencada no §1º do artigo 52:

> § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:
> I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
> II - a boa-fé do infrator;
> III - a vantagem auferida ou pretendida pelo infrator;
> IV - a condição econômica do infrator;
> V - a reincidência;
> VI - o grau do dano;
> VII - a cooperação do infrator;
> VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
> IX - a adoção de política de boas práticas e governança;
> X - a pronta adoção de medidas corretivas; e
> XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Apesar de tais sanções se destinarem à esfera administrativa, com caráter repreensivo aos agentes de tratamento, nada impede o Poder Judiciário de analisar as atenuantes e as agravantes no momento da quantificação do dano ao titular dos dados violados. Não se está afirmando que todas devem ser consideradas e

---

[249] BRASIL. Superior Tribunal de Justiça. **O método bifásico para fixação de indenizações por dano moral**. 2018. Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias-antigas/2018/2018-10-21_06-56_O-metodo-bifasico-para-fixacao-de-indenizacoes-por-dano-moral.aspx>. Acesso em 19/01/2021.

detidamente analisadas, mas na falta de parâmetros específicos ao tema, torna-se pertinente utilizá-los na análise do caso concreto.

Primeiro, quanto à gravidade e a natureza da conduta ilícita, apesar de relevante para responsabilização de entes privados, perante o Poder Público, não seria tão relevante diante da responsabilidade objetiva e da redação do artigo 403, do Código Civil.

A questão da boa-fé, como princípio e cláusula geral do direito, sempre terá seu espaço, especialmente, nas relações de consumo junto à administração pública.

A boa-fé está presente de forma expressa no Código de Defesa do Consumidor como princípio da Política Nacional das relações de consumo, conforme redação do artigo 4º, inc. III.

Em resumo, a boa-fé pode ser definida como uma regra de conduta humana, ou seja, a boa e correta conduta que se espera de todos dentro da sociedade. Para Menezes Cordeiro, "o comportamento das pessoas deve respeitar um conjunto de deveres reconduzidos, num prisma juspositivo e numa óptica histórico-cultural, a uma regra de actuação de boa-fé."[250]

A boa-fé objetiva pode ser conceituada como:[251]

> [...] o agir segundo a boa-fé objetiva concretiza as exigências de probidade, correção e comportamento leal, hábeis a viabilizar um adequado tráfico negocial, consideradas a finalidade e a utilidade do negócio em vista do qual se vinculam, vincularam ou cogitam vincular-se (...);

Neste sentido, Khouri:[252]

> [...] um padrão de conduta, padrão este objetivo que impõe um dever de agir. Dever de agir esse de acordo com determinados padrões, socialmente recomendados de correção, lisura, honestidade, para não frustrar a confiança legítima da outra parte;

Para Aguiar Junior:[253]

> [...] um dever de agir de acordo com padrões socialmente recomendados. Trata-se de uma cláusula geral, expressão do princípio de lealdade, que o juiz utilizará para verificar, nas circunstâncias daquele caso, qual a conduta que satisfaria essa exigência de lealdade (quanto a cuidado, informação, proteção, cumprimento da prestação, etc.). Assim criada pelo juiz a regra de

---

[250] CORDEIRO, Menezes. **Da boa-fé no direito civil**. Coimbra: Edições Almedina S/A, 2011. p. 632.
[251] MARTINS-COSTA, Judith. **A boa-fé no direito privado**: critérios para sua aplicação. 2ª ed. São Paulo: Saraiva, 2018. p. 43.
[252] KHOURI, Paulo Roberto Roque Antonio. **Direito do consumidor:** contratos, responsabilidade civil e defesa do consumidor em juízo. 3 ed. São Paulo: Atlas, 2006. p. 66
[253] AGUIAR JUNIOR, Ruy Rosado. Proteção da boa-fé subjetiva. **Revista da AJURIS**. v. 39. n. 126. Junho 2012. <www.ajuris.org.br/OJS2/index.php/REVAJURIS/article/download/781/475>. Acesso em 10.05.2019. p. 191.

> conduta, será feita a verificação entre a conduta devida, segundo a boa-fé, e a conduta efetiva, concluindo-se pela ilicitude da que dela destoa.

Tamanha a importância da boa-fé, que a LGPD exige como regra de conduta no tratamento de dados pessoais (art. 6º, *caput*).[254] Ainda que se esteja diante de dados pessoais cujo acesso é público, o artigo 7º, § 3º, dispõe que "deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização."

O princípio da boa-fé dentro da relação jurídica que envolve dados pessoais, permite dizer que há uma fidelidade depositada pelo titular dos dados ao agente de tratamento, na legítima expectativa de que esse agente de tratamento a quem confiou seus dados irá usá-los e compartilhá-los tanto de acordo com a lei, como de acordo com a finalidade para qual foram coletados.

Dessa forma, ainda que a conduta não seja relevante quando se está diante da responsabilidade objetiva, o agir de boa-fé sempre será um aspecto importante no momento da quantificação do dano.

O terceiro critério a ser analisado, seria a existência de vantagem auferida ou pretendida pelo infrator, que denota uma preocupação do legislador com o caráter efetivamente sancionador da penalidade, no caso seria da indenização.

Na esfera judicial, isso quer dizer que não se pode fixar uma indenização baixa quando o agente de tratamento obteve elevada vantagem econômica ao praticar a conduta ilícita (por exemplo: a condenação ao pagamento de R$ 10.000,00 à um titular de dados que teve seus dados pessoais compartilhados por um determinado órgão do governo, sendo que através desse acesso o órgão ou o terceiro tiveram um benefício econômico milionário).

O contrário, também, é importante, pois se não houve o recebimento de qualquer vantagem e o dano decorreu mesmo de uma falha pontual, deve o agente indenizar de forma justa ao dano causado, mas dentro dos critérios de proporcionalidade e razoabilidade. Aqui cabe mencionar a questão da reincidência, pois falhas pontuais podem ser passíveis de valores mais baixos de indenização, mas se há diversos casos de violação e mesmo assim o agente de tratamento segue falhando, sua punição precisa ser cada vez maior, a fim de que se adeque à lei.

---

[254] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

Já a questão de considerar a condição econômica do responsável pelo dano, é algo conhecido no ordenamento jurídico, especialmente, em razão do CDC. Obviamente, não se pode punir da mesma forma órgãos com capacidades e orçamentos diversos de investimentos em tecnologia.

Quanto ao grau do dano, dependerá de ponderar no caso concreto qual foi o impacto do dano na vida do titular de dados, quais foram as principais consequências diretas da violação e buscar classificar o dano dentro de níveis (leve, moderado, grave, gravíssimo), para ao longo dos anos poder chegar na aplicação de um método bifásico, já aplicado pelo STJ para fixação de valor para o dano extrapatrimonial.

Ainda, a LGPD aponta para ser considerada a cooperação do infrator, o que na esfera judicial poderá se fundar na análise de como se deu a conduta do agente de proteção de dados na apuração dos fatos, no auxílio ao titular de dados e na sua tentativa de excluir o dano ou minimizá-lo. Esse ponto se mistura com o oitavo parâmetro ligado à adoção de medidas capazes de minimizar o dano e a utilização de procedimentos nos termos do artigo 48, §2º, II, da LGPD.

Assim, a adoção de medidas de segurança e prevenção será “decisiva para resguardar os agentes de tratamento da aplicação de sanções mais graves e onerosas”, com isso, tem-se que o critério do inciso IX. Ou seja, “a verificação da existência de políticas de boas práticas e governança corporativa, como critério para o arbítrio punitivo, demonstra clara intenção do legislador em estimular no mercado o exercício de comportamento ético e precavido no tocante ao cuidado com dados pessoais.”[255]

Igualmente, será importante que o órgão público demonstre como se deu a medida corretiva interna vinculada ao fato que resultou no dano e como, eventualmente, o servidor responsável foi punido.

Por fim – mas não menos importante porque permeia todas as indenizações–, imprescindível que a condenação ao ressarcimento pelo dano seja proporcional, ou seja:[256]

> aplica-se o princípio da proporcionalidade, para afastar a reparação integral e mitigar a condenação do ofensor, quando estar provado que a negligência do causador do dano foi mínima, quase uma fatalidade, não sendo justo transferir a desgraça da vítima para o ofensor, a ponto de enfrentar vastíssimo prejuízo.

---

[255] FEIGELSON, Bruno. SIQUEIRA, Antonio. **Comentários à Lei Geral de Proteção de dados.** São Paulo: Thompson Reuters Brasil, 2019. p. 191.
[256] FARIAS, Cristiano Chaves de. ROSENVALD, Nelson. **Curso de direito civil**: obrigações. 11 ed. Salvador: JusPodivm, 2017. p. 597.

Tal regra, já se encontra disposta no parágrafo único do artigo 944 do Código Civil: “Se houver excessiva desproporção entre a gravidade da culpa e o dano, poderá o juiz reduzir, equitativamente, a indenização.”

Dessa forma, os parâmetros e critérios elencados no artigo 52, §1º, da LGPD podem, analogicamente, ser utilizados na esfera judicial no momento da quantificação do dano causado pelo Magistrado, obviamente, dialogando com os demais critérios previstos nas demais normas do ordenamento jurídico, em especial, o Código Civil e o CDC.

Ao final, o que realmente se busca é que a indenização decorrente da violação de dados pessoais seja equitativa, de forma a evitar que novos danos ocorreram, mas sem enriquecer uma parte em detrimento da outra, levando em consideração as peculiaridades de cada caso concreto.

5. CONCLUSÃO

A presente pesquisa corroborou com as hipóteses pretendidas, apontando para a importância da proteção de dados pessoais sob o domínio do Estado, bem como para a relevante função do instituto da responsabilidade civil, como um grande incentivador de boas práticas e como estímulo para que o Poder Público atue em consonância com a legislação.

Apesar da regulamentação tardia do Brasil, a proteção de dados é algo iminente, não apenas para o setor privado, mas como também junto ao setor público.

Ao longo da pesquisa foi possível demonstrar a evolução legislativa e jurisprudencial do Brasil no tema proteção de dados.

Apesar do direito de proteção de dados, ainda, não estar consagrado na Constituição Federal, ao que tudo indica, é só uma questão de tempo, pois já há proposta de emenda constitucional neste sentido.

A LGDP trouxe um capítulo todo dedicado ao tratamento de dados pelo Poder Público, o qual deve adotar as medidas legais para proteger os dados que estão sob o seu controle.

Ocorre que a questão dos dados ainda é negligenciada por muitos brasileiros, que por opção se expõem gratuitamente no mundo virtual, fornecendo seus dados sem preocupações futuras. Não é de se estranhar que não se preocupem com a questão da privacidade e violação de dados pessoais perante o Estado.

É essa falta de percepção que preocupa, já que o controle estatal pode já estar ocorrendo. O acesso amplo à informação e aos dados concede ao Estado um grande poder, capaz de manipular e alterar situações sociais.

Já são diversos os aplicativos do Governo, os quais se fazem necessários para inúmeros cidadãos (por exemplo: Bolsa família, CNH digital, Meu imposto de renda, programas de nota fiscal como Nota Paraná, etc), que coletam dados acima do necessário e acabam por acessar outras áreas do celular, até mesmo de localização. Tudo isso, com um simples aceite aos termos de uso, termos que não são objeto de leitura por quase a totalidade da população.

Fato é que os titulares de dados pessoais precisam se conscientizar da importância de zelar e buscar seus direitos, assim como fizeram aos consumidores quando da entrada em vigor do CDC, utilizando-se dos instrumentos existentes no ordenamento jurídico para impor ao Estado a adoção das condutas que dele são esperadas.

Em que pese a dispensa de consentimento na grande maioria das hipóteses legais, bem como do nítido legítimo interesse do Estado em utilizar os dados na consecução de políticas públicas, isso não significa a entrega de um “cheque em branco” através do qual pode o Estado pode fazer tudo o que quiser com os dados por ele coletados.

Busca-se evitar a criação de grandes bancos de dados, que contenham características aptas a dividir e polarizar a sociedade, a utilização indevida de dados pode gerar, até mesmo, discriminação.

O compartilhamento dos grandes bancos de dados do Estado com o setor privado é muito grave, por exemplo, um cidadão que utiliza o SUS pode ter negado algum tipo de seguro com a iniciativa privada de acordo com seu histórico de atendimentos médicos. O compartilhamento excessivo e despropositado deve ser combatido, em especial, pelos órgãos de defesa dos cidadãos, como Ministério Público e Associações.

Quanto à responsabilidade civil, sem a pretensão de esgotar o tema, restou demonstrado que, em que pese a ausência de menção específica ao Poder Público, as disposições gerais acerca da responsabilidade civil são suficientes quando dialoga com as demais normas do ordenamento jurídico, em especial, do CDC, que acabará englobando grande parte das lides, já que se aplica para defeitos na prestação de serviços públicos.

Com isso, entende-se que a responsabilidade do Estado se dá na modalidade objetiva em virtude dos danos causados pelo tratamento de dados pessoais, bastando a comprovação do dano e do nexo causal.

Apesar do receio de excessiva judicialização dos conflitos dos cidadãos com o Poder Público na matéria de proteção de dados, a atuação do Poder Judiciário será primordial para coibir abusos e reparar danos. Como visto na pesquisa, na Europa, marcada pelo baixo índice de judicialização, ainda mais se comparado com o Brasil, ativistas estão ingressando no Judiciário para satisfazer as demandas de proteção de dados diante da inércia de autoridades administrativas.

Diferentemente do que ocorre em outros países, a ANPD no Brasil está atrelada ao poder político, assim, apesar da exigida imparcialidade do órgão, fato é que está inserido dentro da Administração Pública federal, o que pode implicar em uma visão mais protetiva e complacente com seus entes – o que realmente não se espera.

Nesse cenário, em um primeiro olhar, espera-se que a judicialização não seja priorizada. Contudo, a judicialização poderá impulsionar grandes alterações nas medidas de prevenção e investimentos e implantação em segurança. A adoção de meios judiciais para coibir abusos por parte do Estado como agente de dados pessoais pode estimular essas condutas preventivas.

Reparar eventuais danos, sempre foi e será uma obrigação legal. A reparação do dano no campo material deve ser integral (CDC) e no campo imaterial proporcional à gravidade de se restringir o direito fundamental à privacidade.

Ainda que tenha ocorrido debate da questão junto à ANPD, a esfera cível é independente, mesmo que se utilize dos resultados dos processos administrativos como meio de prova e meio de convicção do Magistrado. É difícil prever, mas dentro do cenário político atual, é muito provável que o Judiciário se posicione de forma mais intensa e incisiva do que a ANPD.

Aos poucos, os Tribunais vão se familiarizando com a matéria, aumentando a complexidade e a riqueza do debate, fixando entendimentos, até que, no decorrer dos anos, assim como ocorreu com o CDC, as discussões envolvendo dados se tornem comuns. E, obviamente, vão se tornar. As inovações tecnológicas não param, os algoritmos vieram para ficar e os litígios certamente existirão. Cabe ao Direito correr atrás para regular tais conflitos da sociedade informacional e digital.

Seja pela via administrativa, seja pela via judicial, fato é que não se pode legitimar as intervenções na vida privada dos cidadãos, o Estado precisa ter limites, precisa respeitar a Lei e precisa ser vigiado por todos, evitando a situação de panóptico.

Da mesma forma, caberá ao Estado a contratação de agentes/profissionais competentes e habilitados na área tecnológica, em constante aperfeiçoamento e sujeito a cobranças (p. ex. programas efetivos de compliance). Pois, as inovações tecnológicas são capazes de demonstrar que os problemas se modificam constantemente, devendo a administração pública antever as situações possíveis de danos e evitá-las, dentro do possível dela esperado.

Enfim, considerando a existência de falhas da administração pública, o cidadão precisa ter o controle de seus dados pessoais e o pleno conhecimento do direito a eles inerente, até mesmo porque o direito de ser livre, de viver em uma democracia e de ter sua privacidade preservada foram conquistados pela sociedade à duras penas e não há inovação tecnológica capaz de alterar ou retirar-lhe isso, basta se posicionar.

6. REFERÊNCIAS

ABREU, Jacqueline de Souza; LAGO, Lucas; MASSARO, Heloisa. As “permissões” de acesso a dados em apps do governo. **Internet Lab**, 2018. Disponível em: <https://www.internetlab.org.br/pt/privacidade-e-vigilancia/especial-as-permissoes-de-acesso-dados-em-apps-do-governo/>. Acesso em 08.11.2020.

ABREU, Jacqueline de Souza; LAGO, Lucas; MASSARO, Heloisa. Por que se preocupar com o que o Estado faz com nossos dados pessoais?. **Internet Lab**, 2018. Disponível em: <https://www.internetlab.org.br/pt/privacidade-e-vigilancia/especial-apps-do-governo/>. Acesso em 08.11.2020.

AGUIAR JUNIOR, Ruy Rosado. Proteção da boa-fé subjetiva. **Revista da AJURIS**. v. 39. n. 126. Junho 2012. Disponível em: <www.ajuris.org.br/OJS2/index.php/REVAJURIS/article/download/781/475>. Acesso em 10.05.2019.

BARROSO, Luís Roberto. **Curso de Direito Constitucional Contemporâneo:** os conceitos fundamentais e a construção do novo modelo. [Recurso Eletrônico], 7. ed., São Paulo: Saraiva Educação, 2018.

BASU. Kaushik. **The Republic of Beliefs**. Princeton University Press, 2018.

BENTHAM. JEREMIAS. **O Panóptico.** TADEU, Tomaz. (Org.). 2ª ed. Belo Horizonte: Autêntica Editora, 2008.

BESSA, Leonardo Roscoe Bessa. **Relação de Consumo e Aplicação do Código de Defesa do Consumidor**. 2ª ed. São Paulo: Revista dos Tribunais, 2009.

BIONI, Bruno R. **Autodeterminação informacional:** Paradigmas inconclusos entre os direitos da personalidade, regulação dos bancos de dados eletrônicos e a arquitetura da internet. Dissertação de Mestrado. Faculdade de Direito da Universidade de São Paulo, 2016.

BIONI, Bruno. Compreendendo o conceito de anonimização e dado anonimizado. **GEN Jurídico**. 2020. Disponível em: <https://genjuridico.jusbrasil.com.br/artigos/889500718/compreendendo-o-conceito-de-anonimizacao-e-dado-anonimizado>. Acesso em 10/01/2021.

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

BLANCHET, Luiz Alberto. **Administração Pública, Ética e Desenvolvimento**. 3ª Edição. Curitiba: Juruá, 2020.

BOBBIO, Norberto. **Teoria da Norma Jurídica.** Trad. Fernando Pavan Baptista e Ariani Bueno Sudatti. São Paulo: EDIPRO, 2001.

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

BRAMAN, Sandra. **Change of state**: information, policy and power. Cambrige: The MIT Press, 2006.

BRASIL. Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo. **Incidentes**, 2020. Disponível em: <https://emnumeros.ctir.gov.br/incidentes/>. Acesso em 10.01.2020.

BRASIL. Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo. **Estatísticas resultantes do trabalho de detecção, triagem, análise e resposta a incidentes cibernéticos**, 2020. Disponível em: <https://emnumeros.ctir.gov.br/>. Acesso em 05.10.2020.

BRASIL. Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo. **Sobre**, 2020. Disponível em: <https://www.ctir.gov.br/sobre/>. Acesso em 05.10.2020.

BRASIL. Conselho Nacional de Justiça. Justiça em Números – 2019. Disponível em:<https://paineis.cnj.jus.br/QvAJAXZfc/opendoc.htm?document=qvw_l%2FPainelCNJ.qvw&host=QVS%40neodimio03&anonymous=true&sheet=shResumoDespFT>. Acesso em: 28.12.2020.

BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo: para além da informação credíticia**, elaboração Danilo Doneda. – Brasília: SDE/DPDC, 2010.

BRASIL. Governo Digital. **Guias Operacionais para adequação à LGPD**. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd>. Acesso em: 02.01.2021.

BRASIL. Presidência da República. **Autoridade Nacional de Proteção de Dados contribui para a segurança jurídica de cidadãos**. 2020. Disponível em: <https://www.gov.br/casacivil/pt-br/assuntos/noticias/2020/novembro/autoridade-nacional-de-protecao-de-dados-contribui-para-a-seguranca-juridica-de-cidadaos-1>. Acesso em: 28.12.2020.

BRASIL. Superior Tribunal de Justiça. **O método bifásico para fixação de indenizações por dano moral**. 2018. Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias-

antigas/2018/2018-10-21_06-56_O-metodo-bifasico-para-fixacao-de-indenizacoes-por-dano-moral.aspx>. Acesso em 19/01/2021.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nª 1.758.799-MG**. Relatora: Ministra Nancy Andrighi. Publicado em 19/11/2019. Disponível em: <https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1888267&num_registro=201700065219&data=20191119&formato=PDF>. Acesso em 12/01/2021.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1721669/SP**, Rel. Ministro Herman Benjamin, Segunda Turma, julgado em 17/04/2018, DJe 23/05/2018. Disponível em: <https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201800461115&dt_publicacao=23/05/2018>. Acesso em 12/01/2021.

BRASIL. Superior Tribunal de Justiça. **STJ Notícias destaca reforço na segurança de informações digitais do tribunal após o ataque hacker**. 2020. Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/04122020-STJ-Noticias-destaca-reforco-na-seguranca-de-informacoes-digitais-do-tribunal-apos-o-ataque%E2%80%AFhacker.aspx>. Acesso em 10/01/2021.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 6.387.** Relatora: Min. Rosa Weber. Julgado em 07/05/2020. Disponível em: < http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629>. Acesso em 02.01.2021.

BRASIL. Supremo Tribunal Federal. **Agravo Regimental em Recurso Extraordinário nº 788009**. Relator: Min. DIAS TOFFOLI, Primeira Turma, julgado em 19/08/2014. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=6924973>. Acesso em 02.01.2021.

BRASIL. Supremo Tribunal Federal. **Agravo Regimental em Recurso Extraordinário nº 662563**. Relator: Min. Gilmar Mendes, Segunda Turma. Julgado em 20/03/2012. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=11879845>. Acesso em 02.01.2021.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 1.055.941.** Relator: Min. Dias Toffoli. Tribunal Pleno. Julgado em 04/12/2019. Disponível em:<http://www.stf.jus.br/portal/diarioJustica/verDiarioProcesso.asp?numDj=243&dat

aPublicacaoDj=06/10/2020&incidente=5213056&codCapitulo=5&numMateria=168&codMateria=1>. Acesso em 28.12.2020.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 418.416**. Relator: Min. Sepúlveda Pertence. Tribunal Pleno. Julgado em 10/05/2006. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=395790>. Acesso em 28.12.2020.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 601.314.** Relator: Min. Edson Fachin. Tribunal Pleno. Julgado em 24/02/2016. Disponível em:<redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=11668355>. Acesso em: 28.12.2020.

BRASIL. Supremo Tribunal Federal**. Recurso Extraordinário nº 608880**. Relator: MARCO AURÉLIO, Relator(a) p/ Acórdão: ALEXANDRE DE MORAES, Tribunal Pleno, julgado em 08/09/2020. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=753981868>. Acesso em 02.01.2021.

BRASIL. Supremo Tribunal Federal. **Agravo Regimental em Recurso Extraordinário nº 1137891**. Relator: Min. Edson Fachin, Segunda Turma. Julgado em 14/12/2018. Disponível em: < https://jurisprudencia.stf.jus.br/pages/search?classeNumeroIncidente=%22ARE%201137891%22&base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&sort=_score&sortBy=desc&isAdvanced=true>. Acesso em 02.01.2021.

BRITO, Carlos; HERRASTI, Santiago Narváez. Medir y acotar la vigilancia estatal para no perder derechos. IN: BIANCHI, Matías (comp.) **Recuperar la política**: Agendas de Innovación Política en América Latina. Assuntos del Sur – Democracia en Red. Buenos Aires, 2017. P. 301-302.

BRUNO, Marcos Gomes da Silva. Dos agentes de tratamento de dados pessoais. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **LGPD**: Lei Geral de Proteção de dados comentada. São Paulo: Thomson Reuters Brasil, 2019. p.305-327.

CAHALI, Yussef Said. **Responsabilidade Civil do Estado**. 5ª ed. São Paulo: Revista dos Tribunais, 2014.

CAVALIERI FILHO, Sergio. Responsabilidade por omissão. **Interesse Público – IP**, Belo Horizonte, ano 19, n. 104, p. 15-23, jul/ago. 2017.

COPETTI, Rafael; CELLA, José Renato. A salvaguarda da privacidade e a autoridade nacional de proteção de dados. **Revista de direito, governança e novas Tecnologias**, v.5, n.1, p. 44-62, jan./jun., 2019.

CORDEIRO, Menezes. **Da boa-fé no direito civil**. Coimbra: Edições Almedina S/A, 2011.

CORREIA, Pedro Miguel Alves Ribeiro; JESUS, Inês Oliveira Andrade de. O lugar do conceito de privacidade numa sociedade cada vez mais orwelliana. **Direito, Estado e Sociedade**, n. 43, p. 135-161, jul./dez., 2013.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada**. 2ª ed. São Paulo: Thompson Reuters Brasil, 2019.

CUEVA, Ricardo Villas Bôas. A insuficiente proteção de dados pessoais no Brasil. **Revista de Direito Civil Contemporâneo**, v. 13, Out./Dez., 2017.

DONEDA, Danilo. Princípios e proteção de dados pessoais. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira. (Coords.). **Direito & Internet III**: Marco Civil de Internet – Tomo I. Quartier Latin, 2015.

EFING, Antônio Carlos, **Fundamentos do Direito das Relações de Consumo**, 4ª Edição - Revista, Ampliada e Atualizada, Juruá Editora, 2020.

EFING, Antônio Carlos. **Banco de Dados e Cadastro de Consumidores**, São Paulo: Revista dos Tribunais, 2002.

FARIAS, Cristiano Chaves de. ROSENVALD, Nelson. **Curso de direito civil**: obrigações. 11 ed. Salvador: JusPodivm, 2017.

FEIGELSON, Bruno. SIQUEIRA, Antônio. **Comentários à Lei Geral de Proteção de dados.** São Paulo: Thompson Reuters Brasil, 2019.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito, Universidade de São Paulo**, [S. l.], v. 88, p. 439-459, 1993. Disponível em: <https://www.revistas.usp.br/rfdusp/article/view/67231>. Acesso em: 15 dez. 2020.

FERREIRA, Heline Sivini. A dimensão ambiental da teoria da sociedade de risco. In: FERREIRA, Heline Sivini; Freitas, Cinthia Obladen de Almendra (orgs). **Direito Socioambiental e Sustentabilidade**: Estados, Sociedades e Meio Ambiente. Curitiba: Letra da Lei, 2016. p. 108-158.

FERREIRA, Rubens da Silva. A Sociedade da Informação como Sociedade de Disciplina, Vigilância e Controle. **Información, cultura y sociedad**. n. 31, pp. 109-119. Diciembre, 2014.

FOCAULT. Michel. **Vigiar e punir: nascimento da prisão.** Tradução de Lígia M. Pondé Vassalo. Rio de Janeiro: Vozes, 1999.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thompson Reuters Brasil, 2019.

GONDIM, Glenda Gonçalves. Responsabilidade civil no uso indevido dos dados pessoais. In: AMORIM, José de Campos; VEIGA, Fabio da Silva.; AZEVEDO, Patrícia Anjos (Org.). **Desafios do Legaltech**. 1ed.Porto: Instituto Iberoamericano de Estudos Jurídicos, 2020, v. 1, p. 75-84.

GREENFIELD, Adam. **Everyware**: The dawning age of ubiquitoues computing. AIGA: New Riders, 2006.

GROSSMANN, Luís Osvaldo. **LGPD**: governo terá plataforma de consentimento e monitoramento do uso de dados, 2019. Disponível em: <https://www.lgpdbrasil.com.br/lgpd-governo-tera-plataforma-de-consentimento-e-monitoramento-do-uso-de-dados/>. Acesso em 02.01.2020.

HAN, Byung-Chul. **A sociedade da transparência.** Lisboa: Relógio D' Água, 2014.

JUSTEN FILHO, Marçal. **Curso de direito administrativo**. 10 ed. São Paulo: Revista dos Tribunais, 2014.

KELSEN, Hans. **Teoria Geral das Normas**. Trad. José Fiorentino Duarte. Porto Alegre: Fabris, 1986.

KHOURI, Paulo Roberto Roque Antonio. **Direito do consumidor:** contratos, responsabilidade civil e defesa do consumidor em juízo. 3 ed. São Paulo: Atlas, 2006.

LEVIN, Alexandre. Tratamento de dados pelo Poder Público – particularidades previstas na LGPD (Lei 13.709/2018). In: DAL POZZO, Augusto Neves E MARTINS, Ricardo Marcondes (coords.). **LGPD & Administração Pública**. São Paulo: Thomson Reuters Brasil, 2020. P. 233-248.

MANANCOURT, Vicent. Have a GDPR complaint? Skip the regulator and take it to court. **Politico**. 2020. Disponível em:<https://www.politico.eu/article/have-a-gdpr-complaint-skip-the-regulator-and-take-it-to-court/>. Acesso em 28.12.2020.

MARQUES, Claudia Lima. **Contratos Submetidos às Regras do Código de Defesa do Consumidor**. 8ª ed. São Paulo: Revista dos Tribunais, 2016.

MARQUES, Claudia Lima**.** Diálogo Entre o Código de Defesa do Consumidor e o novo Código Civil – do “Diálogo Das Fontes” no Combate às Cláusulas Abusivas. **Revista de Direito do Consumidor**, vol. 45/2003, p. 71-99, Jan./Mar., 2003.

MARTINS-COSTA, Judith. **A boa-fé no direito privado**: critérios para sua aplicação. 2ª ed. São Paulo: Saraiva, 2018.

MAURMO, Júlia Gomes Pereira. A tutela da privacidade nas constituições brasileiras. **Revista de Direito Constitucional e Internacional**, v. 101, p. 105-124, mai./jun., 2017.

MEIRELLES, Hely Lopes; FILHO, José Emmanuel Burle. **Direito administrativo brasileiro**. 42ª ed. São Paulo: Malheiros, 2016.

MELLO. Celso Antônio Bandeira de. **Curso de Direito Administrativo**. 32ª ed. São Paulo: Malheiros, 2015.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 10. ed., rev. e atual. São Paulo: Saraiva, 2015.

MENDES, Laura Schertel Mendes. O direito básico do consumidor à proteção de dados pessoais. **Revista de Direito do Consumidor**, Vol. 95, p.53-75, set./out., 2014.

MORAES, Alexandre. **Direito Constitucional.** 33ª ed. São Paulo: Atlas, 2017.

MORIN, Edgar; KERN, Anne Brigitte. **Terra-pátria.** Porto Alegre: Sulina, 2003.

NERY, Rosa Maria de Andrade; NERY JÚNIOR, Nelson**. Instituições de Direito Civil**: volume II: Das obrigações, dos contratos e da responsabilidade civil. 2ª ed. São Paulo: Thompson Reuters Brasil, 2019.

NERY, Rosa Maria de Andrade; NERY JÚNIOR, Nelson. **Instituições de direito civil:** direito das obrigações. Vol. II. São Paulo, Revista dos Tribunais, 2015.

PEREIRA, Caio Mário da Silva (atualizador Gustavo Tepedino). **Responsabilidade civil**. 11ª ed. Rio de Janeiro: Forense, 2016.

PIETRO, Maria Sylvia Zanella Di. **Direito Administrativo**. [Recurso Eletrônico] 31ª ed. Rio de Janeiro: Forense, 2018.

PINHEIRO, Patrícia Peck. **Direito digital**. [recurso eletrônico]. 5ª ed. São Paulo: Saraiva, 2013.

RODRIGUES, Lucas Troyan; STANSKY, Maria Claudia. A Proteção de Dados Pessoais sob Domínio do Estado no Brasil. In: VEIGA, Fabio da Silva.; LEVATE, Luiz Gustavo; GOMES, Marcelo Kokke. (Org.). **Novos Métodos Disruptivos no Direito**. 1ed.Porto: Instituto Iberoamericano de Estudos Jurídicos e Escola de Direito Dom Helder, 2020, v. 1, p. 823-833.

ROSSO, Angela Maria. LGPD e setor público: aspectos gerais e desafios. **Migalhas**. 2019. Disponível em: <https://migalhas.uol.com.br/depeso/300585/lgpd-e-setor-publico--aspectos-gerais-e-desafios>. Acesso em: 02.01.2021.

SAMPAIO, José Adércio Leite. Comentário ao Artigo 5º, inciso X. In: CANOTILHO, José Joaquim Gomes; MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; STRECK, Lenio Luiz. (Coords.). **Comentários à Constituição do Brasil**. São Paulo: Saraiva/Almedina, 2013. P. 276-285.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel Francisco. **Curso de direito constitucional**. 4. ed., ampl. São Paulo: Saraiva, 2015.

SARMENTO, Daniel. Comentário ao Artigo 220. In: CANOTILHO, José Joaquim Gomes; MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; STRECK, Lenio Luiz. (Coords.). **Comentários à Constituição do Brasil**. São Paulo: Saraiva/Almedina, 2013. P. 2034-2042.

SARTORI, Ellen Carina Mattias. Privacidade e Dados Pessoais: a proteção contratual da personalidade do consumidor na internet. **Revista de Direito Civil Contemporâneo**, v. 9, out./dez., p. 49-104, 2016.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 37ª ed. São Paulo: Malheiros, 2014.

SILVA, Virgílio Afonso da. **Direitos fundamentais**: conteúdo essencial, restrições e eficácia. São Paulo: Malheiros, 2010.

TASSO, Fernando Antonio. Do tratamento de dados pessoais pelo Poder Público. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord). **LGPD**: Lei Geral de Proteção de dados comentada. São Paulo: Thomson Reuters Brasil, 2019. p. 245-284.

TORCHIA, Bruno Martins. MACHADO, Tacianny Mayara Silva. A reponsabilidade subjetiva prevista ne lei geral de proteção de dados e a relação jurídica centre controlador e o encarregado de proteção de dados. In: DAL POZZO, Augusto Neves E MARTINS, Ricardo Marcondes (coords.). **LGPD & Administração Pública**. São Paulo: Thomson Reuters Brasil, 2020. P. 829-847.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, vol. IV, n. 5, 1890.

ZARDO, Francisco. As sanções administrativas de multa simples e multa diária na LGPD. In: DAL POZZO, Augusto Neves E MARTINS, Ricardo Marcondes (coords.). **LGPD & Administração Pública**. São Paulo: Thomson Reuters Brasil, 2020, p. 695-708.