Universidade do Estado do Rio de Janeiro
Centro de Ciências Sociais
Faculdade de Direito

Chiara Antonia Spadaccini de Teffé

Dados pessoais sensíveis:
uma análise funcional da categoria e das hipóteses de tratamento

Rio de Janeiro
2022

Chiara Antonia Spadaccini de Teffé

Dados pessoais sensíveis: uma análise funcional da categoria e das hipóteses de tratamento

Tese de doutorado apresentada, como requisito parcial para obtenção do título de Doutora, ao Programa de Pós-Graduação em Direito, da Universidade do Estado do Rio de Janeiro. Área de concentração: Pensamento Jurídico e Relações Sociais. Linha de Pesquisa: Direito Civil.

Orientador: Prof. Dr. Gustavo Tepedino

Rio de Janeiro

2022

CATALOGAÇÃO NA FONTE
UERJ/REDE SIRIUS/BIBLIOTECA CCS/C

T259 Teffé, Chiara Antonia Spadaccini de.

Dados pessoais sensíveis: uma análise funcional da categoria e das hipóteses de tratamento/ Chiara Antonia Spadaccini de Teffé. - 2022.
310 f.
Orientadora: Prof. Dr. Gustavo Tepedino..

Tese (Doutorado). Universidade do Estado do Rio de Janeiro, Faculdade de Direito.

1.Proteção de dados - Teses. 2. Brasil. [Lei geral de proteção de dados pessoais (2018)] –Teses. 3. Segurança – Teses. I.Tepedino, Gustavo. II. Universidade do Estado do Rio de Janeiro. Faculdade de Direito. III. Título.

CDU 343.45

Bibliotecária: Marcela Rodrigues de Souza CRB7/5906

Autorizo, apenas para fins acadêmicos e científicos, a reprodução total ou parcial desta tese, desde que citada a fonte.

_____ _____

Assinatura Data

Chiara Antonia Spadaccini de Teffé

Dados pessoais sensíveis: uma análise funcional da categoria e das hipóteses de tratamento

Tese de doutorado apresentada, como requisito parcial para obtenção do título de Doutora, ao Programa de Pós-Graduação em Direito, da Universidade do Estado do Rio de Janeiro. Área de concentração: Pensamento Jurídico e Relações Sociais. Linha de Pesquisa: Direito Civil.

Aprovada em 25 de março de 2022

Banca examinadora:

_____

Prof. Dr. Gustavo Tepedino (Orientador)

Faculdade de Direito - UERJ

_____

Prof.ª Dr.ª Milena Donato Oliva

Faculdade de Direito - UERJ

_____

Prof. Dr. Carlos Affonso Pereira de Souza

Faculdade de Direito - UERJ

_____

Prof. Dr. Sérgio Vieira Branco Júnior

Grupo Ibmec Educacional S/A

_____

Prof.ª Dr.ª Caitlin Sampaio Mulholland

Pontifícia Universidade Católica do Rio de Janeiro

Rio de Janeiro

2022

Para Susana e Maria de Lourdes.

AGRADECIMENTOS

Para a conclusão da presente tese, algumas pessoas foram imprescindíveis e marcaram profundamente a minha trajetória acadêmica, profissional e pessoal. De 2017 para cá, construí laços, relações e amizades que foram fundamentais tanto para o meu desenvolvimento enquanto pesquisadora de Direito Civil e de Direito Digital quanto para a elaboração de minha tese de doutorado na Universidade do Estado do Rio de Janeiro (UERJ).

Em primeiro lugar, agradeço ao meu orientador, Professor Gustavo Tepedino, por todo o apoio que sempre ofereceu, pela confiança que depositou em mim quando aceitou me orientar e pelas excelentes aulas e lições ministradas desde a época de mestrado. Sua dedicação à docência e profissionalismo são valores que busco replicar e levar comigo. Deixo, aqui, o meu mais sincero agradecimento e destaco minha grande admiração pelo professor Tepedino.

Ao Professor Carlos Affonso Souza, agradeço pelas grandes lições sobre Direito, Tecnologia e Regulação da rede, pela disponibilidade para discutir os temas abordados nesta tese e pelas valiosas trocas profissionais. Muito obrigada por ter acompanhado toda a minha trajetória na UERJ e por fazer parte de minha banca de doutorado.

À Professora Milena Donato Oliva, agradeço pelos preciosos ensinamentos jurídicos, pelas palavras sempre gentis e amáveis, pelas oportunidades que me ofereceu e, também, por aceitar o convite de compor a banca examinadora desta tese. Sua excelência e didática são muito significativas na vida de seus alunos.

Agradeço igualmente ao Professor Sérgio Branco por todos os valiosos conselhos e trocas, pelas oportunidades que sempre me ofereceu e por aceitar o convite para compor a presente banca. Sua dedicação ao ensino, suas intervenções precisas e organização são uma fonte de inspiração para mim.

À Professora Caitlin Mulholland, agradeço as importantes orientações, o acolhimento sempre afetuoso e a disponibilidade para sempre debater relevantes questões sobre a LGPD. Sua pesquisa sobre dados sensíveis e gênero é uma referência. Obrigada por fazer parte deste momento tão especial de avaliação da tese.

Pela convivência e pelos sólidos ensinamentos, agradeço aos Professores Maria Celina Bodin de Moraes, Anderson Schreiber, Heloisa Helena Barboza e Carlos Konder.

À doutoranda Fernanda Paes Leme Rito, agradeço pela amizade, por todo o apoio e pelo incentivo em continuar os estudos. Pelas trocas acadêmicas e ricas discussões jurídicas, agradeço com todo o meu coração Gabriel Schulman, André Andrade, Vitor Almeida, Elora Fernandes, Maria Regina Rigolon Korkmaz, Priscilla Silva, José Faleiros, Flavia Zangerolame, Christian Perrone e Vanessa Vargas.

Pelo estímulo em estudar cada vez mais e por terem me permitido confirmar o ideal de prosseguir na vida acadêmica, agradeço aos meus queridos alunos de graduação e de pós-graduação da Universidade do Estado do Rio de Janeiro (UERJ), da Universidade Federal do Rio de Janeiro (UFRJ), do Instituto de Tecnologia e Sociedade do Rio (ITS Rio), da Pontifícia Universidade Católica do Rio de Janeiro (PUC Rio) e da Faculdade de Direito do IBMEC. Agradeço também ao ITS Rio pelas inúmeras oportunidades e pelo apoio nos estudos nos últimos anos.

Agradeço o apoio incondicional dos meus amigos queridos Felipe Miranda, Paula Morgado, Tamara Porto, Tiago Rodrigues, Ana Carolina Gouveia e Rafael Magnanini. Ter laços e suporte foi fundamental nesta caminhada.

Por fim, agradeço a minha amada mãe por todo carinho, afeto e paciência.

The processing of personal data should be designed to serve mankind.[1]

[1] Considerando nº 4 do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

RESUMO

TEFFÉ, Chiara Antonia Spadaccini de. *Dados pessoais sensíveis*: uma análise funcional da categoria e das hipóteses de tratamento.2022. 310 f. Tese (Doutorado em Direito Civil) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2022.

Conforme a sensibilidade da informação pessoal aumenta, maiores são as possibilidades de seu titular sofrer interferências indevidas em sua liberdade e tratamentos discriminatórios ilícitos ou abusivos. Diante disso, verificou-se a importância de se estabelecer uma categoria especial de informações: os dados sensíveis. O tratamento de dados de natureza sensível deverá ser mais restrito e encontrar garantias e proteções ampliadas. Na Lei Geral de Proteção de Dados, houve o estabelecimento de rol de bases legais específico para o processamento dessas informações e de tutelas direcionadas tanto técnicas quanto jurídicas. Na presente tese, foi realizado estudo com ênfase em uma análise funcional da referida categoria e das hipóteses para o seu tratamento na LGPD, por meio de pesquisa em doutrina, jurisprudência e legislação nacionais, bem como em referências europeias, especialmente quando voltadas ao Regulamento Geral sobre a Proteção de Dados. Realizou-se, assim, estudo acerca da função da categoria dos dados sensíveis e de seus fundamentos, quais sejam, os princípios do livre desenvolvimento da personalidade e da não discriminação. Em seguida, discutiu-se a possibilidade de serem qualificados dados como altamente sensíveis, em razão, por exemplo, da hipervulnerabilidade de seus titulares e do conteúdo que guardam. As espécies de dados sensíveis foram também analisadas, dentro de uma abordagem dinâmica e contextual. Após, a disciplina normativa aplicável para o tratamento de dados sensíveis foi desenvolvida, focando-se nas bases legais estabelecidas na LGPD. Por fim, foram apresentadas questões específicas relativas à segurança e boas práticas com dados sensíveis, como a aplicação do *privacy by design*, as hipóteses de desenvolvimento do relatório de impacto à proteção de dados pessoais e questões acerca do término e da conservação de tais dados.

Palavras-chave: Dados pessoais sensíveis. Livre desenvolvimento da personalidade. Princípio da não discriminação. Tratamento de dados pessoais.

ABSTRACT

TEFFÉ, Chiara Antonia Spadaccini de. *Sensitive personal data*: a functional analysis of the category and the requirements for its processing. 2022. 310 p. Tese (Doutorado em Direito Civil) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2022.

As the sensitivity of personal information increases, the possibilities of data subjects suffering undue interferences in their freedom and unlawful discrimination become greater. Taking this into account, it was necessary to establish a special category of information: Sensitive Personal Data. The processing of sensitive data should be more restricted, and bear increased guarantees and protections. In the Brazilian General Data Protection Law, the legislation established a list of the specific legal basis for the processing of sensitive personal data as well as technical and legal protections aimed at ensuring extended guarantees. In the present thesis, the study was carried out with an emphasis on a functional analysis of the referred category and the requirements for its processing in LGPD. To this end, there was an analysis of national doctrine, jurisprudence, and legislation, as well as European content, when especially focused on the General Data Protection Regulation. Thus, a study was carried out on the function of the category of sensitive data and its foundations, namely, the principles of free development of personality and non-discrimination. Then, the possibility of qualifying some data as highly sensitive was discussed, due, for example, to the hypervulnerability of their data subjects and the specific content they present. The types of sensitive data were also analyzed, within a dynamic and contextual approach. Afterward, normative discipline applicable to the processing of sensitive personal data was developed, focusing on the legal basis established in the LGPD. Finally, specific issues related to security and good practices with sensitive data were presented, such as the application of privacy by design, the hypotheses for developing data protection impact assessments, and questions about the termination and storage of such data.

Keywords: Sensitive personal data. Free development of personality. Principle of non-discrimination. Personal data processing.

SUMÁRIO

	INTRODUÇÃO	11
1	**DADOS SENSÍVEIS: ESTUDO ACERCA DA FUNÇÃO DA CATEGORIA E DE SEUS FUNDAMENTOS**	15
1.1	**A Lei Geral de Proteção de Dados Pessoais: cenário tecnológico e estrutura do modelo brasileiro**	15
1.2	**A categoria especial dos dados sensíveis: tutela do livre desenvolvimento da personalidade e da não discriminação**	33
1.2.1	Dados sensíveis: análise crítica acerca de sua definição e qualificação	47
1.2.1.1	A definição dos dados sensíveis no contexto do Regulamento Geral Europeu sobre a Proteção de Dados	66
1.3	**Dados altamente sensíveis: uma possibilidade a se discutir**	72
2	**ESPÉCIES DE DADOS SENSÍVEIS: UMA DEFINIÇÃO DINÂMICA E CONTEXTUAL**	82
2.1	**O rol de dados sensíveis da LGPD: por uma tutela ampliada das informações pessoais**	83
2.2	**Estudo dos dados sensíveis no cenário jurídico brasileiro**	88
2.2.1	Dados pessoais sensíveis sobre origem étnica ou racial	90
2.2.2	Dados pessoais sensíveis acerca de crenças e filiações	98
2.2.3	Dados pessoais sensíveis corporais	102
2.2.3.1	Dados referentes à saúde	105
2.2.3.1.1	Dados de saúde e a pandemia de COVID-19	119
2.2.3.2	Dados genéticos	123
2.2.3.3	Dados biométricos	128
2.2.4	Dados referentes à vida sexual	136
3	**DISCIPLINA NORMATIVA APLICÁVEL PARA O TRATAMENTO DE DADOS SENSÍVEIS**	148
3.1	**Tratamento de dados pessoais: requisitos e características**	148
3.2	**Seleção da base legal mais adequada para o tratamento de dados sensíveis**	157

3.2.1 Consentimento específico, destacado e para finalidades específicas.....167
3.2.2 Cumprimento de obrigação legal ou regulatória pelo controlador 180
3.2.3 Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos 183
3.2.4 Realização de estudos por órgão de pesquisa 185
3.2.5 Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral 188
3.2.6 Proteção da vida ou da incolumidade física do titular ou de terceiro 191
3.2.7 Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.....191
3.2.8 Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos 194
3.2.9 Compartilhamento de dados sensíveis pelo setor privado 197
3.2.10 Tratamento de dados públicos sensíveis 201
3.3 **Tratamento de dados sensíveis de crianças e de adolescentes** 206
4 **SEGURANÇA E BOAS PRÁTICAS COM DADOS SENSÍVEIS**.....226
4.1 **Cuidados específicos e boas práticas no tratamento de informações pessoais sensíveis** 226
4.1.1 Aplicação do Privacy by Design no tratamento de dados sensíveis 231
4.1.2 Hipóteses de desenvolvimento do relatório de impacto à proteção de dados pessoais 238
4.2 **Gestão de riscos e mitigação de incidentes de segurança** 247
4.3 **Término do tratamento de dados e conservação de dados sensíveis** 254
CONCLUSÃO 263
REFERÊNCIAS 284

INTRODUÇÃO

Os dados contam histórias sobre nós: indivíduos, grupos e sociedades. Quanto mais dados pessoais são tratados e tecnologias sofisticadas empregadas, mais perfis são criados e análises e predições realizadas. A partir de informações pessoais é possível conhecer hábitos, comportamentos, gostos, preferências, ascendência, estado de saúde e crenças de uma pessoa natural. Ao longo do tempo, a qualidade e a precisão das análises vêm sendo aperfeiçoadas, havendo, inclusive, a utilização de complexas estruturas de inteligência artificial por agentes públicos e privados.

Na era da informação, o corpo não se resume ao aspecto físico e materialmente visível, mas abrange também o conjunto de dados pessoais sobre o indivíduo, formando o que foi denominado por Stefano Rodotà[2] de "corpo eletrônico". Ao desenvolver o referido conceito, o jurista italiano realçou a importância da proteção de dados pessoais para o exercício da cidadania e como instrumento contra a expansão do monitoramento estatal e o uso indiscriminado de dados por instituições de diversos segmentos.

Dados pessoais são continuamente tratados nas mais variadas relações, seja em compras em farmácias, na manutenção de perfis em mídias sociais, na abertura de contas em bancos ou por meio de ferramentas de vigilância e reconhecimento facial. Traços de cada um de nós restam armazenados em inúmeros bancos de dados, onde nossa identidade é dissecada e desmembrada, onde aparecemos ora como consumidores, ora como eleitores, devedores, trabalhadores ou usuários de serviços.[3]

Daniel Solove[4] aponta que as pessoas costumam afirmar que valorizam a privacidade, porém as próprias, por vezes, fornecem informações pessoais, inclusive sensíveis, para obterem pequenos descontos, benefícios e facilidades em bens e serviços. Os indivíduos expressam preocupação com a privacidade e a proteção de

---

[2] Cf. RODOTÀ, Stefano. *A vida na sociedade da vigilância – a privacidade hoje.* Coord. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. CLERICI, Giovanna Bianchi. *Corpo elettronico e tecnologie informatiche*. Roma, 30 de janeiro de 2018. Disponível em: <https://www.garanteprivacy.it/documents/10160/0/Convegno+Uomini+e+Macchine+-+Intervento+di+Giovanna+Bianchi+Clerici.pdf/5156d23d-7a35-45fb-9b8d-f803a10426b3?version=1.0> Acesso em: 02.02.21.

[3] RODOTÀ, Stefano. *Salviamo il corpo.* Trecho de discurso proferido em conferência sobre "Transformações do corpo e dignidade da pessoa", Roma, 04 de maio de 2005. Disponível em: <https://www.privacy.it/archivio/rodo20050504.html> Acesso em: 02.02.21

[4] SOLOVE, Daniel J. The Myth of the Privacy Paradox. *George Washington Law Review* 1, 89, jan. 2021. Disponível em: <https://ssrn.com/abstract=3536265> Acesso em: 02.02.21.

dados, mas algumas vezes falham em tomar medidas simples e não custosas para protegê-las. Esse fenômeno, segundo o autor, é conhecido como o "paradoxo da privacidade" e impacta profundamente a tutela dos dados pessoais. Em atividades do cotidiano, muitas vezes, ocorre o fornecimento voluntário ou a pedido de terceiros de informações pessoais, sem que um efetivo questionamento sobre o porquê da solicitação, a finalidade do tratamento e a política de tratamento desenvolvida seja realizado.

Conforme o grau de sensibilidade da informação aumenta, maiores são as possibilidades de seu titular sofrer interferências indevidas em sua liberdade e tratamentos discriminatórios ilícitos ou abusivos. Por tal razão, além da criação de uma categoria especial para tutelar determinadas informações pessoais – os dados sensíveis – , mostrou-se necessário regular de forma mais restrita seu tratamento e instituir instrumentos amplos para a sua proteção.

Nesse sentido, no capítulo 1 da presente tese, busca-se realizar uma análise profunda da categoria dos dados sensíveis, levando em conta sua relevância, dinamicidade e função, bem como compreender seus fundamentos. Para tanto, em primeiro lugar, será analisada a Lei Geral de Proteção de Dados (LGPD) e os cenários social e tecnológico que promoveram a sua criação e desenvolvimento. Em seguida, passa-se para os principais fundamentos para a elaboração de uma categoria especial de dados pessoais: o livre desenvolvimento da personalidade e o princípio da não discriminação. Após esse estudo, chega-se à definição, à qualificação e aos contornos dos dados sensíveis, havendo a análise de tais informações tanto no contexto brasileiro quanto no europeu. No final do capítulo, é desenvolvida proposta de proteção ainda mais ampliada para determinados dados sensíveis, levando-se em conta questões como características e vulnerabilidades de seus titulares, conteúdo envolvido e possibilidades de discriminação.

No capítulo 2, busca-se desenvolver contribuição acerca das diversas espécies de dados pessoais considerados sensíveis, analisando-se seus conceitos, conteúdos e quais informações tutelam. Em alguns casos, entender quais dados são, de fato, sensíveis pode ser uma atividade complexa e depender de questões bastante específicas acerca do tratamento realizado e da finalidade dos agentes. Análise essa que se alinha com o primeiro tema abordado no capítulo: a natureza do rol dos dados sensíveis, se

exemplificativo ou taxativo. Em seguida, passa-se para a análise crítica das espécies de dados sensíveis positivadas no Art. 5º, inciso II, da LGPD, quais sejam: dados pessoais sensíveis sobre origem étnica ou racial; dados pessoais sensíveis acerca de crenças e filiações; dados pessoais sensíveis corporais, que englobam dados genéticos, biométricos e referentes à saúde, havendo especial destaque para o tratamento dessas informações no cenário de pandemia de COVID-19; e dados referentes à vida sexual. Por fim, serão analisados dados potencialmente sensíveis, que não foram mencionados expressamente na LGPD como sensíveis, mas que por sua natureza e possibilidades de uso e inferências merecem especial atenção e salvaguardas ampliadas.

Após desenvolver a categoria dos dados sensíveis, realçar a sua importância para o livre desenvolvimento e expressão da pessoa humana e discutir o seu conteúdo, no capítulo 03 serão analisadas normas relativas ao tratamento dos dados pessoais sensíveis e às bases legais aplicáveis a eles. Para tanto, inicialmente, será realizado estudo acerca das hipóteses de tratamento de dados pessoais na LGPD e da estrutura de aplicação da referida lei. Em seguida, a atenção será dirigida ao Artigo 11 da LGPD, que traz o rol de bases legais para o tratamento de dados pessoais sensíveis. Posteriormente, será aprofundado estudo a respeito do tratamento de dados sensíveis de crianças e adolescentes, levando-se em consideração a sua especial condição de pessoa em desenvolvimento, que deve ser tutelada de forma integral e com base em seu melhor interesse.

No capítulo 04 da tese, busca-se finalizar o estudo funcional dos dados sensíveis, por meio da análise de questões relativas à segurança, aos cuidados específicos e às boas práticas no tratamento de tais informações. Será oferecida especial ênfase à lógica do *privacy by design* em todo o ciclo de tratamento de dados e ao relatório de impacto à proteção de dados pessoais, documento relevante, e por vezes fundamental, em determinados tratamentos realizados por sujeitos públicos e privados que envolverem dados sensíveis. No tema da gestão de riscos, serão abordadas algumas questões de ordem técnica – ainda que a presente tese se proponha a ser um texto integralmente jurídico –, diante da compreensão de que a temática necessita de uma aplicação de recursos multidisciplinares. Após, serão desenvolvidas algumas orientações com base em guias da Autoridade Nacional de Proteção de Dados (ANPD) para a mitigação de incidentes de segurança, especialmente envolvendo dados sensíveis. Ao final, o estudo

será dirigido aos artigos da LGPD referentes ao término do tratamento de dados e à conservação de informações pessoais sensíveis.

A presente tese foi estruturada, portanto, em quatro capítulos, além da introdução e das considerações finais. Para a pesquisa, foram utilizados como fontes legislações nacionais, especialmente a LGPD, o Regulamento geral europeu de proteção de dados e doutrinas nacional e estrangeira pertinentes à temática desenvolvida. Julgados nacionais relevantes foram apresentados, quando adequados à discussão em pauta. Em relação à metodologia empregada, utilizou-se como referencial o direito civil-constitucional,[5] o qual preconiza que o intérprete deve permanentemente reler todo o sistema do Código e das leis especiais à luz da Constituição Federal, de forma a obter a máxima realização dos valores constitucionais na seara das relações privadas e, consequentemente, respostas mais adequadas às escolhas de fundo da sociedade contemporânea. A tese foi elaborada buscando representar estudo significativo acerca dos dados pessoais sensíveis conforme as premissas da metodologia do direito civil-constitucional. Justamente por isso optei por não aplicar um recorte mais específico para o tema, e sim desenvolver análise que perpassa uma série de questões desafiadoras, tanto no campo teórico quanto prático, as quais para a sua melhor interpretação exigem uma análise pautada na referida metodologia e nos valores e princípios da Constituição Federal de 1988. Compreender os riscos e tratar adequadamente os dados sensíveis representam tarefa complexa, que impõe aos agentes o cumprimento de deveres legais e éticos, assim como constante prestação de contas. Por sua vez, recomenda-se que os titulares de dados adotem posturas que observem boas práticas em segurança e proteção de dados, questionando tratamentos de informações pessoais, visto que influenciam não apenas a esfera pessoal do indivíduo, mas também a de terceiros.

[5] PERLINGIERI, Pietro. *O Direito Civil na legalidade constitucional.* Rio de Janeiro: Renovar, 2008. p.137-138.

1 DADOS SENSÍVEIS: UMA ANÁLISE FUNCIONAL DA CATEGORIA E DE SEUS FUNDAMENTOS

No primeiro capítulo, será realizada análise da categoria dos dados pessoais sensíveis, levando-se em conta sua relevância, função e dinamicidade, bem como haverá o estudo de seus fundamentos e princípios norteadores. Para tanto, inicialmente, será examinada a Lei Geral de Proteção de Dados (LGPD) e os cenários social e tecnológico que promoveram a sua criação e desenvolvimento. Em seguida, passa-se para os principais fundamentos para a elaboração de uma categoria especial de dados pessoais: o livre desenvolvimento da personalidade e o princípio da não discriminação.

Após esse estudo, chega-se à definição, à qualificação e aos contornos dos dados sensíveis, havendo a análise de tais informações tanto no contexto brasileiro quanto no europeu. No final do capítulo 01, será desenvolvida proposta de proteção ainda mais elevada para determinados dados sensíveis, a partir de questões como características e vulnerabilidades de seus titulares, conteúdos que guardam e possíveis cenários de discriminação ilícita ou abusiva. Discute-se, então, uma possível classificação de dados como altamente sensíveis.

1.1 A Lei Geral de Proteção de Dados Pessoais: cenário tecnológico e estrutura do modelo brasileiro

Informações pessoais são extraídas, transferidas e organizadas de forma cada vez mais rápida e integrada, dialogando com diversos sistemas e bases de dados. Identificação pessoal por biometria, rastreio de localização em dispositivos móveis e logins em aplicativos são exemplos de interações que permitem elevado tratamento de dados, inclusive para fins de segurança e controle, de indivíduos e coletividades. Quanto maior a conexão e a inteligência de bens e serviços, maior será a vigilância imposta sobre os nossos corpos e dados. Gostos, preferências, relacionamentos, rotas e consumo: tudo é minuciosamente coletado para o desenvolvimento de inferências, predições e

informações cada vez mais sensíveis sobre a pessoa humana, o que impõe uma tutela ampla dos dados pessoais e que se encontre atualizada com os avanços científicos e tecnológicos.

A proteção dos dados pessoais é tema de fundamental importância para a sociedade da informação[6]. Conforme crescem os graus de exposição dos indivíduos e de sua sujeição a estruturas tecnológicas, pertencentes a Estados e grandes empresas, verifica-se a relevância de se desenvolver instrumentos que coloquem os direitos à proteção de dados e à privacidade em posição de preeminência, em face de situações estritamente patrimoniais. Nesse sentido, inclusive, certas categorias de dados – pela sensibilidade e pela qualidade das informações que guardam – deverão receber garantias adicionais e não ser utilizadas para fins meramente negociais.[7]

Cabe ao Direito, portanto, atuar tanto no aspecto preventivo da proteção de dados, valorizando a autonomia das pessoas e impondo deveres específicos aos agentes, quanto no aspecto ressarcitório, buscando compreender as violações à privacidade e aos dados pessoais, assim como aplicar instrumentos para a efetiva compensação dos danos sofridos.[8] Em adição, além de seguir estritamente normas, decretos e resoluções, as instituições devem obedecer a todo o arcabouço regulatório pertinente à atividade desenvolvida e criar normas internas – como Códigos de Ética e boas práticas[9] –,

---

[6] CASTELLS, Manuel. *A Sociedade em Rede*. 21ª edição. Paz & Terra: 2013. _____. Fim de milênio - A Era da Informação (vol. 3). 1ª edição. Paz e Terra: 2020.

[7] RODOTÀ, Stefano. *A vida na sociedade da vigilância – a privacidade hoje.* Coord. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p.19.

[8] "Mostra-se útil, nessa esteira, a invocação do que se tem designado como razoável expectativa de privacidade, a ser construída caso a caso, como meio de proteção da pessoa humana e incentivo à lealdade recíproca e mútua confiança nas relações. Todavia, a adoção do critério da legítima expectativa somente se justifica se a ponderação conseguir se desprender da lógica proprietária que, tradicionalmente, acaba por associar a liberdade existencial à prerrogativa de se murar contra agressões alheias ou interferências externas." (TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. O consentimento na circulação de dados pessoais. *Revista Brasileira de Direito Civil – RBDCivil*, Belo Horizonte, v. 25, p. 83-116, jul./set. 2020.)

[9] "Na forma do art. 50 da LGPD, os controladores e operadores, no âmbito de suas competências, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. Tais regras deverão, inclusive, ser publicadas e atualizadas periodicamente. Estar em conformidade deve significar alterar a cultura da instituição no que tange ao tema em destaque, observando-se de forma específica os princípios da LGPD (especialmente a responsabilidade e a prestação de contas, a segurança, a prevenção, a transparência e a não discriminação), além da necessidade de se capacitar todos os sujeitos para que atuem conforme as normas que apresentem relevância jurídica por força de lei ou contrato." (TEFFÉ, Chiara Spadaccini de. LGPD em programas de compliance: vantagem competitiva e aderência às práticas ESG. Jota, publicado em 10 de junho de 2021. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/lgpd-em-programas-de-compliance-vantagem-competitiva-e-aderencia-as-praticas-esg-10062021> Acesso em: 11.06.21)

visando a direcionar o comportamento de seus diretores, executivos e funcionários, coibindo comportamentos negativos, desvios de conduta e inconformidades com as normas.[10] A proteção dos dados relativos à pessoa natural mostra-se, hoje, vital para que o indivíduo se realize integralmente e se relacione, com liberdade e em condições de igualdade, na sociedade. Representa, também, garantia de maior segurança às informações e age impedindo práticas discriminatórias e de vigilância em massa.

O desenvolvimento de mecanismos jurídicos e técnicos destinados a regular o tratamento dos dados auxilia a evitar incidentes de segurança[11], usos indevidos e discriminações ilícitas ou abusivas em face do titular e do grupo de que ele faz parte. Além disso, tais mecanismos afastam práticas que podem prejudicar concretamente as liberdades dos indivíduos, como, por exemplo, determinadas decisões tomadas a partir de análises de dados não informadas ao titular e sob critérios não transparentes que afetem aspectos relevantes de seu perfil pessoal, profissional, de consumo ou de crédito. A depender da forma como os algoritmos são programados, as bases de dados selecionadas e os processos estabelecidos e valorados, o resultado do tratamento pode ampliar assimetrias, preconceitos e desigualdades, situação essa violadora dos fundamentos e objetivos da República e dos Direitos Fundamentais expressos na Constituição de 1988.

O Brasil, até agosto de 2018, não dispunha de lei específica para a proteção de dados pessoais. Sua tutela era pleiteada com base em determinadas previsões

---

[10] Doutrina destaca a importância do compliance, sendo ele responsável pela: "(...) estruturação de políticas e procedimentos corporativos que se traduzam em ações sistemáticas com o objetivo de atender ao cumprimento aos preceitos normativos, a permitir a prevenção do ato ilícito ou, caso tal não seja possível, minorar seus efeitos e sancionar eventuais responsáveis. Os programas de *compliance* relacionam-se à fixação de controles internos que, em reforço à regulação estatal, auxiliem os agentes econômicos a se manterem em conformidade com a lei (e, de forma mais ampla, também com suas políticas corporativas). Sua relevância aprofundou-se nas últimas décadas diante da ampliação do papel sancionador do Estado: paradoxalmente, ao mesmo tempo em que se os agentes econômicos passaram a se preocupar com as (cada vez mais elevadas) sanções aplicadas pelo Estado, passou-se a denotar que apenas essa perspectiva era incapaz de apresentar as soluções necessárias." (FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. Compliance de dados pessoais. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coords.). *A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Revista dos Tribunais, 2019. p. 683-684.)

[11] Cf. SOUZA, Carlos Affonso. Segurança e Sigilo dos Dados Pessoais: primeiras impressões à luz da Lei nª 13.709/18. In: Gustavo Tepedino; Ana Frazão; Milena Donato. (Org.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. 1ed.São Paulo: Revista dos Tribunais, 2019, v. 1, p. 417-440. SOUZA, Carlos Affonso; PADRAO, V. Incidentes de segurança e dever de notificação à luz da Lei Geral de Proteção de Dados Pessoais. In: Carlos Affonso Souza; Eduardo Magrani; Priscilla Silva. (Org.). *Lei Geral de Proteção de Dados (LGPD)*. 1ed.São Paulo: Revista dos Tribunais, 2019, v. 1, p. 213-226.

estabelecidas na Constituição Federal e em algumas normas setoriais, que direta ou indiretamente tratam de questões relacionadas à privacidade e aos dados pessoais, como, por exemplo, o Código de Defesa do Consumidor (Lei nº 8.078/90), o Marco Civil da Internet (Lei nº 12.965/14), a Lei de Acesso à Informação (Lei nº 12.527/11) e a Lei do Cadastro Positivo (Lei nº 12.414/11). Todavia, esse arcabouço regulatório mostrava-se pouco preciso e não oferecia garantias adequadas às pessoas, o que, além de gerar insegurança jurídica e de deixar as informações pessoais mais vulneráveis, acabava tornando o País menos competitivo frente ao cenário externo.

Diante do desenvolvimento de tecnologias cada vez mais sofisticadas para o tratamento de dados, da maior aplicação da inteligência artificial em sistemas e processos e da ampliação da capacidade de armazenamento de informações, mostrou-se urgente a edição e a atualização de legislações (em âmbitos nacional, regional e internacional) que visassem a tutelar de maneira mais específica os dados pessoais. Até o momento, aproximadamente 140 países já adotaram legislações nacionais para garantirem a proteção dos dados e da privacidade[12] da pessoa natural. Muitos instituíram também autoridades nacionais responsáveis pela efetividade das normas voltadas à temática.[13]

Realizar a distinção entre o que é um dado pessoal e o que não é vem se tornando mais difícil e depende, muitas vezes, de uma análise contextual. O progresso tecnológico permite que, de forma rápida, fácil e acessível, dados sejam vinculados a

---

[12] BANISAR, David. National Comprehensive Data Protection/Privacy Laws and Bills 2021. Disponível em: <https://ssrn.com/abstract=1951416>. Acesso em: 28.01.22. Em publicação no início de 2022, o autor afirmou que: "There has been significant developments in the past year with new data protection laws in 9 UN member states (Belarus, China, Ecuador, Mongolia, Rwanda, Saudi Arabia, United Arab Emirates, Zambia, and Zimbabwe), the most ever new countries in a single year, as well as the British Virgin Islands. A law was also approved by the parliament in El Salvador but vetoed by the President. All of the new jurisdictions have an oversight body, but nearly all are not independent, but part of a ministry. (...) There are now a total of 123 UN member states with laws, as well as 20 independent jurisdictions with comprehensive data protection laws applying to the private and all but a couple to the public sector in a single law. 60 of those laws have been adopted since 2011. Again, this does not include countries with only sectoral (such as e-commerce) or sub national laws such as the USA (someday?!?!). A few countries including the US have laws regulating personal information held by the public sector. Around 30 counties have pending initiatives (project of law or bills). In 2021, new initiatives emerged in Bangladesh, Belize, Cambodia, and Vietnam. There are still almost 40 countries with no law, serious initiative, or where there is no information available." Fonte: <https://www.linkedin.com/posts/david-banisar-a3587152_dataprotection-activity-6892784393241649152--p8U> Acesso em: 28.01.22. Outro mapa de leis de proteção de dados relevante para análise encontra-se disponível em página do United Nations Conference on Trade and Development: <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide> Acesso em: 18.01.22.

[13] Cf. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. *Proposta para a criação da Autoridade Brasileira de Proteção aos Dados Pessoais.* Rio de Janeiro: ITS Rio, 2018.

indivíduos de maneiras antes não previstas.[14] Além disso, dados podem ser combinados com outros dados e, no processo, tornar indivíduos identificáveis, havendo alto grau de precisão na atividade. Por exemplo, embora haja algum debate se os endereços IP podem ser considerados informações pessoais, é possível entender que, pelo menos em determinados contextos, eles assim devem ser tratados. Mostra-se possível identificar um indivíduo vinculando um endereço IP a outras informações, como pesquisas na web. As informações coletadas em pesquisas podem revelar, inclusive, informações muito sensíveis sobre as práticas, as preferências e as crenças de um indivíduo. Além disso, ressalta-se que o volume de endereços IP da próxima geração (IPv6) permitirá maior uso de endereços estáticos, aumentando a facilidade com que os indivíduos poderão ser identificados.[15] Adicionalmente, sabe-se que muitos bancos de dados "anônimos" podem ter seus dados vinculados novamente aos seus titulares, se utilizadas técnicas específicas e cruzamentos de informações.[16]

A tecnologia expande o alcance da capacidade humana, registrando referências geográficas, preferências pessoais, dados sensíveis e pessoas com quem nos relacionamos em diferentes esferas. Para a melhor tutela dos direitos fundamentais, há

---

[14] The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines. *OECD Digital Economy Papers*, n. 176, OECD Publishing, Paris, 2011, p. 31-32. Disponível em: <https://doi.org/10.1787/5kgf09z90c31-en> Acesso em: 03.01.21.

[15] Acerca da identificação de pessoas online, cabe trazer de forma sucinta o debate relativo à guarda de portas-lógicas por parte dos provedores. Até que seja concluída a transição da versão "IPv4" para a "IPv6", foi adotado protocolo de rede no Brasil que possibilita o compartilhamento de um IP por mais de um usuário. Nesse ambiente, a porta lógica de origem é um dado que permite identificar um usuário que esteja conectado a um endereço de IP compartilhado. Em 5 de novembro de 2019, a Terceira Turma do Superior Tribunal de Justiça decidiu, no Recurso Especial nº 1.784.156/SP, que os provedores de aplicações de internet devem fornecer dados de porta lógica de origem para a identificação do autor de conteúdo danoso publicado nas plataformas digitais. Segundo o relator, Min. Marco Aurélio Bellizze, "**6.** A versão 4 dos IPs (IPv4), em razão da expansão e do crescimento da internet, esgotou sua capacidade de utilização individualizada e se encontra em fase de transição para a versão 6 (IPv6), fase esta em que foi admitido o compartilhamento dos endereços IPv4 como solução temporária. **7.** Nessa fase de compartilhamento do IP, a individualização da navegação na internet passa a ser intrinsecamente dependente da porta lógica de origem, até a migração para o IPv6. **8.** A revelação das portas lógicas de origem consubstancia simples desdobramento lógico do pedido de identificação do usuário por IP." No mesmo sentido, o REsp 1777769/SP estabeleceu que: "8. Pelo cotejamento dos diversos dispositivos do Marco Civil da Internet mencionados acima, em especial o art. 10, caput e § 1º, percebe-se que é inegável a existência do dever de guarda e fornecimento das informações relacionadas à porta lógica de origem. 9. Apenas com a porta lógica de origem é possível fazer restabelecer a univocidade dos números IP na internet e, assim, é dado essencial para o correto funcionamento da rede e de seus agentes operando sobre ela. Portanto, sua guarda é fundamental para a preservação de possíveis interesses legítimos a serem protegidos em lides judiciais ou em investigações criminais." (REsp 1777769/SP, Rel. Ministra Nancy Andrighi, Terceira Turma, DJe 08/11/2019)

[16] SOUZA, Carlos Affonso. Eles sabem quem é você? Entenda o monitoramento de celulares na quarentena, *Tecfront*, publicado em 17 de abril de 2020. Disponível em: <https://tecfront.blogosfera.uol.com.br/2020/04/17/eles-sabem-quem-e-voce-entenda-o-monitoramento-de-celulares-na-quarentena/?cmpid=copiaecola> Acesso em: 03.01.21.

que se definir, além de hipóteses específicas para o tratamento de dados, quando, onde, como e para quais finalidades poderão ser tratadas as informações pessoais, devendo ser estabelecidas salvaguardadas à pessoa humana, tendo em vista, especialmente, os valores estratégico, financeiro e comercial que elas detêm.

Com a inteligência gerada a partir da análise de dados, as informações pessoais converteram-se em fatores vitais para impulsionar a economia e o mercado, sendo incrementadas, por consequência, estruturas de vigilância e de extração de dados. Tim Wu afirma que haveria uma verdadeira disputa das diversas formas de comunicação pela atenção do consumidor[17] e por seus dados pessoais. Não existiria, assim, acesso gratuito à Internet, a e-mail, à mídia social, à programação de TV ou a blog. Tudo seria pago indiretamente por nós, por meio do interesse e do tempo despendidos. Empresas acompanhariam e monetizariam nossas compras, desejos, interações e medos. Wu identifica este momento como uma importante fase na industrialização da captura da atenção humana e questiona, até que ponto, os "mercadores de atenção" poderiam buscar sua obtenção, já que isso, inevitavelmente, acabaria afetando a privacidade e a proteção de dados dos milhões de usuários da rede.[18]

Na economia digital, o valor dos dados encontra-se relacionado à captura e à mobilização da atenção dos usuários nas plataformas. O ideal é que eles passem o máximo de tempo nesses ambientes, pois, quanto mais engajados, maior será a quantidade de dados acumulados e a acuidade preditiva dos mecanismos algorítmicos, o que, consequentemente, aumentará o valor das receitas dos serviços. Por tal razão, muitas estratégias desse mercado vêm sendo voltadas a desenvolver mecanismos para capturar a atenção de seus usuários, para que eles sejam ativos nas plataformas e para que alimentem o ambiente com informações que, mais tarde, serão tratadas e monetizadas a curto, médio e longo prazo.[19]

---

[17] WU, Tim. *The Attention Merchants: The Epic Scramble to Get Inside Our Heads.* Knopf, 2016.

[18] "A corrida para obter dados já começou, liderada por gigantes como Google, Facebook e Tencent. Até agora, muitos deles parecem ter adotado o modelo de negócios dos "mercadores da atenção". Eles capturam nossa atenção fornecendo-nos gratuitamente informação, serviços e entretenimento, e depois revendem nossa atenção aos anunciantes. Mas provavelmente visam a muito mais do que qualquer mercador de atenção anterior. Seu verdadeiro negócio não é vender anúncios. E sim, ao captar nossa atenção, eles conseguem acumular imensa quantidade de dados sobre nós, o que vale mais do que qualquer receita de publicidade. Nós não somos seus clientes — somos seu produto." (HARARI, Yuval Noah. *21 lições para o século 21*. 1.ed. Companhia das Letras: 2018, p. 107-108)

[19] Sobre o assunto, ver os seguintes autores: WILLIAMS, James. *Liberdade e resistência na economia da atenção*: como evitar que as tecnologias digitais nos distraiam dos nossos verdadeiros propósitos. 1.ed. Arquipélago Editorial, 2021; CITTON, Y. *The ecology of attention*. Malden: Polity Press, 2016;

O poder de uma plataforma vem sendo avaliado, dentre outros fatores e elementos, com base no tempo gasto pelos usuários nela e na quantidade de interações que eles realizam em seu ambiente, uma vez que o acesso e a permanência deles facilita, por exemplo, a coleta de dados e permite maior exposição à publicidade e a outras formas de exploração. Além disso, eles ficam sujeitos a ações que visam a influenciar suas preferências e visões de mundo,[20] desenhadas, por vezes, a partir dos interesses de agentes que remuneram diretamente a plataforma, sem que haja transparência e uma análise ética de suas reais motivações.[21]

No contexto atual, verifica-se o quão difícil se tornou evitar estruturas estabelecidas por grandes agentes de tecnologia e pelos Estados, seja pela utilidade e

---

CALIMAN, Luciana. Os regimes da atenção na subjetividade contemporânea. *Arq. bras. psicol*., Rio de Janeiro, v. 64, n. 1, p. 02-17, abr. 2012; CRARY, J. *24/7 – Capitalismo tardio e os fins do sono*. São Paulo: Cosac Naify, 2014; DAVENPORT, T; BECK, J. *The attention economy: understanding the new currency of business*. Boston: Harvard Business School Press, 2001; EYAL, N. *Hooked: how to build habit-forming products.* New York: Penguin Group, 2014; FRANCK, Georg. The economy of attention. *Telepolis*, dezembro, 1999. Disponível em <https://www.heise.de/tp/features/The-Economy-of-Attention-3444929.html> Acesso em: 23.01.19; GOLDHABER, M. The Attention Economy and the Net, 1997. Disponível em: <https://firstmonday.org/article/view/519/440> Acesso em 15.12.19.

[20] Com base nas lições de Wu, Frazão afirma que: "(...) a partir do momento em que atenção se torna comoditizada, o tempo em que as pessoas passam em determinadas plataformas passa a ser importante fator não apenas para sujeitá-las à publicidade e à coleta dos seus dados, mas também para sujeitá-las a estratégias que visam influenciar e alterar suas preferências e visões de mundo. É por essa razão que Tim Wu sustenta que o verdadeiro negócio de muitas das indústrias da nova economia é o de influenciar consciências. Vista a questão por esse ângulo, a tecnologia pode estar sendo utilizada contra aquilo que temos de mais precioso: a nossa individualidade. A partir do momento em que as máquinas conseguem nos conhecer melhor do que nós mesmos, podem utilizar nossas fragilidades para manipular nossas emoções, crenças e opiniões para os mais diversos fins, inclusive políticos. Aliás, as eleições de Donald Trump e do Brexit ilustram bem tal preocupação." (FRAZÃO, Ana. Data-driven economy e seus impactos sobre os direitos de personalidade. *Jota*, publicado em 17 de julho de 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/data-driven-economy-e-seus-impactos-sobre-os-direitos-de-personalidade-17072018> Acesso em: 14.01.21)

[21] Segundo Yuval Harari, a médio prazo, esse acúmulo de dados abriria caminho para um modelo de negócio cuja primeira vítima seria a própria indústria da publicidade. O novo modelo seria baseado na transferência da autoridade de humanos para algoritmos, inclusive a autoridade para escolher e comprar coisas. Para o autor, quando algoritmos escolherem e comprarem coisas para nós, a indústria da publicidade tradicional irá à falência, pois serão levadas em conta diversas informações, inclusive pessoais de quem faz a pergunta, para o direcionamento da melhor resposta, segundo o provedor. O autor questiona: se aprendermos com a experiência a confiar no bom senso do Google, em vez de em nossos sentimentos facilmente manipuláveis, qual será a utilidade de publicidades? (HARARI, Yuval Noah. *21 lições para o século 21*. 1.ed. Companhia das Letras: 2018, p. 107-109.) Já em uma estrutura a longo prazo, Harari destaca que: "(...) ao reunir informação e força computacional em quantidade suficiente, os gigantes dos dados poderão penetrar nos mais profundos segredos da vida, e depois usar esse conhecimento não só para fazer escolhas por nós ou nos manipular mas também na reengenharia da vida orgânica e na criação de formas de vida inorgânicas. Vender anúncios pode ser necessário para sustentar os gigantes no curto prazo, mas eles frequentemente avaliam aplicativos, produtos e companhias em função dos dados que colhem deles, e não do dinheiro que eles geram. Um aplicativo popular pode não ter um bom modelo de negócios e até mesmo perder dinheiro no curto prazo, mas na medida em que absorver dados pode valer bilhões." (HARARI, Yuval Noah. *21 lições para o século 21*. 1.ed. Companhia das Letras: 2018, p. 108-109.)

pela qualidade dos serviços oferecidos, seja em razão de sua essencialidade para o exercício de direitos e deveres como cidadão. Isso pode se tornar ainda mais difícil, inclusive, se as pessoas começarem a depender de redes e algoritmos tanto para tomarem grande parte de suas decisões quanto para contratarem e utilizarem bens e serviços.

Essa dinâmica é bem analisada por Shoshana Zuboff, que desenvolveu o conceito de *capitalismo de vigilância*: estrutura que considera a experiência humana como material cru, gratuito e disponível para práticas comerciais ocultas de extração, predição e venda de dados.[22] Através do oferecimento de serviços aparentemente gratuitos para bilhões de pessoas, os provedores responsáveis por esses serviços monitoram o comportamento dos usuários, obtendo detalhes surpreendentes, inferindo e, até mesmo, moldando comportamentos. Os capitalistas de vigilância descobriram que poderiam tratar dados não apenas para conhecer nosso comportamento, mas também para moldá-lo. Isso tornou-se um imperativo econômico. Já não bastava automatizar o fluxo de informações sobre nós; o objetivo passou a ser automatizar-nos.[23] Dessa forma, quase todo produto ou serviço "inteligente" ou "personalizado", dispositivo habilitado para internet e assistente digital seria parte da cadeia de suprimentos para o tratamento em massa de dados comportamentais. Estaríamos diante de mais uma fase da evolução do capitalismo: ele visaria à exploração de previsões comportamentais derivadas da vigilância dos usuários.

Embora alguns desses dados sejam aplicados à melhoria dos serviços, boa parte alimenta processos avançados, conhecidos como inteligência de máquina, sendo importantes para a elaboração de produtos de previsão que antecipam o que você fará agora, em breve e mais tarde. Esses produtos de previsão são negociados em um novo tipo de mercado, o qual é chamado, pela autora, de *mercados futuros comportamentais*. Neste cenário, os agentes do capitalismo de vigilância teriam enriquecido imensamente com tais operações comerciais, pois muitas empresas estariam dispostas a apostar em nosso comportamento futuro.[24] Zuboff afirma que conhecimento, autoridade e poder

[22] Cf. ZUBOFF, Shoshana. *The Age of Surveillance Capitalism*: The Fight for a Human Future at the New Frontier of Power. 1.ed. PublicAffairs: 2019.

[23] Disponível em: <https://www.washingtonpost.com/opinions/surveillance-capitalism-has-gone-rogue-we-must-curb-its-excesses/2019/01/24/be463f48-1ffa-11e9-9145-3f74070bbdb9_story.html> Acesso em: 26.12.20

[24] Em entrevista, Shoshana Zuboff afirma que: “Surveillance capitalism was invented around 2001 as the solution to financial emergency in the teeth of the dotcom bust when the fledgling company faced the loss

dependeriam do capital de vigilância, para o qual seríamos apenas "recursos humanos naturais".

Criou-se, então, o que foi chamado por Frank Pasquale de *one way mirror*[25], em que os dados pessoais dos cidadãos têm sido utilizados por governos e grandes *players* para que tais agentes saibam tudo sobre nós, enquanto nada ou pouco sabemos sobre os dois primeiros. Suas previsões são *sobre* nós, mas não *para* nós. Tudo isso acontece por meio de monitoramento e controle constantes acerca de cada passo da vida dos indivíduos, o que leva a um verdadeiro capitalismo de vigilância, cuja principal consequência é a consolidação de uma sociedade também de vigilância.[26]

Nesse ambiente, insere-se a Lei Geral de Proteção de Dados brasileira (Lei 13.709/18) que, após longo processo legislativo, alterações em seu texto e dúvidas sobre a data de sua efetiva entrada em vigor, teve sua aplicação praticamente integral consagrada em setembro de 2020.[27] Na norma, foi estabelecido um modelo legislativo

---

of investor confidence. As investor pressure mounted, Google's leaders abandoned their declared antipathy toward advertising. Instead they decided to boost ad revenue by using their exclusive access to user data logs (once known as "data exhaust") in combination with their already substantial analytical capabilities and computational power, to generate predictions of user click-through rates, taken as a signal of an ad's relevance. Operationally this meant that Google would both repurpose its growing cache of behavioural data, now put to work as a behavioural data surplus, and develop methods to aggressively seek new sources of this surplus. The company developed new methods of secret surplus capture that could uncover data that users intentionally opted to keep private, as well as to infer extensive personal information that users did not or would not provide. And this surplus would then be analysed for hidden meanings that could predict click-through behaviour. The surplus data became the basis for new predictions markets called targeted advertising. Sheryl Sandberg, says Zuboff, played the role of Typhoid Mary, bringing surveillance capitalism from Google to Facebook. Here was the origin of surveillance capitalism in an unprecedented and lucrative brew: behavioural surplus, data science, material infrastructure, computational power, algorithmic systems, and automated platforms. As click-through rates skyrocketed, advertising quickly became as important as search. Eventually it became the cornerstone of a new kind of commerce that depended upon online surveillance at scale." (Disponível em: <https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook?CMP=share_btn_link&fbclid=IwAR2OjTc2gx9HR19EmerWV_99KeVEi9Kfcw-sQJgyH41m1WtaNbui2rlDIas> Acesso em: 25.12.20)

[25] "We do not live in a peaceable kingdom of private walled gardens; the contemporary world more closely resembles a one-way mirror. Important corporate actors have unprecedented knowledge of the minutiae of our daily lives, while we know little to nothing about how they use this knowledge to influence the important decisions that we—and they—make." (PASQUALE, Frank. *The black box society*. Cambridge: Harvard University Press. 2015. p. 9)

[26] "The corporate strategists and governmental authorities of the future will deploy their massive resources to keep their one-way mirrors in place; the advantages conferred upon them by Big Data technologies are too great to give up without a fight. But black boxes are a signal that information imbalances have gone too far. We have come to rely on the titans of reputation, search, and finance to help us make sense of the world; it is time for policymakers to help us make sense of the sensemakers." (PASQUALE, Frank. *The black box society*. Cambridge: Harvard University Press. 2015. p. 17.)

[27] LGPD, Art. 65. Esta Lei entra em vigor: (Redação dada pela Lei nº 13.853, de 2019) I - dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e (Incluído pela Lei nº 13.853, de 2019) I-A – dia 1º de agosto de 2021, quanto aos

que privilegia a prevenção de danos à pessoa humana[28] e a segurança no tratamento de dados pessoais, instituindo deveres e responsabilidades específicas aos agentes, além de amplo rol de princípios e direitos aos titulares dos dados. Busca-se minimizar os riscos de violação à privacidade e aos dados pessoais, como também evitar tratamentos abusivos e vazamentos de informações.[29]

A proteção de dados e a norma jurídica referente à matéria podem ser percebidas como formas de: (i) conter os efeitos nefastos do capitalismo de vigilância e as manipulações oriundas de grandes plataformas; (ii) afastar os riscos que determinadas aplicações com algoritmos podem oferecer às liberdades fundamentais; e (iii) trazer garantias às pessoas diante da opacidade e da ausência de *accountability* de muitas estruturas políticas e econômicas. [30] As inferências e predições realizadas por meio de tratamentos de dados mostram-se bastante preocupantes, pois podem determinar ou influenciar destinos, desejos e classificações, inclusive, restringindo indevidamente o acesso a bens e oportunidades, bem como ampliando cenários de discriminações e desigualdades.

Conforme pontua Harari:

> À medida que, através de sensores biométricos, cada vez mais dados fluírem de seu corpo e seu cérebro para máquinas inteligentes, será fácil para corporações e agências do governo conhecer você, manipular você e tomar decisões por você. Mais importante ainda, eles serão capazes de decifrar os mecanismos profundos de todos os corpos e cérebros, e com isso adquirir o poder de fazer a engenharia da vida. Se quisermos evitar que uma pequena elite monopolize esses poderes, que parecem divinos, e se quisermos impedir que a humanidade se fragmente em castas biológicas, a questão chave é: quem é dono dos dados? Os dados de meu DNA, meu cérebro e minha vida pertencem a mim, ao governo, a uma corporação ou ao coletivo humano?[31]

---

arts. 52, 53 e 54; (Incluído pela Lei nº 14.010, de 2020) II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos. (Incluído pela Lei nº 13.853, de 2019)

[28] O caráter preventivo da LGPD é lembrado, por exemplo, nos seguintes dispositivos: Art. 6º, II, VI, VII, VIII e X; Art. 44; Art. 46; Art. 47; Art. 48; Art. 49; e Art. 50

[29] Recomenda-se a leitura de estudo da IBM intitulado "Relatório de custo da violação de dados de 2021". Disponível em: <https://www.ibm.com/br-pt/security/data-breach> Acesso em: 03.02.22.

[30] Cf. FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coords.). *A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Revista dos Tribunais, 2019. p. 23-52.

[31] HARARI, Yuval Noah. *21 lições para o século 21*. 1.ed. Companhia das Letras: 2018. p. 109.

A lei brasileira estabelece que toda pessoa natural tem assegurada a titularidade[32] de seus dados pessoais e parte do pressuposto de que todo dado pessoal[33] é relevante. Essa proteção especial às informações do ser humano resta consagrada no próprio conceito (expansionista)[34] de dado pessoal positivado pelo legislador: "informação relacionada a pessoa natural identificada ou identificável"[35]. A LGPD seguiu, portanto, o modelo europeu, que oferece conceituação ampla. [36]

Como será analisado em pormenor, estabeleceu-se, também, a categoria dos dados sensíveis, com tutela própria e ampliada. Entende-se que dados que não pareçam relevantes em determinado momento, ou que não façam referência a alguém

---

[32] Cf. MAIA, Roberta Mauro Medina. A natureza jurídica da titularidade dos dados pessoais. In: MULHOLLAND, Caitlin. *A LGPD e o novo marco normativo no Brasil*. Arquipélago, 2020.

[33] Danilo Doneda afirma que, "[e]m relação à utilização dos termos "dado" e "informação", é necessário notar preliminarmente que o conteúdo de ambos se sobrepõe em várias circunstâncias, o que justifica uma certa promiscuidade na sua utilização. Ambos os termos servem a representar um fato, um determinado aspecto de uma realidade." O autor continua: "[n]ão obstante, cada um deles possui suas peculiaridades a serem levadas em conta. Assim, o 'dado' apresenta conotação um pouco mais primitiva e fragmentada, como se observa em um autor que o entende como uma informação em estado potencial, antes de ser transmitida. O dado, assim, estaria associado a uma espécie de "pré-informação", anterior à interpretação e a um processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição. Mesmo sem aludir ao seu significado, na informação, já se pressupõe a depuração de seu conteúdo – daí que a informação carrega em si também um sentido instrumental, no sentido da redução da incerteza" (idem, p. 136). (DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados*. 2.ed. São Paulo: Thomson Reuters Brasil, 2019, p. 136.) O art. 5º, I, da LGPD, estabelece que dado pessoal é: "informação relacionada a pessoa natural identificada ou identificável", de modo que se torna possível realizar uma equivalência entre os mencionados termos ("dado" e "informação"). Ademais, a expressão "informação sensível" já se apresentava na Lei nº 12.414/2011 (Lei do Cadastro Positivo).

[34] "(...) via de regra, prevalece conceito *expansionista* pelo qual dado pessoal equivale a uma informação que, direta ou indiretamente, identifica um sujeito. Essa definição abraça, portanto, mesmo as informações que têm o potencial de identificar alguém, ainda que de maneira remota. Desde a década de 1980, organismos internacionais, blocos econômicos, países norte-americanos e latino-americanos conceituam dados pessoais como uma informação a respeito de uma pessoa identificada ou identificável." (BIONI, Bruno. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. E-book)

[35] "(...) o direito comunitário europeu e a LGPD valeram-se do critério da razoabilidade para delimitar o espectro do conceito expansionista de dados pessoais. Não basta a mera possibilidade de que um dado seja atrelado a uma pessoa para atrair o termo identificável. Essa vinculação deve ser objeto de um "esforço razoável", sendo esse o perímetro de elasticidade do conceito de dado pessoal como aquele relacionado a uma pessoa identificável. *A contrario sensu*, se para a correlação entre um dado e uma pessoa demanda-se um esforço fora do razoável, não há que se falar em dados pessoais. Nessa situação, o dado é considerado como anônimo, uma vez que o "filtro da razoabilidade" barra o seu enquadramento como aquele relacionado a uma pessoa identificável." (BIONI, Bruno. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. E-book)

[36] A disposição brasileira segue o previsto no GDPR: "Artigo 4.º Definições. Para efeitos do presente regulamento, entende-se por: «Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;".

diretamente, uma vez transferidos, cruzados e/ou organizados, podem resultar em dados bastante específicos sobre determinada pessoa, trazendo informações, inclusive, de caráter sensível sobre ela. A preocupação, além de envolver o dado em si, engloba também a finalidade do tratamento realizado e as possibilidades de processamentos posteriores.

Nas últimas décadas, a privacidade vem sendo compreendida, também, como o direito de manter controle sobre as próprias informações,[37] passando a fazer referência à possibilidade de a pessoa natural conhecer, controlar, endereçar e, até mesmo, interromper o fluxo das informações a ela relacionadas. Abriu-se, assim, espaço para a chamada *autodeterminação informativa*[38], que, em apertada síntese, representa o direito de o particular controlar a obtenção, a titularidade, o tratamento e a transmissão de seus dados, ou seja, consagra o poder de decisão do indivíduo sobre suas informações, podendo ser invocado tanto em face do Estado quanto em face de particulares.

Nessa esteira, não se mostra mais suficiente, para proteger a privacidade, a garantia de não ingerência alvitrada por Warren e Brandeis, em seu *right to be left alone*, do final do século XIX.[39] A relação entre a privacidade e a autodeterminação informativa pressupõe que o Direito atue de maneira a proteger, da forma mais ampla possível, a pessoa humana, especialmente seus interesses existenciais, fornecendo-lhe,

---

[37] RODOTÀ, Stefano. *A vida na sociedade da vigilância – a privacidade hoje.* Coord. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p.92.

[38] "Em resumo, de acordo com a jurisprudência do Tribunal Constitucional, o direito da autodeterminação informativa se baseia principalmente em três propriedades. Primeiramente, o poder de decisão é formulado como o âmbito de proteção do direito, de tal modo que o indivíduo pode decidir, ele próprio, sobre a coleta e utilização de informações de cunho pessoal (ALBERS, 2005, p. 235). Daí resulta a segunda propriedade, qual seja, a de que o direito fundamental à autodeterminação informativa não abrange um teor de proteção fixo e definido, desviando-se, assim, do modelo de esfera privada de atribuição de dados a uma esfera íntima. Em terceiro lugar, a referência pessoal do dado atua decisivamente sobre o teor da proteção na medida em que cada registro que se revela como pessoal é merecedor de proteção. Em princípio, pode-se observar que o direito à autodeterminação informativa se encontra em uma relação de continuidade com a concepção do direito da personalidade geral. É certo que o Tribunal Constitucional alemão teve que desenvolver um novo conceito na sentença referente ao recenseamento, a fim de proteger o indivíduo contra o processamento automatizado de dados, todavia logrou formular o novo direito fundamental como uma expressão do direito da personalidade geral, ou seja, dentro do já existente quadro da proteção da personalidade. (...) A importância do direito à autodeterminação informativa reside no fato de que a sua fórmula de proteção abstrata oferece grande flexibilidade como poder de decisão (ALBERS, 2005, p. 235). Como não designa um conteúdo de garantia fixo, esse direito pode ser aplicado em múltiplos casos concernentes à coleta, processamento ou transmissão de dados ou informações pessoais." (MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. *Pensar*, Fortaleza, v. 25, n. 4, p. 1-18, out./dez. 2020. p.12.)

[39] WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. *Harvard Law Review*, vol. 4, n. 5, dez. /1890, p. 193-220.

assim, meios para efetivamente compreender, decidir e agir acerca do tratamento realizado sobre seus dados.

O oferecimento aos cidadãos de instrumentos que lhes garantam assumir efetivamente controle acerca do uso e da integridade de suas informações representa garantia de tutela da própria dignidade da pessoa humana, tendo em vista o papel predominante da informação para as escolhas do indivíduo. Nesse sentido, há alguns anos a doutrina brasileira vem defendendo a qualificação da proteção de dados pessoais como direito fundamental autônomo, figurando a privacidade como uma de suas referências axiológicas.[40] [41]

Da mesma forma, em 2020, o Supremo Tribunal Federal (ADI 6387 MC-REF/DF)[42] afirmou que a proteção de dados pessoais e a autodeterminação informativa seriam direitos fundamentais autônomos, extraídos do texto constitucional a partir da garantia da inviolabilidade da intimidade e da vida privada (Art. 5º, X), do princípio da dignidade da pessoa humana (Art. 1º, III) e da garantia processual do *habeas data* (Art. 5º, LXXII). Em seguida, em significativa ação do legislativo, por meio da Emenda Constitucional nº 115/22, foi assegurado como direito fundamental o direito à proteção dos dados pessoais, inclusive nos meios digitais.

No contexto europeu, recorda-se que a privacidade e a proteção de dados são

[40] A tese vem sendo defendida por Danilo Doneda há mais de uma década. Cf. por todos DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: elementos da formação da Lei geral de proteção de dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019. Neste sentido, Frazão destaca que: "(...) seja em razão do amplo alcance da LGPD, seja em razão da sua preocupação com a tutela das situações existenciais dos titulares de dados, pode-se dizer que foi acolhida concepção convergente com a daqueles que, a exemplo de Rodotà, sustentam que a proteção de dados corresponde a verdadeiro direito fundamental autônomo, expressão da liberdade e da dignidade humana, que está intrinsecamente relacionada à impossibilidade de transformar os indivíduos em objeto de vigilância constante" (FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. *Lei Geral de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, p. 103).

[41] SARLET, Ingo. Precisamos da previsão de um direito fundamental à proteção de dados no texto da CF? *Conjur*, publicado em 4 de setembro de 2020. Disponível em: <https://www.conjur.com.br/2020-set-04/direitos-fundamentais-precisamos-previsao-direito-fundamental-protecao-dados-cf> Acesso em: 26.12.20.

[42] Em decisão proferida em maio de 2020, o Supremo Tribunal Federal, em votação quase unânime (10 votos a 1), referendou a medida cautelar deferida pela ministra Rosa Weber no âmbito de cinco ações diretas de inconstitucionalidade — propostas pelo Conselho Federal da Ordem dos Advogados do Brasil e por quatro partidos políticos (PSB, PSDB, PSOL e PCdoB). A decisão referendada suspendeu a eficácia da Medida Provisória nº 954, de 17/4/2020, que "Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020."

identificadas como direitos fundamentais desde a Carta dos Direitos Fundamentais da União Europeia (2000), nos artigos 7º e 8º. Inclusive, a Convenção Europeia de Direitos Humanos (1950) já previa a proteção da vida privada e familiar. Ela possui especial relevância, visto que é de aplicação vinculativa a todos os Estados signatários.

Entende-se que a defesa da privacidade e dos dados pessoais deve integrar as proteções individuais e coletivas dos direitos fundamentais, tendo em vista a importância de ambas para a tutela integral da pessoa humana e de sua comunidade. Quando se controla o tratamento de informações pessoais, não se resguarda apenas o indivíduo, cujos dados estão relacionados, mas também o seu grupo social, interesses coletivos e as futuras gerações.

A partir de coletas massivas de dados, é possível realizar perfilizações (*profiling*)[43], marketing personalizado, inferências discriminatórias em face de determinados grupos e análises preditivas de comportamentos, tratamentos esses que mostram a relevância de se trabalhar o direito à proteção de dados e o direito à privacidade também como direitos de grupos. [44]

Entende-se que a criação de perfis pode perpetuar estereótipos e ampliar a segregação social. Ela também pode prender uma pessoa em uma categoria e restringi-la às preferências sugeridas, o que prejudicaria sua liberdade de escolher, por exemplo, certos produtos ou serviços, como livros, música ou feeds de notícias. Em alguns casos, a criação de perfil pode levar a previsões imprecisas. Em outros, pode levar à negação

[43] O GDPR define profiling no Artigo 4 (4) como: qualquer forma de processamento automatizado de dados pessoais consistindo na utilização de dados pessoais para avaliar certos aspectos pessoais relativos a uma pessoa singular, em particular para analisar ou prever aspectos relativos ao desempenho dessa pessoa no trabalho, situação econômica, saúde, preferências pessoais, interesses, confiabilidade, comportamento, localização ou movimentos.

[44] "The idea that groups may have a right to privacy is not new (see for example Bloustein (1978, 2003)) and it is open to debate (Bisaz 2012). But it has not received the attention it deserves, although it is becoming increasingly important. This because, by far, most people are not targeted by ICTs as individuals but as members of specific groups, where the groups are the really interesting focus, as carriers of rights, values, and potential risks. Think of owners of such and such kind of car, shoppers of such and such kind of food, people who like this kind of music, or people who go to that kind of restaurant, cats owners, dogs owners, people who live at that kind of postal code address, carriers of a specific gene, people affected by a certain disease, … Open Data is more likely to treat types (of customers, users, citizens, demographic population, etc.) rather than tokens (you, Alice, me…), and hence groups rather than individuals. But re-identifiable groups are *ipso facto* targetable groups. It is therefore a very dangerous fallacy to think that if we protect personal data that identify individuals, the protection of the groups will take care of itself." (FLORIDI, Luciano. Open Data, Data Protection, and Group Privacy. *Philos. Technol.* 27, 1–3, 2014. Disponível em: <https://doi.org/10.1007/s13347-014-0157-8> Acesso em: 23.12.20) Ver também: ZANATTA, Rafael. A tutela coletiva na proteção de dados pessoais. *Revista do Advogado*, São Paulo, a.39, n.144, nov. 2019, p.201-208.

de serviços e bens e discriminação injustificada.[45]

Nesse sentido, como destacado expressamente pela própria LGPD[46], também às coletividades devem ser garantidos meios jurídicos e técnicos que aumentem seu poder e controle sobre os dados. Ferramentas como a Ação Civil Pública (ACP), termos de ajustamento de conduta (TAC)[47], a tutela inibitória e o dano moral coletivo

[45] Article 29 Working Party. *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*. Bruxelas: Comissão Europeia, 2018.

[46] LGPD, Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

LGPD, 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. (...) § 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.

[47] Em janeiro de 2019, o Ministério Público do Distrito Federal e Territórios (MPDFT) firmou termo de ajustamento de conduta (TAC) com a empresa Netshoes. O acordo foi proposto pela Unidade Especial de Proteção de Dados e Inteligência Artificial (Espec) do MPDFT, após o vazamento de dados de quase 2 milhões de clientes. No incidente de segurança envolvendo a base de dados de clientes da empresa Netshoes, datado de dezembro de 2017, foram comprometidos dados pessoais como nome, data de nascimento, endereço, CPF e informações de pedidos de milhões de usuários. Dentre outras disposições estabelecidas, a empresa se comprometeu a pagar indenização no valor de R$ 500 mil, a título de indenização pelo dano moral coletivo de caráter nacional em razão do incidente de segurança que comprometeu milhões de titulares dos dados pessoais, a ser recolhido mediante depósitos no Fundo de Defesa de Direitos Difusos (FDD). Ainda que a LGPD não estivesse ainda em vigor, suas bases e princípios foram considerados na lógica do termo, conforme pode ser verificado: <https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/10570-mpdft-e-netshoes-firmam-acordo-para-pagamento-de-danos-morais-coletivos-apos-vazamento-de-dados> Acesso em: 22.12.20

Recorda-se também TAC firmando entre o Ministério Público Federal e a Microsoft com o objetivo de sanar as dúvidas sobre o atendimento dos requisitos de privacidade da lei brasileira pelo sistema operacional Windows 10. No documento, a base legal do consentimento para o tratamento de dados foi bastante reforçada e buscou-se que a empresa promovesse maior transparência aos procedimentos de coleta de informações. Por exemplo, de acordo com a cláusula primeira a Microsoft se comprometeu a promover modificações na interface de instalação do Windows 10, para usuários brasileiros, que lhes permita escolher, de forma livre, informada e inequívoca, qual a opção de coleta de dados ele definirá para o seu equipamento, com amplo esclarecimento sobre a coleta de dados pelo sistema. (Referência: Ação Civil Pública sob o nº 5009507-78.2018.4.03.6100. Tramitou perante a 9ª Vara Cível Federal de São Paulo). Disponível em: <http://www.mpf.mp.br/sp/sala-de-imprensa/noticias-sp/acordo-entre-mpf-e-microsoft-traz-melhorias-na-coleta-de-dados-pessoais-no-windows-10-mediante-esclarecimentos-e-atualizacoes-na-forma-de-obtencao-de-anuencia-expressa-e-inequivoca-dos-usuarios> Acesso em: 22.12.20.

Em 2020, a Unidade Especial de Proteção de Dados e Inteligência Artificial do Ministério Público firmou três termos de ajustamento de conduta: a) Termo de Ajustamento de Conduta nº 003/2020 – Firmado pela empresa Nugo Smart 4U Serviços Operacionais Ltda. com o Ministério Público do Distrito Federal e Territórios, para o pagamento de indenização pelos danos morais coletivos de caráter nacional causados pelo uso indevido de números de Comprovantes de Situação Cadastral - CPFs para a habilitação de chips de telefonia móvel. b) Termo de Ajustamento de Conduta nº 002/2020 – Firmado pela empresa Unitfour Tecnologia da Informação Ltda. com o Ministério Público do Distrito Federal e Territórios, para a criação de um canal de comunicação onde os titulares dos dados pessoais possam exercer seus direitos. c) Termo de Ajustamento de Conduta nº 001/2020 - Firmado pela empresa Garupa Desenvolvimento de Sistemas Ltda com o Ministério Público do Distrito Federal e Territórios, para proteção dos dados pessoais de clientes (passageiros e motoristas) da plataforma. Disponíveis em:

mostram-se fundamentais para a proteção de interesses coletivos *lato sensu*. Além disso, ressalta-se, também, a importância do incremento de legitimados para a tutela coletiva, seja em juízo ou fora dele, bem como de sujeitos habilitados a participar como *amicus curiae* em ações sobre a matéria. Além disso, instituições governamentais como secretarias[48] e PROCONs merecem maior destaque, emitindo notificações e recebendo reclamações.

A Lei Geral de Proteção de Dados brasileira e o Regulamento Geral Europeu para a Proteção de Dados[49] representam, no contexto atual, instrumentos para a proteção e garantia da pessoa humana, uma vez que facilitam o controle dos dados tratados, impõem deveres e responsabilidades aos agentes de tratamento e proporcionam segurança à circulação de informações. Os dois sistemas encontram-se fortemente alinhados, como desejou o legislador brasileiro. Visa-se, com isso, que nos próximos anos o Conselho Europeu entenda que o país dispõe de um conjunto normativo adequado ao europeu, no que concerne à qualidade da proteção conferida aos dados pessoais, visto que isso facilitará a realização de transações com países do bloco e com a Organização para a Cooperação e Desenvolvimento Econômico (OCDE)[50].

<https://www.mpdft.mp.br/portal/index.php/mpdft-acao/termos-de-ajustamento-de-conduta/10567-unidade-especial-de-protecao-de-dados-e-inteligencia-artificial-espec> Acesso em: 22.12.20.

[48] No início da pandemia em 2020, o aplicativo de videoconferências Zoom foi questionado por questões relativas à sua segurança e à privacidade dos usuários. As discussões estavam relacionadas a uma série de vulnerabilidades da plataforma, à falta de recursos adequados de criptografia e ao compartilhamento de dados com parceiros de forma não transparente. Foi nesse contexto que a Secretaria Nacional do Consumidor (Senacon), do Ministério da Justiça e Segurança Pública, notificou a empresa de teleconferências em abril de 2020, solicitando que prestasse determinadas informações sobre suas práticas e políticas. Mais informações em: <https://agenciabrasil.ebc.com.br/geral/noticia/2020-04/senacon-pede-zoom-esclarecimentos-sobre-suposta-troca-de-informacoes> Acesso em 23.12.20

Em janeiro de 2020, a Senacon afirmou que notificaria os aplicativos de relacionamento Tinder e Grindr para esclarecerem sobre um suposto compartilhamento ilegal de dados pessoais dos usuários que foi identificado pelo Conselho de Consumidores da Noruega no relatório *Out of Control*. Mais informações em: <https://g1.globo.com/economia/tecnologia/noticia/2020/01/15/ministerio-da-justica-vai-notificar-tinder-e-grindr-por-suposta-venda-ilegal-de-dados-pessoais-dos-usuarios.ghtml?utm_source=meio&utm_medium=email> Acesso em 23.12.20

[49] No dia 25 de maio de 2018, o GDPR entrou em vigor. Apesar de ser uma norma da União Europeia, ela apresenta eficácia e aplicação extraterritorial. Por essa razão, por exemplo, muitas empresas nacionais que têm filiais na Europa ou oferecem serviços a pessoas localizadas no continente tiveram que se adaptar, sob pena de severas sanções ou de perderem contratos. A norma cria também obstáculos para a transferência internacional de dados pessoais para países que não sejam considerados com um nível adequado de proteção.

[50] No final de 2020, a OCDE publicou relatório específico sobre o Brasil e questões relacionadas à digitalização e proteção de dados. Cf. OECD, *A Caminho da Era Digital no Brasil*, OECD Publishing, Paris, 2020. Disponível em: <https://doi.org/10.1787/45a84b29-pt.> Acesso em: 18.12.20.

Perante o Conselho, na América Latina,[51] apenas Argentina e Uruguai obtiveram, até o momento, tal reconhecimento.[52] [53]

Vivemos em um ambiente marcado por elevada assimetria informacional: uma parte, geralmente grandes empresas e Estados, detém mais poder, recursos e melhores informações do que a outra, o cidadão comum, por vezes, consumidor nas relações desenvolvidas. Esse cenário enseja diversos questionamentos acerca, por exemplo, da validade do consentimento do titular dos dados nos contratos celebrados, principalmente quando eles são de adesão. Tal assimetria informacional não se revela apenas no poder que os agentes dispõem sobre os dados pessoais de terceiros, mas também nas novas modalidades de negócios, em que informações pessoais de seus usuários representam uma das bases centrais do sistema desenvolvido.

A posição de destaque que o tratamento de dados tem em muitos produtos e serviços oferecidos ao público por empresas – as quais, por vezes, não exigem remuneração direta dos usuários, mas o preenchimento de cadastro, a criação de perfil e/ou o acesso a contatos, imagens e mensagens trocadas[54] – revela a importância dos

[51] Na América do Sul, Argentina, Chile, Colômbia, Peru, Uruguai, Paraguai e Guiana Francesa também possuem leis gerais para a proteção dos dados dos titulares. Na Argentina, a Lei de Proteção de Dados Pessoais foi aprovada em 2000 (Lei n. 25.326 de 2000). No Uruguai, a Lei n. 18.331, que trata da proteção de dados pessoais e da ação de *habeas data*, está publicada desde o ano de 2008.

[52] Tradução livre: A Comissão Europeia tem o poder de determinar, com base no artigo 45.º do Regulamento (UE) 2016/679, se um país fora da UE oferece um nível adequado de proteção de dados. O efeito de tal decisão é que os dados pessoais podem fluir da UE (e Noruega, Liechtenstein e Islândia) para esse país terceiro sem que seja necessária qualquer outra salvaguarda. Por outras palavras, as transferências para o país em questão serão equiparadas às transmissões de dados intra-UE. A Comissão Europeia reconheceu até agora Andorra, Argentina, Canadá (organizações comerciais), Ilhas Faroé, Guernsey, Israel, Ilha de Man, Japão, Jersey, Nova Zelândia, República da Coreia, Suíça, Reino Unido sob o GDPR e o LED, e Uruguai como com proteção adequada. Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>. Acesso em: 03.02.22.

[53] No dia 16 de julho de 2020, o Tribunal Superior de Justiça da União Europeia invalidou o *Privacy Shield*, protocolo de compartilhamento de dados que permitia às empresas norte-americanas transferir informações pessoais sobre os cidadãos da UE aos EUA para processamento de dados. O tribunal alega que o regulamento não pode ser confiável, pois não protege os cidadãos da UE dos programas de vigilância em massa operados por agências de inteligência dos EUA, como a Agência de Segurança Nacional. A decisão traz efeitos para várias empresas americanas, mas impactará particularmente as empresas de tecnologia e mídia social que processam grandes quantidades de dados pessoais, exatamente as informações que a UE deseja proteger. Mais informações em: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf> Acesso em 05.08.2020.

[54] Entende-se que a relação entre os usuários das redes sociais e o provedor de aplicações de internet responsável por elas não seria marcada pela gratuidade, havendo uma situação de remuneração indireta entre as partes, visto que, apesar de o provedor não receber um valor financeiro diretamente de seus usuários, ele seria remunerado diretamente pela publicidade, que tem como público alvo os usuários da rede, e, indiretamente, pelos próprios usuários, que disponibilizam seus dados pessoais para a empresa, ao criarem perfis, interagirem com outros usuários e postarem conteúdos. Há, portanto, uma estrutura de

dados na criação e no desenvolvimento de diversos modelos de negócio na Web 3.0. Exemplos significativos são as mídias sociais, os aplicativos para a entrega de bens e serviços e as ferramentas de intermediação de compra e venda online.

Por essa razão, recomenda-se a escolha de aplicações seguras e transparentes que demonstrem estar plenamente adequadas à LGPD.[55] Além disso, cada pessoa deverá realizar a gestão de sua identidade e de sua privacidade online, avaliando que tipo de dados deseja expor ao público, bem como verificar cuidadosamente as configurações de privacidade de aplicativos e de programas para personalizá-las e para reduzir a coleta e o uso de dados pessoais.

Todos os sujeitos deverão se adaptar a uma nova cultura de tutela dos dados pessoais[56], cabendo especialmente à doutrina, às entidades de defesa de interesses coletivos, ao Judiciário e à Autoridade Nacional de Proteção de Dados harmonizarem a interpretação e a aplicação da Lei. Percebe-se, até o momento, baixa adequação das instituições à LGPD, bem como um aumento significativo no número de ataques cibernéticos, vazamentos de dados e fraudes, envolvendo, inclusive, dados sensíveis. Isso releva a necessidade de uma maior sensibilização das instituições quanto à importância da LGPD, de modo que implementem programas de compliance robustos que visem a sua adequação às normas de proteção de dados, tanto jurídicas quanto técnicas, e aderência aos valores ESG (*environmental, social and corporate*

---

remuneração capaz de assegurar facilmente a manutenção dessas redes, sem haver qualquer contraprestação financeira direta e imediata por parte de seus usuários. É de conhecimento público que o marketing direcionado promovido nas redes sociais vai muito além de *banners* e *links* patrocinados e tem como base o próprio conteúdo inserido pelos usuários. (TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. Redes sociais virtuais: privacidade e responsabilidade civil: análise a partir do Marco Civil da Internet. *Pensar*, Fortaleza, v. 22, n. 1, p. 108-146, jan./abr. 2017.) Esse raciocínio foi chancelado pela jurisprudência do Superior Tribunal de Justiça: "O fato de o serviço prestado pelo provedor de serviço de Internet ser gratuito não desvirtua a relação de consumo, pois o termo 'mediante remuneração' contido no art. 3º, § 2º, do CDC deve ser interpretado de forma ampla, de modo a incluir o ganho indireto do fornecedor". (STJ. 3ª T., REsp 1.193.764, Rel. Min. Nancy Andrighi, DJe de 08.08.2011).

[55] Nesse ambiente, muitas instituições já vêm enxergando o investimento no processo de adequação à LGPD como vantagem competitiva dentro do nicho em que atuam. O cuidado com a privacidade e as informações pessoais dos clientes passa a ser apresentado como elemento adicional ao serviço prestado e diferencial da empresa em termos de segurança e prevenção de riscos.

[56] Como apontado por Lawrence Lessig, o ambiente regulatório é composto não apenas por normas jurídicas, identificando-se também um conjunto de elementos relevantes a influenciar e moldar condutas, como o mercado, a arquitetura e as normas sociais. Esses quatro elementos, operando de forma conjunta e relacionada, servirão tanto para incentivar quanto para desestimular comportamentos de indivíduos e organizações, moldando estruturas e regulando situações. Serão eles, portanto, essenciais para garantirem efetividade e cumprimento da LGDP. (LESSIG, Lawrence. The Law of the Horse: What Cyberlaw Might Teach, 113 *Harvard Law Review*, p. 501-549, 1999. Disponível em: https://cyber.harvard.edu/works/lessig/finalhls.pdf. Acesso em: 13 out. 2018.)

governance), sigla usada para se referir e mensurar as práticas ambientais, sociais e de governança de um negócio.[57]

A LGPD toma corpo em um momento extremamente delicado para a sociedade: a pandemia de COVID-19. Diante desse cenário, o debate em torno de medidas e sistemas que utilizam dados pessoais sensíveis tornou-se ainda mais importante e trouxe novas preocupações para os titulares dos dados e organizações. Compreender, dentro do contexto brasileiro, o que são os dados sensíveis, como eles podem ser tratados e quais ferramentas de proteção deverão ser estabelecidas e garantidas, mostra-se contribuição pertinente no presente momento, diante da recente entrada em vigor da norma e da urgência de se proteger, com a devida atenção e destaque, essa categoria de informações.

1.2 A categoria especial dos dados sensíveis: tutela do livre desenvolvimento da personalidade e da não discriminação

Dispõe o Art. 1º da LGPD que a norma tem como objetivo expresso proteger os direitos fundamentais de liberdade e de privacidade, além do livre desenvolvimento da personalidade da pessoa natural. Sua relevância, em verdade, é ainda maior, atuando na promoção da dignidade da pessoa humana e na garantia dos direitos fundamentais nas mais diversas relações estabelecidas. Ao se aplicar, tanto ao setor público quanto ao privado e ao ambiente físico e virtual, a LGPD impõe completa releitura das formas de tratamento de dados pessoais, nas mais variadas áreas e pelos mais diversos sujeitos.

Quando se afirma a relevância do livre desenvolvimento da personalidade, entende-se que cada pessoa deve eleger o seu modo de viver e que cada uma tem o

[57] Empresas comprometidas com a redução de seus impactos ambientais, com a construção de um ambiente socialmente responsável e com os melhores processos de administração vêm se destacando, por mostrarem o quanto são resilientes e sustentáveis. Esses cuidados beneficiam, além da coletividade, a própria empresa, que se torna mais competitiva, tem melhor controle sobre os riscos e tende a alcançar melhores resultados. Sistemas de gestão de compliance comprometidos com as questões acima protegem a instituição, por exemplo, de sanções impostas pela Autoridade Nacional de Proteção de Dados, que já poderão ocorrer a partir de 1º de agosto de 2021, pelo Poder Judiciário e agências reguladoras, bem como de questionamentos de autoridades. (TEFFÉ, Chiara Spadaccini de. LGPD em programas de compliance: vantagem competitiva e aderência às práticas ESG. Jota, publicado em 10 de junho de 2021. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/lgpd-em-programas-de-compliance-vantagem-competitiva-e-aderencia-as-praticas-esg-10062021> Acesso em: 11.06.21)

direito a desenvolver e a expor, de forma ampla, seu projeto de vida, agindo conforme o mesmo.[58] Garante-se autonomia para que cada um constitua sua personalidade livremente,[59] sem qualquer imposição ou interferência de outrem, havendo tanto um direito à individualidade quanto um direito à diferença. A proteção da integridade da pessoa dar-se-á para além dos direitos positivados expressamente no ordenamento. Em contraponto a uma lógica paternalista, segundo a qual as pessoas deveriam ser protegidas de si próprias pelo Estado, promove-se a autonomia individual e a liberdade de escolha acerca do próprio destino.

O livre desenvolvimento da personalidade, enquanto direito, deve ser também garantido pelo Estado e por terceiros, através da constituição de atos, iniciativas e políticas que possibilitem aos indivíduos desenvolverem sua personalidade. Ele demanda a elaboração de um quadro normativo de regulação que propicie o reconhecimento de capacidades, a atribuição de poderes e a determinação de deveres. O papel do ordenamento deve ser o de garantir à pessoa humana amplo espaço para o desenvolvimento de suas escolhas, havendo, claro, consciência de que de toda liberdade

[58] "A personalidade tem relevância positiva nem tanto no momento processual – isto é, nos remédios aos quais recorrer para a cessação da atividade lesiva, para a reintegração de forma específica, para a averiguação, para o ressarcimento -, quanto na avaliação substancial do interesse merecedor de concretização, destinado a modificar, a partir do interior, a maior parte dos institutos jurídicos, mudando a sua função. A exigência do respeito da personalidade, de seu livre desenvolvimento, incide sobre a noção de ordem pública, sobre os limites e sobre a função da autonomia negocial, sobre a interpretação dos atos através dos quais se manifesta – na individuação das fronteiras do ilícito e de seu fundamento, sobre as configurações não apenas das relações familiares, mas também daquelas patrimoniais, sobre a concepção e a tutela da relação de trabalho, sobre o juízo de valor do associativismo e de seus possíveis escopos; incide, em suma, sobre toda a organização da vida em «comunidade»" (PERLINGIERI, Pietro. *O direito civil na legalidade constitucional.* Rio de Janeiro: Renovar, 2008, p. 768-769) Rodotà nos ensina: "O direito ao livre desenvolvimento da personalidade não é uma descoberta dos últimos tempos. É solenemente reconhecido pelo parágrafo 2º da Constituição alemã (...) e, de forma menos evidente, do artigo 2º da Constituição italiana, onde se afirma "a República reconhece e garante os direitos invioláveis do homem, seja como indivíduo, seja nas formações sociais nas quais se desenvolve sua personalidade. Pode-se legitimamente indagar, portanto, se a escolha de redefinir a própria identidade na internet pode ser considerada como um elemento essencial do desenvolvimento da personalidade e se as comunidades virtuais podem ser consideradas como "formações sociais"." (RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 116.) Ver também: RODOTÀ, Stefano. *Il diritto di avere diritti.* Roma-Bari: Laterza, 2012, p. 275.

[59] Cf. MORAES, Maria Celina Bodin de. *Na medida da pessoa humana*: estudos de direito civil. Rio de Janeiro: Renovar, 2010. PINTO, Carlos Alberto da Mota. *Teoria Geral do Direito Civil,* 4ª Ed. atualizada por António Pinto Monteiro e Paulo Mota Pinto, Coimbra: Coimbra Editora, 2005. PINTO, Paulo Mota. A influência dos direitos fundamentais sobre o direito privado português. In. MONTEIRO, António Pinto; NEUNER, Jörg; SARLET, Ingo (Orgs.). *Direitos fundamentais e direito privado:* uma perspectiva de direito comparado. Coimbra: Almedina, 2007. PINTO, Paulo Mota. O direito ao livre desenvolvimento da personalidade. In: CANOTILHO, José Joaquim Gomes (coordenador). *Portugal-Brasil ano 2000*. Coimbra: Coimbra, 1999, p. 160; MIRANDA, Felipe Arady. O direito fundamental ao livre desenvolvimento da personalidade. *Revista do Instituto do Direito Brasileiro.* Ano 2, n. 10, p. 11175-11211. Lisboa, 2013, p. 11176; MOREIRA, Rodrigo Pereira. *Direito ao Livre Desenvolvimento da Personalidade*. Juruá: 2016.

decorrerá uma responsabilidade. O limite ao referido direito será a proteção da dignidade de terceiro(s). Ao se tutelar os dados pessoais, tutela-se diretamente a liberdade, a igualdade e a integridade tanto do indivíduo quanto das coletividades.

Nesse sentido, a proteção dos dados sensíveis mostra-se especialmente relevante para a garantia dos direitos e liberdades fundamentais de seu titular, devendo ser protegidos de forma mais específica e cuidadosa pelas diversas estruturas sociais, tecnológicas e normativas. Isso porque, em virtude da qualidade e da natureza das informações que trazem, seu tratamento ou eventual vazamento poderá gerar riscos significativos à pessoa humana, podendo ser fonte para preconceitos e discriminações ilícitas ou abusivas em face do titular.[60]

Nas palavras de Rodotà,

> (...) dados sensíveis são aqueles relativos à saúde e vida sexual, às opiniões e ao pertencimento étnico ou racial, com uma lista semelhante às encontradas nas normas relativas a casos de discriminações. Assim, somos confrontados com algo que vai além da simples proteção da vida privada e se apresenta como defensor da mesma igualdade entre as pessoas.[61]

Verifica-se, na categoria em questão, importante conteúdo relacionado à intimidade, à identidade e à proteção da igualdade material da pessoa, conteúdo esse que, como regra, só a ela diz respeito. Contudo, diante das novas dinâmicas de poder e de expressão, verifica-se também que nela há informações sensíveis que vêm integrando a esfera pública em que se encontra seu titular, constituindo as convicções que ele deve poder manifestar publicamente e que fazem parte de sua identidade pública.[62]

A seleção sobre quais dados são sensíveis demonstra que a circulação de determinadas informações pessoais pode acarretar maior potencial lesivo aos seus titulares em uma determinada configuração social e política. Diante disso, a

---

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

[61] Tradução livre de: "È necessario sottolineare, infatti, che i dati sensibile sono quelli che riguardano la salute e la vita sessuale, le opinioni e l'appartenenza etnica o razziale, con una elencazione analoga a quella che si trova nelle norme riguardanti i casi di discriminazione. Siamo così di fronte a qualcosa che eccede la semplice tutela della vita privata e si pone come presidio della stessa eguaglianza tra le persone". (RODOTÀ, Stefano. *Il mondo nella rete*: Quali i diritti, quali i vincoli. Roma: Laterza & Figli – Gruppo Editoriale L'Espresso, 2019.p.36)

[62] RODOTÀ, Stefano. *A vida na sociedade da vigilância.* A privacidade hoje. Rio de Janeiro: Renovar, 2008. KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. Dados Sensíveis na Lei Geral de Proteção de Dados Pessoais: mecanismos de tutela para o livre desenvolvimento da personalidade. Orientador: Sergio Marcos Carvalho de Ávila Negri. Dissertação (mestrado acadêmico) - Universidade Federal de Juiz de Fora, Faculdade de Direito. Programa de Pós-Graduação em Direito, 2019. p. 43.

compreensão sobre os mecanismos que devem ser empregados na tutela de dados sensíveis perpassa um entendimento substancial sobre as dinâmicas discriminatórias que estão articuladas nas sociedades.

Scott Skinner-Thompson[63] destaca como as proteções legais escassas para a privacidade causam diretamente danos concretos a comunidades marginalizadas, incluindo discriminações de toda ordem, assédio e violência. Segundo ele, estruturas de vigilância opressiva e sistemática têm sido historicamente destinadas às minorias, como negros[64], homossexuais e transexuais, definindo suas condições de vida e bloqueando sua capacidade de influenciar e moldar a governança democrática. Defende, assim, a necessidade de serem ampliados os instrumentos que efetivamente garantam o direito à privacidade, diante da capacidade do referido direito de promover objetivos relacionados à igualdade, servindo como uma forma de resistência expressiva às vigilâncias governamental e corporativa, bem como de libertação da opressão.

É imperioso ressaltar que, mesmo com o avanço na garantia dos direitos fundamentais, grupos mais vulneráveis e minorias vêm sendo os mais perseguidos e violentados na sociedade brasileira, o que torna essencial e urgente a tutela ampliada dos dados sensíveis, assim como o questionamento efetivo de estruturas discriminatórias e opressivas de poder e vigilância. Nessa lógica, Mulholland e Kremer[65] afirmam a necessidade de um olhar atento para a diversidade no processo de efetivação da tutela dos dados sensíveis. O Direito precisa ser mobilizado para a aplicação dos princípios da igualdade material e da não discriminação, rompendo com o manto da desigualdade formal e a perversa utilização de características étnico-raciais, sexuais e de gênero como mecanismos de exclusão e segregação[66].

---

[63] SKINNER-THOMPSON, Scott. *Privacy at margins*. Cambridge: Cambridge University Press, 2021.
[64] BROWNE, Simone. *Dark Matters*: On the Surveillance of Blackness. Durham: Duke University Press Books, 2015.
[65] MULHOLLAND, Caitlin; KREMER, Bianca. Responsabilidade civil por danos causados pela violação do princípio da igualdade no tratamento de dados pessoais. In: Rodrigo da Guia Silva; Gustavo Tepedino. (Org.). *O Direito Civil na era da inteligência artificial*. São Paulo: Revista dos Tribunais, 2020, p.565-584.
[66] MULHOLLAND, Caitlin; KREMER, Bianca. Responsabilidade civil por danos causados pela violação do princípio da igualdade no tratamento de dados pessoais. In: Rodrigo da Guia Silva; Gustavo Tepedino. (Org.). *O Direito Civil na era da inteligência artificial*. São Paulo: Revista dos Tribunais, 2020, p. 580.

Não há dúvidas de que o tratamento de dados sensíveis por parte, por exemplo, de empregadores[67], recrutadores, companhias seguradoras, planos de saúde ou governos, se não observadas garantias adequadas, poderá ampliar cenários de violações a direitos. Outro ponto de preocupação é o desenvolvimento contínuo de análises e de perfis comportamentais[68] com tais dados, visando a direcionar e a personalizar, com elevada precisão, bens e serviços.

Diante disso, observa-se grande preocupação de estudiosos com o uso indevido de dados como elemento impulsionador de discriminação em atividades bancárias, financeiras, de seguro[69] e de saúde[70], por exemplo. Sobre a questão, Thiago Junqueira afirma:

> A ligação entre proteção de dados e prevenção da discriminação é intuitiva. Ao se restringir ou condicionar o uso de determinados dados pessoais pelos agentes de tratamento, tem-se, como corolário, o impedimento de sua consideração em prejuízo do titular deles. Em uma sociedade cada vez mais digital, os instrumentos fornecidos aos indivíduos pelas leis de proteção de dados, como o direito de acesso aos dados tratados pelo controlador e os direitos à explicação e revisão das decisões automatizadas, afiguram-se

[67] A Convenção 111 da Organização Internacional do Trabalho (OIT- 1960), ratificada pelo Brasil, traz medidas para eliminar toda discriminação em matéria de emprego e ocupação, incentivando leis e programas de educação sobre o tema e que invistam na política promovida no documento. Em relação ao ambiente laboral, o artigo 7º, incisos XXX e XXXI, da Constituição da República, proíbem diferença de salários, de exercício de funções e de critério de admissão por motivo de sexo, idade, cor ou estado civil, bem como qualquer discriminação no tocante a salário e critérios de admissão do trabalhador portador de deficiência.

[68] LGPD, Art. 12. (...) § 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.

[69] "A necessidade da inovação no debate em torno do uso de dados pessoais na contratação de seguros é definida especialmente pela realidade de nossa sociedade que associa o fenômeno do *big data* ao uso de Inteligência Artificial em sistemas de predição. A atividade das seguradoras é sobremaneira facilitada pelo advento destas novas tecnologias, pois permite não só a capacidade de tratar os dados de maneira mais eficiente, como, consequentemente, gera uma minimização de custos nas operações e uma maior velocidade nas tomadas de decisão. Estas vantagens, por sua vez, implicam a possibilidade de negociação de preços contratuais mais adequados, na medida em que os riscos estão previstos, em tese, de forma mais realista. Ao mesmo tempo em que a tecnologia traz vantagens excepcionais para o mercado de seguros, é necessário encontrar um equilíbrio adequado entre o tratamento de dados pessoais dentro deste ambiente e a proteção de direitos fundamentais dos segurados, tais como, a privacidade, a proteção de seus dados e a igualdade de tratamento. Em último juízo, a tutela destes direitos visa a coibir a potencial discriminação abusiva que o uso dos dados coletados massivamente pode ocasionar no mercado de seguros, segregando e retirando de inteiras parcelas da população a possibilidade de contratação de forma equitativa." (MULHOLLAND, Caitlin. Os contratos de seguro e a proteção dos dados pessoais sensíveis. In: GOLDBERG, Ilan; JUNQUEIRA, Thiago (Coords.). *Temas Atuais de Direito dos Seguros*, Tomo I. São Paulo: Thomson Reuters. 2020.)

[70] Acerca dos dados sensíveis, Rodotà ensina que: "(...) não há dúvida de que o conhecimento, por parte do empregador ou de uma companhia seguradora, de informações sobre uma pessoa infectada pelo HIV, ou que apresente características genéticas particulares, pode gerar discriminações. Estas podem assumir a forma da demissão, da não admissão, da recusa em estipular um contrato de seguro, da solicitação de um prêmio de seguro especialmente elevado." (RODOTÀ, Stefano. A *Vida na Sociedade de Vigilância: privacidade hoje*. Rio de Janeiro: Renovar, 2008, p. 70.)

> essenciais para a exposição e minimização de tratamentos discriminatórios. Some-se a eles, ainda, a explicitação de um princípio da não discriminação ilícita ou abusiva, a possível exigência de um relatório de impacto à proteção de dados pessoais (RIPD) e uma auditoria pela ANPD para verificação de aspectos discriminatórios nos tratamentos automatizados, e logo se conclui: o controle da discriminação nas relações entre privados no Brasil tende a mudar de patamar com a entrada em vigor da Lei Geral de Proteção de Dados (LGPD). [71]

O direito constitucional brasileiro e o direito internacional dos direitos humanos compreendem o direito à igualdade como mandamento de proibição de discriminação. [72] Almeja-se, assim, "(...) afastar toda e qualquer diferenciação injusta, em especial práticas e regimes de subordinação contra indivíduos e grupos histórica e socialmente injustiçados e vítimas de preconceito."[73] Na Constituição Federal de 1988, foi estabelecido que é objetivo fundamental da República a promoção do bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação.

O esforço de efetivação do mandamento antidiscriminatório resultou na formulação de doutrina, legislação e jurisprudência específicas, trazendo à tona um "direito da antidiscriminação".[74] Como salienta Roger Rios:

> Passa-se a atentar para os prejuízos injustos suportados pelos destinatários de tratamentos desiguais, objetivando enfrentar situações de estigma e subordinação experimentadas por grupos discriminados (RIOS, 2008, p. 36; MOREIRA, 2017, p. 67; SOLANKE, 2017). A discriminação enfrentada pelo direito da antidiscriminação é, portanto, tomada por uma perspectiva mais substantiva que formal: importa enfrentar a desigualdade prejudicial e injusta, pois nem sempre a adoção de tratamentos distintos se revela maléfica, sendo mesmo tantas vezes exigida, como alerta a dimensão material do princípio da

---

[71] JUNQUEIRA, Thiago. *Tratamento de Dados Pessoais e Discriminação Algorítmica nos Seguros.* Revista dos Tribunais, 2020, p. 240.

[72] Recorda-se que, em janeiro de 2022, foi promulga a Convenção Interamericana contra o Racismo, a Discriminação Racial e Formas Correlatas de Intolerância, firmada pela República Federativa do Brasil, na Guatemala, em 5 de junho de 2013.

[73] RIOS, Roger Raupp; LEIVAS, Paulo Gilberto Cogo; SCHÄFER, Gilberto. Direito da antidiscriminação e direitos de minorias: perspectivas e modelos de proteção individual e coletivo. Rev. direitos fundam. democ., v. 22, n. 1, p. 126-148, jan./abr. 2017.

[74] "Assim designado, tal campo surge a partir da experiência jurídica estadunidense (McCRUDDEN, 1991), com os avanços do movimento de direitos civis pós II Guerra Mundial (POLE, 1993, p. 311), tendo como marco jurisprudencial indisputável a decisão da Suprema Corte dos Estados Unidos no célebre caso *"Brown vs. Board of Education"*, de 1954 (SCHWARTZ, 1993, p. 286; RUTHERGLEN, 2001), passando a exercer uma influência seminal no continente europeu, tanto nos direitos nacionais (BURCA, 2011), como no direito comunitário europeu (COUNCIL OF EUROPE, 2011)." (RIOS, Roger Raupp. Tramas e interconexões no Supremo Tribunal Federal: Antidiscriminação, gênero e sexualidade. *Rev. Direito Práx.*, Rio de Janeiro, v. 11, n. 2, p. 1332-1357, abr. 2020. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S2179-89662020000201332&lng=en&nrm=iso> Acesso em: 28.12. 2020.)

> igualdade (o de tratar igualmente os iguais e desigualmente os desiguais na medida de suas desigualdades).[75]

No direito da antidiscriminação são analisadas duas modalidades de discriminação: a direta e a indireta. A primeira ocorre quando se dá de modo intencional e consciente. A última se dá mediante atitudes aparentemente neutras, mas com impacto prejudicial, ainda que sem intencionalidade, em face de indivíduos e de grupos discriminados. Ela pode alastrar-se pelas estruturas organizacionais formais e informais, como acontece na discriminação institucional, havendo a reprodução de privilégios invisibilizados ou naturalizados.[76] As duas modalidades podem ser aplicadas especialmente havendo o tratamento de dados sensíveis realizado por humanos e/ou máquinas, trazendo sérias consequências a indivíduos e grupos.

O fundamento comum para a proteção dos dados sensíveis gira em torno da necessidade de se prevenir formas prejudiciais de discriminação em face dos titulares de dados. Em 1990, a Organização das Nações Unidas (ONU) emitiu Diretrizes para a Regulamentação de Arquivos de Dados Pessoais Computadorizados. Tratando do princípio da não discriminação, o documento destacou que: "(...) data likely to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin,

---

[75] RIOS, Roger Raupp. Tramas e interconexões no Supremo Tribunal Federal: Antidiscriminação, gênero e sexualidade. *Rev. Direito Práx.*, Rio de Janeiro, v. 11, n. 2, p. 1332-1357, abr. 2020. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S2179-89662020000201332&lng=en&nrm=iso> Acesso em: 28.12. 2020.

[76] "No aspecto trabalhista, o mandamento constitucional de tratamento igualitário para situações iguais ganha ênfase especial, pois partindo da inequívoca desigualdade estrutural na relação entre empregado e empregador e respeitando a necessidade de ser ter meios de compensação dessa desigualdade, o desafio de se dar efetividade aos direitos fundamentais, dentre eles, o preceito isonômico constitucional é ainda maior. (...) Assim e com o fito de amenizar o desequilíbrio entre empregado e empregador, o princípio isonômico na seara trabalhista impede que o empregador proceda com tratamento diferenciado desfavorável baseado em motivo desarrazoado em face dos seus empregados. Pode o empregador, contudo, utilizar critérios diferenciadores caso o cargo a ser ocupado assim o exija, por exemplo, pode o ente patronal invocar o artigo 390 da CLT, que impede a contratação de mulheres para prestar serviços em atividades que demande o emprego de força física superior a 20 quilos para o trabalho contínuo. Ainda, o princípio isonômico deve ser observado durante todo o contrato de trabalho, desde a admissão do trabalhador até o momento da extinção do pacto laboral." (BRUGINSKI, Márcia Kazenoh. Discriminação no trabalho: práticas discriminatórias e mecanismos de combate. Disponível em: <https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/90942/2015_bruginski_marcia_discriminacao_trabalho.pdf?sequence=1&isAllowed=y> Acesso em: 05.04.21.
Cf. MALLET, Estêvão. Igualdade, discriminação e direito do trabalho. *Revista da Faculdade de Direito, Universidade de São Paulo*, v. 103, p. 241-267, 2008. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/67804. Acesso em: 5 abr. 2021. VIANA, Marcio Túlio. Os dois modos de discriminar e o futuro do Direito do Trabalho. In: RENAULT, Luiz Otávio Linhares. VIANA, Márcio Tulio (coord). Discriminação: estudos. São Paulo: LTr, 2000. p. 321-328. _____. A proteção trabalhista contra atos discriminatórios (análise da Lei 9.029/95). In: RENAULT, Luiz Otávio Linhares. VIANA, Márcio Tulio (coord). Discriminação: estudos. São Paulo: LTr, 2000. p. 354-367.

colour, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union, should not be compiled."[77]

Recorda-se, também, a fundamentação desenvolvida no Relatório Explicativo ao Protocolo que alterou a Convenção para a Proteção das Pessoas, no que diz respeito ao Tratamento Automático de Dados Pessoais, publicado em 2018.[78] No documento, afirmou-se que o processamento de certos tipos de dados ou determinados processamentos direcionados à obtenção de dados sensíveis poderia levar a violações de interesses, direitos e liberdades. Como exemplo, destacou-se que o tratamento de dados relacionados à vida sexual ou à orientação sexual de uma pessoa pode acarretar risco potencial de discriminação ou de lesão à dignidade dela.

Dessa forma, a fim de prevenir efeitos adversos para o titular dos dados, o tratamento de dados sensíveis deve vir acompanhado de salvaguardas adequadas, que considerem os riscos em jogo e os interesses, direitos e liberdades a serem protegidos, como, por exemplo: a solicitação de um consentimento explícito do titular dos dados; uma disposição legal cobrindo os casos em que o processamento de tais dados será permitido, através do desenvolvimento de bases legais específicas; obrigação de sigilo profissional; gestão de riscos; e medidas de segurança organizacional e técnicas específicas. O referido documento[79] prossegue afirmando que tipos específicos de processamento de dados podem implicar risco particular para os titulares dos dados, independentemente de seu contexto. Seria o caso, por exemplo, do tratamento de dados genéticos, que podem revelar informações sobre a saúde ou sobre a filiação da pessoa ou de terceiros. Recorda também que, embora o processamento de sobrenomes não apresente, como regra, riscos para os indivíduos, tal processamento pode, em alguns casos, envolver dados sensíveis, por exemplo, quando o objetivo for revelar a origem étnica ou as crenças religiosas dos indivíduos, com base na origem linguística de seus nomes.

Ressaltou-se, também, que dados relativos à saúde incluem informações sobre o passado, o presente e o futuro de um indivíduo, bem como sobre sua saúde física e mental, podendo referir-se a uma pessoa doente ou saudável. O tratamento de imagens

[77] Disponível em: <https://digitallibrary.un.org/record/99493> Acesso em: 09.01.21
[78] Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223> Acesso em: 09.01.21
[79] Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223> Acesso em: 09.01.21

de pessoas com óculos grossos, uma perna quebrada, pele queimada ou quaisquer outras características visíveis relacionadas à saúde só poderá ser considerado como tratamento de dados sensíveis, segundo o texto, quando ele for baseado nas informações de saúde que puderem ser extraídas das fotos.

A fundamentação acima dialoga com os considerandos do GDPR. De acordo com o considerando 51, merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e das liberdades fundamentais, visto que o contexto do tratamento desses dados poderá implicar riscos significativos para direitos e liberdades. Acerca das decisões automatizadas a partir de dados pessoais que possam impactar seu titular, o considerando 71 afirma que:

> A fim de assegurar um tratamento equitativo e transparente no que diz respeito ao titular dos dados, tendo em conta a especificidade das circunstâncias e do contexto em que os dados pessoais são tratados, o responsável pelo tratamento deverá utilizar procedimentos matemáticos e estatísticos adequados à definição de perfis, aplicar medidas técnicas e organizativas que garantam designadamente que os fatores que introduzem imprecisões nos dados pessoais são corrigidos e que o risco de erros é minimizado, e proteger os dados pessoais de modo a que sejam tidos em conta os potenciais riscos para os interesses e direitos do titular dos dados e de forma a prevenir, por exemplo, efeitos discriminatórios contra pessoas singulares em razão da sua origem racial ou étnica, opinião política, religião ou convicções, filiação sindical, estado genético ou de saúde ou orientação sexual, ou a impedir que as medidas venham a ter tais efeitos. A decisão e definição de perfis automatizada baseada em categorias especiais de dados pessoais só deverá ser permitida em condições específicas.[80]

Por fim, o considerando 85 do GDPR destaca que, se não forem adotadas medidas adequadas, a violação de dados pessoais poderá causar danos físicos, materiais ou imateriais às pessoas, como a perda de controle sobre os seus dados pessoais, limitação dos seus direitos, discriminação, roubo ou usurpação de identidade, perdas financeiras, inversão não autorizada de pseudonimização, danos à reputação, perda de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem econômica ou social significativa em face do indivíduo.

Como se sabe, a depender da base de dados utilizada para treinar o algoritmo e de sua programação, ele poderá produzir resultados discriminatórios.[81] Tão importante

---

[80] Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN> Acesso em: 06.02.22

[81] "A discriminação pode ser ilícita por se basear diretamente em elementos vedados para certos fins, como a cor ou o gênero (discriminação direta), ou quando, embora com amparo em critérios aparentemente inofensivos, como o endereço residencial, acaba por atingir negativamente pessoas de

quanto o algoritmo é a base de dados a ele subjacente e o treinamento recebido, tendo em vista o enviesamento que pode vir a reboque, como, por exemplo, em situações que envolvam análises de saúde[82], probabilidade de cometimento de crimes[83], crédito para empréstimos[84], participação em processos seletivos de emprego[85] e interpretação de imagens[86].

A gravidade dessa utilização de dados pode ser bem compreendida na obra *Automating Inequality:* How high-tech tools profile, police, and punish the poor, publicada em 2018 por Virginia Eubanks.[87] Nela, a autora lança luzes sobre como

---

determinada raça, por exemplo (discriminação indireta). Decisões automatizadas, efetuadas com base em algoritmos, podem apresentar conteúdo discriminatório (direto ou indireto). Mostra-se emblemático o famoso caso da Amazon, em que um algoritmo de recrutamento utilizado pelo setor de recursos humanos favorecia a contratação de funcionários do sexo masculino. O algoritmo foi alimentado com dados que refletem a predominância masculina no mercado de trabalho, daí concluindo que candidatos homens seriam preferíveis às candidatas mulheres. Como se percebe, a qualidade dos dados utilizados influi na qualidade dos resultados alcançados: se os dados trazem vieses, os resultados também serão enviesados, pois os algoritmos aprendem com os dados que os alimentam." (OLIVA, Milena; Silva, Jeniffer. Discriminação algorítmica nas relações de consumo. Migalhas, publicado em 23 de fevereiro de 2021. Disponível em: <https://www.migalhas.com.br/depeso/340680/discriminacao-algoritmica-nas-relacoes-de-consumo> Acesso em: 03.07.21

[82] OBERMEYER, Ziad. Et al. Dissecting racial bias in an algorithm used to manage the health of populations. *Science*, 25.10.2019: Vol. 366, Issue 6464, pp. 447-453. Disponível em: <https://science.sciencemag.org/content/366/6464/447>. Acesso em: 01.12.2020.

[83] Cf. BRAYNE, Sarah. *Predict and Surveil*: Data, Discretion, and the Future of Policing. 1.ed. Oxford University Press: 2020. SKINNER-THOMPSON, Scott. *Privacy at the Margins.* Cambridge university press: 2020. COSTANZA-CHOCK, Sasha. *Design Justice*. Community-Led Practices to Build the Worlds We Need. The MIT Press: 2020. NOBLE, Safiya Umoja. *Algorithms of Oppression*: How Search Engines Reinforce Racism. NYU Press, 2018.

[84] TELFORD, Taylor. Apple Card algorithm sparks gender bias allegations against Goldman Sachs. *Washington Post*, 11.11.2019. Disponível em: <https://www.washingtonpost.com/business/2019/11/11/apple-card-algorithm-sparks-gender-bias-allegations-against-goldman-sachs/>. Acesso em: 26.11.2020. "Entrepreneur David Heinemeier Hansson says his credit limit was 20 times that of his wife, even though she has the higher credit score"

[85] DASTIN, Jeffrey. Amazon scraps secret AI recruiting tool that showed bias against women. Reuters, 10.11.2018. Disponível em: <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G>. Acesso em: 26.11.2020.

[86] HOWLEY, Daniel. Google Photos Mislabels 2 Black Americans as Gorillas. Yahoo! Finance, 29.06.2015. Disponível em: <https://finance.yahoo.com/news/google-photos-mislabels-two-black-americans-as-122793782784.html>. Acesso em: 26.11.2020.

HYPENESS. Tecnologia racista: Zoom é questionado por 'cortar cabeça' de professor negro. 19.09.2020. Disponível em: <https://www.hypeness.com.br/2020/09/tecnologia-racista-zoom-e-questionado-por-cortar-cabeca-de-professor-negro/>. Acesso em 12.12.2020.

ALVES, Paulo. Twitter é acusado de racismo após ferramenta priorizar pessoas brancas. Techtudo, 21.09.2020. Disponível em: <https://www.techtudo.com.br/noticias/2020/09/twitter-e-acusado-de-racismo-apos-ferramenta-priorizar-pessoas-brancas.ghtml> Acesso em 12.12.2020. "(...) usuários apontam que a rede social sempre escolhe pessoas brancas ao selecionar a porção de destaque em uma foto comprida demais e que precisa ser cortada para encaixar no post. Tweets que tomaram conta da plataforma mostram que, independentemente da quantidade de rostos de pessoas negras, o rosto branco costuma ser selecionado pela inteligência artificial."

[87] EUBANKS, Virginia. *Automating Inequality*: How High-Tech Tools Profile, Police, and Punish the Poor. St. Martin's Publishing Group, 2018.

instrumentos tecnológicos de análise de dados vêm impactando relevantes decisões sobre a vida de determinadas pessoas, especialmente as menos favorecidas economicamente e consideradas da classe trabalhadora: desde a seleção de currículos para uma vaga de emprego, chegando aos seguros, ao acesso ao crédito e a serviços do governo. Em sua obra, a autora questiona: quais os valores e crenças embutidos nos algoritmos? Como isso tem reforçado as desigualdades? Em seguida, ela traz perguntas que deveriam ser feitas antes de serem implantadas tais ferramentas tecnológicas: (a) a ferramenta aumenta a autonomia e a dignidade das pessoas menos favorecidas economicamente e consideradas da classe trabalhadora? (b) Se essa ferramenta visasse, focalizasse, a qualquer outro grupo de pessoas, além de mais pessoas da classe trabalhadora, sua existência seria tolerada? Sem dúvida, a reflexão promovida pela obra mostra-se urgente tanto nos Estado Unidos quanto em países em desenvolvimento que apresentam elevado índice de desigualdade, como é o caso do Brasil.

Decisões que, até pouco tempo, eram tomadas exclusivamente por seres humanos vêm sendo delegadas — no todo ou em parte — para sistemas automatizados, para algoritmos de ranking e para modelos de risco preditivo, que, por sua vez, acabam controlando desde a concessão de crédito a uma pessoa até quem tem mais chances de delinquir, com base em análises computadorizadas e estatísticas.[88] Pretende-se por meio de decisões algorítmicas superar, através do uso de critérios objetivos e quantitativos e da linguagem matemática, vieses e problemas verificados em julgamentos humanos.[89]

[88] "As decisões automatizadas, referentes a um indivíduo determinado, que se baseiam em um método estatístico para análise de grande volume de dados e informações, podem ter grande impacto sobre os direitos individuais, especialmente no que se refere à autonomia, igualdade e personalidade. Afinal, na sociedade atual, caracterizada pelas relações remotas, os dados pessoais acabam por se constituir na única forma de representação das pessoas perante as mais diversas organizações estatais e privadas, sendo determinantes para "abrir ou fechar as portas de oportunidades e acessos" (LYON, 2003, p. 27). Dessa forma, uma eventual representação equivocada em determinados contextos sociais – por meio de um equívoco do algoritmo ou dos dados em que o algoritmo se baseou – afetaria tanto a forma como o indivíduo se percebe como também o modo como a sociedade o enxerga e o avalia, afetando a sua integridade moral e a sua personalidade (BRITZ, 2008, p. 179). Ademais, se essa representação, conforme alertado por Lyon (2003), acarretar a perda de chances e oportunidades do indivíduo na sociedade, dar-se-á uma restrição indevida à sua autonomia, limitando a sua liberdade de ação, suas escolhas econômicas e até mesmo existenciais. Por fim, destaca-se também a possibilidade de violação do princípio da igualdade, na hipótese de que a classificação e seleção operada por algoritmos produza resultados desiguais para pessoas em situações semelhantes, afetando negativamente as suas oportunidades de vida na sociedade (LYON, 2003, p. 27)." (DONEDA et al. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. *Pensar*, Fortaleza, v. 23, n. 4, p. 1-17, 2018.)

[89] FRAZÃO, Ana. Discriminação algorítmica. *Jota*, publicado em 23 de junho de 2021. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/discriminacao-algoritmica-2-

Apesar das vantagens oferecidas por modelos e fórmulas matemáticas, elas também apresentam limitações, "especialmente em razão das dificuldades naturais para se converter aspectos complexos da natureza humana para critérios objetivos".[90] Percebeu-se, com o tempo, o potencial das decisões automatizadas de violarem direitos fundamentais[91], se tomadas sem o cumprimento de determinados parâmetros éticos e constitucionais, por exemplo. Para a sua aplicação, pois não se nega em momento algum a sua relevância, mostra-se imprescindível garantir transparência ao titular, possibilidade de controle e de implementação de medidas de segurança, a participação do indivíduo no âmbito do processo decisório que lhe disser respeito e a correção dos dados que servirem como *input* ao algoritmo. [92]

Nesse contexto, alude-se ao tratamento conferido ao tema pela LGPD, que previu o direito de o titular dos dados solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou aspectos de sua personalidade. Segundo parte da doutrina, o artigo 20 da LGPD[93] seria sede do "direito à explicação"[94], o qual derivaria do princípio da transparência.

23062021?amp&fbclid=IwAR1oD_HSvSGJ1cDD9UsBMgHUIj8lmTxoohT5tQp1m8Vrjv5h8qv_NX5vW0k> Acesso em: 23.06.21

[90] FRAZÃO, Ana. Discriminação algorítmica. *Jota*, publicado em 23 de junho de 2021.

[91] Cf. CHENEY-LIPPOLD, John. *We are data. Algorithms and the making of our digital selves*. New York: New York University Press, 2017.

[92] Cf. TEFFÉ, Chiara Spadaccini de; MEDON, Filipe. responsabilidade civil e regulação de novas tecnologias: questões acerca da utilização de inteligência artificial na tomada de decisões empresariais. *Revista estudos institucionais*, v. 6, p. 301-333, 2020.

[93] LGPD, Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

[94] No processo de aprovação da LGPD houve veto a trecho do artigo 20 que determinava o direito de revisão como um direito de revisão humana, ou seja, feito por uma pessoa natural. A crítica que se faz é a possibilidade então de tal revisão ser feita apenas por máquinas, ao contrário do que dispõe o direito europeu sobre a temática. Cf. FRAZAO, Ana; MULHOLLAND, Caitlin (Org.). *Inteligência Artificial e Direito*: Ética, Regulação e Responsabilidade - revisto e atualizado. 2. ed. São Paulo: Revista dos Tribunais, 2020. FRAZÃO, Ana. Algoritmos e inteligência artificial, Jota, publicado em 15 de maio de 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/algoritmos-e-inteligencia-artificial-15052018> ZANATTA, Rafael A. F. *Perfilização, Discriminação e Direitos:* do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados

O princípio da não discriminação – relevante fundamento para a tutela ampliada dos dados sensíveis – aparece na LGPD duas vezes: na primeira, no inciso IX do Art. 6º, que o conceitua como "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos", e na segunda, no § 2º do Art. 20, que prevê a possibilidade de a ANPD realizar auditoria para verificar aspectos discriminatórios em tratamento automatizado de dados pessoais.

Como define Cathy O'Neil[95], matemática e cientista de dados, algoritmos são opiniões embutidas em código, que repetem práticas e padrões passados e, assim, automatizam o *status quo*. Para que os algoritmos sejam justos, é preciso fiscalizá-los, repará-los e aprimorá-los. Dessa forma, além de se ter uma regulamentação adequada, que privilegie a transparência e a explicação quanto às decisões algorítmicas, o princípio da não discriminação deve estar presente desde a concepção dos sistemas de inteligência artificial — tanto na parte técnica dessa construção quanto na garantia de diversidade dos times responsáveis pelo desenvolvimento dos algoritmos —, sendo aplicado em todo o ciclo de vida desses sistemas. Mostra-se fundamental exigir responsabilidade e prestação de contas de corporações e Estados que tomam decisões capazes de prejudicar pessoas e comunidades.

Entende-se que aplicações de inteligência artificial devem ser desenvolvidas a partir de orientações que considerem princípios[96] e valores éticos[97], além de haver o respeito e a proteção aos direitos humanos embutidos no desenho de todo o sistema.[98] Medidas de precaução devem ser tomadas no desenvolvimento e ao longo do ciclo de vida do sistema, incluindo avaliações prévias de impacto e medidas técnicas e

---

Pessoais. Disponível em: <https://www.researchgate.net/publication/331287708> Acesso em: 09.01.21. SOUZA, Carlos Affonso; PERRONE, C.; MAGRANI, Eduardo. O Direito à Explicação entre a experiência europeia e a sua positivação na LGPD. *Tratado de Proteção de Dados Pessoais*. 1ed.Rio de Janeiro: Forense, 2020, v. 1, p. 243-270.

[95] O'NEIL, Cathy. *Weapons of Math Destruction*: How Big Data Increases Inequality and Threatens Democracy. Crown: 2016.

[96] BURLE, Caroline; CORTIZ, Diogo. Mapeamento de princípios de inteligência artificial. Disponível em: <https://ceweb.br/publicacoes/mapeamento-de-principios-de-inteligencia-artificial/?page=1> Acesso em: 30.12.20

[97] Cf. MULHOLLAND, Caitlin; FRAJHOF, I. Entre as leis da robótica e a ética: regulação para o adequado desenvolvimento da Inteligência Artificial. In: Mafalda Miranda Barbosa; Felipe Braga Netto; Michael César Silva; José Luiz de Moura Faleiros Júnior. (Org.). *Direito Digital e Inteligência Artificial*: diálogos entre Brasil e Europa. 1ed.Belo Horizonte: Editora Foco, 2021, v. 1, p. 65-80.

[98] Cf. TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (Org.). *O Direito Civil na era da inteligência artificial*. 1. ed. São Paulo: Thomson Reuters Brasil, 2020. v. 1. 800p. MEDON, FILIPE. *Inteligência Artificial e Responsabilidade Civil*: autonomia, riscos e solidariedade. 1. ed. Salvador: JusPodivm, 2020. 448p.

organizacionais de prestação de contas (*accountability*). Do ponto de vista técnico, alguns procedimentos devem ser observados, como, por exemplo, a minimização das informações tratadas, devendo-se dar preferência à anonimização dos dados e ao uso de ferramentas tecnológicas capazes de dar transparência aos critérios utilizados para a tomada de decisões automatizadas.

De forma a ampliar as garantias aos dados sensíveis e a afirmar a relevância do princípio da não discriminação nas atividades de tratamento, recorda-se ainda que, na LGPD, o titular dos dados poderá revogar o consentimento manifestado (Art. 18, IX) ou pleitear o direito à oposição (Art.18 §2º), quando o tratamento ocorrer com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei. Destaca-se, também, a relevância do princípio da minimização (ou princípio da necessidade) no trato dos dados sensíveis. Se o agente estiver coletando dados sensíveis, ele deverá certificar-se de coletar apenas o mínimo necessário. Devido às restrições legais, havendo dúvidas sobre a necessidade da informação, a solução mais simples será a sua não coleta ou, se já coletada, a sua eliminação.[99]

Ter documentados os tratamentos que envolvem tais dados, as técnicas adotadas e as estruturas de compartilhamento e de descarte implementadas, assim como diagnosticar riscos com precisão e trabalhar em sua mitigação, mostra-se também fundamental quando se lida com informações sensíveis. Ainda que no Brasil o relatório de impacto à proteção de dados pessoais[100] não seja obrigatório para o tratamento de dados sensíveis, além de ser uma boa prática e um instrumento relevante contra a discriminação, ele poderá ser requerido pela ANPD, a depender do caso. [101] Conforme

[99] Disponível em: <https://www.cnil.fr/en/sheet-ndeg7-minimize-data-collection> Acesso em: 02.11.20.

[100] LGPD, Art. 5º XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

[101] LGPD, Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados. 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

será desenvolvido nos capítulos 3 e 4, defende-se a sua feitura em relações que envolvam, por exemplo, tratamento de grande quantidade de dados sensíveis e tratamento de dados sensíveis de menores.

Tratar dados sensíveis é inevitável no mundo contemporâneo e nem sempre terá por objetivo práticas negativas ou discriminatórias, podendo contribuir para a melhor organização de instituições, para a ampliação da qualidade de bens e serviços e para melhorar a saúde e o bem-estar das pessoas, gerando, então, resultados benéficos para os titulares dos dados. Contudo, é imprescindível que tais dados sejam utilizados respeitando-se estritamente os princípios e os limites impostos na Constituição Federal e na LGPD.

Cuidados adicionais para a proteção de dados sensíveis são essenciais para o seu regular tratamento, uma vez que a tônica de sua tutela é "permitir uma igualdade substancial no tratamento dos dados, vedando a discriminação e o abuso que dele podem surgir."[102] Isso se mostra relevante, pois a mera proibição do tratamento de dados sensíveis seria inviável e desproporcional, já que, em alguns momentos, o uso de tais dados será legítimo e necessário. Além disso, existem determinados organismos cuja própria razão de ser estaria comprometida caso não pudessem obter informações desse gênero, como, por exemplo, algumas entidades de caráter político, religioso ou filosófico.[103] Dessa forma, entende-se que o tratamento de dados sensíveis é possível e, inclusive, pode ser essencial em determinadas circunstâncias. Entretanto, deverá ser pautado estritamente nos ditames legais, pela relevância dos valores em questão, e legitimado apenas quando se mostrar proporcional.

1.2.1 Dados sensíveis: análise crítica acerca de sua definição e qualificação

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. (...)

[102] MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. Migalhas, publicado em 22 de junho de 2020. Disponível em: <https://migalhas.uol.com.br/coluna/migalhas-de-vulnerabilidade/329261/dados-pessoais-sensiveis-e-consentimento-na-lei-geral-de-protecao-de-dados-pessoais> Acesso em: 02.11.20.

[103] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, cit, p. 144.

A Lei Geral de Proteção de Dados, ainda que não defina expressamente o que são dados sensíveis, apresenta em seu Art. 5º, inciso II, dados assim considerados, como aqueles que versam sobre origem racial ou étnica, convicção religiosa, opinião política e filiação a sindicato ou a organização de caráter religioso, filosófico ou político. São também sensíveis aqueles referentes à saúde ou à vida sexual e dados genéticos ou biométricos. A legislação brasileira seguiu em grande parte a noção europeia de dados sensíveis, estabelecida em 2016 pelo Regulamento Geral de Proteção de Dados Pessoais, e expandiu rol já desenvolvido pela Lei do Cadastrado Positivo (Lei n. 12.414/11).[104]

Mas o que torna um dado pessoal um dado sensível? Como o legislador brasileiro chegou à mencionada seleção de dados? Há uma noção universal do que sejam dados sensíveis? Como identificar um tratamento de informações que possa ter efeitos discriminatórios ilícitos ou abusivos em face do titular? Nesta parte do trabalho, será realizado estudo crítico acerca da definição dos dados sensíveis, bem como de seu conteúdo, qualificação e contornos. Além disso, será defendida a necessidade de se realizar uma análise dinâmica e contextual do tratamento para se definir a tutela aplicável para a situação concreta e os dados pessoais envolvidos.

Desenvolver e tutelar de forma ampliada os dados sensíveis é fundamental para a proteção de dados. Nesse sentido, muitos países já conferem especial atenção a tal categoria: no *General Data Protection Regulation* (GDPR)[105], os dados sensíveis são chamados de *categorias especiais de dados pessoais*[106]; nas leis argentina[107] e uruguaia[108] encontra-se a expressão *datos sensibles*; na principal lei japonesa sobre o

---

[104] "Art. 3º Os bancos de dados poderão conter informações de adimplemento do cadastrado, para a formação do histórico de crédito, nas condições estabelecidas nesta Lei. § 3º Ficam proibidas as anotações de: (...) II - informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas."

[105] Regulation (EU) 2016/679. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679>. Acesso: 30/11/2020.

[106] Disponível em: <https://www.dataprotection.ie/en/organisations/know-your-obligations/lawful-processing/special-category-data> Acesso em: 23.06.21

[107] Ley 25.326 (Ley de Protección de los Datos Personales). Disponível em: https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/texto. Acesso: 30/11/2020. "Art. 2º (...) — Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual."

[108] Ley nº 18331/2008. Disponível em: <https://www.impo.com.uy/bases/leyes/18331-2008>. Acesso: 30/11/2020. "Art. 4º (…) E) Dato sensible: datos personales que revelen origen racial y étnico,

tema, em versão em inglês, o termo foi traduzido como *special care-required personal information*[109]; e *sensitive personal data/information* aparece nas leis filipina[110], islandesa[111] e australiana[112].

A sensibilidade de determinados dados pessoais ganhou tamanha expressividade que, recentemente, passou a constar em uma das principais normas estadunidenses reguladoras do tema: o *California Privacy Rights Act* (CPRA), que vai alterar e substituir o texto do *California Consumer Privacy Act* (CCPA), a partir de 1º de janeiro de 2023[113]. O CPRA mantém as categorias de informações pessoais (Personal Information - PI) do CCPA, mas adiciona uma nova: as Informações Pessoais Sensíveis (Sensitive PI). Os consumidores, agora, terão direitos ampliados quando dados sensíveis estiverem envolvidos. Eles incluem dados de: (1) seguro social, carteira de motorista, identidade ou número de passaporte; (2) informações de login da conta com uma senha; (3) a localização geográfica precisa de um consumidor; (4) origem racial ou étnica,

---

preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual."

[109] Act on the Protection of Personal Information (The amended Act fully put into effect on May 30,2017). Disponível em <https://www.ppc.go.jp/en/legal/>. Acesso: 18.01.2021. "Special care-required personal information" in this Act means personal information comprising a principal's race, creed, social status, medical history, criminal record, fact of having suffered damage by a crime, or other descriptions etc. prescribed by cabinet order as those of which the handling requires special care so as not to cause unfair discrimination, prejudice or other disadvantages to the principal."

[110] Republic Act 10173 – Data Privacy Act of 2012. Disponível em: <https://www.privacy.gov.ph/data-privacy-act/>. Acesso: 30/11/2020. "(l) *Sensitive personal information* refers to personal information: (1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations; (2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings; (3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and (4) Specifically established by an executive order or an act of Congress to be kept classified."

[111] Act on the Protection of Privacy as regards the Processing of Personal Data no. 77/2000 <https://www.personuvernd.is/information-in-english/greinar/nr/438>. Acesso em: 30/11/2020. 8. Sensitive data: a. Data on origin, skin colour, race, political opinions, religious beliefs and other life philosophies. b. Data on whether a man has been suspected of, indicted for, prosecuted for or convicted of a punishable offence. c. Health data, including genetic data and data on use of alcohol, medical drugs and narcotics. d. Data concerning sex life (and sexual behaviour) e. Data on trade-union membership.

[112] Privacy Act No. 119 1988 (as amended) ('the Privacy Act') . Disponível em: <https://www.legislation.gov.au/Details/C2020C00237> Acesso: 18.01.21. "sensitive information means: (a) information or an opinion about an individual's: (i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual orientation or practices; or (ix) criminal record; that is also personal information; or (b) health information about an individual; or (c) genetic information about an individual that is not otherwise health information; or (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or (e) biometric templates."

[113] Disponível em: <https://iapp.org/resources/article/the-california-privacy-rights-act-of-2020/> Acesso em: 18.01.21.

crença religiosa ou filiação a sindicatos; (5) conteúdo da correspondência, e-mail ou texto de um consumidor, a menos que a empresa seja o destinatário pretendido; (6) informação genética do consumidor; (7) processamento de informações biométricas para identificação do consumidor; (8) dados sensíveis analisados em relação à saúde da pessoa; e (9) dados sensíveis analisados sobre a vida sexual ou orientação sexual de um consumidor[114].

Contudo, doutrina[115] recorda que a categoria dos dados sensíveis nem sempre esteve presente nas leis de proteção de dados e que as discussões sobre como o conceito deve ser reconhecido continuam até os dias atuais. Embora seja possível afirmar que alguns dados, especialmente em certos usos e contextos, sejam mais sensíveis do que outros, historicamente mostrou-se difícil encontrar consenso sobre quais tipos de dados deveriam ser considerados sensíveis e como os tratados e as legislações deveriam ser redigidos para protegê-los.

A noção de dados sensíveis começou a ser discutida com maior seriedade a partir de documento da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), de 1980, denominado *Diretrizes sobre a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais*.[116] Essas diretrizes não vinculativas recomendaram que os Estados-Membros da OCDE introduzissem o conceito de dados sensíveis na legislação nacional que tratava da proteção de dados. Contudo, elas não elaboraram o conceito nem delinearam precisamente quais tipos de dados deveriam ser considerados sensíveis. Entendeu-se que, provavelmente, não seria possível identificar um conjunto de dados que seria universalmente considerado sensível.[117]

No mencionado documento, na parte referente ao memorando explanatório, foi desenvolvido um comentário acerca do princípio da limitação da coleta de dados, afirmando-se que ele trataria de duas questões, a saber: a) ele ofereceria limites à coleta de dados que, devido ao modo como devem ser tratados, à sua natureza, ao contexto em

---

[114] Disponível em: <https://www.lexology.com/library/detail.aspx?g=5a7edce9-26af-487c-8877-7a815945954d> Acesso em: 18.01.21.

[115] QUINN, Paul; MALGIERI, Gianclaudio. The Difficulty of Defining Sensitive Data – the Concept of Sensitive Data in the EU Data Protection Framework. *Brussels Privacy Hub Research Paper*, publicado em 16 de outubro de 2020. Disponível em: <https://ssrn.com/abstract=3713134> Acesso em: 02.01.21

[116] MCCULLAGH, K. Data Sensitivity: Proposals for Resolving the Conundrum, *Journal of International Commercial Law and Technology* 2, 2007, p. 190–201.

[117] Disponível em: <http://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> Acesso em: 02.01.21

que devem ser utilizados ou a outras circunstâncias, fossem considerados especialmente sensíveis; e b) traria requisitos relativos aos métodos de coleta de dados. Segundo o documento, seria possível e desejável enumerar tipos ou categorias de dados que fossem *per se* sensíveis e cuja coleta deveria ser restrita ou mesmo proibida. Lembrou que já existiam precedentes na legislação europeia nesse sentido (raça, crenças religiosas, antecedentes criminais, por exemplo). Por outro lado, afirmou que nenhum dado seria intrinsecamente "privado" ou "sensível", mas poderia assim se tornar devido ao seu contexto e uso.

Outro passo importante ocorreu com a criação, em 1981, da Convenção do Conselho da Europa para a Proteção de Indivíduos com Relação ao Tratamento Automático de Dados Pessoais (*Convenção 108*).[118] Ao contrário das diretrizes da OCDE, a Convenção foi considerada vinculativa para os signatários. Ela trouxe, em seu artigo 6º, categorias especiais de dados e indicou como deveria se dar o seu tratamento: "Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions." Essa categoria não se destinava a ser exaustiva.[119] Entendia-se que cada Estado poderia incluir, em seu direito interno,

[118] Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108> Acesso em: 02.01.21

[119] Em relatório explicativo sobre a Convenção, destacou-se que: "43. While the risk that data processing is harmful to persons generally depends not on the contents of the data but on the context in which they are used, there are exceptional cases where the processing of certain categories of data is as such likely to lead to encroachments on individual rights and interests. Categories of data which in all member States are considered to be especially sensitive are listed in this article. 44. The expression "revealing ... political opinions, religious or other beliefs" covers also activities resulting from such opinions or beliefs. 45. The meaning of the term "personal data concerning health" has been carefully studied by the Committee of Experts on Data Protection in connection with its work on medical data banks. It includes information concerning the past, present and future, physical or mental health of an individual. The information may refer to a person who is sick, healthy or deceased. This category of data also covers those relating to abuse of alcohol or the taking of drugs. 46. In the same way as under Article 4 (paragraph 39 above) the expression "domestic law" may be taken in a wide sense, i.e. not only legislation but also appropriate or specific regulations or administrative directives, as long as the necessary level of protection is secured. 47. By "criminal convictions" in the sense of this article should be understood: convictions based on criminal law and in the framework of a criminal procedure. 48. The list of this article is not meant to be exhaustive. A Contracting State may, in conformity with Article 11, include in its domestic law other categories of sensitive data, the processing of which is prescribed or restricted. The degree of sensitivity of categories of data depends on the legal and sociological context of the country concerned. Information on trade union membership for example may be considered to entail as such a privacy risk in one country, whereas in other countries it is considered sensitive only in so far as it is closely connected with political or religious views." (Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg, 28.I.1981. p.09)

outras categorias de dados sensíveis, cujo tratamento seria prescrito ou restrito. O grau de sensibilidade das categorias de dados dependeria do contexto jurídico e sociológico do país em questão.[120]

A *Diretiva de Proteção de Dados da União Europeia 95/46/EC* foi mais longe, especificando claramente em seu artigo 8º as categorias de dados que deveriam ser considerados sensíveis: "(...) dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual."[121] Doutrina[122] afirma que tais categorias de dados sensíveis deveriam encontrar proteção em todos os Estados-Membros da UE. Todavia, a forma como tal proteção era tomada ficava em parte a critério da jurisdição em questão. A principal maneira pela qual a Diretiva impôs requisitos extras sobre aqueles que desejavam processar dados sensíveis foi através da criação de barreiras adicionais antes que tal processamento pudesse ser permitido. Isso foi alcançado por meio da criação de bases jurídicas específicas que deveriam ser utilizadas para o tratamento de dados sensíveis.

A criação de categorias especiais obrigatórias de dados pessoais significava que todos os Estados-Membros sujeitos à Diretiva eram obrigados a criar leis de proteção contemplando certas categorias definidas de dados sensíveis. Isso criou certeza pelo menos em relação a um número mínimo de categorias que deveriam ser protegidas. Contudo, dado o uso de uma Diretiva como forma legislativa, e na falta de qualquer menção explícita em contrário, existia a possibilidade de os Estados-Membros

---

[120] Propostas de modernização, elaboradas pelo Comitê da Convenção 108, foram analisadas entre 2013 e 2016 por um comitê intergovernamental. Em setembro de 2016, esta comissão encaminhou a sua proposta para discussão e adoção ao Comitê de Ministros do Conselho da Europa. Em 18 de maio de 2018, o Comitê de Ministros adotou o protocolo de alteração, que foi aberto à assinatura em Estrasburgo em 10 de outubro deste ano. Informação disponível em: <https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet> Acesso em: 03.04.21. O artigo sobre dados sensíveis tem atualmente a seguinte redação: "**Article 6 – Special categories of data** 1. The processing of: – genetic data; – personal data relating to offences, criminal proceedings and convictions, and related security measures; – biometric data uniquely identifying a person; – personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life, shall only be allowed where appropriate safeguards are enshrined in law, complementing those of this Convention. 2. Such safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination."

[121] Disponível em: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A31995L0046> Acesso em: 02.01.21

[122] QUINN, Paul; MALGIERI, Gianclaudio. The Difficulty of Defining Sensitive Data – the Concept of Sensitive Data in the EU Data Protection Framework. *Brussels Privacy Hub Research Paper*, publicado em 16 de outubro de 2020. p.06. Disponível em: <https://ssrn.com/abstract=3713134> Acesso em: 02.01.21

adicionarem outras categorias de dados sensíveis, como ocorreu com os dados genéticos, por exemplo. A escolha de uma Diretiva, portanto, segundo doutrina[123], criou problemas em termos de heterogeneidade dos sistemas jurídicos em toda a Europa. Isso criou empecilhos, por exemplo, para quem queria tratar dados sensíveis em uma base paneuropeia. O resultado foi uma incerteza considerável para potenciais controladores de dados que desejavam operar para fins de *eHealth*[124] ou em grandes consórcios de pesquisa científica.

Nos dias atuais, o *Regulamento Geral de Proteção de Dados europeu* contém várias adaptações e inovações importantes relacionadas aos dados sensíveis, especialmente em seu artigo 9º. Ele trouxe uma lista fechada de *categorias especiais de dados pessoais* e ampliou o escopo de proteção, adicionando mais espécies de dados sensíveis, conforme será analisado na presente tese em seção própria.

Entende-se que a identificação dos dados sensíveis pode variar a depender da forma como eles forem compreendidos em cada legislação e cultura. A priori, parece que um grupo relativamente amplo de informações pessoais pode ser considerado sensível, especialmente diante de alguns tratamentos específicos realizados. Por consequência, os dados pessoais deverão ser avaliados considerando-se, por exemplo: (I) a natureza e as características da informação pessoal, além do contexto que determina seu tratamento; (II) interesses específicos do responsável pelo tratamento, assim como dos destinatários potenciais dos dados; (III) finalidade e propósito para os quais os dados serão tratados, ou seja, se há intenção de inferir ou tratar atributos sensíveis;[125] (IV) condições do tratamento; (V) relações que podem ser estabelecidas

---

[123] QUINN, Paul; MALGIERI, Gianclaudio. The Difficulty of Defining Sensitive Data – the Concept of Sensitive Data in the EU Data Protection Framework. *Brussels Privacy Hub Research Paper*, publicado em 16 de outubro de 2020. p.06. Disponível em: <https://ssrn.com/abstract=3713134> Acesso em: 02.01.21

[124] eHealth (ou eSaúde) representa o uso de tecnologias de informação e comunicação (TIC) para a saúde, visando a atender as necessidades dos pacientes, profissionais de saúde e provedores de saúde. O termo pode abranger uma gama de serviços ou sistemas, como o Prontuário Eletrônico do Paciente ou Sistema de Registro Eletrônico de Saúde; telemedicina; sistemas de informação em saúde e uso de dispositivos móveis para a captação de dados de saúde, fornecendo informações de saúde para profissionais, pesquisadores e pacientes. É o uso da tecnologia em conjunto com a internet para melhorar o ecossistema da saúde, envolvendo os processos clínicos, tratamentos e informações dos pacientes e a prestação de serviço. Mais informações em: <https://www.who.int/ehealth/about/en/> Acesso em: 02.02.21

[125] "Despite the fragility of the distinction between sensitive and non-sensitive data, the higher level of protection afforded to the former in data protection law means it must be taken seriously. The fact that non-sensitive data can reveal information about sensitive category attributes through linkage and inference begs a question: Under what conditions should non-sensitive personal data be reclassified as sensitive personal data? Much academic discussion has been devoted to this question, according to which

com as demais informações disponíveis sobre o titular e/ou o grupo de que ele faz parte; (VI) as possibilidades tecnológicas atuais e futuras envolvendo dados; (VII) como a informação pode afetar o indivíduo a quem ela diz respeito e o livre desenvolvimento de sua personalidade; e (VIII) a potencialidade do tratamento servir como instrumento de estigmatização ou discriminação ilícita ou abusiva da pessoa.[126]

Acerca da finalidade e do propósito do agente de tratamento, cabe questionar: ele pretende tirar conclusões do tratamento que possam ser consideradas dados de natureza sensível? Para que os dados sejam considerados sensíveis em um determinado tratamento, o agente deve necessariamente estar ciente de que há a possibilidade de que eles sejam tratados de forma a produzir conclusões de natureza sensível? Como ficaria a questão se, neste mesmo caso, o agente não tivesse a intenção/ a finalidade de realizar um tratamento para obter informações sensíveis?

Intenções são, em geral, importantes no processo de decisão se os dados que estão sendo tratados podem ser considerados sensíveis. Para se analisar a questão, mostra-se relevante verificar, entre outros aspectos, o histórico do agente, o potencial de ganho comercial ou financeiro com o tratamento e se a intenção declarada é, de fato, objetivamente verificável. Imagine, por exemplo, um controlador que coletou grandes quantidades de dados pessoais, relativos a certas características comportamentais de determinadas pessoas, na esperança de que alguma forma de tratamento de dados possa estar disponível no futuro, permitindo tirar conclusões sobre o estado de saúde dos titulares dos dados. Usar uma definição muito restrita para os dados sensíveis pode significar que o referido tratamento não será considerado de

---

the classification of proxy data as "sensitive data" potentially depends on two conditions: (1) the *intention* of inferring sensitive attributes, and (2) the *reliability* of the data in question for inferring sensitive attributes. (…) Regarding intentionality, several legal commentators have argued that the classification of data as sensitive depends on the stated purpose of processing. Data controllers must have the intention of inferring sensitive information from a selection of data for it to be classified as sensitive.318 Schulz gives the example of a pizzeria delivering to customers in a drug abuse center. Transaction records would not be considered sensitive data unless the pizzeria intended to infer information about the health status of their customers." (WACHTER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review*, vol. 2019, Issue 1. p.73-74)

[126] "(...) mais importante do que identificar a natureza própria ou conteúdo do dado, é constatar a potencialidade discriminatória no tratamento de dados pessoais. Isto é, a limitação para o tratamento de dados se concretizaria na proibição de seu uso de maneira a gerar uma discriminação, um uso abusivo e não igualitário de dados. Não só a natureza de um dado, estruturalmente considerado, deve ser avaliada para sua determinação como sensível, mas deve-se admitir que certos dados, ainda que não tenham a princípio essa natureza especial, venham a ser considerados como tal, a depender do uso que deles é feito no tratamento de dados." (MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. *Migalhas*, publicado em 22 de junho de 2020.)

caráter sensível, visto que, no momento, não se pode tirar tais conclusões. Essa maneira de definir os dados pessoais pode ser insuficiente, dada a probabilidade de que futuras evoluções tecnológicas tornem esses dados sensíveis. Diante disso, uma definição que ignore completamente o propósito do agente não parece ser adequada, uma vez que ele poderá reunir dados não sensíveis esperando que futuras evoluções tecnológicas permitam acessar conclusões sensíveis sobre seus titulares.

Observa-se, por outro lado, que uma definição de dados sensíveis baseada exclusivamente no propósito do agente pode aumentar os riscos de imprudência ou de tratamento negligente de dados pessoais, como, por exemplo, casos em que o próprio controlador não tinha a intenção de tirar conclusões sensíveis, mas, ainda assim, processou os dados de tal forma que terceiros poderão ter acesso a eles e serem capazes de extrair tais conclusões. Além disso, embora um controlador possa afirmar estar tratando dados para uma determinada finalidade, pode, na realidade, ser difícil demonstrar que o que fora afirmado é, de fato, a verdadeira finalidade por trás da operação. Basear-se em propósitos declarados pode, em muitos casos, deixar a porta aberta para abusos, ao permitir situações em que o controlador pode, simplesmente, declarar que não tem intenção de processar dados sensíveis, mesmo quando, em verdade, realizar o oposto.

Além disso, mostra-se necessário considerar também quais outros dados podem estar disponíveis para o agente, além daqueles que ele vem diretamente tratando. Isso é importante porque a combinação de vários conjuntos de dados pode aumentar a probabilidade de que conclusões de natureza sensível sejam alcançadas, mesmo quando isso não for aparente, ao se olhar para conjuntos de dados específicos de forma isolada. Em ambientes cada vez mais interconectados, isso pode envolver levar em consideração não apenas outros dados que possam estar em posse do controlador, mas também dados que ele possa ter acesso em outro lugar e, inclusive, com terceiros.

Outro fator que deve ser avaliado diz respeito às habilidades técnicas do controlador de dados (ou outros controladores em potencial). Isso incluirá a capacidade computacional e o *know-how* técnico disponíveis. Tendo em vista que tais fatores estão em constante evolução e que o acesso a conjuntos de dados complementares está sempre aumentando, o contexto específico de um tratamento deverá, como regra, ser

compreendido de forma dinâmica. O tratamento de dados que pode não ter sido considerado sensível no passado pode muito bem ser considerado sensível no futuro.

Como apresentado, não se mostra possível definir, antecipadamente e de forma absoluta e permanente, os efeitos concretos de um tratamento de informações nem a real sensibilidade de um dado. Por exemplo, dados pessoais que pareçam não relevantes em determinado momento, que não façam referência a alguém diretamente ou, ainda, que não sejam formalmente sensíveis, uma vez transferidos, cruzados e/ou organizados, podem resultar em dados bastante específicos sobre determinada pessoa, trazendo informações, inclusive, de caráter sensível sobre ela.

Acerca da categoria dos dados sensíveis, Danilo Doneda destaca que:

> A elaboração desta categoria e de disciplinas específicas a ela aplicadas não foi isenta de críticas, como a que afirma que é impossível, em última análise, definir antecipadamente os efeitos do tratamento de uma informação, seja ela da natureza que for. Desta forma, mesmo dados não qualificados como sensíveis, quando submetidos a um determinado tratamento, podem revelar aspectos sobre a personalidade de alguém, podendo levar a práticas discriminatórias. Afirma-se, em síntese, que um dado, em si, não é perigoso ou discriminatório – mas o uso que dele se faz pode sê-lo. (...) deve-se ter em conta que o próprio conceito de dados sensíveis atende à uma necessidade de delimitar uma área na qual a probabilidade de utilização discriminatória da informação é potencialmente maior – sem deixarmos de reconhecer que há situações onde tal consequência pode advir sem que sejam utilizados dados sensíveis, ou então que a utilização destes dados se preste a fins legítimos e lícitos. [127]

Entende-se que, além de se realizar uma proteção mais ampla de dados positivados como sensíveis, tal proteção também deverá ser observada nos casos em que houver tratamento sensível de dados pessoais. Isso porque, com base estritamente em considerações a respeito da natureza dos dados tratados, nem sempre será possível predizer os efeitos que o tratamento poderá causar em seu titular ou em interesses coletivos *lato sensu*. Recomenda-se, então, que sejam verificadas, entre outras questões apontadas acima, as intenções do controlador e se, a partir do tratamento realizado, era previsível que os dados poderiam revelar informações sensíveis. Quando se pretender tratar dados para se inferir ou tirar conclusões sensíveis, a proteção deverá ser ampliada. Nesse sentido, de acordo com a LGPD (Art. 11, § 1º), a proteção disposta em seu artigo 11 (que traz o rol de bases legais para o tratamento de dados sensíveis) será aplicada,

[127] DONEDA, Danilo. *A proteção de dados pessoais nas relações de consumo*: para além da informação creditícia. Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010. p. 26-27

também, a qualquer tratamento de dados pessoais que *revele* dados sensíveis e que possa causar danos ao titular, ressalvado o disposto em legislação.

As novas e complexas formas de tratar dados vêm expandindo as possibilidades de classificação dos dados pessoais, o que tem levado à defesa do estabelecimento de novas categorias, relações e tutelas. Diante dos avanços tecnológicos e científicos, até mesmo informações pessoais que tradicionalmente não eram classificadas como sensíveis podem causar tanto (a) um tratamento discriminatório ilícito ou abusivo quanto (b) a dedução ou a inferência de dados sensíveis.[128]

Como exemplo disso, recorda-se caso em que se verificou que motoristas com nomes não ingleses, como *Mohammed Ali*, recebiam cotações de seguros de carros mais altas do que *Johns*. Segundo reportagem de 2018, grandes firmas ofereciam valores menores quando o motorista tinha nome considerado inglês, como, por exemplo, *John*, *Jack Jones* ou *David Smith*.[129] Há casos, também, de negativa de concessão de crédito para pessoas cujos nomes são, estatisticamente, os mais recorrentes na comunidade afrodescendente.[130] Ou seja, o simples prenome, em certo contexto, pode ser considerado dado sensível para fins de tutela da igualdade.

Doneda e Monteiro analisam caso de solicitação de dados de nacionalidade, que ensejou questionamentos a respeito da razão de seu requerimento e de possíveis tratamentos discriminatórios que poderia promover[131]. Determinado pró-reitor da Universidade Federal de Santa Maria solicitou algumas informações aos programas de pós-graduação da instituição, estando, entre elas, questionamento acerca da presença de alunos e/ou professores de nacionalidade israelense.[132] O pedido procurava atender a uma solicitação de acesso à informação dirigida à Universidade por algumas entidades.

---

[128] DONEDA, Danilo. op. cit., p. 27.

[129] Disponível em: <https://www.thesun.co.uk/motors/5393978/insurance-race-row-john-mohammed/> Acesso em: 02.11.20

[130] Disponível em: <https://www.oabrj.org.br/colunistas/gustavo-tepedino/as-tecnologias-renovacao-direito-civil> Acesso em: 02.11.20

[131] DONEDA, Danilo; MONTEIRO, Marília. Acesso à informação e privacidade no caso da Universidade Federal de Santa Maria. *Jota*. 2 jul. 2015. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/acesso-a-informacao-e-privacidade-no-caso-da-universidade-federal-de-santa-maria-02072015. Acesso em: 14 jun. 2020, n.p.

[132] Para mais dados sobre o caso, cf. BACKES, Vanessa. Em ofício, UFSM pede dados sobre a presença de israelenses no campus. *G1*, publicado em 03 de junho de 2015. Disponível em: <http://g1.globo.com/rs/rio-grande-do-sul/noticia/2015/06/em-oficio-ufsm-pede-dados-sobre-presenca-de-israelenses-no-campus.html> Acesso em: 14.06.20. FAMER, Vitória. MPF investiga antissemitismo em universidade federal. *Estadão*. publicado em 9 de junho de 2015. Disponível em: <https://brasil.estadao.com.br/noticias/geral,mpf-investiga-antissemitismo-em-universidade-federal-gaucha,1702478> Acesso em: 14.06.20.

Analisando o caso e a ponderação entre transparência e proteção de dados, os autores destacaram que:

> [...] o fato de a informação referente à nacionalidade ter elevado potencial discriminatório – ainda que a nacionalidade não seja comumente considerada em si como uma informação sensível – depreende-se do tratamento sensível que pode ser dado a tal informação, capaz de estigmatizar, classificar, pré-julgar e mesmo comprometer a segurança dos cidadãos afetados. Note-se que a discriminação em razão da procedência nacional é, inclusive, tipificada como crime no Art. 1º da Lei 7.716/1989. Para tal ponderação contribui, igualmente, a motivação discriminatória passível de ser inferida pela série de considerandos ao pedido de acesso à informação, ao julgar de forma contundente atos que eventualmente teriam sido praticados pelo Estado de Israel.[133]

Ainda sobre informações que podem se tornar sensíveis, vale lembrar o histórico de compras de uma pessoa em um supermercado ou em uma farmácia[134] ou o acesso à fatura de seu cartão de crédito, uma vez que, a partir disso, seria possível inferir dados sensíveis, como convicções religiosas, estado de saúde[135] ou orientação sexual. Dados de geolocalização[136] podem, também, ser manipulados para usos lesivos a seu titular e

---

[133] DONEDA, Danilo; MONTEIRO, Marília. Acesso à informação e privacidade no caso da Universidade Federal de Santa Maria. *Jota*. 2 jul. 2015. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/acesso-a-informacao-e-privacidade-no-caso-da-universidade-federal-de-santa-maria-02072015> Acesso em: 14.06.20.

[134] "Por exemplo, ao fornecer o número do CPF para obter descontos nas farmácias, a lista de medicamentos associada a esse dado pode conter informações delicadas sobre nossa saúde. É possível que essas informações sejam utilizadas de maneira discriminatória por seguradoras de saúde, alterando o valor da franquia de acordo com o perfil. Da mesma forma, nosso histórico de compras *online* diz bastante sobre poder aquisitivo e preferências pessoais. Por meio dessas informações, é possível embasar o direcionamento de propagandas compatíveis com o nosso gosto, tentando-nos a comprar algo que não precisamos, bem como cobrar preços mais altos ou limitar o acesso ao crédito para determinados perfis. Dados sobre orientação sexual, em uma sociedade que ainda vive preconceitos contra a diversidade, também podem servir a práticas de segregação, restringindo, por exemplo, as oportunidades de trabalho." (VARON, Joana. Entrevista II. *Panorama Setorial da Internet*, v. 11, n. 2, p. 12-14, 2019. Privacidade e dados pessoais. Disponível em: <https://www.cetic.br/media/docs/publicacoes/6/15122520190717-panorama_setorial_ano-xi_n_2_privacidade_e_dados_pessoais.pdf> Acesso em: 31 maio 2020, p. 12).

[135] Caso famoso envolve a empresa *Target* e o uso de dados para a realização de previsão de gravidez de clientes. Cf. DUHIGG, Charles. How companies learn your secrets. *The New York Times*. 26 fev. 2012. Disponível em: <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp>. Acesso em: 31 maio 2020. RODRIGUES, Alexandre; SANTOS, Priscilla. A ciência que faz você comprar mais. *Galileu*. out. 2012. Disponível em: <http://revistagalileu.globo.com/Revista/Common/0,,EMI317687-17579,00-A+CIENCIA+QUE+FAZ+VOCE+COMPRAR+MAIS.html> Acesso em: 31 maio 2020.

[136] No Mandado de Segurança 38.061, em decisão de 12 de julho de 2021 acerca da quebra de sigilos telefônico e telemático de José Matheus Salles Gomes, assessor especial do presidente Jair Bolsonaro, determinada pela CPI da Pandemia, o ministro Ricardo Lewandowski manteve as mesmas, porém não autorizou a quebra relativa aos dados de geolocalização. Lembrou que: "(...) a quebra de sigilo de dados de geolocalização é objeto de debate no RE 1.301.250 RG/RJ, de relatoria da Ministra Rosa Weber, que teve repercussão geral reconhecida (tema 1.148) em 7/6/2021, o qual ainda não foi submetido a julgamento." A questão da quebra de sigilo de dados referentes à geolocalização, por meio de tecnologias como GPS, Bluetooth, sinal Wi-Fi e torres de celular, para determinar o histórico localizações geográficas específicas de um usuário de telefone celular, é objeto do Recurso Extraordinário. Esse recurso foi

para a verificação de informações íntimas. Eles podem revelar, por exemplo, sua religião (pessoa localizada em determinado templo religioso) ou permitir que seja presumida alguma condição de saúde (pessoa localizada em clínica de saúde especializada em determinada doença). O CEP do domicílio de uma pessoa natural apresenta a potencialidade de ser utilizado para se analisar o padrão de vida e a renda dela, assim como a profissão e eventual especialização podem ajudar a inferir a renda média do sujeito. O próprio dado relativo à identidade de gênero – entendido dentro de um contexto amplo – por vezes é utilizado para discriminações ilícitas ou abusivas, conforme será analisado no capítulo 2.

Proteção específica também pode se mostrar relevante em tratamentos que envolvam, por exemplo, dados sobre origem social, dados financeiros[137] [138] de pessoas

---

interposto pelo Google no âmbito da investigação do assassinato da vereadora Marielle Franco e do motorista Anderson Gomes. Por esse motivo, na avaliação de Lewandowski, seria "prematura" qualquer decisão nesse sentido. Informações disponíveis em: <http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=469193&tip=UN> Acesso 15.07.21

[137] A segurança da informação deve ser um pilar estratégico e prioritário para todas as instituições financeiras, especialmente aquelas que oferecem serviços digitais. Para garantir a segurança dos usuários e da própria empresa, alguns investimentos mostram-se essenciais, como, por exemplo: o uso amplo de criptografia e a constituição de equipe de segurança de alto padrão, havendo, portanto, profissionais capacitados em *cyber security*. Para a segurança dos dados financeiros, também é necessário que a empresa esteja em *compliance* com a LGPD e com padrões mundiais, como o CIS (Center for Internet Security) e o ISO/IEC 27001, tanto a nível de hardware quanto a nível de software. Por fim, deve-se incrementar dentro da instituição uma elevada cultura de segurança e proteção de dados, bem como a realização de certificações na área. Fonte: <https://cryptoid.com.br/identidade-digital-destaques/seguranca-digital-quais-cuidados-as-fintechs-devem-ter-com-os-dados-financeiros-dos-clientes/> Acesso em: 17.03.21.

[138] "(...) há fundamento legal razoável apto a justificar que tais dados devam ser tratados com cuidados técnicos especiais e que seu vazamento ou uso indevido podem ensejar reparações próprias para sua natureza peculiar, conforme passa-se a demonstrar: Como já foi dito, a jurisprudência pátria já correlacionou o sigilo dos dados pessoais financeiros à proteção da intimidade. Não é difícil perceber que, no atual momento e circunstâncias da sociedade moderna, descortinar a vida financeira de alguém é praticamente o mesmo que adentrar e devassar a própria vida íntima dessa pessoa, a qual, conforme explanado, possui proteção constitucional e legal pelo Código Civil. E mais, conhecendo dados financeiros de titular identificável, é possível descobrir dados pessoais sensíveis desse titular, tais como filiação a sindicato ou a organização de caráter religioso, filosófico ou político (identificando o pagamento de mensalidade a uma instituição, como a maçonaria por exemplo), dado referente à saúde (identificando o pagamento a um profissional de saúde, como um renomado especialista em oncologia por exemplo) e dado referente à vida sexual (como pagamentos em estabelecimentos especializados desse segmento).(...) É importante considerar que os dados financeiros podem levar à associação e à descoberta de outros dados, incluindo sensíveis, razão pela qual, muito embora a LGPD não tenha classificado os dados bancários como sensíveis, tais dados são capazes de gerar danos complexos aos titulares de dados e, portanto, demandam uma classificação de, no mínimo, como dados críticos, adotando-se medidas mais eficazes para o tratamento desses dados. (CASTRO, Dayane Marciano de Oliveira; MANO, Janini Nogueira D'Alessandro; BARONOVSKY, Thainá. Dados pessoais bancários e financeiros são considerados dados sensíveis para a LGPD? *Migalhas*, publicado em 18 de agosto de 2021. Disponível em: <https://www.migalhas.com.br/depeso/350335/dados-pessoais-bancarios-sao-considerados-dados-sensiveis-para-a-lgpd> Acesso em 19.08.21.)

naturais, dados sobre antecedentes[139], processos ou condenações criminais e dados relativos a alguma forma de deficiência.

Em um primeiro momento, a idade de uma pessoa não é considerada um dado sensível. Todavia, o referido dado pode ser utilizado, por exemplo, para segregar e impedir que uma pessoa idosa se candidate a uma vaga de emprego, em razão dos recrutadores partirem da premissa de que pessoas a partir de certa idade teriam menos habilidades com novas tecnologias. Esse seria um caso de *ageísmo*, que pode ser compreendido como o ato de estereotipar de maneira preconceituosa alguém pela idade. Esse tipo de preconceito tem o potencial de, até mesmo, diminuir a expectativa de vida de quem o sofre e vai de encontro com as tendências do mercado de trabalho, visto que a participação de pessoas idosas vem crescendo de forma constante, bem como sua inserção em aparatos tecnológicos.[140]

Outro exemplo de tratamento de informação pessoal que, como

[139] Acerca dos dados relativos a antecedentes criminais, vale ressaltar o tratamento realizado a partir da análise de certidões e documentos que trazem antecedentes cíveis e criminais, além de informações acadêmicas e profissionais de uma pessoa, no chamado *background check:* processo realizado pelas organizações que iniciam processos seletivos para novos colaboradores, sobretudo para cargos estratégicos, para avaliar a sua idoneidade. Isso costuma ser levantado, por exemplo, nos perfis nas redes sociais, junto a tribunais de justiça ou em órgãos como SPC e Serasa. No Brasil, tanto a legislação trabalhista quanto a Justiça do Trabalho são rigorosos em relação à realização de *background check* e possíveis procedimentos discriminatórios em relação aos trabalhadores. Segundo Iuri Pinheiro e Vólia Bomfim: "(...) a busca de referência e bons antecedentes funcionadas dos candidatos são uma espécie de discriminação positiva e são importantes para verificar o denominado ajuste da empresa ("company fit") ou integração do empregado a cultura organizacional conforme foi abordado no tópico anterior. Por fim, a exigência de certidão de antecedentes criminais já foi objeto de decisão vinculante do Tribunal Superior do Trabalho (TST), em acórdão publicado em 22/09/2017, no julgamento do Recurso Repetitivo (RR) 243000-58.2013.5.13.0023, com a fixação da tese jurídica prevalecente que a exigência de certidões de antecedentes criminais somente se justifica em casos excepcionais, em virtude da existência de lei, natureza do ofício ou elevado grau de fidúcia. A própria tese fixada no Tema 01 da Tabela de Recursos Repetitivos elenca atividades em relação às quais é legítima a exigência de certidão de antecedentes criminais: II) a exigência de Certidão de Antecedentes Criminais de candidato a emprego é legítima e não caracteriza lesão moral quando amparada em expressa previsão legal ou justificar-se em razão da natureza do ofício ou do grau especial de fidúcia exigido, a exemplo de empregados domésticos, cuidadores de menores, idosos ou deficientes (em creches, asilos ou intuições afins), motoristas rodoviários de carga, empregados que laboram no setor da agroindústria no manejo de ferramentas de trabalho perfurocortantes, bancários e afins, trabalhadores que atuam com substâncias tóxicas, entorpecentes e armas, trabalhadores que atuam com informações sigilosas. Vencidos parcialmente os Exmos. Ministros Augusto César de Carvalho, relator, Aloysio Corrêa da Veiga, Walmir Oliveira da Costa e Cláudio Mascarenhas Brandão, que não exemplificavam; Como ilustração de trabalhadores que lidam com informações sigilosas pode-se citar o caso de operador de telemarketing, que atuam diariamente com intenso fluxo de dados, sendo, assim, justificável a exigência a luz da jurisprudência da SBDI-1 do C. TST." (PINHEIRO, Iuri; BOMFIM, Vólia. A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho. Disponível em: <http://trabalhoemdebate.com.br/artigo/detalhe/a-lei-geral-de-protecao-de-dados-e-seus-impactos-nas-relacoes-de-trabalho> Acesso em: 14.07.21.)

[140] Preconceito etário traz falsas ideias sobre idosos no mercado de trabalho. Instituto de Longevidade MAG. 2021. Disponível em: <https://institutodelongevidademag.org/longevidade-e-trabalho/carreira/preconceitos-idosos-no-mercado-de-trabalho> Acesso em: 05.09.21.

regra, assume um viés discriminatório ilícito envolve o fato de a mulher ter ou não filhos, a idade dos menores e/ou se ela se encontra em um momento provável da vida de querer engravidar. Em determinados casos, os recrutadores costumam entender – em uma prática nociva e antiquada, baseada em uma cultura machista – que determinado perfil de candidata mulher poderia apresentar riscos de se ausentar mais vezes da empresa ou de oferecer menos entregas e disponibilidade.[141]

Recorda-se, aqui, análise de Sandra Wachter e Brent Mittelstadt[142] sobre inferências obtidas a partir de dados pessoais e se as mesmas, a depender do conteúdo que oferecerem, podem ser consideradas dados sensíveis:

> It is important to note that gender, age, information about a person's financial situation, geolocation and personal profiles are not considered sensitive data under Article 9, despite often serving as grounds for discrimination. A general prohibition on sensitive data processing is established with several exceptions, including explicit consent, scientific or statistical purposes, and when "processing relates to personal data which are manifestly made public by the data subject." Concerns about inferences are implicit in the definition of "special categories of personal data." The phrase "personal data revealing" suggests that the definition is intended to cover data that both directly discloses and indirectly reveals protected attributes. (…) in a later set of guidelines on profiling, the Article 29 Working Party noted that profiling activities can create sensitive data "*by inference* from data which is not special category data in its own right but becomes so when combined with other data." While such proxy data, such as a postcode, is not sensitive by nature, the Article 29 Working Party clearly believes it must be treated as such if it "indirectly reveals" or can be used to infer sensitive attributes.[143] [144]

---

[141] De acordo com estudo do IBGE publicado em 2021 - *Estatísticas de gênero*: indicadores sociais das mulheres no Brasil: "O indicador Nível de ocupação das pessoas de 25 a 49 anos (CMIG 15) mostra que a presença de crianças com até 3 anos de idade vivendo no domicílio é uma característica importante na determinação da ocupação das mulheres no mercado de trabalho. Entre aquelas que possuem crianças nesse grupo etário, a proporção de ocupadas em relação à PIT é de 54,6%, abaixo dos 67,2% daquelas que não possuem. O nível de ocupação dos homens é superior ao das mulheres em ambas as situações, sendo inclusive maior entre os homens com crianças com até 3 de idade vivendo no domicílio, situação em que a diferença para as mulheres chegou a 34,6 pontos percentuais em 2019. As mulheres pretas ou pardas com crianças de até 3 anos de idade no domicílio apresentaram os menores níveis de ocupação – menos de 50% em 2019 –, ao passo que, entre as mulheres brancas, a proporção foi de 62,6%. Para aquelas sem a presença de crianças nesta faixa etária, os percentuais foram de, respectivamente, 63,0% e 72,8%. O maior envolvimento no trabalho não remunerado contribui para explicar a menor participação das mulheres no mercado de trabalho." (IBGE. *Estatísticas de gênero*: indicadores sociais das mulheres no Brasil. Coordenação de População e Indicadores Sociais. Rio de Janeiro: IBGE, 2021. Disponível em: <https://biblioteca.ibge.gov.br/index.php/biblioteca-catalogo?view=detalhes&id=2101784> Acesso em: 05.09.21.)

[142] WACHTER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review*, vol. 2019, issue 1, p.01-130.

[143] Tradução livre: É importante observar que gênero, idade, informações sobre a situação financeira de uma pessoa, geolocalização e perfis pessoais não são considerados dados sensíveis nos termos do Artigo 9º [do GDPR], apesar de muitas vezes servirem como motivo de discriminação. Foi estabelecida uma proibição geral de tratamento de dados sensíveis com várias exceções, incluindo consentimento explícito,

Os autores entendem que padrões mais altos de proteção de dados, como os concedidos a dados sensíveis, podem se aplicar a inferências em dois sentidos. Primeiro, quando dados inferidos ou derivados divulgarem diretamente atributos protegidos – como, por exemplo, se um controlador inferir a etnia de uma pessoa a partir de seu histórico educacional. Segundo, quando dados pessoais puderem ser mostrados para permitir que atributos sensíveis sejam inferidos, ou seja, revelados indiretamente. A partir de dados de origem, inferências sensíveis podem ser extraídas. Por consequência, eles poderão ser tratados como dados sensíveis. Por exemplo, a partir do sobrenome de uma pessoa natural ou do local de seu nascimento, seria possível inferir sua raça, segundo os autores.

Eles[145] alertam também que dados não sensíveis podem se tornar sensíveis se usados para inferir atributos de natureza sensível, porém o conteúdo de tais dados permanecerá o mesmo. Isso sugere que a distinção entre dados pessoais gerais e dados pessoais sensíveis seria fundamentalmente falha, pelo menos quando usada para controlar a coleta de dados pessoais. Na era de análise de Big Data, essa distinção torna-se cada vez mais fluída, pois aparentemente qualquer dado pode se tornar sensível, se for encontrada uma maneira de, a partir dele, serem inferidas informações sobre atributos assim protegidos.

As referidas preocupações aparecem em pesquisas há mais de uma década. Segundo estudo desenvolvido por pesquisadores da Universidade de Cambridge, afirmou-se[146] que registros digitais de comportamento facilmente

---

fins científicos ou estatísticos ou quando "o tratamento se referir a dados pessoais que sejam manifestamente tornados públicos pelo titular dos dados". Preocupações com inferências estão implícitas na definição de "categorias especiais de dados pessoais". A frase "revelação de dados pessoais" sugere que a definição se destina a cobrir dados que divulgam diretamente ou indiretamente atributos protegidos. (…) em um conjunto posterior de diretrizes sobre a criação de perfis, o Grupo de Trabalho do Artigo 29 observou que as atividades de criação de perfis podem criar dados sensíveis "por inferência de dados que não são dados de categoria especial por direito próprio, mas se tornam assim quando combinados com outros dados". Embora esses dados proxy, como um código postal, não sejam sensíveis por natureza, o Grupo de Trabalho do Artigo 29 acredita claramente que devem ser tratados como tal se "revelarem indiretamente" ou puderem ser usados para inferirem atributos sensíveis.

[144] WACHTER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review*, vol. 2019, Issue 1, p.70-72.

[145] WACHTER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review*, vol. 2019, Issue 1, p.73.

[146] KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. Private traits and attributes are predictable from digital records of human behavior. *PNAS*, vol. 110, n. 15, abril/2013, p. 5802-5805. Disponível em: <https://doi.org/10.1073/pnas.1218772110> Acesso em: 19.01.21.

acessíveis, como curtidas no Facebook, poderiam ser usados para prever, automaticamente e com precisão, atributos pessoais sensíveis como: orientação sexual, etnia, pontos de vista religiosos e políticos, traços de personalidade, inteligência, felicidade, uso de substâncias viciantes, separação dos pais, idade e sexo. Dos perfis analisados, o modelo identificou, com elevada acuidade, homossexuais e heterossexuais, usuários brancos e negros e pessoas com ligações partidárias republicana ou democrata. [147] Mulholland apresenta dois casos graves em que o perfilamento (*profiling*) gerou tratamentos discriminatórios:

> Os casos ocorreram nos EUA e se referiram à contratação de serviços médicos e de seguridade. No primeiro caso, algumas seguradoras utilizaram dados pessoais relacionados às vítimas de violência doméstica, acessíveis em banco de dados públicos. O resultado do tratamento dos dados levou a uma discriminação negativa, ao sugerir que mulheres vítimas de violência doméstica não poderiam contratar seguros de vida, saúde e invalidez, pois o risco contratado seria muito alto. Em outro caso, relacionado a dados de saúde, "quando uma pessoa tem um derrame, alguns bancos, ao descobrir tal fato, começam a cobrar o pagamento dos empréstimos realizados". [148]

Além disso, a partir de metadados é possível inferir diversas informações sensíveis sobre uma pessoa. Praticamente todos os dispositivos geram metadados conforme são utilizados, sendo exemplo emblemático o *smartphone*, ferramenta cada vez mais utilizada por adultos e menores de idade. Ao tirar uma foto, por exemplo, além

---

[147] Recorda-se também, aqui, pesquisa de emoções realizada no Facebook com usuários da plataforma. Em janeiro de 2012, pesquisadores ajustaram o feed de notícias de quase 690 mil usuários para exibir histórias mais "positivas" ou "negativas", a fim de descobrir se as emoções seriam contagiosas nas redes sociais, ou melhor, se a transferência de emoções que acontece cara-a-cara também poderia ocorrer digitalmente. A equipe criou um algoritmo para analisar palavras no feed de notícias, que categorizou cada post como emocionalmente mais positivo ou negativo. Eles então usaram essas informações para ajustar os feeds de notícias de diversos usuários: em alguns feeds, o usuário deixava de ver status mais negativos; outros destacavam posts mais tristes. Verificou-se um efeito direto a partir disso: apesar de não ocorrer nenhuma interação humana real, os participantes que viram feeds artificialmente mais positivos postaram atualizações de status mais felizes e pessoas com feeds mais tristes postaram mensagens mais amargas. Os resultados indicaram que emoções expressas por outras pessoas no Facebook influenciavam as nossas emoções. O trabalho também sugeriu que a interação pessoal e as dicas não-verbais não eram estritamente necessárias para o contágio emocional e que a observação das experiências positivas dos outros constituiria experiência positiva para as pessoas. Entretanto, pergunta que logo veio à tona logo após a publicação do estudo foi: pode uma rede social financiar uma pesquisa como essa? O Facebook poderia manipular as emoções de usuários através do feed de notícias? (KRAMER, Adam D. I.; GUILLORY, Jamie E.; HANCOCK, Jeffrey T. Experimental evidence of massive-scale emotional contagion through social networks. *PNAS*, vol. 111, n. 24, jun. 2014, p. 8788-8790. Disponível em: <https://doi.org/10.1073/pnas.1320040111> Acesso em: 19.01.21)

[148] MULHOLLAND, Caitlin. Os contratos de seguro e a proteção dos dados pessoais sensíveis. In: GOLDBERG, Ilan; JUNQUEIRA, Thiago (Coords.). *Temas Atuais de Direito dos Seguros*, Tomo I. São Paulo: Thomson Reuters. 2020.

da imagem ficar gravada na memória do celular, metadados são associados a ela, descrevendo informações sobre o modelo da câmera, data, tamanho e formato do arquivo e o local de onde a foto foi tirada.

O conteúdo de comunicações pode revelar informações sensíveis sobre as pessoas envolvidas[149], desde experiências pessoais e emoções até condições médicas, preferências sexuais e visões políticas, cuja divulgação pode resultar em danos pessoais e sociais, perdas econômicas e/ou constrangimentos. Da mesma forma, metadados derivados de comunicações eletrônicas também podem revelar informações muito pessoais. Números chamados, os sites visitados, a localização geográfica e a data e a duração de uma chamada são informações que permitem tirar conclusões sobre a vida privada de uma pessoa, como suas relações sociais, seus hábitos, atividades da vida cotidiana e seus interesses e gostos. [150] [151]

Tendo em vista as diversas possibilidades de utilização e cruzamento de dados, bem como o oferecimento de ferramentas tecnológicas cada vez mais sofisticadas, mostra-se, hoje, difícil pensar em um dado pessoal que não seja potencialmente sensível. Adicionalmente, o intenso desenvolvimento da *Internet das Coisas*[152] e a

[149] HOF, Simone van der. I agree, or do I? A rights-based analysis of the law on children's consent in the digital world. *Wisconsin International Law Journal*, v. 34, n. 2, p. 409-445, 2016.

[150] Proposal for a regulation of the european parliament and of the council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM/2017/010 final - 2017/03 (COD). Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010> Acesso em: 01.01.21

[151] "A partir das técnicas de mineração de dados aplicadas ao conteúdo de nossas comunicações eletrônicas pode-se obter informações de caráter sensível relacionadas a experiências e emoções pessoais, preferências sexuais e visões políticas, cuja divulgação pode resultar em danos pessoais e sociais, perda econômica ou constrangimento. Além disso, os metadados relativos a essas comunicações, como números discados, sites visitados, localização geográfica, hora, data, podem permitir que conclusões precisas sejam inferidas sobre as pessoas envolvidas na comunicação, tais como as suas opções religiosas, políticas, hábitos, interesses e medos." (DALESE, Pedro. Os dados pessoais sensíveis na era do Big Data. Migalhas, publicado em 03 de março de 2021. Disponível em: <https://www.migalhas.com.br/depeso/341100/os-dados-pessoais-sensiveis-na-era-do-big-data> Acesso em: 06.03.21)

[152] O universo da Internet da Coisas (*Internet of Things*) representa a integração de objetos físicos e virtuais em redes conectadas à Internet, permitindo que "coisas" coletem, troquem e armazenem uma enorme quantidade de dados, inclusive, em uma nuvem. Por meio da IOT, é possível o gerenciamento de dispositivos, mesmo à distância, para aumentar a eficiência de sistemas e processos. Uma vez processados e analisados, esses dados geram informações e serviços em escala inimaginável. Cada vez mais, percebe-se a incorporação da IOT na vida de adultos, adolescentes e crianças. Relógios, geladeiras, leitores de digitais, vibradores sexuais, detectores de movimento, câmeras, peças de vestuário e brinquedos já se encontram conectados à Internet e presentes nas casas e corpos das mais diversas pessoas, enquanto empresas coletam dados sobre movimentos, preferências e hábitos de seus usuários, que não têm, por vezes, nem mesmo plena capacidade civil. (Cf. TEFFÉ, Chiara Spadaccini de. Dados sensíveis de crianças e adolescentes: aplicação do melhor interesse e tutela integral. In: LATERÇA, Priscilla Silva;

chegada gradativa do IPV6 foram relevantes na expansão dos conjuntos informacionais, o que permite que os agentes de tratamento possam alcançar rapidamente conclusões sensíveis sobre determinada pessoa.

Vive-se intensamente, nos últimos tempos, o fenômeno da *datificação*: ato de datificar (pôr em dados) a vida e as relações de uma pessoa[153]. As informações são formatadas de maneira que possam ser registradas, monitoradas e analisadas, permitindo a extração de mais informações e a análise preditiva dos sujeitos[154], o que facilita, sobremaneira, inferências de caráter sensível sobre eles.

A datificação combina a transformação da vida humana em dados, fluindo por diversas arquiteturas como plataformas, serviços, aplicativos, bancos de dados e dispositivos de hardware. Há a geração de diferentes tipos de valor e de interações a partir desses dados, como, por exemplo, em processos de monetização, meios de controle governamental, produção cultural, personalização de produtos e serviços e direcionamento de conteúdos.[155] A tendência é a de que todo o ser humano tenha um prolongamento e uma projeção de si no ambiente digital, de modo que muitos aspectos de sua vida poderão ser decididos a partir de sua extensão eletrônica.[156]

FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (Coords.). *Privacidade e Proteção de Dados de Crianças e Adolescentes*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021. E-book. TEFFÉ, Chiara Spadaccini de; SOUZA, Carlos Affonso. Infância conectada: direitos e educação digital. In: Comitê Gestor da Internet no Brasil. (Org.). Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil: TIC kids online Brasil 2017. 1ed.São Paulo: Comitê Gestor da Internet no Brasil, 2018, v. 1, p. 31-40.) Tendo em vista que os dispositivos conectados estão cada vez mais complexos — inclusive com maior autonomia e, por vezes, com comportamento imprevisível — e sendo direcionados para os mais variados públicos e idades, é necessário que os desenvolvedores tenham maior responsabilidade na produção desses dispositivos, bem como empreguem maior atenção à fase de testes controlados antes que eles sejam destinados à comercialização.

[153] "(...) uma das consequências mais palpáveis do capitalismo movido a dados é a progressiva estruturação de uma sociedade baseada em classificações e julgamentos algorítmicos. A partir do fenômeno que alguns estudiosos chamam de datificação, toda e qualquer experiência humana torna-se um dado a partir do qual se podem inferir aspectos importantes sobre as pessoas. (...) Como bem sintetiza John Cheney-Lippold, os algoritmos hoje agregam e controlam nossas identidades datificadas (*datafied selves*) e nossos "futuros algorítmicos", pois o processo de classificação em si já é uma importante demarcação de poder, assim como a organização do conhecimento e da vida molda as condições e as possibilidades daqueles que serão classificados. Afinal, são as categorias para as quais nossas vidas datificadas serão convertidas que passarão a definir não apenas quem somos, mas também quem seremos, na medida em que os dados, ao mesmo tempo em que nos representam, também nos regulam." (FRAZÃO, Ana. Discriminação algorítmica. *Jota*, publicado em 23 de junho de 2021.)

[154] MAYER-SCHOENBERGER, V.; CUKIER, K. *Big Data*: a revolution that will transform how we live, work, and think. Londres: John Murray, 2013.

[155] MEJIAS, Ulises A.; COULDRY, Nick. Datafication. *Internet Policy Review*, 8(4). 2019. Disponível em: <https://policyreview.info/concepts/datafication>. Acesso em: 27 jul. 2021.

[156] BIONI, Bruno Ricardo. *Proteção de Dados Pessoais*: a função e os limites do consentimento. 2.ed. Rio de Janeiro: Editora Forense, 2020. p. 87.

O reconhecimento de padrões e o incremento das técnicas de previsão comportamental podem conduzir a decisões mais eficientes e reduzir custos. Na área privada, informações e perfis vêm orientando estratégias competitivas e serviços ofertados. Podem também determinar a cotação de proposta de seguro ou de crédito; o direcionamento de publicidade; a recomendação de filmes e músicas; ou a seleção em oportunidades de emprego. No ambiente público, dados permitem reconhecer e extrair informações de políticas públicas, programas e operações para subsidiar tomadas de decisão, bem como fornecem recursos e previsões sobre onde agir para lidar com eventuais riscos e identificar oportunidades.[157]

Passamos a integrar variadas ferramentas tecnológicas em nossas atividades habituais e a fornecer cada vez mais dados sobre nossos corpos, personalidades, interesses, estilos de vida, comportamentos, movimentos, comunicações e relações interpessoais. Por meio de perfis e aplicações, compartilhamos desde como gastamos nosso dinheiro e quais músicas gostamos de escutar até nossa frequência cardíaca, hábitos sexuais, orações diárias e ciclo menstrual.

Os conjuntos de dados que deixamos, de forma voluntária ou não, tornam-se rastros e objeto de análise, tanto do setor privado quanto público. Despontam, assim, tentativas de identificar padrões, estabelecer classificações, criar correlações, fazer inferências e, inclusive, prever nossos comportamentos. Vale lembrar, contudo, que a extração e a análise de dados servem não apenas para entender e prever comportamentos, mas também para influenciar e manipular o indivíduo e suas emoções. A manipulação na identidade e nos desejos da pessoa pode ser acompanhada de distorções na autoestima ou de deturpações de narrativas.

Diante disso, não mais parece fazer sentido considerar um dado ou um conjunto de dados de forma isolada e estática, mas, sim, dentro de uma perspectiva dinâmica que considere diversos fatores e sujeitos. Entretanto, tal perspectiva deve levar em conta, também, a necessidade de não ocorrer um alargamento excessivo da categoria dos dados sensíveis, já que isso tanto limitaria uma série de tratamentos e bases legais importantes para os agentes quanto deixaria a categoria com menos relevo e valor no futuro, diante de uma possível banalização.

---

[157] Organização das Nações Unidas. Data Strategy of the Secretary-General for Action by Everyone, Everywhere with Insight, Impact and Integrity. 2020. Disponível em: <https://un.org/en/content/datastrategy/images/pdf/UN_SG_Data-Strategy.pdf>. Acesso em: 28 jun. 2021.

Como forma de concretização da dignidade da pessoa humana, e figurando como direito da personalidade, a proteção de dados pessoais revela-se fundamental, sendo condição para que o sujeito se realize e se relacione em sociedade. Como apresentado, tutelar dados sensíveis e tratamentos de caráter sensível significa proteger a pessoa contra discriminações abusivas ou ilícitas[158], assegurar igualdade material no seu tratamento e permitir o livre desenvolvimento da sua personalidade, levando-se em conta suas diferenças e características particulares.

1.2.1.1 A definição dos dados sensíveis no contexto do Regulamento Geral Europeu sobre a Proteção de Dados

O Regulamento Geral Europeu sobre a Proteção de Dados (RGPD - Regulamento (UE) nº 2016/679) traz uma lista de "categorias especiais de dados pessoais", conferindo proteção específica para os dados sensíveis.[159] Entende-se que a utilização do Regulamento[160] trouxe mais segurança para o tema, ao estabelecer, precisamente, quais dados deveriam ser de natureza sensível[161] e oferecer definições claras para algumas espécies assim consideradas. No rol, foram listados como sensíveis: dados pessoais que revelam origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas ou filiação em sindicatos; dados genéticos; dados biométricos para o propósito de unicamente identificar uma pessoa natural; dados relativos à saúde;

---

[158] Cf. MULHOLLAND, Caitlin. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). *Revista de Direitos e Garantias Fundamentais*, v. 19, p. 159-180, 2018. MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. *Revista do advogado*, v. 144, p. 47-53, 2019. MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. In: Mulholland, Caitlin. (Org.). *LGPD e o novo marco normativo no Brasil*. 1ed.Porto Alegre: Arquipélago Editorial, 2020, p. 121-156.

[159] Ao longo dos capítulos 2 e 3 da tese, serão feitas outras referências ao GDPR, em questões específicas. Ainda que se reconheça a grande importância da norma europeia para a interpretação e a aplicação da LGPD, na presente tese não foi realizado estudo com base no direito comparado.

[160] Diretivas são, em resumo, atos legislativos que harmonizam as legislações nacionais e estabelecem determinados objetivos que devem ser alcançados pelos Estados Membros da UE. As diretivas devem ser transpostas pelos países da UE para a legislação nacional. Nesse caso, cada país pode decidir como incorporar as diretivas em sua legislação nacional. Por outro lado, o Regulamento é obrigatório e diretamente aplicável, em sua totalidade, em todos os Estados-Membros, ainda que ofereça certa flexibilidade para que alguns aspectos sejam ajustados por cada Estado-Membro. O GDPR foi adotado em abril de 2016 e tornou-se aplicável a partir de 25 de maio de 2018. Visa a criar um regime de proteção de dados pessoais mais eficaz e consistente na UE.

[161] A questão do rol dos dados sensíveis – se exemplificativo ou taxativo – será examinada no capítulo 2.

e dados relativos à vida sexual de uma pessoa ou orientação sexual.

Diante disso, os Estados-Membros já não podem criar outras categorias de dados sensíveis, como faziam ao abrigo da Diretiva 95/46/CE. Esta harmonização geral foi, porém, limitada no que diz respeito aos dados genéticos, biométricos ou relativos à saúde, pois os Estados-Membros estão autorizados a manter ou a introduzir outras condições, incluindo limitações, relativas ao seu tratamento. Embora essa exceção não cubra todas as formas de dados sensíveis descritas no Artigo 9º, ela se aplica a categorias importantes, que são centrais para muitas áreas críticas, como segurança, saúde e pesquisa científica. A norma europeia trouxe bases específicas para o tratamento de categorias especiais de dados, bem como positivou restrições para a tomada de decisões automatizadas que utilizarem dados sensíveis. Adicionalmente, o Regulamento estabeleceu requisitos administrativos que deverão ser aplicados quando houver o tratamento de dados sensíveis em grande escala: o controlador de dados será obrigado a nomear um responsável pela proteção de dados, de acordo com o Artigo 37 (1) (c), e a realizar uma avaliação de impacto sobre a proteção de dados, conforme o Artigo 35 (3) (b). Portanto, além da necessária escolha e aplicação da base legal pertinente ao tratamento, o controlador terá deveres adicionais.

Acerca do tratamento de categorias especiais de dados no GDPR, mostra-se majoritário o entendimento de que a lista de dados sensíveis contida no Artigo 9º, nº 1, é exaustiva [162], de forma que não poderão ser acrescentadas espécies adicionais de dados sensíveis a ela. Dados pessoais relativos a condenações criminais e ofensas não se encontram no referido rol.[163] Segundo Georgieva e Kuner, a

[162] GEORGIEVA, Ludmila; KUNER, Christopher. Article 9 Processing of special categories of personal data In: KUNER, Christopher; BYGRAVE, Lee; DOCKSEY, Christopher. *The EU General Data Protection Regulation (GDPR): A Commentary*. 1.ed. Oxford University Press: 2020. p. 373.

[163] "Modernised Convention 108 includes personal data relating to offences, criminal proceedings and convictions, and related security measures in the list of special categories of personal data. Within the framework of the GDPR, personal data relating to criminal convictions and offences or related security measures are not mentioned as such in the list of special categories of data, but are dealt with in a separate article. Article 10 of the GDPR stipulates that processing such data may only be carried out "under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects". Comprehensive registers holding information on criminal convictions, on the other hand, can only be kept under the control of specific official authorities. In the EU, processing personal data in the context of law enforcement is governed by a specific legal instrument, Directive 2016/680/EU. The directive stipulates specific rules for data protection, which are binding upon competent authorities when they process personal data specifically to prevent, investigate, detect and prosecute criminal offences (see Section 8.2.1)." **(**EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS AND COUNCIL OF

lista inclui não apenas indicações diretas de dados sensíveis, mas também informações que podem ser usadas para indicá-los, conforme evidenciado pelo uso da palavra *revealing*[164] no mencionado artigo.[165] Por exemplo, no relatório "Investigação sobre o uso de análise de dados em campanhas políticas", publicado pelo *Information Commissioner's Office* (ICO), afirmou-se que a empresa processou dados pessoais obtidos de usuários do Facebook para fazer previsões sobre suas afiliações políticas e opiniões e que, portanto, tais dados deveriam ser considerados sensíveis nesse contexto.[166] No parágrafo 1º do Art. 9º, o GDPR propõe uma definição baseada no contexto para todos os tipos de dados sensíveis ("dados pessoais que revelem" ou "dados relativos à"), exceto os biométricos, para os quais propõe uma definição baseada na finalidade do agente. [167] São dados sensíveis:

> (…) personal data *revealing* racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data *concerning* health or data *concerning* a natural person's sex life or sexual orientation (…). (grifo nosso)

Um dos objetivos da exceção relativa a dados biométricos parece ser o de excluir fotografias e imagens da consideração automática de que elas seriam sensíveis. Isso

---

EUROPE. *Handbook on European data protection law*. Luxembourg: Publications Office of the European Union, 2018. p. 96-97)

[164] "The term "data *revealing* racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership" is to be understood that not only data which by its nature contains sensitive information is covered by this provision, but also data from which sensitive information with regard to an individual can be concluded." (Article 29 Working Party: Advice Paper on Special Categories of Data. p. 06. Publicado em: 04 de abril de 2011.)

[165] "To summarize, the definition of "special categories of personal data" in the GDPR clearly indicates that any personal data that directly discloses or contains information about a special category must be treated as "sensitive data'." In contrast, the classification of data, which indirectly reveals or can be used to infer sensitive information, is not so straightforward. The necessity of intentionality and reliability are a point of disagreement among commentators, the Article 29 Working Party, and the ECJ: one, both, or perhaps neither condition must be met to re-classify non-sensitive source data as sensitive data capable of revealing sensitive information." (WACHTER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review*, vol. 2019, Issue 1. p.77)

[166] "Since CA used the information collected to make predictions about data subjects' political affiliations and opinions, it is clear that the data should be considered sensitive personal data." (ICO 2018: Investigation into the use of data analytics in political campaigns. Publicado em: 06 de novembro de 2018. Disponível em: <https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/> Acesso em: 01.04.21.)

[167] QUINN, Paul; MALGIERI, Gianclaudio. The Difficulty of Defining Sensitive Data – the Concept of Sensitive Data in the EU Data Protection Framework. *Brussels Privacy Hub Research Paper*, publicado em 16 de outubro de 2020. p.06. Disponível em: <https://ssrn.com/abstract=3713134> Acesso em: 02.01.21

ocorre porque, se uma definição puramente contextual de dados sensíveis fosse aplicada, coleções de fotografias de indivíduos identificáveis poderiam ser potencialmente consideradas dados biométricos, mesmo quando o controlador não tivesse a intenção de aplicar processos biométricos a elas. Diante disso, a inserção do termo "para o propósito de unicamente identificar uma pessoa natural", em relação aos dados biométricos, significa que eles só serão sensíveis quando houver uma intenção clara de aplicar processos biométricos a imagens ou a outro material que possa ser potencialmente usado para identificar indivíduos. Acerca da exceção em comento, vale ressaltar que, no Brasil, a LGPD não adotou tal noção para os dados biométricos, conforme será analisado em pormenor em item na presente tese.

Diante do avanço do uso de reconhecimento facial[168] para algumas atividades públicas e privadas, sem dúvida, mostra-se necessário discutir, com maior profundidade, o uso de dados biométricos, bem como se a imagem de uma pessoa natural pode ser considerada um dado pessoal sensível. Conforme dispõe o considerando 51 do *General Data Protection Regulation*, o tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que elas serão apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular. Em adição ao considerando, mostra-se necessário observar, também, no caso concreto, o contexto, os dados revelados pela imagem e a finalidade de seu tratamento.[169]

Além de questões biométricas, considerando-se que uma imagem pode revelar, em alguns casos, informações pessoais sobre origem étnica ou racial, saúde e orientação

---

[168] TEFFÉ, Chiara Spadaccini de; FERNANDES, Elora. Tratamento de dados sensíveis por tecnologias de reconhecimento facial: proteção e limites. In: Gustavo Tepedino, Rodrigo da Guia Silva. (Org.). *O Direito Civil na Era da Inteligência Artificial.* 1ed.São Paulo: Editora do Tribunais, 2020, v. 1, p. 283-310.

[169] De acordo com o *Explanatory Report* da Convenção 108, em texto modernizado: "59. The context of the processing of images is relevant to the determination of the sensitive nature of the data. The processing of images will not generally involve processing of sensitive data as the images will only be covered by the definition of biometric data when being processed through a specific technical mean which permits the unique identification or authentication of an individual. Furthermore, where processing of images is intended to reveal racial, ethnic or health information (see the following point), such processing will be considered as processing of sensitive data. On the contrary, images processed by a video surveillance system solely for security reasons in a shopping area will not generally be considered as processing of sensitive data."

sexual[170], além de questões religiosas de determinada pessoa natural, é possível defender seu enquadramento, em determinados contextos e diante de certos usos, como um dado pessoal sensível. Se a finalidade do processamento da imagem (e demais dados adicionados) relacionar-se com a obtenção de informações sensíveis, isso acarretará a aplicação das normas especiais relacionadas. [171] Nesse sentido, doutrina já afirmou que:

> For example, photographs or paintings may indicate an individual's race (i.e. based on the colour of their skin) or religion (e.g. if they are wearing religious garb), but subjecting all images of individuals in photographs and artistic representations to Article 9 would seem overly broad, and could conflict with other rights. Recital 51 GDPR therefore suggests that photographs are to be considered sensitive data only when they fall under the definition of biometric data. The EDPB has stated that 'video footage showing a data subject wearing glasses or using a wheelchair are not per se considered to be special categories of personal data'. However, if video footage is processed to deduce sensitive data from it, then Article 9 would apply. The EDPB gives the following examples: 'Political opinions could for example be deduced from images showing identifiable data subjects taking part in an event, engaging in a strike, etc. This would fall under Article 9', and 'a hospital installing a video camera in order to monitor a patient's health condition would be considered as processing of special categories of personal data (Article 9)'.[172]

Vale ressaltar, porém, que na Europa vem sendo firmado entendimento de que imagens processadas por sistemas de vigilância por vídeo, sem reconhecimento facial, apenas para segurança em área comercial, geralmente não serão consideradas como dentro de um tratamento de dados sensíveis. Nos últimos anos, as autoridades nacionais de proteção de dados europeias e o *European Data Protection Board* (Comitê Europeu para a Proteção de Dados) vêm estabelecendo diversos parâmetros para o tratamento de dados pessoais por meio de dispositivos de vídeo. Dessa forma, antes de operar um

---

[170] WANG, Y.; KOSINSKI, M. Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. Disponível em: <psyarxiv.com/hv28a> Acesso: 02.11.20.

[171] "59. The context of the processing of images is relevant to the determination of the sensitive nature of the data. The processing of images will not generally involve processing of sensitive data as the images will only be covered by the definition of biometric data when being processed through a specific technical mean which permits the unique identification or authentication of an individual. Furthermore, where processing of images is intended to reveal racial, ethnic or health information (see the following point), such processing will be considered as processing of sensitive data. On the contrary, images processed by a video surveillance system solely for security reasons in a shopping area will not generally be considered as processing of sensitive data." (Relatório Explicativo ao Protocolo que altera a Convenção para a Proteção das Pessoas no que diz respeito ao Tratamento Automático de Dados Pessoais publicado em 2018. Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223> Acesso em: 31.12.20.)

[172] GEORGIEVA, Ludmila; KUNER, Christopher. Article 9 Processing of special categories of personal data In: KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher. *The EU General Data Protection Regulation (GDPR): A Commentary.* 1.ed. Oxford University Press: 2020. p. 374.

sistema de câmera, o controlador deverá avaliar onde e se as medidas de vigilância por vídeo são estritamente necessárias. Em geral, como princípio, sempre que instalar tal sistema, ele deverá considerar cuidadosamente o princípio da minimização de dados e aspectos relacionados à segurança da informação, sob pena de severas sanções. Assim, mesmo nos casos em que o artigo 9º, nº 1, não se aplicar, o responsável pelo tratamento dos dados deverá minimizar o risco de captura de imagens que revelem outros dados sensíveis (para além do artigo 9º).[173] No Brasil, esse entendimento parece ter sido bem aceito nas adequações à LGPD, visto que dialoga com o sistema desenvolvido na norma. [174]

No presente cenário, verifica-se que tanto instituições quanto estudiosos da temática dos dados pessoais sensíveis vêm levantando três importantes questões: (a) diante do avanço tecnológico e do contexto de hiperconectividade, mais e mais dados vêm sendo compreendidos como pessoais, ou seja, vinculados direta ou indiretamente a indivíduos identificados ou identificáveis[175]; (b) há cada vez mais formas de análises que podem identificar indivíduos e revelar dados sensíveis sobre eles; e (c) não obstante a proximidade entre os textos legais do GDPR e da LGPD, há pontos específicos de diferença entre as normas, bem como legislação setorial diversa, não sendo possível importar sempre e diretamente interpretações europeias para o cenário brasileiro. Assim, ainda que o estudo da norma europeia seja fundamental e represente base inicial para se analisar a LGPD, mostra-se essencial o desenvolvimento de documentos institucionais e de doutrina que expressem e interpretem amplamente o contexto brasileiro de proteção de dados.

---

[173] EDPB. Guidelines 3/2019 on processing of personal data through video devices - version adopted after public consultation. Versão 2.0. Adotada em 29 de janeiro de 2020. Disponível em: <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en> Acesso em: 20.01.21. "Video surveillance systems usually collect massive amounts of personal data which may reveal data of a highly personal nature and even special categories of data. Indeed, apparently non-significant data originally collected through video can be used to infer other information to achieve a different purpose (e.g. to map an individual's habits). However, video surveillance is not always considered to be processing of special categories of personal data." (p.17)

[174] ANDRADE, Vander Ferreira de. Limites e cautelas no uso de imagens gravadas por câmeras de condomínio e a responsabilidade correlata do síndico. Migalhas, publicado em 04 de setembro de 2020. Disponível em: <https://migalhas.uol.com.br/depeso/332871/limites-e-cautelas-no-uso-de-imagens-gravadas-por-cameras-de-condominio-e-a-responsabilidade-correlata-do-sindico> Acesso em: 20.01.21

[175] Cf. Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data.

1.3 Dados altamente sensíveis: uma possibilidade a se discutir

Dados sensíveis podem alcançar diferentes níveis de sensibilidade, a depender da espécie de dado em questão, da informação em si que guardam e/ou do titular a quem dizem respeito, impactando em graus de intensidade diversos a esfera de seu titular. Quanto mais sensíveis forem as informações pessoais, maiores serão os riscos e danos, se houver um tratamento discriminatório ou incidente de segurança. Por tal razão, garantias específicas jurídicas e técnicas deverão ser implementadas e constantemente analisadas em programas de privacidade, compliance e governança.

Indaga-se, inclusive, se não seria mais adequado, e inclusive necessário, desenvolver categorias especiais de dados e, consequentemente, tutelas diferenciadas para eles, havendo níveis de segurança e garantia ampliados. Nesse sentido, mostra-se possível defender a existência de dados pessoais altamente sensíveis. Dentro da referida categoria, duas possibilidades de tratamento de dados podem ser destacadas: a) dados sensíveis relacionados a determinadas informações de saúde, genéticas ou biométricas; e b) determinados dados sensíveis de pessoas hipervulneráveis ou de vulnerabilidade agravada.

No primeiro caso, é possível pensar na seguinte situação: as informações de contato profissional de uma pessoa são dados pessoais, mas é pouco provável que ela sofra danos se tais informações forem disponibilizadas publicamente. Da mesma forma, informações sobre alguém ter quebrado uma perna ou sobre a cor de pele branca de um indivíduo, se expostas, dificilmente causarão um dano grave a ele ou alguma forma de discriminação prejudicial. Por outro lado, se informações específicas de saúde de um indivíduo, como, por exemplo, ser portador do vírus da imunodeficiência humana (HIV)[176], detalhes sobre sua saúde mental ou determinados dados genéticos, forem

[176] Diante do cenário de elevada discriminação que os portadores do vírus da imunodeficiência humana (HIV) e doentes de aids sofrem, em razão, muitas vezes, da falta de conhecimento acerca dos avanços científicos no tratamento da doença e acerca das formas de contágio, o legislador entendeu necessário tipificar como crime, por meio da Lei nº 12.984/2014, as seguintes condutas discriminatórias contra o portador do HIV e o doente de aids, em razão da sua condição de portador ou de doente: I - recusar, procrastinar, cancelar ou segregar a inscrição ou impedir que permaneça como aluno em creche ou estabelecimento de ensino de qualquer curso ou grau, público ou privado; II - negar emprego ou trabalho; III - exonerar ou demitir de seu cargo ou emprego; IV - segregar no ambiente de trabalho ou escolar; V - divulgar a condição do portador do HIV ou de doente de aids, com intuito de ofender-lhe a dignidade; e VI - recusar ou retardar atendimento de saúde. Ainda antes, o Ministro do Trabalho e Emprego, por meio da Portaria MTE n.º 1.246/2010, passou a orientar as empresas e os trabalhadores em relação à submissão

acessadas indevidamente por terceiros, isso poderá causar um alto risco de lesão a ele[177] e, até mesmo, a terceiros. Em decorrência dos avanços científicos, vem sendo debatida a chamada discriminação genética. Nesse caso, é possível a partir de exames e testes genéticos preditivos antecipar a tendência de certas pessoas para o desenvolvimento de algumas doenças e condições, podendo tais dados serem usados, por exemplo, como óbice a uma vaga de emprego ou posição.

---

destes ao teste da imunodeficiência adquirida – HIV, no sentido de proibir, de forma direta ou indireta, nos exames médicos por ocasião da admissão, mudança de função, avaliação periódica, retorno, demissão ou outros ligados à relação de emprego, a testagem do trabalhador quanto ao HIV. Em suma, o poder diretivo do empregador, que lhe proporciona buscar profissionais capacitados no mercado, de acordo com as exigências do cargo, em momento algum pode ter cunho discriminatório, sob pena de responsabilização civil e penal. Em âmbito trabalhista, já se verifica proteção especial conferida às pessoas portadoras do vírus HIV, como na Súmula 443 do TST: "Presume-se discriminatória a despedida de empregado portador do vírus HIV ou de outra doença grave que suscite estigma ou preconceito. Inválido o ato, o empregado tem direito à reintegração no emprego." Adicionalmente, doutrina destaca que: "(...) na fase pré-contratual e por aplicação analógica da Lei 9.029/95, é ofensora da intimidade e dignidade do trabalhador e por consequência ao princípio da igualdade, a exigência de teste de HIV para fins de comprovação da AIDS, sendo possível quando requisito para o exercício da função, como médico, enfermeiro, laborista etc." (ALVARENGA, Rúbia Zanotelli de. Os direitos do trabalhador portador do HIV. *Revista Eletrônica Tribunal Regional do Trabalho do Paraná*. Curitiba, v. 3, n.27, p. 9-23, jan./fev. 2014. p. 12-13) Feitas essas considerações, cabe lembrar recente caso julgado pelo Tribunal Superior do Trabalho (TST). A Segunda Turma do TST condenou a Pullmantur S.A., operadora de navios de cruzeiro, a pagar R$ 10 mil de compensação a uma camareira de São Bento do Sul submetida à realização de teste de HIV para poder ser admitida. A exigência como requisito para admissão no emprego constituiu, segundo o colegiado, conduta discriminatória e violou a intimidade e a privacidade da trabalhadora. Na reclamação, a empregada disse que a empresa havia exigido a apresentação de exame de HIV, teste antidrogas e certidão de antecedentes criminais. Por sua vez, a empresa argumentou que, em razão das particularidades do trabalho, a identificação de um tripulante portador de HIV era necessária, visto que suas condições de saúde seriam "especiais". A Min. Relatora do caso entendeu que: "(...) não há razão para a submissão dos trabalhadores a testes de HIV, considerando o avanço da medicina quanto ao controle dos sintomas da referida moléstia. Registre-se que os navios de cruzeiro dispõem de serviços de assistência médica a bordo, com profissionais qualificados e equipamentos hospitalares básicos, o que possibilita o pronto atendimento de trabalhadores e passageiros, em caso de problemas de saúde. (...) resta caracterizado o dano moral, pois a exigência de teste de HIV como requisito para admissão no emprego constitui conduta discriminatória vedada pela ordem jurídica (Lei 9.029/95, art. 1º) que viola a intimidade e a privacidade do trabalhador." (Processo nº TST-RR-248-91.2016.5.09.0013. 2ª Turma. Rel. Min. Maria Helena Mallmann. Acórdão publicado em 12 de março de 2021.)

[177] APELAÇÕES CÍVEIS. DANOS MORAIS. DANOS MATERIAIS. DIVULGAÇÃO DE PRONTUÁRIO MÉDICO. HIV. **Dados médicos do autor disponibilizados ao público no site da prefeitura mediante a simples inserção de seu CPF e sua data de nascimento, informações essas de fácil acesso. Ausência de senha de acesso que torna a informação, na prática, pública. O vazamento do prontuário médico do requerente (fls. 31/35), ao indicar ser ele portador do vírus do HIV, gerou situação embaraçosa e degradante no ambiente de trabalho.** A responsabilidade civil objetiva exige apenas a ocorrência do dano, a existência de nexo causal entre a conduta e este dano e a ausência de culpa excludente da vítima (art. 37, § 6º CF). O sigilo dos dados pessoais ganha contornos cada vez mais sensíveis, sendo matéria cada dia mais regulada na seara legislativa. Eventuais vazamentos de dados particulares são evidentes fatos geradores de danos, seja de ordem moral ou material, e o legislador tende a protegê-los, especialmente quando digam respeito aos direitos de personalidade. Art. 5º, X, Constituição Federal, art. 42 da Lei nº 13.709/2018 (LGPD) e art. 4º da Lei 13.787/2018. Danos morais configurados. Quantum indenizatório majorado. Danos materiais não configurados. Ausência de prova de nexo de causalidade entre a exposição dos dados médicos e a efetiva demissão do autor." (grifou-se) (TJSP. Apelação Cível nº 1016844-03.2020.8.26.0068. Rel. Heloísa Martins Mimessi. Julgado em: 5 de julho de 2021)

Acerca do segundo caso destacado, que versa sobre o tratamento de determinados dados sensíveis de pessoas hipervulneráveis, salienta-se que a proteção especial se fundamenta na junção que envolve conteúdos altamente sensíveis em titulares de dados que apresentam vulnerabilidade agravada[178], como crianças, adolescentes, idosos e pessoas com deficiência.[179] Exemplos significativos disso seriam tratamentos de dados biométricos de crianças e de dados de saúde de menores de idade com deficiência. Na seara do Direito do Consumidor, os referidos sujeitos costumam ser compreendidos como hipervulneráveis[180] ou sujeitos de vulnerabilidade agravada. Entende-se que certas qualidades pessoais do consumidor podem dar causa a uma soma de fatores de reconhecimento de vulnerabilidade, razão pela qual se poderia falar em situação de vulnerabilidade agravada.[181] Essa intensificação da suscetibilidade ao dano pode provir de distintas fontes, como questões etárias e falta de discernimento completo para certos atos, em razão da pouca idade[182], doenças específicas ou deficiências graves.

---

[178] MIRAGEM, Bruno. *Curso de Direito do Consumidor.* 3ed. São Paulo: RT, 2012, p.102.

[179] MARQUES, Cláudia Lima. O diálogo das fontes como método da nova teoria geral do direito: um tributo a Erik Jayme. In.: _____ (coord.) *Diálogo das fontes:* do conflito à coordenação de normas no direito brasileiro novo regime das relações contratuais. São Paulo: RT, 2012, p.17-66, p. 48.

[180] A construção da noção de hipervulnerabilidade pelos Tribunais parece estar associada à ideia de que as pessoas assim qualificadas se encontram em situação de maior desigualdade e, por essa razão, carentes de maior proteção. Nesse sentido, Cláudia Lima Marques explica que a noção foi desenvolvida "como um corolário positivo da proibição de discriminação, logo do princípio da igualdade (um dever ser), e mandamento de pleno desenvolvimento da personalidade, diretamente ligada, pois, a nossa visão de dignidade da pessoa humana." (MARQUES, Cláudia Lima. O diálogo das fontes como método da nova teoria geral do direito: um tributo a Erik Jayme. In.: _____ (coord.). *Diálogo das fontes:* do conflito à coordenação de normas no direito brasileiro novo regime das relações contratuais. São Paulo: RT, 2012, p.17-66, p. 46-47.) "Quanto à pergunta sobre se os hipervulneráveis são apenas os mencionados no texto constitucional (crianças, adolescentes, idosos e portadores de deficiência), parece-me cedo para responder de forma definitiva. A diferença está em que os hipervulneráveis mencionados nas normas constitucionais se beneficiam do mandamento de proteção constitucional (com efeitos e força normativa no direito privado), enquanto, por exemplo, os doentes e analfabetos são hipervulneráveis cuja proteção especial dependerá da atuação ativa do Judiciário e das especificidades do caso concreto (por exemplo, conhecimento pelo parceiro contratual de sua condição agravada de vulnerabilidade, tipo de contrato, onerosidade ou gratuidade deste, etc.)." (MARQUES, Cláudia Lima. O diálogo das fontes como método da nova teoria geral do direito: um tributo a Erik Jayme. In.: _____ (coord.) *Diálogo das fontes*: do conflito à coordenação de normas no direito brasileiro novo regime das relações contratuais. São Paulo: RT, 2012, p.17-66, p. 48.)

[181] MARQUES, Claudia Lima; MIRAGEM, Bruno. *O novo direito privado e a proteção dos vulneráveis.* 2. ed. São Paulo: Revista dos Tribunais, 2014.

[182] "(...) a hipervulnerabilidade pode estar presente tanto na criança e no adolescente, que são seres em formação física e intelectual, quanto no idoso, que pode ter déficit quanto a novas tecnologias ou mesmo pode ser mais suscetível de ser influenciado quanto a promessas de resultados que não podem ser alcançados ou cuja eficácia seja distorcida ou exacerbada". (PASQUALOTTO, Adalberto; SOARES, Flaviana. Consumidor hipervulnerável: análise crítica, substrato axiológico, contornos e abrangência. *Revista de Direito do Consumidor*, vol. 113, p. 81-109, Set.-Out./2017.)

Havendo hipervulnerabilidade do consumidor na relação, é possível exigir do fornecedor maior cuidado na formação do vínculo e na sua execução. O sistema jurídico deve oferecer proteção diferenciada ao hipervulnerável, inclusive no que concerne à tutela de seus dados pessoais. Contudo, ao se reconhecer a vulnerabilidade ou hipervulnerabilidade da pessoa não se está reduzindo a sua capacidade e autonomia. Há uma salutar tendência no Direito, hoje, em empoderar e ampliar direitos de grupos e minorias que, por vezes, são discriminados, conforme ocorreu com o Estatuto da Pessoa com Deficiência (Lei nº 13.146/15), o qual tem como pilares assegurar a liberdade e a igualdade material dessas pessoas. Caminha, assim, o Direito buscando harmonizar, de um lado, o respeito à capacidade e autodeterminação das pessoas e, de outro, a necessária proteção jurídica que deve ser conferida a determinados grupos, para que gozem plenamente de seus direitos fundamentais. Longe de uma ótica paternalista, busca-se garantir efetividade e aplicação direta das nomas constitucionais.[183]

Ainda que outros grupos também possam ser reconhecidos como de maior vulnerabilidade, dentro da presente tese buscou-se desenvolver uma proteção especial para os menores de idade, idosos e pessoas com deficiência, diante das previsões estabelecidas na Constituição Federal e em leis especiais, bem como das dinâmicas de poder e assimetrias informacionais constituídas na sociedade.

Todas as ações direcionadas a crianças e adolescentes devem necessariamente visar ao seu melhor interesse, como, por exemplo, no fornecimento, regulamentação, design, gestão e uso do ambiente digital. O reconhecimento e a tutela de sua hipervulnerabilidade podem ser inferidos do artigo 227 da Constituição Federal, o qual dispõe acerca do princípio da prioridade absoluta aos direitos da criança e do adolescente.[184] A construção da doutrina da proteção integral e prioritária das crianças e dos adolescentes, segundo a qual tais pessoas em desenvolvimento devem receber total

[183] "10. Configura dano moral coletivo ofensa a direitos coletivos ou difusos de caráter extrapatrimonial associados a *sujeitos ou bens vulneráveis e hipervulneráveis - pessoas com deficiência, consumidor, criança e adolescente, idoso, meio ambiente, ordem urbanística*, entre outros. Impossível, nesse campo, preconizar ou antecipar catálogo de infrações capazes de disparar tal resposta jurídica, bastando realçar o cuidado que se deve ter para não banalizar mecanismo tão medular na proteção de direitos, valores e bens preciosos da sociedade contemporânea." (REsp 1793332/MG, Rel. Ministro HERMAN BENJAMIN, SEGUNDA TURMA, julgado em 05/09/2019, DJe 26/08/2020) (grifo nosso)

[184] Art. 227. É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão.

amparo e proteção do sistema jurídico[185], remonta à Declaração dos Direitos da Criança adotada pela Assembleia-Geral das Nações Unidas no ano de 1959.[186]

Posteriormente, em 1989, por meio da Convenção das Nações Unidas sobre os Direitos da Criança[187], houve a ampliação dos direitos da criança no cenário internacional. Este documento considerou como criança todo ser humano com menos de 18 anos de idade, salvo quando, em conformidade com a lei aplicável à criança, a maioridade seja alcançada antes. A referida Convenção foi ratificada pelo Brasil em 1990 e influenciou diretamente a elaboração do Estatuto da Criança e do Adolescente (Lei 8.069/90 - ECA), que em seus artigos 3º e 4º destaca que todas[188] as crianças (pessoa até doze anos de idade incompletos) e adolescentes (aquela entre doze e dezoito anos de idade incompletos) gozam dos direitos fundamentais inerentes à pessoa humana, sem prejuízo da proteção integral de que trata esta Lei, sendo assegurados a eles todas as oportunidades e facilidades, a fim de lhes facultar o desenvolvimento físico, mental, moral, espiritual e social, em condições de liberdade e de dignidade.

A tutela diferenciada das crianças e adolescentes em qualquer relação na qual participem justifica-se exatamente por lhes faltar o completo discernimento, radicando nesse ponto a *ratio* protetiva. Aqui, o melhor interesse e o dever de cuidado impõem grau de zelo maior com seus dados pessoais, especialmente quando sensíveis. Contudo, deve-se ressaltar que não se trata apenas de uma proteção adequada ao estágio de desenvolvimento em que crianças e adolescentes se encontram, mas de uma proteção prospectiva, a fim de garantir a dignidade deles hoje e no futuro.[189]

---

[185] STJ. REsp 1.587.477. Quarta Turma. Rel. Min. Luis Felipe Salomão, DJe 27/08/2020.

[186] Princípio II - A criança gozará de proteção especial e disporá de oportunidade e serviços, a serem estabelecidos em lei por outros meios, de modo que possa desenvolver-se física, mental, moral, espiritual e socialmente de forma saudável e normal, assim como em condições de liberdade e dignidade. Ao promulgar leis com este fim, a consideração fundamental a que se atenderá será o interesse superior da criança. (Declaração dos Direitos da Criança, 1959).

[187] Disponível em: <https://www.unicef.org/brazil/convencao-sobre-os-direitos-da-crianca> Acesso em: 05.06.21.

[188] Art. 3°, parágrafo único: "Os direitos enunciados nesta Lei aplicam-se a todas as crianças e adolescentes, sem discriminação de nascimento, situação familiar, idade, sexo, raça, etnia ou cor, religião ou crença, deficiência, condição pessoal de desenvolvimento e aprendizagem, condição econômica, ambiente social, região e local de moradia ou outra condição que diferencie as pessoas, as famílias ou a comunidade em que vivem."

[189] Pietro Perlingieri apresenta a definição de igual dignidade social em duas perspectivas convergentes: "como o instrumento que confere a cada um o direito ao respeito inerente à qualidade de homem, assim como a pretensão de ser colocado em condições idôneas a exercer as próprias aptidões pessoais." (PERLINGIERI, Pietro. *Perfis do direito civil*: introdução ao direito civil-constitucional. Rio de Janeiro: Renovar, 1997, p.37.)

Temos, nos últimos tempos, a geração mais observada de toda a história. Cada vez mais, o rastro digital de menores vem sendo iniciado mais cedo e de forma ampliada, seja por meio de aplicativos para serem usados pelas mães durante a gestação, seja por meio de postagens realizadas pelos próprios pais ou pelos menores em mídias sociais. Diante desse quadro, a LGPD protege de forma clara e específica crianças e adolescentes, em seu Art.14, conforme será analisado no capítulo 3 da presente tese.

Aplicar uma proteção ainda maior a dados sensíveis de crianças e adolescentes requer uma série de instrumentos, recursos e boas práticas, sendo fundamental a implantação de programas de compliance[190] comprometidos com as questões acima. Contar com a atuação das instituições públicas no tema também é de suma importância, havendo tanto a aplicação de severas sanções, por descumprimento das normas de proteção de dados, quanto a adequada orientação dos agentes por meio da publicação de guias e instruções.

Neste sentido, a Autoridade irlandesa de proteção de dados publicou, até março de 2021, um *draft* para consulta pública intitulado *Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing*. Os Fundamentos estabelecem 14 princípios-chave que as organizações devem seguir ao tratar dados de crianças (na Irlanda, para fins de proteção de dados, uma criança é alguém com menos de 18 anos.). Isso inclui serviços direcionados / destinados ou que provavelmente serão acessados por crianças.[191] Meses antes, a Autoridade do Reino Unido (*Information Commissioner's Office* - ICO) publicou o relevante *Age appropriate design*: *a code of practice for online services*, devendo as organizações estarem em conformidade com ele até setembro de 2021.[192]

A respeito do idoso, vale lembrar que a idade avançada pode trazer consigo a diminuição ou mesmo a perda de determinadas aptidões físicas e/ou intelectuais, o que torna o indivíduo mais suscetível a práticas abusivas e, até mesmo, a fraudes. Como já

---

[190] TEFFÉ, Chiara Spadaccini de. LGPD em programas de compliance: vantagem competitiva e aderência às práticas ESG. Jota, publicado em 10 de junho de 2021. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/lgpd-em-programas-de-compliance-vantagem-competitiva-e-aderencia-as-praticas-esg-10062021> Acesso em: 11.06.21 OLIVA, Milena. GUIA, R. Notas sobre o compliance no direito brasileiro. *Revista quaestio iuris*, v. 11, p. 2708-2729, 2018.

[191] Fonte: <https://www.dataprotection.ie/en/dpc-guidance/blogs/the-children-fundamentals> Acesso em: 06.06.21.

[192] Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/executive-summary/> Acesso em: 06.06.21

se afirmou, em se tratando de idoso, sua proteção há de ser feita sob as luzes do Art. 230 da Constituição Federal[193], do Estatuto do Idoso (Lei nº 10.741/03) e sempre considerando a sua peculiar situação de consumidor hipervulnerável.[194] Recorda-se, inclusive, que dentre os idosos é assegurada prioridade especial aos maiores de oitenta anos, atendendo-se suas necessidades sempre preferencialmente em relação aos demais idosos (Art. 3º, § 2º, do Estatuto do Idoso). Na LGPD, em seu artigo 55-J, inciso XIX, há atenção destacada à condição do idoso, competindo à ANPD garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e do Estatuto do Idoso.

Uma crítica bastante relevante acerca da tutela especial conferida aos idosos (pessoas com idade igual ou superior a 60 anos) é o fato de ela considerá-los como uma "classe" geral e sempre necessitada de uma tutela preferencial. Nos últimos anos, as pessoas idosas cada vez mais vêm se mostrando atuantes no mercado de trabalho e saudáveis. Ainda que possam existir algumas limitações psicofísicas, em alguns casos, isso vem sendo relativizado pelo uso de insumos diversos. Como destaca Perlingieri, o decurso do tempo não influencia, automaticamente, em sentido negativo a capacidade natural normal de uma pessoa, de forma que se faz necessário rever soluções legislativas que, presumindo a decadência da pessoa em razão da idade, tiveram a pretensão de parecer normas construídas no interesse dos idosos.[195] Afirma: "Deve-se verificar a real capacidade de efetuar e de realizar as escolhas e os comportamentos correlatos às situações subjetivas interessadas."[196] Para o autor, as limitações poderão ser entendidas e aplicadas quando, concretamente, faltarem aptidões intelectiva e volitiva na pessoa em questão.

Dentro dessa lógica, a Resolução CD/ANPD nº 2, de 27 de janeiro de 2022[197], afirma que não poderão se beneficiar do tratamento jurídico diferenciado previsto neste

[193] Art. 230. A família, a sociedade e o Estado têm o dever de amparar as pessoas idosas, assegurando sua participação na comunidade, defendendo sua dignidade e bem-estar e garantindo-lhes o direito à vida. § 1º Os programas de amparo aos idosos serão executados preferencialmente em seus lares. § 2º Aos maiores de sessenta e cinco anos é garantida a gratuidade dos transportes coletivos urbanos.
[194] STJ. REsp 1.871.326/RS, Rel. Ministra Nancy Andrighi. Terceira Turma. DJe 09/09/2020. REsp 1.680.686/RJ, Rel. Ministro Herman Benjamin. Segunda Turma. DJe 07/08/2020.
[195] PERLINGIERI, Pietro. *O direito civil na legalidade constitucional*. Rio de Janeiro: Renovar, 2008. p. 785-788.
[196] PERLINGIERI, Pietro. *O direito civil na legalidade constitucional*. Rio de Janeiro: Renovar, 2008. p. 785.
[197] Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte.

Regulamento os agentes de tratamento de pequeno porte que, dentre outras situações, realizarem tratamento de alto risco para os titulares. De acordo com seu Art. 4º, para fins deste regulamento, será considerado de alto risco o tratamento de dados pessoais que atender cumulativamente a pelo menos um critério geral e um critério específico, dentre os a seguir indicados:

> I - critérios gerais:
> a) tratamento de dados pessoais em larga escala; ou
> b) tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares;
> II - critérios específicos:
> a) uso de tecnologias emergentes ou inovadoras;
> b) vigilância ou controle de zonas acessíveis ao público;
> c) decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, inclusive aquelas destinadas a definir o perfil pessoal, profissional, de saúde, de consumo e de crédito ou os aspectos da personalidade do titular; ou
> *d) utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos.*
> § 1º O tratamento de dados pessoais em larga escala será caracterizado quando abranger número significativo de titulares, considerando-se, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica do tratamento realizado.
> § 2º O tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais será caracterizado, dentre outras situações, naquelas em que a atividade de tratamento puder impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade. (...) (grifou-se)

Houve, assim, um cuidado adicional imposto aos agentes de tratamento de pequeno porte[198] que tratam dados sensíveis e dados pessoais – de qualquer natureza – de crianças, adolescentes ou idosos, em razão (I) da natureza e conteúdo sensível das informações; e/ou (II) dos sujeitos envolvidos apresentarem maior vulnerabilidade e proteção constitucional robusta.

A Lei Brasileira de Inclusão da Pessoa com Deficiência (Estatuto da Pessoa com Deficiência - Lei nº 13.146, de 6 de julho de 2015) dispõe que se considera pessoa com deficiência aquela que tem impedimento de longo prazo de natureza física, mental,

[198] Art. 2º Para efeitos deste regulamento são adotadas as seguintes definições: I - agentes de tratamento de pequeno porte: microempresas, empresas de pequeno porte, *startups*, pessoas jurídicas de direito privado, inclusive sem fins lucrativos, nos termos da legislação vigente, bem como pessoas naturais e entes privados despersonalizados que realizam tratamento de dados pessoais, assumindo obrigações típicas de controlador ou de operador;

intelectual ou sensorial, o qual, em interação com uma ou mais barreiras, pode obstruir sua participação plena e efetiva na sociedade em igualdade de condições com as demais pessoas. Observa-se que a avaliação da deficiência, quando necessária, será biopsicossocial, realizada por equipe multiprofissional e interdisciplinar e considerará os impedimentos nas funções e nas estruturas do corpo, os fatores socioambientais, psicológicos e pessoais, a limitação no desempenho de atividades e a restrição de participação.

A tutela das pessoas com deficiência, hoje, no Brasil, tem como fonte também a Convenção Internacional sobre os Direitos das Pessoas com Deficiência.[199] Dentro de seu rol de princípios, o direito à acessibilidade recebe destaque em face do uso da internet e das novas ferramentas tecnológicas, devendo os Estados e agentes privados assegurarem o amplo acesso desses sujeitos à informação e à comunicação, inclusive por meio de sistemas e dispositivos. Todavia, na prática, percebe-se que diversas ferramentas não se encontram desenhadas para atender também pessoas com determinadas deficiências, o que acaba as excluindo de interações e meios tecnológicos ou tornando a participação delas precária. As pessoas com deficiência ainda enfrentam barreiras significativas no acesso às tecnologias da informação e comunicação. Essas barreiras são, por exemplo, a falta de audiodescrição e de textos descritivos de imagens, a indisponibilidade de legendas, o uso necessário de controles remotos para acessar dispositivos e a ausência de acionamento e controle por voz de sistemas.

Diante disso, cada vez mais, verifica-se a ampliação de demandas que solicitam modificações e acomodações em projetos de serviços tecnológicos e em dispositivos, que sejam capazes de promover maior acessibilidade. Adicionalmente, há também preocupação com os dados pessoais que vêm sendo tratados e com os perfis desenvolvidos, visto que a proteção de dados de integrantes de grupos vulneráveis já necessita ser, desde o início, mais elevada, sendo ampliada quando houver o tratamento

[199] A Convenção Internacional sobre os Direitos das Pessoas com Deficiência define, em seu artigo primeiro, o conceito de pessoas com deficiência, assim dispondo: "O propósito da presente Convenção é promover, proteger e assegurar o exercício pleno e equitativo de todos os direitos humanos e liberdades fundamentais por todas as pessoas com deficiência e promover o respeito pela sua dignidade inerente. Pessoas com deficiência são aquelas que têm impedimentos de longo prazo de natureza física, mental, intelectual ou sensorial, os quais, em interação com diversas barreiras, podem obstruir sua participação plena e efetiva na sociedade em igualdades de condições com as demais pessoas." A Convenção foi promulgada no Brasil em 2009, através do Decreto nº 6.949. Trata-se do primeiro tratado internacional de direitos humanos aprovado nos termos do artigo 5º, par. 3º, da Constituição Federal, sendo equivalente às emendas constitucionais.

de dados sensíveis. Nesse sentido, "(...) as pessoas com deficiência constituem grupo estigmatizado e inferiorizado socialmente que representa significativa parcela da população e que o Direito brasileiro somente em tempos mais recentes se voltou à sua tutela na medida de suas vulnerabilidades".[200]

Como apontado no início do capítulo, determinadas práticas negociais e estruturas tecnológicas vêm se mostrando bastante agressivas e pouco transparentes em sua aplicação. O controle e a vigilância empregados em nossos corpos e dados vêm sendo substancialmente ampliados, afetando de formas e intensidades distintas as pessoas, especialmente determinados grupos mais vulneráveis e historicamente discriminados. Ainda que a LGPD não ofereça dispositivos específicos direcionados aos referidos sujeitos, mas apenas a crianças e adolescentes, discutir e oferecer uma tutela destacada a sujeitos mais vulneráveis, ainda que em casos concretos específicos, parece uma interpretação adequada das normas jurídicas, que valoriza os corolários da dignidade da pessoa humana. Não se busca, aqui, tecer uma conclusão ou um rol fechado de situações em que os dados classificados como altamente sensíveis estarão presentes, mas, sim, colocar luzes na questão e nas potencialidades da categoria.

[200] BARBOZA, Heloisa Helena; PEREIRA, Paula Moura Francesconi de Lemos; ALMEIDA, Vitor. Proteção dos dados pessoais da pessoa com deficiência. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters: 2020.

2. ESPÉCIES DE DADOS SENSÍVEIS: UMA DEFINIÇÃO DINÂMICA E CONTEXTUAL

No presente capítulo, busca-se desenvolver contribuição acerca das diversas espécies de dados pessoais considerados sensíveis, analisando-se seus conceitos, conteúdos e quais informações tutelam. Em alguns casos, entender quais dados são, de fato, sensíveis pode ser uma atividade complexa e depender de questões bastante específicas acerca do tratamento e da finalidade dos agentes. Análise essa que se alinha com o primeiro tema abordado no capítulo: a natureza do rol de dados sensíveis, se exemplificativa ou taxativa. Definir tal ponto mostra-se essencial para a construção da presente tese e implica, em aspectos práticos, trabalhar em maior detalhe: gestão de riscos, bases legais aplicáveis para o tratamento de dados (lembrando-se que o Art. 11 da LGPD apresenta hipóteses mais restritas, conforme será estudado no capítulo 3), o desenvolvimento de relatórios de impacto e o incremento de mecanismos de proteção ampliada para dados sensíveis.

Em seguida, passa-se para a análise crítica das espécies de dados sensíveis positivadas no Art. 5º, II, da LGPD, quais sejam: dados pessoais sensíveis sobre origem étnica ou racial; dados pessoais sensíveis acerca de crenças e filiações; dados pessoais sensíveis corporais, que englobam dados genéticos, dados biométricos e dados referentes à saúde, havendo especial destaque para o tratamento dessas informações no cenário de pandemia de COVID-19; e dados referentes à vida sexual. Por fim, serão analisados dados potencialmente sensíveis, que não foram mencionados diretamente na LGPD como sensíveis, mas que por sua natureza e possibilidades de uso merecem especial atenção, como dados financeiros, dados sobre origem social e dados relativos a antecedentes e condenações criminais.

Portanto, no capítulo 2, visa-se a discutir três relevantes perguntas: o rol de dados sensíveis é exemplificativo ou exaustivo? Quais informações devem ser efetivamente tuteladas como sensíveis, a partir de uma leitura que afirme a metodologia civil-constitucional na interpretação e aplicação da Lei Geral de Proteção de Dados Pessoais? Além das espécies positivadas na LGPD como dados sensíveis, quais outros dados – mesmo que apenas em determinados contextos – devem assim ser tutelados e

por qual razão? Quando pertinente, serão realizadas referências ao GDPR e a normas nacionais setoriais.

2.1 O rol de dados sensíveis na LGPD: por uma tutela ampliada das informações pessoais

A LGPD em seu Art. 5º, inciso II, trouxe espécies de dados pessoais considerados sensíveis: "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural". Todavia, não esclareceu o que seriam dados sensíveis em termos conceituais ou se o rol de tais dados seria taxativo ou exemplificativo. Adicionalmente, conforme será enfrentado neste capítulo, trouxe termos, por vezes, pouco precisos ou extremamente abrangentes, como, por exemplo, "opinião política" ou "dado referente à saúde ou à vida sexual".

No Direito, quando se afirma que um rol é taxativo (exaustivo ou *numerus clausus*), isso significa dizer que a lista de situações ou direitos estabelecida é determinada e fechada, não dando margem a interpretações extensivas. Além da técnica legislativa empregada em cada caso, mostra-se relevante observar a natureza dos direitos envolvidos, se existenciais ou patrimoniais, e a relação da tutela oferecida com a promoção do princípio da dignidade da pessoa humana. Como exemplos de róis taxativos, vale mencionar: o Art. 1º da Lei nº 8.072/90 (Lei dos Crimes Hediondos) e o Art. 102, I, d, da Constituição Federal de 1988[201].

Por outro lado, o rol exemplificativo (*numerus apertus*) apresenta, de forma não exaustiva, itens de uma categoria ou lista.[202] Ele encontra-se aberto para que outros casos e direitos sejam ali inseridos. Como exemplos, é possível mencionar: os direitos

[201] Entende-se que a competência originária do Supremo Tribunal Federal, por se qualificar como um complexo de atribuições jurisdicionais de extração essencialmente constitucional – e ante o regime de direito estrito a que se acha submetida – não comportaria a possibilidade de ser estendida a situações que extravasem os rígidos limites fixados, em *numerus clausus*, pelo rol exaustivo inscrito na mencionada disposição legal. Posição consolidada no Supremo Tribunal Federal. Disponível em: <http://www.stf.jus.br/portal/jurisprudencia/menuSumarioSumulas.asp?sumula=2815> Acesso em: 02.04.21

[202] Por vezes, os róis exemplificativos trazem expressões como: "entre outros", "demais hipóteses previstas em lei", "em especial", "a lei poderá" etc.

da personalidade[203]; o Art. 7º da Lei nº 11.340/06 (Lei Maria da Penha, que estabelece as hipóteses de atos que configuram violência contra a mulher); e as cláusulas abusivas previstas no Art. 51 da Lei nº 8.078/90 (Código de Defesa do Consumidor).

Conforme analisado no capítulo 1, diante dos fundamentos da categoria dos dados sensíveis, da proteção de dados pessoais ser considerada um direito da personalidade e de sua natureza relacionada diretamente a aspectos existenciais da pessoa humana, entende-se que o rol de dados sensíveis na LGPD deve ser considerado exemplificativo[204], sendo tutelado de forma ampla e contextualizada. Na referida lei, não há qualquer previsão que estabeleça o rol do Art. 5º, II, como exaustivo. Ao

[203] Acerca dos direitos da personalidade, a concepção pluralista preconiza a existência de distintos direitos que se reuniriam em razão das características e elementos em comum. Defende-se que os direitos da personalidade constituem uma categoria composta por direitos autônomos e distintos, que gozam de uma regulamentação própria, e não um mero desdobramento de um direito geral. Para Gomes, a teoria dos direitos de personalidade apenas se liberta de imprecisões quando a sua construção se apoia no direito positivo e é reconhecido o pluralismo desses direitos, em virtude da diversidade dos bens jurídicos em que recaem. (GOMES, Orlando. Direitos da personalidade e responsabilidade civil. *Revista de direito comparado luso-brasileiro*. Rio de Janeiro, ano II, n. 2, 1983.) Dentro da concepção pluralista, salienta Perlingieri que há teorias que sustentam a existência de uma série aberta de direitos da personalidade (atipicidade) e outras que sustentam que o rol desses direitos deveria ser fechado (tipicidade), sendo tal contraposição essencialmente ligada a opções ideológicas e culturais. Para o autor, a lógica baseada na tipicidade exauriria a relevância de tais direitos no aspecto patrimonial do ressarcimento de danos e não levaria em conta que poderiam existir outros interesses da pessoa mais decisivos e qualificantes, ainda que não presentes no Código Civil, mas sim em alguma lei especial. (PERLINGIERI, Pietro. *O direito civil na legalidade constitucional*. Rio de Janeiro: Renovar, 2008. p. 762.) Analisando o artigo 2º da Constituição italiana, Perlingieri afirma que essa seria uma norma diretamente aplicável e que exprimiria um princípio fundamental de tutela da pessoa humana. O conteúdo dessa norma não se limitaria a resumir os direitos tipicamente previstos por outros dispositivos da Carta, mas permitiria estender a tutela às situações atípicas. (PERLINGIERI, Pietro. *O direito civil na legalidade constitucional*. Rio de Janeiro: Renovar, 2008. p. 763.) O autor conclui que a personalidade não seria um direito, mas sim um valor — o valor fundamental do ordenamento —, que estaria na base de "uma série aberta de situações subjetivas existenciais, nas quais se traduz a sua incessantemente mutável exigência de tutela." (PERLINGIERI, Pietro. *O direito civil na legalidade constitucional.* Rio de Janeiro: Renovar, 2008. p. 764.) Não haveria uma série fechada de situações tuteladas: tutelado seria o valor da pessoa, com exceção dos limites impostos em razão de seu interesse e de outras pessoas. De acordo com o autor, o juiz "não poderá negar tutela a quem pedir garantia de um aspecto de sua própria existência que não tenha previsão específica, pois aquele interesse já tem uma relevância no ordenamento, e, portanto, uma tutela também em via judicial." (PERLINGIERI, Pietro. *O direito civil na legalidade constitucional*. Rio de Janeiro: Renovar, 2008. p.765.) No Brasil, a concepção pluralista foi adotada pelo legislador e encontra ampla adesão na doutrina. Entende-se, assim, que o rol de direitos da personalidade não é taxativo, de forma que o intérprete não deve se restringir aos direitos positivados na Constituição Federal e no Código Civil, mas garantir as diversas manifestações existenciais da pessoa, uma vez que elas, a princípio, já gozariam de relevância no ordenamento. Dispõe o enunciado 274 do Conselho da Justiça Federal que: "Os direitos da personalidade, regulados de maneira não-exaustiva pelo Código Civil, são expressões da cláusula geral de tutela da pessoa humana, contida no art. 1º, III, da Constituição (princípio da dignidade da pessoa humana)." (TEFFÉ, Chiara Antonia Spadaccini de. *A tutela da imagem da pessoa humana na internet:* da identificação do dano à sua compensação. 2016. 226 f. Dissertação (Mestrado em Direito Civil) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2016. p. 22-23)

[204] KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Org.). *A Lei Geral de Proteção de Dados Pessoais e Suas Repercussões no Direito Brasileiro*. Revista dos Tribunais: São Paulo, 2019, p. 455.

contrário, a lei dispõe que se aplica o disposto no Art. 11 a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.[205]

Como direito da personalidade, a proteção de dados pessoais é essencial à pessoa humana, necessária, irrenunciável e inalienável. A elasticidade do rol de dados sensíveis representa instrumento para efetivar formas de proteção também atípicas, pautadas no interesse à existência e no livre exercício da vida de relações.[206] Uma previsão legal exaustiva de dados sensíveis deixaria de fora manifestações e exigências da pessoa que, em razão do progresso da sociedade, exigem uma proteção ampliada.

Nesse sentido, Caitlin Mulholland ressalta que a definição do Art. 5º, II, da LGPD, não é, de forma alguma, taxativa: "Trata-se de conceito que enumera de maneira exemplificativa algumas das hipóteses em que serão identificados os dados pessoais que tenham natureza considerada sensível".[207] Sergio Negri e Maria Regina Korkmaz dispõem que:

> O *standard* protetivo dos dados pessoais sensíveis na LGPD, como apresentado, é mais rigoroso, todavia, o artigo 5º, inciso II, da citada lei (BRASIL, 2018a) não exaure todas as situações nas quais a pessoa pode ser submetida a situações de discriminação e desigualdade, porque baseado em um modelo de *fattispecie*. Assim sendo, a isonomia restaria injustificadamente mitigada ao se negar esse regime jurídico específico de proteção a dados que em sua natureza ostentassem essa configuração, sem estar, contudo, taxativamente previsto naquele rol. Com essa perspectiva, a proteção integral da pessoa nas sociedades de informação, notadamente com relação aos dados sensíveis, perpassa por um conceito normativo amplo.[208]

---

[205] "Com o propósito de evitar lesões a direitos fundamentais da pessoa humana, o § 1º do art. 11 da LGPD dispõe que as regras relativas aos dados sensíveis devem ser aplicadas aos dados pessoais que, quando tratados, possam vir a revelar informações sensíveis de seu titular, tornando-o suscetível a danos. A característica comum a todos os dados sensíveis é a suscetibilidade de sua utilização para fins discriminatórios, de modo que, em decorrência dos efeitos potencialmente lesivos de seu tratamento, não é possível aceitar que exista um rol taxativo de dados sensíveis. A propósito, Stefano Rodotà explica que a formação de perfis com base em dados pessoais pode ensejar discriminação em diferentes situações: (i) há dados pessoais que, embora sejam aparentemente não sensíveis, podem, quando tratados, se tornar sensíveis, viabilizando, inclusive, a identificação da pessoa e dos seus hábitos, relacionamentos, preferências, convicções religiosas, políticas e filosóficas etc.; e (ii) quando o tratamento de dados identifica um grupo de pessoas ao qual são atribuídas conotações negativas. (RODRIGUES, Marco Antonio dos Santos; HIBNER, Davi Amaral. Parâmetros para a proteção de dados pessoais em tempos de pandemia. *Revista de Direito e as Novas Tecnologias*, vol. 8/2020, Jul - Set / 2020.)

[206] PERLINGIERI, Pietro. *O direito civil na legalidade constitucional*. Rio de Janeiro: Renovar, 2008. p. 764-765.

[207] MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. Migalhas, publicado em 22 de junho de 2020. Disponível em: <https://migalhas.uol.com.br/coluna/migalhas-de-vulnerabilidade/329261/dados-pessoais-sensiveis-e-consentimento-na-lei-geral-de-protecao-de-dados-pessoais> Acesso em: 02.11.20.

[208] NEGRI, Sergio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. A normatividade dos dados sensíveis na lei geral de proteção de dados: ampliação conceitual e proteção da

No mesmo sentido, Miragem e Petersen afirmam que:

> A esse conjunto de dados pessoais optou-se por conferir maior proteção, com a previsão de normas mais rigorosas para o seu tratamento, o que se justifica tanto por dizerem respeito a uma esfera de maior reserva do indivíduo como pelo caráter potencialmente discriminatório do seu uso. Nesse sentido, a disciplina dos dados sensíveis guarda íntima conexão com o princípio da não discriminação; mediante normas especiais busca-se coibir práticas discriminatórias abusivas. Ademais, é importante notar que o rol conceitual não é taxativo, sendo possível reconhecer a natureza sensível de outros dados cujo tratamento implique maiores riscos para o titular (art.11, §1º, da LGPD), de modo que dados ordinários podem se tornar sensíveis quando o seu uso der causa a uma situação potencialmente discriminatória.[209]

Na medida em que a criação da categoria de dados sensíveis justifica-se, entre outras razões, para proteger um tipo de informação que pode ocasionar práticas discriminatórias ilícitas ou abusivas, ela pode abranger, por exemplo, dentro de certos contextos e usos, dados sobre orientação sexual, dados relacionados a condições socioeconômicas de uma pessoa[210] e dados relativos a antecedentes e condenações criminais. O ordenamento dispõe de institutos que buscam assegurar ao indivíduo que, após cumprida a sua pena, ele se reabilite e seja ressocializado. Tais informações se tratadas indevidamente podem cristalizar o indivíduo na condição de condenado, impedindo que ele reinicie sua vida.[211] Diante disso, o GDPR positivou proteção específica, em seu Art. 10, para o tratamento de dados pessoais relacionados com condenações penais e infrações, o que não ocorreu expressamente na LGPD.

Inclusive, na Lei do Cadastro Positivo (Lei nº 12.414/11**)**, em seu Art. 3º, §3º, encontra-se disposto que ficam proibidas as anotações de informações sensíveis, "assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas." O termo "origem social" aparece na mencionada norma, mas não na LGPD. Contudo, isso não

---

pessoa humana. *Rev. de Direito, Governança e Novas Tecnologias*, Goiânia, v. 5, n. 1, p. 63-85, Jan/Jun. 2019.

[209] MIRAGEM, Bruno; PETERSEN, Luiza. O contrato de seguro e a lei geral de proteção de dados. *Revista dos Tribunais*, vol.1018, agosto de 2020.

[210] INTERNETLAB. *O que está em jogo no debate sobre dados pessoais no brasil?* Relatório final sobre o debate público promovido pelo ministério da justiça sobre o anteprojeto de lei de proteção de dados pessoais. Associação InternetLab de pesquisa em direito e tecnologia, 2016. p.56.

[211] NEGRI, Sergio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. A normatividade dos dados sensíveis na lei geral de proteção de dados: ampliação conceitual e proteção da pessoa humana. *Rev. de Direito, Governança e Novas Tecnologias*, Goiânia, v. 5, n. 1, p. 63-85, Jan/Jun. 2019.p.78.

impede que informações sobre a origem social de uma pessoa recebam proteção ampliada, visto que, claramente, de forma individual ou conjugada, podem ser usadas para fins discriminatórios.[212] Em acórdãos relatados pelo Ministro Paulo de Tarso Sanseverino, em 2014, que trataram dos limites da prática de *credit scoring* e da aplicação da lei do cadastro positivo, afirmou-se que:

> A vedação de utilização de dados sensíveis busca evitar a utilização discriminatória da informação, conforme claramente definido pelo legislador como aqueles "pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas." Desse modo, no sistema jurídico brasileiro, encontram-se devidamente regulados tanto o dever de respeito à privacidade do consumidor (v.g. informações excessivas e sensíveis), como o dever de transparência nessas relações com o mercado de consumo (v.g. deveres de clareza, objetividade e veracidade).[213]

O mesmo raciocínio pode ser aplicado, por exemplo, no caso de dados financeiros relacionados com despesas médicas. No Conselho Administrativo de Recursos Fiscais (Carf), há processos que envolvem dados sensíveis de saúde dos contribuintes e de seus dependentes. Ele julga, entre outros temas, casos sobre a dedução de gastos relacionados à saúde do Imposto de Renda da Pessoa Física.

Por outro lado, parte da doutrina entende que o rol de dados sensíveis estabelecido na LGPD deveria ser taxativo: "Em razão de sua especialidade e das diversas restrições impostas ao seu tratamento, é efetivamente recomendável que dados sensíveis sejam normalmente definidos de modo taxativo (...)."[214] Sem dúvida, os benefícios desse posicionamento são oferecer maior segurança jurídica para as partes e facilitar as atividades de tratamento, especialmente quando os agentes lidam com grandes volumes de dados sensíveis. Segundo o posicionamento acima, o Art. 5º, II, não traria conceito aberto com elementos exemplificativos, mas sim definição que apresentaria rol fechado de dados sensíveis.

---

[212] KNOP, M.; COLLARES, A. C. M. A influência da origem social na probabilidade de concluir os diferentes cursos de ensino superior. *Sociedade e Estado*, v. 34, n. 02, p. 351-380, 2019. Disponível em: https://periodicos.unb.br/index.php/sociedade/article/view. Acesso em: 2 abr. 2021. ALVES, Fátima; ORTIGÃO, Isabel. Origem social e risco de repetência: interação raça-capital econômico. *Cadernos de Pesquisa*, v. 37, n. 130, p. 161-180, jan./abr. 2007.

[213] REsp 1.419.697 – RS e Resp 1.457.199 – RS. Nesse sentido, a súmula 550 do STJ: "A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo."

[214] LEONARDI, Marcel. Principais bases legais de tratamento de dados pessoais no setor privado. *In*: SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (Coords.). *Lei geral de proteção de dados*. São Paulo: RT, 2019. p. 72.

Todavia, doutrina[215] aponta que não se exclui de tal posicionamento a possibilidade de dados pessoais não elencados no conceito da LGPD receberem tratamento equivalente ao de dados sensíveis, no que se refere às hipóteses de tratamento (que no Art. 11 são mais restritivas), quando, no caso concreto, tiverem a capacidade de revelar informações sensíveis, conforme o par. 1º, do Art. 11. Dados de geolocalização, fotos e hábitos de compra ou navegação não seriam, por si só, sensíveis: "Sensível é a inferência ou o dado que se extrai a partir de interpretação de tais elementos, que, a depender dos propósitos para os quais são tratados, até podem atrair comandos legais mais restritivos da LGPD, como o já mencionado Artigo 11, par. 1º, mas não são, logo de saída, dados sensíveis." [216]

Essas considerações mostram, portanto, que para se definir o caráter sensível de determinada informação deve-se também observar o contexto da atividade de tratamento e sua finalidade, além do uso efetivo da informação e seu potencial quando cruzada com demais dados, assim como se faz dentro da própria definição de "dado pessoal".

2.2 Estudo dos dados sensíveis elencados na LGPD

A partir dos dados caracterizados como sensíveis, pode-se, de forma didática, pensar em pelo menos quatro categorias: a) dados pessoais sensíveis sobre a origem racial ou étnica; b) dados pessoais sensíveis acerca de crenças e filiações: informações sobre convicções religiosas, opiniões políticas e filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político; c) dados pessoais sensíveis corporais: dados referentes à saúde, dados genéticos e dados biométricos; e d) dados pessoais sensíveis sobre a vida sexual.

Dados sobre origem e crenças e dados relacionados a questões sexuais são especiais diante de históricas perseguições, discriminações e preconceitos em face de pessoas de determinadas origens raciais ou étnicas, com certas crenças ou posições políticas ou, ainda, que tenham determinada orientação sexual. Os dados corporais, com

[215] PALHARES, Felipe; PRADO, Luis; VIDIGAL, Paulo. *Compliance digital e LGPD.* São Paulo: Thomson Reuters Brasil, 2021. p.119.
[216] PALHARES, Felipe; PRADO, Luis; VIDIGAL, Paulo. *Compliance digital e LGPD.* São Paulo: Thomson Reuters Brasil, 2021. p.120.

o avanço da ciência e da tecnologia, apresentam uma sensibilidade também elevada, sendo diversas as suas aplicações e tratamentos. Atualmente, por exemplo, eles são fundamentais para alimentar sistemas de Inteligência Artificial que irão colaborar com médicos em diagnósticos e em tratamentos de saúde, na solução de investigações e de crimes e na implantação de tecnologias de vigilância e controle. Vale lembrar que, com a hiperconectividade e a disseminação da Internet das Coisas, os *wearables* produzem[217], cada vez mais, informações desse tipo, que são automaticamente tratadas para variados fins.

Vale lembrar que, diante da expansão do metaverso, os *wearables* terão um papel ainda maior no tratamento de dados sensíveis, auxiliando no processo de integração dos espaços físico e virtual, na experiência de realidade proporcionada pelo ambiente e na própria construção de uma segunda vida digital. Os dispositivos vestíveis se manifestam em muitos formatos e se conectam ao corpo do usuário gerando novas interfaces humano-máquina[218]. Eles podem vir a ser utilizados para captar informações como reconhecimento de íris, impressões digitais, gostos e padrões de digitação e toque. É possível também que tais dispositivos permitam avaliações e o desenvolvimento de perfis comportamentais a partir de situações específicas, além de inferências sobre orientação sexual ou convicção religiosa, por exemplo. Assim, diante da alta tecnologia aplicada, determinados tratamentos de dados gerados a partir do metaverso podem, com relativa facilidade, serem classificados como sensíveis.

Diante disso, mostra-se relevante analisar cada um dos dados sensíveis positivados pelo legislador e quais informações eles guardam e asseguram efetivamente, de forma a melhor aplicar as proteções estabelecidas na lei para a categoria e realizar seu adequado tratamento. Uma vez exploradas as definições, os contornos e os fundamentos dos dados sensíveis, cabe compreender agora cada uma de suas espécies,

---

[217] Cf. TEFFÉ, Chiara Spadaccini de; MAGRANI, E.; STEIBEL, F. Juguetes conectados y tutela de la privacidad de niños y adolescentes: explorando beneficios y desafíos. In: Lionel Ricardo Brossi Garavaglia; Tomás Dodds Rojas; Ezequiel Passeron (Org.). *Inteligencia artificial y bienestar de las juventudes en América Latina*. Santiago: LOM ediciones, 2019, v. 1, p. 197-202. TEFFÉ, Chiara Spadaccini de. Proteção de dados pessoais na Rede: resenha à obra "A internet das coisas", de Eduardo Magrani. *Civilistica.com*. Rio de Janeiro, a. 7, n. 1, 2018. Disponível em: <http:// civilistica.com/protecao-de-dados-pessoais-na-rede/>. Data de acesso: 02.11.20

[218] MASTROCOLA, Vicente Martin. Comunicação, consumo e wearable technologies: um exercício de aplicação da teoria ator-rede no contexto de possíveis reconfigurações humano-tecnológicas. *Conexão – Comunicação e Cultura*, UCS, Caxias do Sul – v. 17, n. 34, jul./dez. 2018, p. 237-256.

visto que a LGPD não definiu as mesmas em seu texto, o que traz, por consequência, dúvidas acerca da abrangência da norma.

2.2.1 Dados pessoais sensíveis sobre origem étnica ou racial

Informações pessoais "sobre origem racial ou étnica" de pessoa natural são dados sensíveis. Contudo, o termo "origem racial" não deve implicar a aceitação de qualquer doutrina de superioridade racial[219] ou de teorias que tentem determinar a existência de distintas raças humanas.[220]

Nesse sentido, cabe recordar o Habeas Corpus nº 82.424, relatado pelo Min. Maurício Corrêa, conhecido como *Caso Ellwanger*. Em setembro de 2003, o Plenário do Supremo Tribunal Federal confirmou, por maioria de votos, a condenação de Siegfried Ellwanger, autor de livros de conteúdo antissemita, pelo crime de racismo. No caso, debateu-se o significado jurídico do termo *racismo*, disposto no Art. 5°, XLII, da Constituição.[221] De acordo com o Min. Maurício Corrêa: "Embora hoje não se reconheça mais, sob o prisma científico, qualquer subdivisão da raça humana, o racismo persiste enquanto fenômeno social, o que quer dizer que a existência das diversas raças decorre da mera concepção histórica, política e social e é ela que deve ser considerada na aplicação do direito". Essa também foi a conclusão do Min. Gilmar Mendes, que assim se pronunciou: "Parece ser pacífico hoje o entendimento segundo o qual a concepção a respeito da existência de raças assentava-se em reflexões pseudocientíficas

[219] No relatório da Conferência mundial contra o racismo, a discriminação racial, a xenofobia e a intolerância correlata, que ocorreu em Durban, em 2001, foi afirmado que: "7. Declaramos que todos os seres humanos nascem livres e iguais em dignidade e direitos e têm o potencial de contribuir construtivamente para o desenvolvimento e bem-estar de suas sociedades. Qualquer doutrina de superioridade racial é cientificamente falsa e, entre outras coisas, moralmente condenável, socialmente injusta e perigosa, devendo ser rejeitada, juntamente com as teorias que tentam determinar a existência de raças humanas distintas;"

[220] Igual consideração encontra-se estabelecida no *recital* 51 do GDPR, quando aborda a categoria dos dados sensíveis: "Deverão incluir-se neste caso os dados pessoais que revelem a origem racial ou étnica, não implicando o uso do termo «origem racial» no presente regulamento que a União aceite teorias que procuram determinar a existência de diferentes raças humanas." Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679> Acesso em: 30.03.21

[221] Constituição Federal - Art. 5º, XLII: a prática do racismo constitui crime inafiançável e imprescritível, sujeito à pena de reclusão, nos termos da lei.

(...).”[222] Raça e etnia são termos que, muitas vezes, são utilizados como sinônimos, mas que apresentam noções e âmbitos distintos.[223] Para alguns, o conceito de etnia entende que a identidade de um indivíduo seria composta por diversos fatores, como ancestralidade comum, religião, língua, território compartilhado, nacionalidade e aparência física. Estaria atrelado também à cultura e à origem do indivíduo. Já o termo raça apresenta uma variedade de definições, geralmente utilizadas para descrever um grupo de pessoas que compartilham certas características morfológicas, como, por

[222] HABEAS-CORPUS. PUBLICAÇÃO DE LIVROS: ANTI-SEMITISMO. RACISMO. CRIME IMPRESCRITÍVEL. CONCEITUAÇÃO. ABRANGÊNCIA CONSTITUCIONAL. LIBERDADE DE EXPRESSÃO. LIMITES. ORDEM DENEGADA. 1. Escrever, editar, divulgar e comerciar livros "fazendo apologia de idéias preconceituosas e discriminatórias" contra a comunidade judaica (Lei 7716/89, artigo 20, na redação dada pela Lei 8081/90) constitui crime de racismo sujeito às cláusulas de inafiançabilidade e imprescritibilidade (CF, artigo 5º, XLII). 2. Aplicação do princípio da prescritibilidade geral dos crimes: se os judeus não são uma raça, segue-se que contra eles não pode haver discriminação capaz de ensejar a exceção constitucional de imprescritibilidade. Inconsistência da premissa. 3. Raça humana. Subdivisão. Inexistência. Com a definição e o mapeamento do genoma humano, cientificamente não existem distinções entre os homens, seja pela segmentação da pele, formato dos olhos, altura, pelos ou por quaisquer outras características físicas, visto que todos se qualificam como espécie humana. Não há diferenças biológicas entre os seres humanos. Na essência são todos iguais. 4. Raça e racismo. A divisão dos seres humanos em raças resulta de um processo de conteúdo meramente político-social. Desse pressuposto origina-se o racismo que, por sua vez, gera a discriminação e o preconceito segregacionista. 5. Fundamento do núcleo do pensamento do nacional-socialismo de que os judeus e os arianos formam raças distintas. Os primeiros seriam raça inferior, nefasta e infecta, características suficientes para justificar a segregação e o extermínio: inconciabilidade com os padrões éticos e morais definidos na Carta Política do Brasil e do mundo contemporâneo, sob os quais se ergue e se harmoniza o estado democrático. Estigmas que por si só evidenciam crime de racismo. Concepção atentatória dos princípios nos quais se erige e se organiza a sociedade humana, baseada na respeitabilidade e dignidade do ser humano e de sua pacífica convivência no meio social. Condutas e evocações aéticas e imorais que implicam repulsiva ação estatal por se revestirem de densa intolerabilidade, de sorte a afrontar o ordenamento infraconstitucional e constitucional do País. 6. Adesão do Brasil a tratados e acordos multilaterais, que energicamente repudiam quaisquer discriminações raciais, aí compreendidas as distinções entre os homens por restrições ou preferências oriundas de raça, cor, credo, descendência ou origem nacional ou étnica, inspiradas na pretensa superioridade de um povo sobre outro, de que são exemplos a xenofobia, "negrofobia", "islamafobia" e o antissemitismo. 7. A Constituição Federal de 1988 impôs aos agentes de delitos dessa natureza, pela gravidade e repulsividade da ofensa, a cláusula de imprescritibilidade, para que fique, ad perpetuam rei memoriam, verberado o repúdio e a abjeção da sociedade nacional à sua prática. 8. Racismo. Abrangência. Compatibilização dos conceitos etimológicos, etnológicos, sociológicos, antropológicos ou biológicos, de modo a construir a definição jurídico-constitucional do termo. Interpretação teleológica e sistêmica da Constituição Federal, conjugando fatores e circunstâncias históricas, políticas e sociais que regeram sua formação e aplicação, a fim de obter-se o real sentido e alcance da norma. (...) O preceito fundamental de liberdade de expressão não consagra o "direito à incitação ao racismo", dado que um direito individual não pode constituir-se em salvaguarda de condutas ilícitas, como sucede com os delitos contra a honra. Prevalência dos princípios da dignidade da pessoa humana e da igualdade jurídica. (...) 16. A ausência de prescrição nos crimes de racismo justifica-se como alerta grave para as gerações de hoje e de amanhã, para que se impeça a reinstauração de velhos e ultrapassados conceitos que a consciência jurídica e histórica não mais admite. Ordem denegada. (HC 82424, Rel. Min. Moreira Alves, Relator p/ Acórdão: Maurício Corrêa, Tribunal Pleno, julgado em 17/09/2003, DJ 19/03/2004)

[223] Cf. PENA, Sérgio Danilo Junho; BIRCHAL, Telma de Souza. A inexistência biológica versus a existência social de raças humanas: pode a ciência instruir o etos social? *Revista USP*, nº 68, fevereiro de 2006, p. 10-21.

exemplo, formato dos olhos ou cor da pele, havendo relação com características físicas da pessoa.[224]

Ainda que tanto a Constituição Federal de 1988 use o termo "raça", para dispor que é objetivo fundamental da República promover o bem de todos, sem preconceitos de origem e *raça* (Art. 3º, IV), quanto a Lei nº 12.288/10 (Estatuto da Igualdade Racial)[225] também recorra ao termo, sua utilização é cercada de questionamentos e críticas dentro do Direito.[226] Inclusive, na pesquisa genética humana, o uso do conceito biológico de raça vem sendo considerado por muitos problemático e nocivo[227].

No Brasil, o Instituto Brasileiro de Geografia e Estatística (IBGE) usa como critério em sua pesquisa a "cor ou raça" da pessoa natural e toma como base de definição a sua autodeclaração. Ou seja, as pessoas são perguntadas sobre sua raça, de acordo com as seguintes opções: branca, preta, parda, indígena ou amarela.[228] Negro

---

[224] Disponível em: <https://peoplehealth.com.br/raca-e-etnia-entenda-o-preenchimento-obrigatorios-nos-sistemas-de-saude/> Acesso em: 29.03.21.

[225] "O conceito de raça deve ser trabalhado pela necessidade de demonstrar o caráter específico de um subconjunto de práticas discriminatórias, pois há uma realidade palpável de desigualdade de poder, de direitos e de cidadania, de certa forma influenciada por teorias e ideologias que respaldam as desigualdades raciais e a justificam. Portanto, embora não exista para a biologia o conceito de raça, há um subconjunto de práticas sociais em que este conceito tem vigência. Para se chegar a um conceito jurídico de raça não se pode olvidar sua existência como um fato social. Sendo assim, tal conceito necessita de um lastro teórico-ideológico, definido por Antônio Sérgio Alfredo Guimarães como *racialismo*, usando um termo de Kwame Anthony Appiah, como sendo um conjunto de marcas físicas, compreendidas como indeléveis e hereditárias, ao qual se associa uma "essência racial", que consiste em valores morais, intelectuais e culturais (11). Portanto, o racialismo concebe a existência de uma essência racial, que relaciona características fenotípicas, usando uma linguagem biológica, com valores próprios de uma pessoa." (FERNANDES, Dauney Oliveira. Direito humano à igualdade racial. *Lex Magister*. Disponível em: <https://www.lex.com.br/doutrina_27550329_DIREITO_HUMANO_A_IGUALDADE_RACIAL.aspx> Acesso em: 30.03.21.

[226] Cf. LIMA, Maria Batista. Identidade étnico/racial no Brasil: uma reflexão teórico-metodológica. *Revista Fórum identidades*. Ano 2, Volume 3, p. 33-46, jan-jun. 2008.

[227] "In the wake of the sequencing of the human genome in the early 2000s, genome pioneers and social scientists alike called for an end to the use of race as a variable in genetic research (*1*, *2*). Unfortunately, by some measures, the use of race as a biological category has increased in the postgenomic age (*3*). Although inconsistent definition and use has been a chief problem with the race concept, it has historically been used as a taxonomic categorization based on common hereditary traits (such as skin color) to elucidate the relationship between our ancestry and our genes. We believe the use of biological concepts of race in human genetic research—so disputed and so mired in confusion—is problematic at best and harmful at worst. It is time for biologists to find a better way." (YUDELL, Michael; ROBERTS, Dorothy; DESALLE, Rob; TISHKOFF, Sarah. Taking race out of human genetics. *Science*, Vol. 351, edição 6273, fev. 2016, p. 564-565. Disponível em: <https://science.sciencemag.org/content/351/6273/564> Acesso em: 29.03.21)

[228] "De acordo com dados da Pesquisa Nacional por Amostra de Domicílios (PNAD) 2019, 42,7% dos brasileiros se declararam como brancos, 46,8% como pardos, 9,4% como pretos e 1,1% como amarelos ou indígenas." Disponível em: <https://educa.ibge.gov.br/jovens/conheca-o-brasil/populacao/18319-cor-ou-raca.html> Acesso em: 29.03.21

para o órgão se refere à agregação de pardos e pretos. Acerca da classificação mencionada, doutrina salienta preocupação:

> Há subjetividade na classificação através da cor da pele e dificuldades na identificação das pessoas em categorias intermediárias entre o preto e o branco. A terminologia de identificação pode variar entre as regiões do Brasil, entre as áreas urbanas e rurais, assim como pelo entrevistado e entrevistador. Esta variação deve-se a diferentes percepções das diferenças da cor da pele e ao contexto cultural das palavras utilizadas para denominar as categorias classificatórias. As diferentes terminologias, critérios e métodos de classificação dificultam a comparação entre pesquisas, principalmente entre países com diferentes experiências e histórico de relações raciais. As diferenças ao se comparar os resultados de pesquisas com a literatura podem ser atribuídas à mistura racial dos brasileiros e ao uso de diferentes métodos de classificação nas pesquisas e nos levantamentos populacionais;[229]

A sensibilidade de informações dessa natureza se dá, principalmente, em razão de diversos cenários de racismo[230], preconceito e discriminação étnico-racial[231] existentes no país, impactando ambientes de trabalho[232], ensino, saúde etc. A população negra[233] possui, historicamente, dificuldades de inclusão socioprodutiva, o que se evidencia pelos maiores índices de pobreza, desemprego e desalento, quando em comparação com a população branca.[234] A sociedade brasileira, em seu contexto histórico, foi consolidada sobre as bases do racismo, do patriarcado e do classismo. E isso não pode ser deixado de lado quando são analisados dados.

---

[229] MIRANDA, Monique. *Classificação de raça, cor e etnia*: conceitos, terminologia e métodos utilizados nas ciências da saúde no Brasil, no período de 2000 a 2009. Dissertação de mestrado. Rio de Janeiro: 2010.p.81

[230] MUNANGA, Kabengele. *Rediscutindo a mestiçagem no Brasil:* identidade nacional versus identidade negra. 5. ed. Autêntica: 2019. _____. *Negritude*: usos e sentidos. 4.ed. Autêntica: 2019.

[231] Estatuto da Igualdade Racial - Art. 1º, I: discriminação racial ou étnico-racial: toda distinção, exclusão, restrição ou preferência baseada em raça, cor, descendência ou origem nacional ou étnica que tenha por objeto anular ou restringir o reconhecimento, gozo ou exercício, em igualdade de condições, de direitos humanos e liberdades fundamentais nos campos político, econômico, social, cultural ou em qualquer outro campo da vida pública ou privada;

[232] A Convenção 111 da Organização Internacional do Trabalho define discriminação como: "a) toda distinção, exclusão ou preferência fundada na raça, cor, sexo, religião, opinião política, ascendência nacional ou origem social, que tenha por efeito destruir ou alterar a igualdade de oportunidade ou de tratamento em matéria de emprego ou profissão;" e "b) qualquer outra distinção, exclusão ou preferência que tenha por efeito destruir ou alterar a igualdade de oportunidades ou tratamento em matéria de emprego ou profissão que poderá ser especificada pelo Membro interessado depois de consultadas as organizações representativas de empregadores e trabalhadores, quando estas existam, e outros organismos adequados."

[233] Estatuto da Igualdade Racial - Art. 1º, IV: população negra: o conjunto de pessoas que se autodeclaram pretas e pardas, conforme o quesito cor ou raça usado pela Fundação Instituto Brasileiro de Geografia e Estatística (IBGE), ou que adotam autodefinição análoga.

[234] Observatório da Diversidade e da Igualdade de Oportunidades no Trabalho. Disponível em: <https://smartlabbr.org/diversidade/localidade/0?dimensao=raca> Acesso em: 29.03.21

Variáveis raciais e identitárias apresentam relevantes implicações sociodemográficas, econômicas e produtivas. O racismo, especialmente se atrelado ao sexismo e a outras formas de discriminação (como a homofobia), tem como resultado o impedimento de acesso a bens e a limitação de oportunidades de desenvolvimento pessoal e profissional de determinados grupos. Diferentes formas de discriminação e preconceito se traduzem no ambiente de trabalho com, por exemplo, disparidades salariais[235]-[236]; a não promoção de determinados funcionários ou a não contratação de determinadas pessoas, mesmo se qualificadas, exclusivamente em razão da cor da pele[237] ou por pertencerem a alguma minoria étnico-racial; e assédios de natureza moral e/ou sexual.

Nesse sentido, entende-se que a falta de igualdade nas oportunidades e a discriminação em razão de questões relacionadas à raça, etnia, cor da pele e outras variáveis identitárias são pautas de discussão obrigatórias, devendo ser trabalhadas em políticas públicas e em ações em âmbito privado, que visem a promover maior inclusão e diversidade na sociedade. Acerca do racismo e da relevância da cor da pele para a sua ocorrência, cabe lembrar passagem de Darcy Ribeiro:

---

[235] O estudo *Desigualdades Sociais por Cor ou Raça no Brasil*, produzido pelo Instituto Brasileiro de Geografia e Estatística, em 2019, apontou que, no mercado de trabalho, os pretos ou pardos representavam 64,2% da população desocupada e 66,1% da população subutilizada. Além disso, o número de trabalhadores negros em ocupações informais era de 47,3%, enquanto o de brancos era de 34,6%. Em relação ao rendimento médio, pessoas brancas ocupadas tiveram salário 73,9% superior ao da população preta ou parda. Entre os trabalhadores com nível superior completo, brancos ganhavam, por hora, 45% a mais do que pretos ou pardos. Quanto à distribuição de renda, os pretos ou pardos representavam 75,2% do grupo formado pelos 10% da população com os menores rendimentos e apenas 27,7% dos 10% da população com os maiores rendimentos. Disponível em: <https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/25989-pretos-ou-pardos-estao-mais-escolarizados-mas-desigualdade-em-relacao-aos-brancos-permanece> Acesso em: 29.03.21

[236] Além das vedações constitucionais no art. 7º, XXX e XXXI, afirma a Consolidação das Leis do Trabalho, em seu art. 461, que, sendo idêntica a função, a todo trabalho de igual valor, prestado ao mesmo empregador, no mesmo estabelecimento empresarial, corresponderá igual salário, sem distinção de sexo, etnia, nacionalidade ou idade. § 1º Trabalho de igual valor, para os fins deste Capítulo, será o que for feito com igual produtividade e com a mesma perfeição técnica, entre pessoas cuja diferença de tempo de serviço para o mesmo empregador não seja superior a quatro anos e a diferença de tempo na função não seja superior a dois anos. Neste sentido, a Lei nº 9.029/95, em seu art. 1º, dispõe que "É proibida a adoção de qualquer prática discriminatória e limitativa para efeito de acesso à relação de trabalho, ou de sua manutenção, por motivo de sexo, origem, raça, cor, estado civil, situação familiar, deficiência, reabilitação profissional, idade, entre outros, ressalvadas, nesse caso, as hipóteses de proteção à criança e ao adolescente previstas no inciso XXXIII do art. 7º da Constituição Federal." Essa lei pode ser aplicada, por exemplo, para caso de discriminação racial. Assim, dispensado o empregado em decorrência de discriminação, a lei assegura a sua readmissão, com o ressarcimento de todo o período de afastamento.

[237] O PL 187/2021 da Câmara dos Deputados visa a proibir a exigência de anexar fotografia em curriculum vitae e fichas de inscrição.

> A característica distintiva do racismo brasileiro é que ele não incide sobre a origem racial das pessoas, mas sobre a cor de sua pele. Nessa escala, negro é o negro retinto, o mulato já é o pardo e como tal meio branco, e se a pele é um pouco mais clara, já passa a incorporar a comunidade branca. Acresce que aqui se registra, também, uma branquização puramente social ou cultural. É o caso dos negros que, ascendendo socialmente, com êxito notório, passam a integrar grupos de convivência dos brancos, a casar-se entre eles e, afinal, a serem tidos como brancos. A definição brasileira de negro não pode corresponder a um artista ou a um profissional exitoso. Exemplifica essa situação o diálogo de um artista negro, o pintor Santa Rosa, com um jovem, também negro, que lutava para ascender na carreira diplomática, queixando-se das imensas barreiras que dificultavam a ascensão das pessoas de cor. O pintor disse, muito comovido: "Compreendo perfeitamente o seu caso, meu caro. Eu também já fui negro. Já no século passado, um estrangeiro, estranhando ver um mulato no alto posto de capitão-mor, ouviu a seguinte explicação: "Sim, ele foi mestiço, mas como capitão-mor não pode deixar de ser branco". A forma peculiar do racismo brasileiro decorre de uma situação em que a mestiçagem não é punida mas louvada. Com efeito, as uniões inter-raciais, aqui, nunca foram tidas como crime nem pecado. Provavelmente porque o povoamento do Brasil não se deu por famílias europeias já formadas, cujas mulheres brancas combatessem todo o intercurso com mulheres de cor. Nós surgimos, efetivamente, do cruzamento de uns poucos brancos com multidões de mulheres índias e negras. Essa situação não chega a se configurar uma democracia racial, como quis Gilberto Freyre e muita gente mais, tamanha é a carga de opressão, preconceito e discriminação antinegro que ela encerra.[238]

Embora no Brasil os instrumentos de segregação, em razão de origem étnica ou racial, tenham sido, em alguma medida, mais sutis do que em determinados países, a discriminação e o preconceito desempem papel relevante na exclusão econômica e social de grandes parcelas da comunidade afrodescendente.[239] Outro grave problema é a dificuldade de acesso a bens que grande parte da população sofre, especialmente quando oriunda de determinadas origens étnicas/raciais.[240]

---

[238] RIBEIRO, Darcy. *O Povo Brasileiro.* Companhia de Bolso, 2006. p. 206-207.

[239] Cf. RIBEIRO, Djamila. Pequeno manual antirracista. São Paulo: Companhia das Letras, 2019.

[240] "O Projeto de Lei 5556/20 torna obrigatório incluir dados sobre sexo, raça, cor, idade e condição de pessoa com deficiência na notificação compulsória de casos de Covid-19 feita por órgãos da administração pública. O texto, que tramita na Câmara dos Deputados, altera a Lei de Vigilância Epidemiológica. Autora do projeto, a deputada Rejane Dias (PT-PI) afirma que o objetivo é aumentar o detalhamento de informações sobre doenças epidemiológicas, como a Covid-19, para aperfeiçoar estratégias e ações de combate ao agente infeccioso, como o novo coronavírus. (...) Ela lembra que a Portaria 344/17 já torna obrigatória a inclusão de raça e cor nos sistemas de informação em Saúde, como estratégia para monitorar o perfil epidemiológico dos diferentes grupos populacionais." Disponível em: <https://www.camara.leg.br/noticias/722237-projeto-exige-dados-sobre-raca-sexo-e-pessoa-com-deficiencia-em-notificacoes-de-covid-19/> Acesso em: 30.03.21 No mesmo sentido, vale recordar os seguintes projetos: a) o PL 2726/2020, que determina aos órgãos integrantes do Sistema Único de Saúde e instituições privadas de assistência à saúde a inclusão nos registros de pessoas suspeitas de contaminação, contaminadas, hospitalizadas e falecidas por Covid-19 de marcador étnico-racial, conforme as categorias do Instituto Brasileiro de Geografia e Estatística, de localização e de gênero, para a produção de dados

Por diversos fatores, o acesso a um ensino superior de qualidade vem se mostrando viável apenas para uma pequena parcela da população. E, quando se pensa no ensino superior público, essa fatia se reduz ainda mais. Diante desse cenário, parte da doutrina entendeu como necessária a implantação de ações afirmativas (cotas para ingresso) no ensino superior brasileiro, o que foi inclusive confirmado pelo Supremo Tribunal Federal na Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 186[241].

Na ADPF, em relação à polêmica noção de raça, o Min. Relator Lewandowski seguiu a jurisprudência do Supremo, ao entender que ela se trata de "um conceito histórico-cultural, artificialmente construído, para justificar a discriminação ou, até mesmo, a dominação exercida por alguns indivíduos sobre certos grupos sociais, maliciosamente reputados inferiores."[242] Ponderou que, não obstante os programas de ação afirmativa[243] tomarem como ponto de partida a consciência de raça existente nas sociedades, eles teriam como escopo final eliminá-la.

Nos últimos anos, além da expansão das universidades e cursos técnicos, ampliou-se também o sistema de cotas[244] nas instituições públicas estaduais e federais.

---

oficiais de contaminação e mortalidade pela Covid-19 e que tais dados passem a fazer parte da apresentação pública dos dados de infecção e mortalidade; b) o PL 3154/2020, que visa a alterar a Lei 13.979/20 para determinar que o Ministério da Saúde inclua nos dados públicos informações relativas a cor e a raça das pessoas suspeitas de contaminação, contaminadas, hospitalizadas e falecidas em decorrência da covid-19; e c) o PL 2151/2020, que altera a Lei nº 13.979/20 para estabelecer medidas que aumentam a transparência das informações relativas à covid-19.

[241] STF. ADPF 186. Relator: Min. Ricardo Lewandowski. Julgado em: 26 de abril de 2012. A ação foi ajuizada pelo Partido Democratas, sob a alegação de que a política de cotas adotada na Universidade de Brasília (UnB) feriria vários preceitos fundamentais da Constituição Federal. Em verdade, tratava-se de uma questão mais ampla, devendo a Corte responder se os programas de ação afirmativa que estabeleciam um sistema de reserva de vagas, com base em critério étnico-racial, para o acesso ao ensino superior, estariam em consonância com a Constituição Federal.

[242] STF. ADPF 186. Voto do min. Relator Ricardo Lewandowski. fl. 20.

[243] A utilização do termo "raças", como critério diferenciador, não é pacífica. Todavia, nos editais universitários e nas leis referentes ao tema, verificou-se a larga utilização deste conceito. Daniela Ikawa leciona que: "O uso do termo raça é justificável nas políticas afirmativas (...) por ser o mesmo instrumento de categorização utilizado para a construção de hierarquias morais convencionais não condizentes com o conceito de ser humano dotado de valor intrínseco ou com o princípio de igualdade de respeito (...). Se a raça foi utilizada para construir hierarquias, deverá também ser utilizada para desconstruí-las. Trata-se de um processo de três diferentes fases: i. a construção histórica de hierarquias convencionais que inferiorizaram o indivíduo quanto ao status econômico e de reconhecimento pela mera pertença a determinada raça (...); ii. a reestruturação dessas hierarquias com base em políticas afirmativas que considerem a raça, voltando-se agora à consolidação do princípio de dignidade; iii. A descaracterização do critério raça como critério de inferiorização e o estabelecimento de políticas universalistas materiais apenas" (IKAWA, Daniela. *Ações Afirmativas em Universidades.* Rio de Janeiro: Lumen Juris, 2008. p. 105-106.)

[244] Entende-se que o sistema de cotas traz maior efetividade para o Direito Fundamental à educação, previsto no artigo 6º da CRFB/88. Por meio desta medida, garante-se que um número maior e mais

Para participar de tal ação afirmativa, deve o candidato indicar sua origem étnica/racial. Na lei federal que trata do tema, Lei nº 12.711/2012[245], estipulou-se que o critério será a autodeclaração, como ocorre no censo demográfico e em diversas outras políticas no Brasil, privilegiando-se a autopercepção do candidato. A lei não utilizou, portanto, como critério a avaliação do fenótipo, que tem como pressuposto a existência de características externas, morfológicas e físicas por meio das quais seria possível estabelecer determinado sujeito como pertencente a determinada raça. Exemplos de fenótipo são o formato dos olhos, a tonalidade da pele e cor e textura do cabelo.

Determinar a origem étnica ou racial de algumas pessoas nem sempre será uma tarefa simples, visto que tal análise depende de múltiplos fatores, os quais, por vezes, mostram-se subjetivos. Nos últimos anos, diversas universidades vêm recebendo denúncias de ocupação irregular de vagas destinadas a pessoas cotistas, o que tem suscitado a abertura de processos administrativos de invalidação de matrícula e, consequentemente, a expulsão ou saída de estudantes. Geralmente, ocorre o preenchimento de vagas destinadas ao grupo racial negro por pessoas que não seriam as verdadeiras destinatárias da ação afirmativa, bem como há fraudes relativas à renda *per capita* familiar e ao local de moradia. Da mesma forma, fraudes vêm ocorrendo em concursos públicos para diversas carreiras, sendo cada vez mais comum a inserção de bancas avaliadoras de identificação em âmbito administrativo.[246]

---

diversificado de pessoas tenha acesso ao ensino superior público no Brasil, podendo se inserir de forma mais qualificada no mercado de trabalho e ter acesso a melhores recursos em termos de saúde e moradia. Dialogando com a referida disposição, encontram-se as normas do Estatuto da Igualdade e da Lei Federal de cotas. Tal ação afirmativa auxilia também no combate ao racismo, ao preconceito e à desigualdade social, o que é inclusive mandamento constitucional (art. 3º, inciso III; art. 5º, incisos XLI e XLII; e Art. 7º XXX). Entende-se que a democracia racial no Brasil seria apenas um mito que serviria para anestesiar e postergar o enfrentamento de graves problemas nacionais: a discriminação racial e a desigualdade de oportunidades. No âmbito das universidades, as cotas significam a efetivação de uma discriminação positiva capaz de ampliar a diversidade cultural, racial e social nas instituições de ensino, trazendo para dentro delas as principais características da nossa sociedade: o pluriculturalismo e a variada composição racial dos cidadãos.

[245] Dispõe sobre o ingresso nas universidades federais e nas instituições federais de ensino técnico de nível médio e dá outras providências. Esta lei é regulada pelo Decreto nº 7.824, de 11 de outubro de 2012 e a portaria normativa nº 18, de 11 de outubro de 2012.

[246] "Desde que esteja prevista no edital, é válida a avaliação de fenótipo (característica visíveis) para confirmar autodeclaração de candidato como preto ou pardo. A decisão é do Órgão Especial do Tribunal Superior do Trabalho ao manter ato que negou a inscrição de candidato autodeclarado pardo em concurso do Tribunal Regional do Trabalho da 1ª Região (RJ). (...) O TRT-1 concedeu a segurança e determinou sua inscrição nas vagas da cota. Porém, o entendimento foi derrubado no TST. Relator, o ministro Ives Gandra, observou que a autodeclaração do candidato quanto ao seu fenótipo não é absoluta e, portanto, goza de presunção relativa de veracidade. Segundo Ives Gandra, é preciso confrontá-la com outros elementos (formas e critérios), "de modo a coibir eventual fraude à política estatal de ação afirmativa alusiva às cotas raciais". O ministro observou que a Comissão de Heteroidentificação do concurso, ao

Ainda que o tratamento de dados sobre origem étnica ou racial necessite de uma série de salvaguardas específicas, diante de cenários de preconceito, discriminação e racismo, tanto por parte de humanos quanto de ferramentas tecnológicas, mostra-se de grande importância realizar tratamentos que visem a analisar e prevenir tais cenários, bem como implementar e monitorar políticas de diversidade e inclusão.[247] Não há dúvidas de que informações sobre origem étnica e racial são elementos sensíveis em questões como, por exemplo, policiamento preditivo, reconhecimento facial, enviesamento de dados e racismo algorítmico. Entretanto, se aplicados recursos jurídicos e técnicos para o adequado controle e proteção de dados dessa natureza, seu tratamento poderá ser realizado, desde que não seja em prejuízo do indivíduo ou de uma coletividade.

2.2.2 Dados pessoais sensíveis acerca de crenças e filiações

Segundo a LGPD, são dados sensíveis também informações de uma pessoa natural sobre convicção religiosa, opinião política e filiação a sindicato ou a organização de caráter religioso, filosófico ou político. A lei brasileira reflete, aqui, o já disposto no GDPR, em seu Art. 9º, que dispõe que são dados sensíveis dados pessoais que revelam opiniões políticas, convicções religiosas ou filosóficas ou a filiação sindical.

As informações acerca da *convicção religiosa* e da *filiação a organização de caráter religioso* de uma pessoa são protegidas pela Constituição Federal, que em seu artigo 5º afirma que "é inviolável a liberdade de consciência e de crença, sendo assegurado o livre exercício dos cultos religiosos e garantida, na forma da lei, a proteção aos locais de culto e a suas liturgias" (inciso VI); e que "ninguém será privado de

---

analisar, conforme previsto no edital, os traços fenotípicos do candidato e a foto tirada no momento do procedimento de aferição concluiu, por unanimidade, que ele não se enquadra nas condições de pessoa preta ou parda, nos termos da Lei de Cotas no Serviço Público (Lei 12.990/2014), por não apresentar fenótipos característicos (cabelo, nariz, cor da pele, boca, etc.)." Processo: RO-101662-28.2018.5.01.0000 Disponível em: <https://www.conjur.com.br/2020-fev-20/avaliacao-fenotipo-excluir-candidato-autodeclarado-pardo> Acesso em: 30.03.21

[247] FARKAS, Lilla. *Data collection in the field of ethnicity.* Analysis and comparative review of equality data collection practices in the European Union. European Commission. Directorate-General for Justice and Consumers. 2017.

direitos por motivo de crença religiosa ou de convicção filosófica ou política, salvo se as invocar para eximir-se de obrigação legal a todos imposta e recusar-se a cumprir prestação alternativa, fixada em lei" (inciso VIII).

A liberdade religiosa representa o direito de cada pessoa exercer a sua religião, se assim desejar, com base em sua autonomia privada existencial. Cuida de permitir a livre escolha, adesão e expressão de uma religião, bem como traz a faculdade de a pessoa se autodeterminar[248] a partir de suas crenças.[249] Além disso, com base nesse direito, pode a pessoa decidir livremente não professar qualquer religião. Como ensina Fábio Leite, a garantia constitucional da liberdade religiosa reflete o compromisso do Estado de respeitar e garantir a expressão das mais variadas crenças e compreensões acerca da vida e de outras temáticas próprias do campo religioso.[250]

Ante o princípio da laicidade do Estado, uma determinada religião e seu conjunto de preceitos, crenças e valores não poderão ser impostos a grupos e indivíduos, mesmo se houver um número substancial de devotos ou praticantes de tal religião.[251] No Brasil, infelizmente, são comuns os casos de preconceito e discriminação em face das mais variadas religiões, desde as de matriz africana até as cristãs.

---

[248] "(...) reconhecer que a liberdade religiosa protege o direito de o cidadão se determinar em razão de uma crença religiosa não assegura, *a priori*, que todas as práticas religiosas, necessárias à sua autodeterminação, estarão protegidas pelo Direito." (LEITE, Fábio. A liberdade de crença e o sacrifício de Animais em cultos religiosos. *Veredas do Direito*, Belo Horizonte, v.10, n.20, p.163-177, jul./dez. 2013. p. 165.)

[249] Recorda-se previsão contida na Convenção Americana sobre Direitos Humanos (Pacto de San José), em seu artigo 12, que versa sobre liberdade de consciência e de religião: "1. Toda persona tiene derecho a la libertad de conciencia y de religión. Este derecho implica la libertad de conservar su religión o sus creencias, o de cambiar de religión o de creencias, así como la libertad de profesar y divulgar su religión o sus creencias, individual o colectivamente, tanto en público como en privado. 2. Nadie puede ser objeto de medidas restrictivas que puedan menoscabar la libertad de conservar su religión o sus creencias o de cambiar de religión o de creencias. 3. La libertad de manifestar la propia religión y las propias creencias está sujeta únicamente a las limitaciones prescritas por la ley y que sean necesarias para proteger la seguridad, el orden, la salud o la moral públicos o los derechos o libertades de los demás. 4. Los padres, y en su caso los tutores, tienen derecho a que sus hijos o pupilos reciban la educación religiosa y moral que esté de acuerdo con sus propias convicciones."

[250] LEITE, Fábio. A liberdade de crença e o sacrifício de Animais em cultos religiosos. *Veredas do Direito*, Belo Horizonte, v.10, n.20, p.163-177, jul./dez. 2013. p. 165.

[251] "A laicidade propicia a devolução da potência pública a todos, sem qualquer distinção, recordando as pessoas de sua mesma dignidade. Tem em seu bojo dois princípios constitucionais: a liberdade de consciência e a igualdade material, permitindo uma união verdadeira entre as pessoas, que não impede as diferenças, mas que organiza a convivência fraterna entre os indivíduos. A laicidade promove o que une os seres humanos, antes de valorizar o que os divide, como crenças e religiões. Assim, a religião não poderá representar óbice para o exercício regular das demais liberdades fundamentais, bem como para a implementação de políticas públicas ou ampliação de direitos fundamentais." (TEFFÉ, Chiara Spadaccini de; ALMEIDA, J. Humor e responsabilidade na Internet. In: Guilherme Martins; Nelson Rosenvald. (Org.). *Responsabilidade civil e novas tecnologias*. 1ed.Indaiatuba: FOCO, 2020, p. 125-144.)

Vale ressaltar, aqui, a relevância de fluxos de tratamentos de dados realizados por igrejas e outras instituições religiosas (sujeitos que igualmente necessitam de adequação à LGPD), por se relacionarem com aspectos pessoais e permitirem por vezes inferências sensíveis, mesmo quando não tratados dados diretamente sensíveis.[252]

Os dados acerca de crenças e organizações de caráter religioso são muito valiosos, de modo que diversas instituições e organizações buscam coletá-los, visando a refinar os perfis criados e aperfeiçoar direcionamentos de conteúdos. Por exemplo, já há recursos técnicos para que igrejas utilizem câmeras de reconhecimento facial para traçar o perfil de seus fiéis e compreender suas emoções, obtendo relatórios sobre a assiduidade de seu público e seu comportamento durante os cultos, prática essa, sem dúvida, bastante questionável.[253]

A operação de igrejas, associações e comunidades religiosas exige o processamento de informações pessoais de seus membros para permitir a comunicação e organização de atividades dentro da congregação. As organizações religiosas podem realizar o processamento de dados por várias razões, como, por exemplo, para manter contato com sua congregação ou para comunicar informações sobre festividades e eventos religiosos ou de caridade. Em qualquer caso, os dados que revelarem crenças religiosas serão dados sensíveis e as igrejas deverão ser responsáveis pelo manuseio e processamento de tais dados, especialmente porque as informações processadas por organizações religiosas, muitas vezes, dizem respeito a crianças, idosos ou outros membros vulneráveis da sociedade.

As crenças religiosas ou filosóficas devem incluir dados como: filiação a uma confissão religiosa ou organização que se concentre em uma crença filosófica; escritos que evidenciem crenças religiosas ou filosóficas; ou comportamentos específicos que demonstrem uma expressão de convicção religiosa ou filosófica (como o uso do véu, rezar o terço ou recusar certos alimentos). Como o conceito de *orientação filosófica* é aberto, a vinculação à maçonaria ou a grupos Rosacruz também poderá ser tida como

---

[252] O PL 5.141/2020 busca alterar a alínea "a", do inciso II, do Art. 4º, da Lei nº 13.709/18, passando a vigorar com a seguinte redação: "a) jornalístico, artístico e religioso, ou". Busca-se que a LGPD não se aplique ao tratamento de dados pessoais realizado para fins exclusivamente religiosos. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2265143> Acesso em: 07.07.21.

[253] Disponível em: <https://www.cartacapital.com.br/sociedade/empresas-lancam-servico-de-reconhecimento-facial-para-igrejas-no-brasil/> <https://canaltech.com.br/mercado/o-reconhecimento-facial-chegou-a-igreja-155437/> Acesso em: 07.07.21.

dado sensível para efeitos legais. O conceito é de difícil concreção, sobretudo porque a própria noção de orientação filosófica pode estender-se para temas que vão desde a defesa do minimalismo até o veganismo.

O dado sensível referente à *opinião política* foi assim designado em razão de históricas perseguições e discriminações dirigidas a pessoas em razão de opiniões políticas e *filiações a organizações de caráter político*. Opiniões políticas podem incluir, por exemplo, filiação partidária, participação em manifestações ou publicações e declarações políticas. Por vezes, conhecer esses dados será necessário para garantir transparência e controle em atuações políticas, devendo ser resguardadas, porém, garantias fundamentais.

Ainda que seja comum, atualmente, a própria pessoa manifestar suas opiniões e filiações neste campo, a lei reserva proteção destacada. Uma das razões para isso é o tratamento que tais informações podem receber em período eleitoral e como isso pode prejudicar as democracias contemporâneas[254], diante do acirramento de polarizações políticas, da microssegmentação de anúncios e propagandas políticas[255] e do direcionamento manipulado de determinados conteúdos a certos grupos.

Os partidos políticos e grupos de campanha vêm, cada vez mais, usando informações pessoais e técnicas sofisticadas de análise de dados para atingirem os eleitores. Modelos comportamentais foram amplamente utilizados nos últimos anos em campanhas políticas, sendo icônico o caso que envolveu o tratamento de dados pessoais realizado pela *Cambridge Analytica*, assessoria britânica que trabalhou para a campanha eleitoral do ex-presidente norte-americano Donald Trump, a partir de informações extraídas do Facebook.

No que diz respeito à filiação a sindicato, a Consolidação das Leis do Trabalho (CLT) prevê a possibilidade de o empregado realizar contribuições sindicais e formalizar sua filiação perante o sindicato representativo de sua categoria por liberalidade.[256] [257] Diante de práticas discriminatórias e antissindicais dirigidas em face

---

[254] Information Commissioner's Office. Democracy disrupted? Personal information and political influence. Publicado em 11 de julho de 2018. Disponível em: <https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/> Acesso em: 07.07.21.

[255] Information Commissioner's Office. Investigation into the use of data analytics in political campaigns. Investigation update. Publicado em 11 de julho de 2018. Disponível em: <https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/> Acesso em: 07.07.21.

[256] CLT, "Art. 540. A tôda emprêsa, ou indivíduo que exerçam respectivamente atividade ou profissão, desde que satisfaçam as exigências desta lei, assiste o direito de ser admitido no sindicato da respectiva

de funcionários sindicalizados, como o impedimento de eles participarem de cursos e treinamentos e a diminuição das possibilidades de serem promovidos[258], o referido dado foi classificado como sensível tanto na LGPD quanto no GDPR.

---

categoria. (...)" "Art. 543 - O empregado eleito para cargo de administração sindical ou representação profissional, inclusive junto a órgão de deliberação coletiva, não poderá ser impedido do exercício de suas funções, nem transferido para lugar ou mister que lhe dificulte ou torne impossível o desempenho das suas atribuições sindicais. (...) § 3º - Fica vedada a dispensa do empregado sindicalizado ou associado, a partir do momento do registro de sua candidatura a cargo de direção ou representação de entidade sindical ou de associação profissional, até 1 (um) ano após o final do seu mandato, caso seja eleito inclusive como suplente, salvo se cometer falta grave devidamente apurada nos termos desta Consolidação."

[257] "Como a contribuição sindical é descontada na folha de pagamento, mediante autorização do empregado, o empregador deve possuir este documento para se resguardar de eventual processo trabalhista, já que o ônus dessa prova é deste. A guarda dessa desse documento de autorização para desconto da contribuição sindical, a folha de pagamento do mês de desconto dos valores devidos e quaisquer outros documentos relacionados a filiação sindical, devem ser arquivados pelo empregador por até 5 anos após da data de saída do empregado, já que é o período máximo de prescrição das ações trabalhistas, nos termos do art. 7°, XXIX da Constituição da República de 1988. Esses documentos devem receber maior proteção no âmbito da segurança, nos termos do art. 6°, VII da LGPD, já que esta lei os considera dados sensíveis, com maior potencial de dano se forem divulgados a terceiros. Assim, como prática de Segurança da Informação, o mínimo de pessoas possível deve ter acesso a tais informações." Disponível em: <https://www.dtibr.com/post/dados-pessoais-de-empregados-sindicalizados> Acesso em: 08.07.21.

[258] DIRIGENTE SINDICAL. CONDUTA DISCRIMINATÓRIA E ANTISSINDICAL. INDENIZAÇÃO DEVIDA. 1. No cenário internacional, constitucional e infraconstitucional, o sistema jurídico veda a prática de condutas antissindicais, como as noticiadas no presente caso, ou seja, de discriminação e assédio de trabalhador que pertence a quadro sindical. 2. A Convenção 87 da OIT especifica que: "Artigo 2 - Os trabalhadores e os empregadores, sem nenhuma distinção e sem autorização prévia, têm o direito de constituir as organizações que estimem convenientes, assim como o de filiar-se a estas organizações, com a única condição de observar os estatutos das mesmas. Artigo 3.1. As organizações de trabalhadores e de empregadores têm o direito de redigir seus estatutos e regulamentos administrativos, o de eleger livremente seus representantes, o de organizar sua administração e suas atividades e o de formular seu programa de ação." 3. No mesmo norte, a Convenção 98 da OIT, ratificada pelo Brasil, por meio do Decreto Legislativo 49/52, dispõe: "Art. 1.1. Os trabalhadores deverão gozar de proteção adequada contra quaisquer atos atentatórios à liberdade sindical em matéria de emprego. 2. Tal proteção deverá, particularmente, aplicar-se a atos destinados a: a) subordinar o emprego de um trabalhador à condição de não se filiar a um sindicato ou deixar de fazer parte de um sindicato; b) dispensar um trabalhador ou prejudicá-lo, por qualquer modo, em virtude de sua filiação a um sindicato ou de sua participação em atividades sindicais, fora das horas de trabalho ou com o consentimento do empregador, durante as mesmas horas. (...)". 4. No sistema constitucional pátrio, há proibição de atos antissindicais, consoante artigos 8º, da Constituição da República e no âmbito infraconstitucional, o art. 543, § 6º, da CLT que prevê a punição de condutas de tal viés. 5. A conduta da ré, representada por abuso no direito diretivo e tratamento ofensivo e discriminatório ao trabalhador que exerce funções sindicais, mediante investidas do representante com condutas desrespeitosas no ambiente de trabalho, tem potencial de causar danos relevantes à saúde psíquica e moral do trabalhador. Imputação de responsabilidade à empresa inclusive, por ato de preposto (art. 932, III, do Código Civil - CLT, art. 8º). A responsabilização, no caso, por atingir direitos fundamentais, inclusive relacionados ao exercício de direitos sindicais (art. 5º, V e X e 8º, da CF), prescinde da prova de efetivo dano suportado, bastando a demonstração da prática do ilícito do qual ele emergiu (dano 'in re ipsa'). ADICIONAL DE INSALUBRIDADE. GRAU MÁXIMO. CONTATO COM ÓLEOS E GRAXAS. A apuração do contato com óleo e graxa é qualitativa, impondo reconhecer que o trabalhador, nas atividades em que mantém contato com tais produtos, cuja ação nociva não é elidida pela utilização de luvas e cremes protetores, faz jus ao adicional de insalubridade em grau máximo, nos termos da NR-15, Anexo 13 da Portaria 3.214/78 do MTE. (TRT-4 - RO: 00016069620135040252, Data de Julgamento: 23/03/2018, 2ª Turma)

2.2.3 Dados pessoais sensíveis corporais

Na categoria dos dados pessoais sensíveis relacionados ao corpo humano são tratadas informações pertinentes à integridade psicofísica da pessoa natural, seu comportamento, bem como condições e características física e mental. A partir da tipologia adotada pela LGPD, busca-se, aqui, desenvolver estudo sobre os dados de saúde, dados biométricos e dados genéticos. Essas informações guardam (ou expõem) conteúdos extremamente íntimos e particulares sobre seu titular e, muitas vezes, sobre seus parceiros e familiares. Elas revelam, de maneira direta ou indireta, hábitos, comportamentos, dietas e propensões a doenças, além de traçarem quadros sobre o passado, o presente e o futuro da pessoa a quem dizem respeito. Tome-se como exemplo um prontuário que indica quem são os pais de uma criança ou os registros de sessões de terapia.

Em estudos sobre o corpo, Stefano Rodotà questiona: de quem é o corpo? Da pessoa interessada, de seus familiares, de um Deus que o doou, de uma natureza que o quer inviolável, de um poder social que de diversas formas dele se apossa, de um médico ou de um magistrado que estabelece seu destino?[259] O corpo como espaço de liberdade ou de coerção?[260] As respostas para as mencionadas questões revelam diretamente a compreensão do intérprete acerca das decisões que poderão ser tomadas em relação à tutela e à disposição do corpo e dos dados que o compõem. Partindo de uma perspectiva que prioriza a autonomia existencial, especialmente a autodeterminação corporal[261], e rechaça a coerção e o paternalismo[262] [263], nos últimos

[259] "Di chi é il corpo? Della persona interessata, della sua cerchia familiare, di un Dio che l'ha donato, di una natura che lo vuole inviolabile, di un potere sociale che in mille modi se ne impadronisce, di un medico o di un magistrato che ne stabiliscono il destino? E di quale corpo stiamo parlando?" (RODOTÀ, Stefano. Salviamo il corpo. Stralcio dell'intervento al convegno su "Trasformazioni del corpo e dignità della persona" - Roma 4/5/2005. Disponível em: <http://www.privacy.it/rodo20050504.html> Acesso em: 01.03.21.

[260] "Il corpo come luogo dela libertà o della coercizione?" (RODOTÀ, Stefano. Costruzione del corpo, XXI Secolo. 2009. Disponível em: <http://www.treccani.it/enciclopedia/costruzione-del-corpo_(XXI_Secolo)/> Acesso em: 01.03.21.

[261] "A autonomia corporal, entendida como a capacidade de autodeterminação da pessoa em relação ao próprio corpo, está inserida na seara da existencialidade ou extrapatrimonialidade, ou seja, é espécie do gênero "autonomia existencial" antes descrito. Contudo, ela compõe o terreno de atuação concreta da

anos, passou-se a falar em um "direito ao próprio corpo", expressão que procura enfatizar que o corpo deve atender à realização da própria pessoa, seu único titular, e não aos interesses de qualquer outra entidade, como a Igreja, empresas privadas, a família ou o Estado.[264]

Sob o respaldo do princípio da dignidade da pessoa humana, o corpo tornou-se espaço para a autodeterminação existencial, para a expressão da personalidade da pessoa, livre para externar suas opções e crenças. O corpo não é mais percebido apenas em sua materialidade, mas nas suas diversas representações, como centro de referência de uma multiplicidade de relações, o que fez com que ele se dividisse e se multiplicasse. O corpo tem sido e continua a ser objeto de intervenções que pretendem conciliar espiritualidade e materialidade, bem como fisicalidade e virtualidade.[265]

Nesse cenário, o princípio da liberdade individual mostra-se de elevada importância para fundamentar e legitimar as condutas da pessoa em relação ao seu corpo. Liberdade significa poder realizar, sem interferências de qualquer gênero, as próprias escolhas individuais e assumir as suas expressões da forma que for mais conveniente ao indivíduo.[266] Como exemplos de situações violadoras da dignidade, em razão de lesão ao princípio da liberdade, pode-se mencionar a incapacidade de controle acerca dos próprios dados pessoais e a restrição à manifestação de pensamento e

---

liberdade, que se exprime, originariamente, na esfera de seu titular, não sendo parte necessária de uma relação entre sujeitos, mas sim do sujeito sobre si mesmo." (BODIN DE MORAES, Maria Celina; CASTRO, Thamis Dalsenter Viveiros de. A autonomia existencial nos atos de disposição do próprio corpo. *Pensar*, Fortaleza, v. 19, n. 3, p. 779-818, set./dez. 2014.)

[262] "Paternalism is the interference of a state or an individual with another person, against their will, and defended or motivated by a claim that the person interfered with will be better off or protected from harm. The issue of paternalism arises with respect to restrictions by the law such as anti-drug legislation, the compulsory wearing of seatbelts, and in medical contexts by the withholding of relevant information concerning a patient's condition by physicians. At the theoretical level it raises questions of how persons should be treated when they are less than fully rational." (DWORKIN, Gerald. Paternalism, *The Stanford Encyclopedia of Philosophy* (Summer 2014 Edition), Edward N. Zalta (ed.). Disponível em: <http://plato.stanford.edu/archives/sum2014/entries/paternalism/> Acesso em: 01.03.21)

[263] Entre os artigos 13 e 15 do Código Civil brasileiro, o legislador limitou-se a tratar do direito à integridade psicofísica sob um único aspecto: o dos atos de disposição do corpo humano. Cuida-se tão somente da relação entre a proteção ao corpo e a vontade do seu titular, procurando determinar em quais circunstâncias pode uma pessoa "dispor", no todo ou em parte, do seu próprio corpo. A opção adotada é bastante criticada pela doutrina, uma vez que, por diversos momentos, limitou a vontade individual.

[264] SCHREIBER, Anderson. *Direitos da Personalidade.* 2. ed. São Paulo: Atlas, 2013.p. 32

[265] RODOTÀ, Stefano. Costruzione del corpo, XXI Secolo. 2009. Disponível em: <http://www.treccani.it/enciclopedia/costruzione-del-corpo_(XXI_Secolo)/> Acesso em: 01.03.21.

[266] RODOTÀ, Stefano. *A vida na sociedade da vigilância – a privacidade hoje.* Coord. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 74-75.

crítica.[267] Nutre-se do princípio da liberdade a autonomia que "(...) expressa a vontade livre, a capacidade do indivíduo de se autodeterminar, em conformidade com a representação de certas leis."[268] Além da liberdade, a integridade psicofísica tem recebido especial atenção por servir de garantia ao projeto de vida, assim como a diversos direitos da personalidade. De acordo com Pietro Perlingieri, tanto o perfil físico quanto o psíquico constituem componentes indivisíveis da estrutura humana (...): "a tutela de um desses perfis se traduz naquela da pessoa no seu todo, e a disciplina na qual consiste esta tutela é, de regra, útil também para cada um de seus aspectos."[269] A integridade seria composta de duas categorias indissociáveis do ser: o corpo e a mente, de modo que, também no campo jurídico, a integridade deveria ser tratada de acordo com a perspectiva da integridade psicofísica.[270]

Na era da informação, o corpo não se resume apenas ao aspecto físico e materialmente visível. Os dados e informações sobre uma pessoa formam aquilo que foi denominado por Stefano Rodotà de "corpo eletrônico", o qual deve ser integralmente tutelado pelo ordenamento, materializando-se sua proteção na Constituição Federal e, em sede infraconstitucional, especialmente na LGPD.

2.2.3.1 Dados referentes à saúde

De acordo com o *General Data Protection Regulation,* dados de saúde são "dados pessoais relacionados à saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelam informações sobre o seu estado de saúde"[271]. Seu considerando 35 dispõe que deverão ser compreendidos como dados

---

[267] BODIN DE MORAES, Maria Celina. *Danos à pessoa humana:* uma leitura civil-constitucional dos danos morais. Rio de Janeiro: Renovar, 2003. p. 107.

[268] BARROSO, Luís Roberto. A dignidade da pessoa humana no direito constitucional contemporâneo: natureza jurídica, conteúdos mínimos e critérios de aplicação. Disponível em: <http://www.luisrobertobarroso.com.br/wp-content/uploads/2010/12/Dignidade_texto-base_11dez2010.pdf> Acesso em: 01.03.21.

[269] PERLINGIERI, Pietro. *O Direito Civil na legalidade constitucional.* Rio de Janeiro: Renovar, 2008. p.776.

[270] BODIN DE MORAES, Maria Celina. La tutela della persona umana in Brasile. *Civilistica.com,* Rio de Janeiro, a. 3, n. 2, jul.-dez./2014.

[271] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação

pessoais relativos à saúde todos os dados relativos ao estado de saúde de um titular que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro. Isso inclui informação sobre a pessoa natural tratada no decurso do registro ou da prestação de serviços de saúde referidos na Diretiva 2011/24/UE do Parlamento Europeu e do Conselho[272]; um número, símbolo ou sinal particular atribuído a uma pessoa para identificá-la de maneira única para fins de saúde; informações derivadas de teste ou exame de uma parte do corpo ou substância corporal, incluindo dados genéticos e amostras biológicas; e qualquer informação sobre, por exemplo, uma doença, deficiência, risco de doença, histórico médico, tratamento clínico ou o estado fisiológico ou biomédico do titular dos dados, independentemente da sua fonte, por exemplo, um médico ou outro profissional de saúde, um hospital, um dispositivo médico ou um teste de diagnóstico *in vitro*.

É possível também compreender dados de saúde como dados relacionados ao estado de saúde, escolha pessoal sobre a seleção de um tratamento, planos e seguros de saúde, relatórios de tratamentos, *causa mortis*, dados psiquiátricos[273] [274], determinados parâmetros socioeconômicos relacionados à saúde e bem-estar de uma pessoa natural e histórico de saúde. Informações de saúde também podem ser encontradas em dados relacionados à prestação de serviços direcionados à saúde física ou mental de uma pessoa, envolvendo observações gerais de saúde, e registros de potenciais diagnósticos, procedimentos e tratamentos. Da mesma forma, registros de flutuação de peso, níveis de

---

desses dados. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679> Acesso em: 21 jan. 2021.

[272] Diretiva 2011/24/UE do Parlamento Europeu e do Conselho, de 9 de março de 2011, relativa ao exercício dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32011L0024> Acesso em: 21 jan. 2021.

[273] Em outubro de 2020, segundo reportagem, "Pacientes de uma grande clínica de psicoterapia na Finlândia foram contatados individualmente por um chantagista, depois que seus dados foram roubados dos servidores da empresa. Os dados têm registros de identificação pessoal e notas sobre o que foi discutido nas sessões de terapia. A clínica se chama Vastaamo, e é uma rede finlandesa de terapia com cerca de 20 agências e milhares de pacientes." Disponível em: <https://www.bbc.com/portuguese/geral-54698957> Acesso em: 10.03.21

[274] Segundo reportagem, a Rede Globo foi condenada a indenizar Suzane von Richthofen em R$ 10 mil por divulgar, em uma reportagem do programa dominical *Fantástico*, o resultado de um teste psicológico, sigiloso, feito para subsidiar um pedido de progressão de pena para regime semiaberto. A decisão foi tomada pela 1ª Câmara de Direito Privado do Tribunal de Justiça do Estado de São Paulo em março de 2021. Os laudos psicológicos e o teste de Rorschach, uma técnica de avaliação psicológica, apontavam que não havia evidências de que Suzane seria perigosa, podendo conviver em sociedade, mas que, por outro lado, dentre outros pontos, tinha personalidade manipuladora e agressividade camuflada. A ação em que a Globo foi condenada tramita com o número 1001243-57.2018.8.26.0025, em segredo de Justiça. Disponível em: <https://www.jota.info/coberturas-especiais/liberdade-de-expressao/suzane-von-richthofen-globo-teste-12032021> Acesso em: 15.03.21.

dor e medições de HbA1c e de frequência cardíaca.[275] Outros exemplos são o tipo sanguíneo, histórico de compras em farmácias[276], a opção por ser doador de órgãos e histórico de doenças. Esse conceito engloba, também, dados pessoais que, em um primeiro momento, possam não parecer serem de saúde, mas que, dentro de determinado contexto, possam permitir inferir dados relacionados à saúde, como informações sobre a frequência de corridas realizadas por um determinado indivíduo[277] e seus hábitos alimentares.[278]

Dados de saúde podem dizer muito sobre o nosso passado, presente e futuro, assim como trazer questões referentes a terceiros, o que torna a sua análise ainda mais delicada e sensível, mesmo quando seu titular já tiver falecido.[279] Como veremos em tópico específico, especialmente os dados genéticos costumam contar a história não

[275] Definição expressa na página 22 do seguinte documento: *A Taxonomy of Definitions for the Health Data Ecosystem*, publicado em maio de 2019. Disponível em: <https://fpf.org/wp-content/uploads/2019/05/A_Taxonomy_of_Definitions_for_the_Health_Data_Ecosystsm_5.29.19_accessible.pdf> Acesso em: 21.01.21

[276] Em São Paulo, a Lei Estadual n. 17.301/2020 proíbe farmácias e drogarias de exigir o CPF do consumidor, no ato da compra, sem informar de forma adequada e clara sobre a concessão de descontos.

[277] No mercado, há inúmeros aplicativos de corrida que fazem coleta de dados pessoais sobre o desempenho atlético de corredores (ex. Strava). Nesse sentido, dados de corrida indicam o percurso habitual, região de residência, condicionamento físico e tantas outras informações.

[278] Além do GDPR, cabe lembrar também importante norma norte-americana sobre o tema: o *Health Insurance Portability and Accountability Act* (HIPAA). Ela exige a criação de padrões para proteger a divulgação de informações sensíveis sobre a saúde do paciente sem o seu consentimento ou conhecimento. Os padrões da Regra de Privacidade do HIPAA tratam do uso e divulgação de informações de saúde de indivíduos por entidades sujeitas à regra. A regra de privacidade também contém *standards* para os direitos dos indivíduos de entender e controlar como suas informações de saúde são tratadas. Um dos principais objetivos da Regra de Privacidade é garantir que as informações de saúde dos indivíduos sejam devidamente protegidas, permitindo fluxos de informações de saúde necessários para fornecer e promover cuidados de saúde de alta qualidade e para proteger a saúde e o bem-estar do público. Informações disponíveis em: <https://www.cdc.gov/phlp/publications/topic/hipaa.html#one> Acesso em: 04.03.21. Nos últimos anos, vem ocorrendo amplo debate para o estabelecimento de novas regulações dentro da norma. Informações disponíveis em: <https://www.hipaajournal.com/new-hipaa-regulations/> Acesso em: 04.03.21.

[279] Jenny Krutzinna, Mariarosaria Taddeo e Luciano Floridi defendem polêmico entendimento acerca da utilização de dados de saúde, com o consentimento de seu titular, após a sua morte: "(…) personal medical data should be made available for scientific research, by enabling and encouraging individuals to donate their medical records once deceased, in a way similar to how they can already donate organs or bodies. This research is part of a project on posthumous medical data donation (PMDD) developed by the Digital Ethics Lab at the Oxford Internet Institute. Ten arguments are provided to support the need to foster posthumous medical data donation. Two major risks are also identified—harm to others, and lack of control over the use of data—which could follow from unregulated donation of medical data. The argument that record-based medical research should proceed without the need to ask for informed consent is rejected, and it instead a voluntary and participatory approach to using personal medical data should be followed. The analysis concludes by stressing the need to develop an ethical code for data donation to minimize the risks providing five foundational principles for ethical medical data donation; and suggesting a draft for such a code." (KRUTZINNA, Jenny; TADDEO, Mariarosaria; FLORIDI, Luciano. Enabling Posthumous Medical Data Donation: A Plea for the Ethical Utilisation of Personal Health Data. In: KRUTZINNA, Jenny; FLORIDI, Luciano (Eds.) *The Ethics of Medical Data Donation*. Springer. 2019.p. 163-180)

apenas de seus titulares, mas também de membros de sua família, sendo possível analisar doenças hereditárias por meio de determinadas informações.[280] Tais dados podem atingir até os filhos ainda não nascidos ou concebidos, haja vista os conhecidos efeitos da hereditariedade genética.

Diferentes tipos de dados pessoais de saúde podem ser obtidos de informações criadas por profissionais de saúde (como registros sobre a saúde do paciente colocados em prontuário e alimentação de bancos de dados nacionais de saúde contendo itens como prescrições, exames laboratoriais e detalhes sobre doenças importantes relacionadas a uma pessoa identificada ou identificável) ou pelos próprios titulares, como, por exemplo, por meio do acompanhamento de doenças através de aplicativos, de dispositivos vestíveis (como *smartwatches*) para o monitoramento do condicionamento físico, do rastreamento de alterações relevantes às condições médicas por meio de testes e através de postagens em redes sociais acerca dos efeitos colaterais de um novo tratamento ou dos cuidados em relação a certa doença.

Nos últimos anos, verifica-se uma explosão no número de aplicações e serviços voltados para a área de saúde, o que inclui, por exemplo, o uso de inteligência artificial para diagnósticos e predições[281][282]; softwares que fazem o acompanhamento e orientam o tratamento de doenças[283]; e aplicativos de controle menstrual[284] ou de cuidados

---

[280] Adriana Espíndola Corrêa chega a afirmar que "os dados que podem revelar os segredos da vida e as características de uma pessoa não estão na alma ou no subconsciente, mas no mapa genético". CORRÊA, Adriana Espíndola. O corpo digitalizado: um novo objeto para o direito. *Revista da Faculdade de Direito (UFPR)*, v. 44, p. 77-94, 2006. p. 78.

[281] Cf. TOPOL, Eric. High-performance medicine: the convergence of human and artificial intelligence. *Nature Medicine*, v. 25, p. 44-56, jan. 2019. *The Cloud, Data, And AI Imperative for Healthcare*. Hospital Readiness and Adoption Paths for Next-Generation Technologies. A Forrester Consulting Thought Leadership Paper Commissioned By IBM. Fevereiro de 2020.

[282] "Cresce também o uso da medicina de precisão (MP) fundada na incorporação de uma ampla variedade de dados coletivos e individuais, de conteúdos clínicos, de estilo de vida, genéticos, biométricos, racial ou étnico, que propiciam um novo paradigma no diagnóstico, prevenção e tratamento de doenças. [...] O paciente, parte vulnerável em vários aspectos, está exposto a inúmeros riscos diante da inteligência artificial, por isso, mister se faz proteger a sua autonomia, observar o seu consentimento, o que precisa ser equacionado com o eventual uso da inteligência artificial para fins decisórios. Além disso, ao paciente deve ser garantida a autodeterminação informativa, com adequada proteção dos seus dados pessoais e sensíveis; a igualdade no acesso ao melhor tratamento médico disponível e de forma ampla; a transparência". (SCHULMAN, Gabriel; PEREIRA, Paula Moura. Futuro da saúde e saúde do futuro: impactos e limites reais da inteligência artificial. In: TEPEDINO, Gustavo; GUIA, Rodrigo da. (Org.). *O Direito Civil na era da inteligência artificial.* São Paulo: RT, 2020, p. 165-182. p. 172-174.)

[283] Interessante recurso que vem sendo aplicado a partir dos nossos dados é o chamado *digital twins* (gêmeos digitais). O gêmeo digital é uma representação digital – por meio de software ou outro sistema computadorizado – de um ativo físico com o objetivo de monitorar, visualizar, simular, prever e tomar decisões sobre ele. Na área da saúde, o gêmeo digital de um órgão ou de um paciente pode ser utilizado para determinar qual procedimento deve ser seguido, tornando o tratamento mais específico e efetivo para ele. (Cf. RAO, Dattaraj Jagdish; MANE, Shraddha. Digital Twin approach to Clinical DSS with

durante a gravidez. A saúde tornou-se em vários aspectos um produto, havendo táticas cada vez mais agressivas para se coletar dados sensíveis dessa natureza. Por trás disso, há indústrias farmacêuticas, empresas de tecnologia[285], seguros, planos de saúde e estruturas de publicidade agindo para coletar mais e mais dados sensíveis e criar com isso perfis e segmentos, bem como campanhas que atinjam com maior eficiência seus atuais e futuros clientes.

O tratamento de dados de saúde também ocorre intensamente em âmbito público, por meio de instituições que regulam e tratam informações pessoais, como a Agência Nacional de Saúde Suplementar (ANS), o Ministério da Saúde, secretarias especializadas, hospitais públicos e médicos da rede pública. A ANS, na qualidade de agência reguladora, vem se dedicando à orientação do setor, como, por exemplo, por meio da edição da Nota Técnica nº 3/2019/GEPIN/DIRAD-DIDES/DIDES[286], que além de tratar em detalhe o tema da proteção de dados traz diretrizes para a adequação da

---

Explainable AI. 2019. Disponível em: <https://arxiv.org/ftp/arxiv/papers/1910/1910.13520.pdf>. Acesso em: 28 jun. 2021)

[284] A maioria desses aplicativos encoraja as usuárias a compartilharem muito mais do que as informações necessárias para o acompanhamento do ciclo menstrual. Dados como a dificuldade de atingir um orgasmo, medicamentos que usam regularmente, estado de humor, hábitos de masturbação, frequência de relações sexuais e, até mesmo, satisfação com a aparência são armazenados nos servidores das empresas e compartilhados com terceiros, que tratam e monetizam esse extenso banco de dados para variados fins.

[285] Como exemplo, recorda-se que a Google abriu uma grande frente relacionada à saúde: "Google Health is partnering with world-class clinical, public health and academic organizations to deploy solutions for transformative healthcare tools and services. Combining our partners' knowledge and experience, Google's technological expertise, and patient insights, we are able to conduct critical research and work towards advanced healthcare solutions for individuals, caregivers and health professionals. Through our collaborative efforts, we aim to bring emerging technologies to routine practice to realize Google Health's mission of improving the lives of all people." Disponível em: <https://health.google/partners/> Acesso em: 24.01.21.

[286] Na parte referente aos dados sensíveis, o documento dispõe que: "O tratamento de dados pessoais sensíveis que viole as regras de proteção à privacidade pode provocar danos materiais e morais ao seu titular. Em matéria de saúde, por exemplo, pelo conhecimento de certas doenças é possível, por exemplo, inferir sobre a sexualidade de um paciente. Essa inferência, acertada ou não, pode afetar suas relações familiares, seus relacionamentos íntimos e até mesmo sua vida profissional, especialmente no caso de pessoas públicas. No campo do trabalho, o conhecimento do empregador sobre o estado de saúde do empregado confere subsídios ao primeiro para o controle de custos dos recursos humanos. Identificados empregados doentes ou com hábitos prejudiciais à saúde, podem os empregadores desenvolver programas de promoção e proteção à saúde para melhorar a qualidade de vida de seus funcionários e, consequentemente, reduzir o índice de absenteísmo da mão de obra. Por outro lado, também é possível que essas informações sejam utilizadas de forma abusiva na gestão dos recursos humanos, seja pela negativa da contratação de mulheres grávidas e de candidatos cujo histórico médico aponte risco de absenteísmo, seja pela demissão de funcionários de maior risco de morbidade. Também há doenças estigmatizantes que submetem seus portadores à repulsa da sociedade como AIDS, a tuberculose e a hanseníase. Os casos citados por Anne Wells Branscomb ilustram como as vidas de pessoas infectadas pelo HIV podem ser devastadas pela revelação pública de suas condições." (p.05)

agência e da regulação da saúde suplementar à LGPD. [287] [288]

No Brasil, há o Sistema Único de Saúde (SUS), garantido pela Constituição Federal em seus artigos 196 e 198 e por meio da Lei nº 8.080/90, o qual atende todas as pessoas de forma gratuita. A rede que compõe o SUS é ampla e abrange tanto ações quanto serviços de saúde. Engloba a atenção primária, média e de alta complexidade, os serviços de urgência e emergência, a atenção hospitalar, as ações e serviços das vigilâncias epidemiológica, sanitária e ambiental e assistência farmacêutica.[289] Aqui, mostra-se relevante ressaltar o DATASUS: departamento de informática do Sistema Único de Saúde. Segundo informação institucional, o departamento é um grande provedor de soluções de software para as secretarias estaduais e municipais de saúde. Ele adapta os seus sistemas às necessidades dos gestores e incorpora novas tecnologias, na medida em que a descentralização da gestão se torna mais concreta.[290] Dentre outras atribuições e deveres, o DATASUS disponibiliza informações que podem servir para subsidiar análises objetivas da situação sanitária, tomadas de decisão baseadas em evidências e elaboração de programas de ações de saúde.[291] Em seu sistema, há importantes iniciativas como o Conecte SUS e a Rede Nacional de Dados em Saúde.

Informações, indicadores de saúde e orientações científicas devem ser a base para a formulação de políticas de saúde.[292] Entende-se que uma adequada política pública para os vários problemas de saúde enfrentados pela população – especialmente no atual momento pandêmico – necessita de uma estrutura de informações segura e confiável, que sustente e direcione as tomadas de decisão.[293] Para tanto, com a LGPD

---

[287] Disponível em: <http://www.ans.gov.br/sdcol/anexo/68347___Nota%20T%C3%A9cnica%20n%C2%BA%201_2019_CODAD_GEPIN_DIRAD-DIDES_DIDES.pdf> Acesso em: 24.01.21

[288] Não se pode deixar de mencionar também a Resolução normativa n° 443, de 25 de janeiro de 2019, a qual dispõe sobre adoção de práticas mínimas de governança corporativa, com ênfase em controles internos e gestão de riscos, para fins de solvência das operadoras de plano de assistência à saúde.

[289] Disponível em: <https://antigo.saude.gov.br/sistema-unico-de-saude> Acesso em: 26.02.21.

[290] Disponível em: <https://datasus.saude.gov.br/sobre-o-datasus/> Acesso em: 26.02.21.

[291] Disponível em: <http://www2.datasus.gov.br/DATASUS/index.php?area=02> Acesso em: 26.02.21.

[292] SOUZA, Maria de Fátima Marinho de. Dos dados à política: a importância da informação em saúde. *Epidemiol. Serv. Saúde*, Brasília, v.17, n.1, p. 5-6, mar. 2008. Disponível em: <http://scielo.iec.gov.br/scielo.php?script=sci_arttext&pid=S1679-49742008000100001&lng=pt&nrm=iso>. Acesso em: 21 jan. 2021.

[293] "Com relação à segurança dos dados, a principal limitação a ser enfrentada pelo sistema público de saúde brasileiro no atendimento à LGPD diz respeito à: a) ausência de uma política nacional única de segurança de dados de saúde; b) limitação de recursos orçamentários [desfinanciamento do SUS] para a adaptação de todos os sistemas informatizados mencionados às regras da LGPD. Como se trata de

em vigor, diversos protocolos e bancos de dados geridos pela Administração Pública deverão ser adequados à norma, para que se garanta seu uso regular e o desenvolvimento de políticas públicas e de ações mais eficientes e que atendam integralmente às necessidades da população.

Durante a pandemia, diversos vêm sendo os ataques cibernéticos e vazamentos de dados envolvendo instituições públicas e privadas que tratam em massa dados de saúde, como o Ministério da saúde[294], operadoras de planos de saúde e hospitais. Isso porque eles têm bancos de dados completos, atualizados e extensos sobre pacientes, bem como vasta quantidade de dados sensíveis armazenados. Conteúdo esse estratégico em razão, por exemplo, de poder ser facilmente negociado com terceiros ou usado como meio de obtenção de elevada quantia financeira por meio de chantagem.

A crescente proliferação de bancos de dados na área de saúde traz à tona a necessidade de se investir, em larga escala, em tecnologia e segurança da informação, uma vez que tais dados sensíveis apresentam ampla aplicação em setores científicos[295],

---

sistemas com diferentes finalidades, atributos técnicos e riscos, torna-se ainda mais dispendiosa a tarefa. Assim, o sistema público de saúde, acostumado a tratar milhares de bytes cotidianamente, terá de definir medidas de segurança que garantam o sigilo e o 'bom uso' dos dados coletados e armazenados em suas bases de Municípios, Estados e União; algo que até então só vem sendo feito, efetivamente, na interface entre SUS e a pesquisa. Tradicionalmente, os Comitês de Ética em Pesquisa (CEP) vinculados a instituições de ensino superior e a hospitais têm se constituído no único 'filtro' formalmente organizado relativo à manipulação de informações pessoais de saúde no país. As diretrizes éticas nacionais para pesquisas envolvendo seres humanos utilizadas pelos CEPs estão definidas na Resolução MS/CNS n° 466/201239. Ocorre que sua limitação deflui justamente de se tratar de normativa vinculada apenas à pesquisa, não diz respeito a outras ações e serviços disponibilizados pelo SUS e por seus prestadores privados. Oportuno consignar que o Plano Diretor de Tecnologia da Informação 2019/2021 do DATASUS cita a necessidade de implantar a LGPD no Ministério da Saúde por meio da preparação para compliance. Entretanto, não apresenta o modo como a operação será materializada. A meta de execução é de cumprimento de 75% das atividades programadas até 2021". (ARAGÃO, Suéllyn Mattos de; SCHIOCCHET, Taysa. Lei Geral de Proteção de Dados: desafio do Sistema Único de Saúde. *RECIIS - Revista Eletrônica de Comunicação, Informação e Inovação em Saúde*, Rio de Janeiro, v. 14, n. 3, p. 692-708, jul./set. 2020.)

[294] Informações disponíveis em: <http://www.conselho.saude.gov.br/ultimas-noticias-cns/1533-nota-publica-cns-pede-explicacoes-ao-ministerio-da-saude-sobre-vazamento-de-dados-de-pacientes-do-sus> <https://g1.globo.com/economia/tecnologia/noticia/2020/12/02/nova-falha-do-ministerio-da-saude-expoe-dados-de-243-milhoes-de-brasileiros-na-internet-diz-jornal.ghtml> Acesso em: 24.01.21.

[295] Recorda-se, aqui, a disposição do art. 13 da LGPD, a qual será melhor desenvolvida, em conjunto com as hipóteses de tratamento do Art. 11, no capítulo 3 da tese: "Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas. § 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais. § 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro. § 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da

industriais, empresariais, governamentais, bélicos e políticos. Deve-se, portanto, impedir acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, sob pena de haver o sancionamento do agente pela via judicial e por parte da Autoridade Nacional de Proteção de Dados (ANPD).

Além de se mostrar complexo, como apresentado, o setor da saúde conta com diversos agentes atuando direta e indiretamente. Ele impacta, em última instância, a qualidade de vida e o bem-estar das pessoas, sendo essencial tanto a sua regulação quanto a existência de instituições especializadas que zelem por boas práticas e ética profissional.

Neste setor, a área médica possui regulamentações próprias relativas ao sigilo profissional e à proteção das informações privadas dos pacientes, a exemplo do Código de Ética Médica e das Resoluções nº 1.821/07 e 2.218/18 do Conselho Federal de Medicina (CFM), que tratam de normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e o manuseio dos documentos dos prontuários dos pacientes. O tema do prontuário é ainda regulado pela Lei nº 13.787/18, que dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente.[296]

---

autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências. § 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro." Acerca do Art. 13, doutrina afirma: "(...)é permitido o tratamento desses dados para estudo em saúde pública, observadas certas restrições (LGPD, art. 13). Deve incidir o princípio da finalidade, ao determinar que o tratamento de dados se restrinja à finalidade do estudo. Em proteção à segurança dos dados, determina-se que o tratamento somente ocorra dentro do órgão, impõe-se o respeito a práticas de segurança previstas em regulamento específico e imputa-se ao órgão de pesquisa a responsabilidade pela segurança da informação, não permitida, em circunstância nenhuma, a transferência dos dados a terceiro. O tratamento deve respeitar os padrões éticos relacionados a estudos e pesquisas, como aqueles impostos por Códigos de Ética, princípios de Bioética, diretrizes internacionais e procedimentos impostos pelo Comitê de Ética em Pesquisa da instituição, ressalvado que o acesso a esses dados deve ser objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências." (MARTINS, Guilherme Magalhães; SOARES, Flaviana Rampazzo. Proteção de dados pessoais em e-saúde: seu confronto com a utilidade do fornecimento e uso de dados, em aplicativos para dispositivos móveis. *Revista de Direito do Consumidor*, vol. 130, jul.-ago / 2020.)

[296] Destacam-se, aqui, os artigos 4º e 6º: "Art. 4º Os meios de armazenamento de documentos digitais deverão protegê-los do acesso, do uso, da alteração, da reprodução e da destruição não autorizados. Parágrafo único. Os documentos oriundos da digitalização de prontuários de pacientes serão controlados por meio de sistema especializado de gerenciamento eletrônico de documentos, cujas características e requisitos serão especificados em regulamento. (...) Art. 6º Decorrido o prazo mínimo de 20 (vinte) anos a partir do último registro, os prontuários em suporte de papel e os digitalizados poderão ser eliminados. §1º Prazos diferenciados para a guarda de prontuário de paciente, em papel ou digitalizado, poderão ser fixados em regulamento, de acordo com o potencial de uso em estudos e pesquisas nas áreas das ciências

Prontuário Eletrônico do Paciente (PEP) é uma tecnologia utilizada para registro, armazenamento e controle digital das informações dos pacientes. Os registros indicam detalhes, que incluem histórico familiar, motivo da queixa inicial, diagnóstico e tratamento, além da prescrição de medicamentos, exames laboratoriais e outros detalhes vitais necessários para fornecer assistência a cada paciente.[297] Os consultórios médicos, clínicas e hospitais geralmente armazenam as informações de saúde dos pacientes em sistemas que possuem servidores em nuvem e criptografia. Além disso, o PEP deve receber a assinatura eletrônica do médico, por meio de um certificado digital.

A questão da confidencialidade e o sigilo dos dados são princípios basilares da ética em saúde. [298] O sigilo médico vem sendo recordado pelas leis brasileiras a fim de não expor a relação de confiança estabelecida entre o paciente e o profissional que o

---

da saúde, humanas e sociais, bem como para fins legais e probatórios. §2º Alternativamente à eliminação, o prontuário poderá ser devolvido ao paciente. §3º O processo de eliminação deverá resguardar a intimidade do paciente e o sigilo e a confidencialidade das informações. §4º A destinação final de todos os prontuários e a sua eliminação serão registradas na forma de regulamento."

[297] Menciona-se caso julgado em 2020, em que o Tribunal de Justiça de SP entendeu que o Hospital das Clínicas da Faculdade de Medicina de Botucatu teria de pagar R$ 5 mil por permitir acesso a prontuário médico de paciente sem autorização judicial ou situação legal de permissão. Conforme a ementa: "RESPONSABILIDADE CIVIL. PRONTUÁRIO MÉDICO. VIOLAÇÃO. Pretensão do autor à indenização a título de danos morais em face dos médicos e do Hospital das Clínicas de Botucatu. Ilegitimidade passiva dos médicos, que foi reconhecida por v. acórdão proferido por esta C. 13ª Câmara de Direito Público nos autos do agravo de instrumento nº 2258438-40.2019.8.26.0000. Prosseguimento do feito somente em relação ao Hospital das Clínicas de Botucatu. MMÉRITO. CABIMENTO DA INDENIZAÇÃO A SER PRESTADA PELO HOSPITAL EM RELAÇÃO AO AUTOR. Dano moral configurado. CONDUTA CULPOSA DO HOSPITAL. Médico, servidor público do Hospital das Clínicas de Botucatu, que atuou como perito judicial em ação no qual o ora autor ajuizou em face do INSS, a fim de pleitear benefício previdenciário. Posterior ajuizamento de ação de indenização pelo ora autor em face do referido médico, sob argumento de emissão de laudos periciais contraditórios. Médico que, em sua defesa e utilizando-se de seu cargo no Hospital das Clínicas de Botucatu, imprimiu cópia do prontuário do autor, que não é seu paciente, a fim de apresentá-lo, juntamente com sua defesa, na ação de indenização anteriormente ajuizada pelo autor. Inexistência de autorização do autor ou autorização judicial. Violação dos dados médicos sigilosos do autor e, consequentemente, de sua intimidade (art. 5º, inciso X da CF/88). Configurada culpa do Hospital das Clínicas de Botucatu, que não tomou as providências para restringir o acesso aos prontuários médicos de seus pacientes lançados em seu sistema. Comprovação da conduta omissiva do Hospital e do nexo causal entre a conduta e o dano moral. Responsabilidade civil subjetiva do Estado configurada (art. 37, §6º, CF). (...) RECURSO DE APELAÇÃO DO AUTOR PARCIALMENTE PROVIDO. (TJSP. Apelação nº 1003219-97.2019.8.26.0079. Rel. Des. Flora Maria Nesi Tossi Silva. Julgado em: 13 de novembro de 2020.)

[298] Código de Ética Médica (2019): É vedado ao médico: **Art. 73.** Revelar fato de que tenha conhecimento em virtude do exercício de sua profissão, salvo por motivo justo, dever legal ou consentimento, por escrito, do paciente. **Parágrafo único.** Permanece essa proibição: a) mesmo que o fato seja de conhecimento público ou o paciente tenha falecido; b) quando de seu depoimento como testemunha (nessa hipótese, o médico comparecerá perante a autoridade e declarará seu impedimento); c) na investigação de suspeita de crime, o médico estará impedido de revelar segredo que possa expor o paciente a processo penal. **Art. 74.** Revelar sigilo profissional relacionado a paciente criança ou adolescente, desde que estes tenham capacidade de discernimento, inclusive a seus pais ou representantes legais, salvo quando a não revelação possa acarretar dano ao paciente.

É vedado ao médico: Art. 85. Permitir o manuseio e o conhecimento dos prontuários por pessoas não obrigadas ao sigilo profissional quando sob sua responsabilidade.

atende. Nesse sentido, o Código de Processo Penal dispõe em seu artigo 207 que: "São proibidas de depor as pessoas que, em razão de função, ministério, ofício ou profissão, devam guardar segredo, salvo se, desobrigadas pela parte interessada, quiserem dar o seu testemunho". Dentro dessa questão, mostra-se ainda importante mencionar a Resolução do CFM nº 1.605/00, que traz questões sobre o consentimento do paciente e a proteção do conteúdo do prontuário ou ficha médica.

Como regra, o médico não pode, sem o consentimento do paciente, revelar o conteúdo do prontuário ou ficha médica. Nos casos do Art. 269 do Código Penal, onde a comunicação de doença é compulsória, o dever do médico restringe-se exclusivamente a comunicar tal fato à autoridade competente, sendo proibida a remessa do prontuário médico do paciente. Na investigação da hipótese de cometimento de crime, o médico está impedido de revelar segredo que possa expor o paciente a processo criminal. Apresenta polêmica, porém, o art. 4º da Resolução acima, que dispõe que: "Se na instrução de processo criminal for requisitada, por autoridade judiciária competente, a apresentação do conteúdo do prontuário ou da ficha médica, o médico disponibilizará os documentos ao perito nomeado pelo juiz, para que neles seja realizada perícia restrita aos fatos em questionamento."

Guilherme Nucci[299] posiciona-se contra a referida previsão, afirmando que o médico não deve enviar o prontuário do paciente ao juiz. Da mesma forma, se o médico não é obrigado a depor sobre seu paciente, não pode, também, mandar o prontuário/ficha clínica ao perito judicial, expondo seu paciente. Acima da resolução do CFM estaria a disposição do Código de Processo Penal. Tratando-se de autoria do crime (ou circunstâncias pessoais do agente, como personalidade, conduta social etc.), segundo ele, há de se preservar o sigilo médico. Por outro lado, cuidando-se de prova da materialidade do crime, o autor não concorda com a omissão do médico, em nome do sigilo, devendo ele enviar a ficha clínica ou prontuário a juízo (ou para instruir inquérito).

Entretanto, após decisão da 4ª Turma do Tribunal Regional Federal da 4ª Região, declarando ilegal o art. 4º da Resolução 1.605/2000 do CFM e o parágrafo primeiro do art. 89 da Resolução 1.931/2009, entendendo que os dispositivos, ao dispor que o prontuário e a ficha médica requisitados judicialmente sejam disponibilizados

[299] Disponível em: <https://www.conjur.com.br/2019-mai-05/guilherme-nucci-limites-sigilo-medico-fins-penais> Acesso em: 26 fev. 21.

apenas ao médico nomeado perito judicial, acabam por limitar a atuação do juiz no âmbito do processo judicial, foi publicada circular do CFM nº 16/2018 que orienta os profissionais médicos e os estabelecimentos de saúde a encaminharem à autoridade responsável os prontuários e fichas médicas (ou documentos médicos equivalentes), quando assim determinado pelo juiz competente, nos termos da decisão judicial.[300]

Acerca do assunto, recorda-se a recente Lei nº 14.289, de 3 de janeiro de 2022, que dispõe sobre a obrigatoriedade de preservação do sigilo sobre a condição de pessoa que vive com infecção pelos vírus da imunodeficiência humana (HIV), hepatites crônicas (HBV e HCV), hanseníase ou tuberculose. Dessa forma, fica vedada a divulgação pelos agentes públicos e privados de informações que permitam a identificação da condição de pessoa que vive com infecção pela HIV, hepatites crônicas, hanseníase e tuberculose, nos seguintes âmbitos: I - serviços de saúde; II - estabelecimentos de ensino; III - locais de trabalho; IV - administração pública; V - segurança pública; VI - processos judiciais; e VII - mídia escrita e audiovisual.

O sigilo profissional sobre a condição das pessoas acima somente poderá ser quebrado nos casos determinados por lei, por justa causa ou por autorização expressa da pessoa acometida ou, quando se tratar de criança, de seu responsável legal, mediante assinatura de termo de consentimento informado, observado o disposto no Art. 11 da LGPD. Entre outras disposições, a lei estabelece que os serviços de saúde, públicos e privados, e as operadoras de planos privados de assistência à saúde estão obrigados a proteger as informações relativas a essas pessoas, bem como a garantir o sigilo das informações que eventualmente permitam a identificação dessas condições. A obrigatoriedade de preservação do sigilo sobre a condição dessas pessoas recai sobre todos os profissionais de saúde e os trabalhadores da área de saúde. Ainda, nos inquéritos ou nos processos judiciais que tenham como parte pessoa que vive com

[300] "Conforme decisão judicial no processo nº 5009152-15.2013.4.04.7200/SC, quando o prontuário médico for solicitado pelo juiz, o documento deve ser entregue à autoridade judiciária e não ao perito nomeado. Neste sentido, o Acórdão do Tribunal Regional Federal da 4ª Região ordenou ao Conselho Federal de Medicina (CFM) e aos Conselhos Regionais de Medicina (CRMs) a não aplicação do artigo 4º da Resolução CFM nº 1.605/2000, ficando suspenso este dispositivo. A mesma decisão afastava, igualmente, o artigo 89, parágrafo 1º, do antigo Código de Ética Médica (Resolução CFM nº 1.931/2009), o qual possuía redação semelhante ao artigo 4º da Resolução CFM nº 1.605/2000. Essa última disposição já foi revogada, tendo sido substituída pela atual redação do artigo 89, parágrafo 1º, do atual Código de Ética Médica (Resolução CFM nº 2.217/2018), a qual está em consonância com a decisão judicial, determinando a entrega dos documentos médicos, se requisitados, ao próprio juízo requisitante." Disponível em: <https://portal.cfm.org.br/noticias/justica-federal-afasta-aplicabilidade-de-norma-sobre-prontuario-medico/> Acesso em: 19.02.22.

infecção pelo vírus da imunodeficiência humana, hepatites crônicas, hanseníase ou tuberculose devem ser providos os meios necessários para garantir o sigilo da informação sobre essa condição.

O descumprimento das disposições desta Lei sujeita o agente público ou privado infrator às sanções previstas no art. 52 da Lei nº 13.709/18, bem como às demais sanções administrativas cabíveis, e obriga-o a indenizar a vítima por danos materiais e morais. Nas situações em que for divulgada informação sobre as condições acima por agentes que, por força de sua profissão ou do cargo que ocupam, estejam obrigados à preservação do sigilo, e essa divulgação ficar caracterizada como intencional e com o intuito de causar dano ou ofensa, aplicar-se-ão em dobro: I - as penas pecuniárias ou de suspensão de atividades previstas no Art. 52 da LGPD; e II - as compensações pelos danos morais causados à vítima.

Outro tema de grande relevância quando se trata de dados de saúde é a Telemedicina[301], "gênero que reúne as diferentes práticas de atenção à saúde realizadas de maneira remota, inclusive consultas, diagnósticos, monitoramento de parâmetros de saúde – tais como pressão e temperatura. Pode envolver a oferta pré-assistencial e até mesmo a realização de procedimentos."[302] Ela é tratada, atualmente, dentro do Conselho Federal de Medicina, na Resolução nº 1.643/2002[303] e no ofício nº 1.756/2020, no qual o CFM decidiu, em caráter de excepcionalidade e enquanto durar o combate ao contágio da covid-19, reconhecer a possibilidade e a eticidade da utilização da telemedicina. Além disso, o regramento da telemedicina também se encontra previsto na portaria nº

[301] "A Telemedicina, por sua vez, está voltada aos aspectos clínicos direcionados ao paciente, individualizado ou individualizável, por meio de procedimentos médicos à distância destinados à medicina curativa. A tecnologia também possui o intuito de oferecer suporte diagnóstico de forma remota, permitindo, com apoio das tecnologias da informação e comunicação, a interpretação de exames e a emissão de laudos médicos à distância. Portanto, o objetivo é melhorar a qualidade e aumentar a eficiência do atendimento médico, expandindo-o às populações localizadas em áreas remotas, onde há pequeno número de profissionais especializados ou as condições da prática médica são limitadas." (JUNIOR, José Luiz de Moura Faleiros Junior, NOGAROLI, Rafaella. Telemedicina e proteção de dados: reflexões sobre a pandemia da COVID-19 e os impactos jurídicos da tecnologia aplicada à saúde. *Revista dos Tribunais*, vol. 1016, Jun./20)

[302] SCHULMAN, Gabriel. Tecnologias de telemedicina, Responsabilidade Civil e Dados Sensíveis. O princípio ativo da Proteção de Dados pessoais do paciente e os efeitos colaterais do coronavírus. *Coronavírus e Responsabilidade Civil.* Foco: Indaiatuba, 2020, p. 335-354.

[303] A norma pouco dispõe sobre proteção de dados pessoais, havendo referência ao tema em seu artigo 2º: "Os serviços prestados através da Telemedicina deverão ter a infraestrutura tecnológica apropriada, pertinentes e obedecer as normas técnicas do CFM pertinentes à guarda, manuseio, transmissão de dados, confidencialidade, privacidade e garantia do sigilo profissional." Todavia, na época em que foi publicada, o tema ainda não era tratado de forma específica nem havia tantas questões relativas à segurança da informação. Mais informações em: https://amb.org.br/noticias/amb/amb-e-cfm-debatem-nova-resolucao-para-a-telemedicina-em-reuniao-do-conselho-cientifico/ Acesso em: 24.01.21.

467/20[304] e na Lei nº 13.989/20, que dispõe sobre o uso da telemedicina durante a crise causada pelo coronavírus (SARS-CoV-2).[305] O tema na área médica desperta várias polêmicas, estando em discussão a elaboração de resolução específica para a prática, bem como de legislação.[306] Certamente, a experiência durante a pandemia e a entrada em vigor da LGPD vêm enriquecendo as discussões.

O uso da telemedicina apresenta uma série de benefícios ao ampliar o acesso à saúde; facilitar atendimentos, análises e acompanhamentos de pacientes; promover o intercâmbio de informações para diagnósticos, a prevenção e tratamento de doenças; e facilitar a contínua educação e pesquisa de prestadores de serviços da área da saúde. Contudo, verifica-se ainda alguma resistência, especialmente em âmbito médico, acerca de sua ampliação. Além disso, ela apresenta determinadas limitações impostas pelo atendimento não presencial e traz à tona diversas questões no que tange ao tratamento de dados sensíveis[307] e à segurança da informação[308].[309] Como apontado na Declaração

---

[304] Dispõe, em caráter excepcional e temporário, sobre as ações de Telemedicina, com o objetivo de regulamentar e operacionalizar as medidas de enfrentamento da emergência de saúde pública de importância internacional previstas no art. 3º da Lei nº 13.979/20, decorrente da epidemia de COVID-19.

[305] Art. 1º Esta Lei autoriza o uso da telemedicina enquanto durar a crise ocasionada pelo coronavírus (SARS-CoV-2). (...) Art. 3º Entende-se por telemedicina, entre outros, o exercício da medicina mediado por tecnologias para fins de assistência, pesquisa, prevenção de doenças e lesões e promoção de saúde.

[306] Recorda-se o PL 1998/2020, que autoriza e define a prática da telemedicina em todo o território nacional.

[307] "(...) são múltiplas as hipóteses de danos com os dados sensíveis de paciente na Telemedicina, inclusive, o uso não autorizado dos dados, invasões de privacidade, falhas de controle de nível de acesso. Questões como a responsabilidade das plataformas e aplicativos pelos dados e por compartilhamentos indevidos, falhas dos usuários em atualizar sistemas e certificados de segurança, perda de dados, níveis de segurança, portabilidade de informações, natureza jurídica de ataques hackers e condutas esperadas em caso de *ransomware* (sequestro de informações e com pedidos de resgate), ainda não estão claras o suficiente (...)". (SCHULMAN, Gabriel. Tecnologias de telemedicina, Responsabilidade Civil e Dados Sensíveis. O princípio ativo da Proteção de Dados pessoais do paciente e os efeitos colaterais do coronavírus. *Coronavírus e Responsabilidade Civil.* Foco: Indaiatuba, 2020, p. 335-354.)

[308] Para o transporte de dados mostra-se fundamental a utilização de padrões de criptografia e determinações claras das autorizações e níveis hierárquicos para o acesso às informações. Nesse sentido, na Diretriz da Sociedade Brasileira de Cardiologia sobre Telemedicina na Cardiologia (2019) consta a recomendação de utilização do padrão da HIPAA (Health Insurance Portability and Accountability Act of 1996), legislação norte americana que estabelece padrões específicos para proteção de dados na saúde e que serve de útil indicação para os profissionais brasileiros. Diretriz disponível em: <http://publicacoes.cardiol.br/portal/abc/portugues/2019/v11305/diretriz-da-sociedade-brasileira-de-cardiologia-sobre-telemedicina-na-cardiologia-2019.asp> Acesso em: 06.03.21 Em complemento, a *American Medical Association* estabeleceu diretrizes para atenção por Telemedicina e Telessaúde, tais como protocolos para integridade e segurança do paciente. Disponível em <https://www.ama-assn.org/press-center/press-releases/ama-adopts-new-guidance-ethical-practice-telemedicine> Acesso em: 06.03.21

[309] WEN, Chao Lung. Instituto de Estudos de Saúde Suplementar: Telemedicina do presente para o ecossistema de saúde conectada 5.0. Disponível em: <https://www.iess.org.br/cms/rep/Telemedicina_Chao.pdf> Acesso em: 26 fev. 21. EUROPEAN UNION. *Market study on telemedicine.* Luxembourg: Publications Office of the European Union, 2018.

de Tel Aviv sobre Telemedicina (Adotada pela 51ª Assembleia Geral da Associação Médica Mundial em Tel Aviv, Israel, em outubro de 1999): "Como em todos os campos da Medicina, a relação médico-paciente deve basear-se no respeito mútuo, na independência de opinião do médico, na autonomia do paciente e na confidencialidade profissional."

As inovações na maneira de prestar atenção à saúde da pessoa humana tornam necessário estabelecer fluxos internos, diretrizes e protocolos clínicos; treinar equipes; desenhar padrões organizacionais; e proteger de maneira adequada os dados pessoais, utilizando inclusive recursos técnicos e padrões internacionais para o trato de informações dessa natureza. O tema impacta diretamente clínicas, consultórios, plataformas virtuais de saúde, laboratórios, hospitais e médicos, os quais precisarão rever, integralmente, seus fluxos de tratamento de informações e promover medidas efetivas de proteção aos dados pessoais, especialmente quando sensíveis. [310]

Diante dos desafios enfrentados para a aplicação e ampliação da telemedicina, deve-se perseguir ativamente a efetivação dos direitos fundamentais, os quais na prática médica se associam aos princípios da ética médica, quais sejam, a autonomia, não-maleficência, beneficência, justiça e equidade, devendo prevalecer, pois, o princípio da prioridade do bem-estar do paciente. Nesse sentido, foi publicada em setembro de 2021 a Lei nº 14.198, que dispõe sobre videochamadas entre pacientes internados em serviços de saúde impossibilitados de receber visitas e seus familiares.

O contexto da COVID-19 torna, sem dúvida, justificável e necessário o emprego e incremento da telemedicina como mecanismo de acesso e atenção à saúde. Nesse novo ambiente, os deveres éticos e as boas práticas em medicina devem ser ainda mais realçados, inclusive em relação à concretização da autonomia e do direito à informação do paciente[311], diante da ampliação dos riscos e possíveis danos ao mesmo, na medida

[310] A respeito do consentimento na telemedicina, cf: KFOURI NETO, Miguel; NOGAROLI, Rafaella. Responsabilidade civil pelo inadimplemento do dever de informação na cirurgia robótica e telecirurgia: uma abordagem de direito comparado (Estados Unidos, União Europeia e Brasil). In: ROSENVALD, Nelson; MENEZES, Joyceane; DADALTO, Luciana (coords.). *Responsabilidade civil e medicina*. Indaiatuba: Foco, 2020. p. 159-185.

[311] Como decidiu o STJ: "3. O dever de informação é a obrigação que possui o médico de esclarecer o paciente sobre os riscos do tratamento, suas vantagens e desvantagens, as possíveis técnicas a serem empregadas, bem como a revelação quanto aos prognósticos e aos quadros clínico e cirúrgico, salvo quando tal informação possa afetá-lo psicologicamente, ocasião em que a comunicação será feita a seu representante legal. 4. O princípio da autonomia da vontade, ou autodeterminação, com base constitucional e previsão em diversos documentos internacionais, é fonte do dever de informação e do correlato direito ao consentimento livre e informado do paciente e preconiza a valorização do sujeito de

em que ocorre a expansão da circulação de dados e das possibilidades de acesso[312] e vazamentos de informações.[313]

2.2.3.1.1. Dados de saúde e a pandemia de COVID-19

Stefano Rodotà em "A Vida na Sociedade da Vigilância*:* a Privacidade Hoje" nos lembra que, em relação aos dados de saúde, "a proteção especial atribuída a estes dados não se justifica somente por se referirem a fatos íntimos, mas também, e às vezes sobretudo, pelo risco que seu conhecimento possa provocar

direito por trás do paciente, enfatizando a sua capacidade de se autogovernar, de fazer opções e de agir segundo suas próprias deliberações. 5. Haverá efetivo cumprimento do dever de informação quando os esclarecimentos se relacionarem especificamente ao caso do paciente, não se mostrando suficiente a informação genérica. Da mesma forma, para validar a informação prestada, não pode o consentimento do paciente ser genérico (*blanket consent*), necessitando ser claramente individualizado. 6. O dever de informar é dever de conduta decorrente da boa-fé objetiva e sua simples inobservância caracteriza inadimplemento contratual, fonte de responsabilidade civil *per se*. A indenização, nesses casos, é devida pela privação sofrida pelo paciente em sua autodeterminação, por lhe ter sido retirada a oportunidade de ponderar os riscos e vantagens de determinado tratamento, que, ao final, lhe causou danos, que poderiam não ter sido causados, caso não fosse realizado o procedimento, por opção do paciente. 7. O ônus da prova quanto ao cumprimento do dever de informar e obter o consentimento informado do paciente é do médico ou do hospital, orientado pelo princípio da colaboração processual, em que cada parte deve contribuir com os elementos probatórios que mais facilmente lhe possam ser exigidos. 8. A responsabilidade subjetiva do médico (CDC, art. 14, §4º) não exclui a possibilidade de inversão do ônus da prova, se presentes os requisitos do art. 6º, VIII, do CDC, devendo o profissional demonstrar ter agido com respeito às orientações técnicas aplicáveis. Precedentes. 9. Inexistente legislação específica para regulamentar o dever de informação, é o Código de Defesa do Consumidor o diploma que desempenha essa função, tornando bastante rigorosos os deveres de informar com clareza, lealdade e exatidão (art. 6º, III, art. 8º, art. 9º).” (STJ. REsp 1.540.580, Rel. Min. Lázaro Guimarães (Desembargador Convocado do TRF 5ª Região), 4a. Turma, DJe 04/09/2018)

[312] “No que tange a autorização paciente, entre as formas de violação dos dados do paciente está a revelação indevida de dados clínicos, tais como resultados de exames, suspeitas de determinados quadros, assim como o tratamento destes dados sem o consentimento do paciente. É preciso também atentar para a hipótese de compartilhamento de dados do paciente com a finalidade distinta ao propósito do consentimento outorgado pelo paciente. Merecem atenção também o tratamento de forma inadequada, como a situação em que há circulação de dados com baixo nível de segurança, sem uso de criptografia, com falhas na organização de níveis de acesso. ou, ainda, a falta de mecanismos de controle para a gestão de dados por colaboradores e/ou outros, quando o consentimento para seu uso for revogado pelo paciente.” (SCHULMAN, Gabriel; CAVET, Caroline Amadori. As violações de dados pessoais na telemedicina: tecnologia, proteção e reparação ao paciente 4.0. In: *Debates Contemporâneos em Direito Médico e da Saúde.* São Paulo, RT, 2020. p. 145-174.)

[313] Neste cenário, vêm ganhando expressividade no mercado brasileiro as *startups* voltadas ao setor da saúde: as *healthtechs*.“Entre outras categorias, as *healthtechs* trazem soluções tanto para o relacionamento com pacientes quanto para exames laboratoriais, terapias digitais, telemedicina, *wearables* (tecnologias vestíveis), gestão clínica e hospitalar, prontuário eletrônico, entrega de medicamentos etc.” (POMPEU, Márcio. A LGPD como condição para as *healthtechs* captarem investimentos. Conjur, publicado em 11 de março de 2021. Disponível em: <https://www.conjur.com.br/2021-mar-11/pompeu-lgpd-condicao-healthtechs-captarem-investimentos#_ftn1> Acesso em: 17 de março de 2021.

discriminações"[314]. No cenário de combate à pandemia de COVID-19[315], tratamentos em massa de dados sensíveis e ferramentas tecnológicas de vigilância foram amplamente utilizados por agentes públicos e privados. Todavia, a falta de transparência, informação e segurança no trato dessas informações foi denunciada por diversos especialistas. [316]

Logo em março de 2020[317], afirmou o *European Data Protection Board*[318] que as normas de proteção de dados não impediriam eventuais medidas tomadas na luta contra a pandemia de coronavírus. Todavia, sublinhou que, mesmo em momentos excepcionais, os agentes deveriam garantir a proteção dos dados pessoais que tratassem. Além disso, qualquer medida tomada deveria respeitar os princípios gerais do Direito, ser proporcional e limitada ao período de emergência e não ser irreversível. Em seguida, a Autoridade de proteção de dados do Reino Unido (*Information Commissioner's Office* - ICO) publicou uma série de documentos com orientações tanto para os titulares dos dados quanto para os agentes de tratamento. [319]

Não obstante o intenso tratamento de dados de saúde, no início da pandemia no Brasil não se dispunha de uma lei geral para a proteção de dados. Recorda-se que a Lei nº 13.979/20[320], chamada lei da pandemia, trouxe importantes questões relativas a tratamentos de saúde e de dados pessoais. Em seu artigo 3º, encontra-se disposto que,

---

[314] RODOTÀ, Stefano. A vida na sociedade da vigilância - a privacidade hoje. Coord. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p.106.

[315] Segundo fonte oficial, até 19 de fevereiro de 2022, havia 28.072.238 casos de COVID-19 notificados no Brasil e 643.340 óbitos. Em termos percentuais, no que concerne à população totalmente vacinada no país, temos 72,5%, sendo no momento administrada, inclusive, dose de reforço. Fonte: Our World In Data.

[316] Cf. TEFFÉ, Chiara Spadaccini de. A saúde na sociedade da vigilância: como proteger os dados sensíveis? *Migalhas*. Publicado em: 14 abr. 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-vulnerabilidade/324485/a-saude-na-sociedade-da-vigilancia-como-proteger-os-dados-sensiveis. Acesso em: 31 maio 2020. MEDEIROS, M. S. de; BORGES, L.; FILHO, J. E. T. ; LUCENA, R. C. B. de . Limites e contradições do uso de tecnologias digitais em saúde no contexto da pandemia da COVID-19 no Brasil. *Serviço Social e Saúde*, Campinas, SP, v. 20, n. 00, p. e021002, 2021. DOI: 10.20396/sss.v20i00.8665391. Disponível em: https://periodicos.sbu.unicamp.br/ojs/index.php/sss/article/view/8665391. Acesso em: 3 jan. 2022.

[317] Em 11 de março de 2020, Tedros Adhanom, diretor geral da Organização Mundial de Saúde (OMS), declarou que a organização elevou o estado da contaminação à pandemia de Covid-19, doença causada pelo novo coronavírus (Sars-Cov-2). Disponível em: <https://www.unasus.gov.br/noticia/organizacao-mundial-de-saude-declara-pandemia-de-coronavirus> Acesso em: 20.01.21.

[318] Disponível em: <https://edpb.europa.eu/our-work-tools/our-documents/outros/statement-processing-personal-data-context-covid-19-outbreak_pt> Acesso em: 20.01.21.

[319] Disponível em: <https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/> Acesso em: 26 fev. 21.

[320] Dispõe sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019.

para o enfrentamento da emergência de saúde pública decorrente do coronavírus, as autoridades poderão adotar, no âmbito de suas competências, dentre outras, as seguintes medidas: "(...) III - determinação de realização compulsória de: a) exames médicos; b) testes laboratoriais; c) coleta de amostras clínicas; d) vacinação e outras medidas profiláticas; ou e) tratamentos médicos específicos; (...)". A norma em comento respaldou-se no poder de polícia, que garante à Administração Pública a prerrogativa de exercer o seu poder com a implementação de restrições à liberdade das pessoas, na forma da legislação vigente.[321][322]

Em um ordenamento que tem como princípio a solidariedade social, mostra-se necessário compreender que há circunstâncias que podem relativizar espaços de liberdade pessoal, não podendo ato de autonomia corporal ser exercido de forma abusiva ou arbitrária, implicando grave lesão ou risco à coletividade.[323] Isso não significa, contudo, legitimar uma flexibilização desproporcional do direito ao próprio corpo ou do direito à proteção de dados pessoais. As relações de prevalência entre interesses privados e públicos não comportam determinações *a priori* e em caráter abstrato, devendo ser analisadas dentro do sistema constitucional e por meio de

[321] "Em diversos casos, a tutela psicofísica não pode inspirar-se apenas no aspecto subjetivo do consentimento do sujeito. Podem-se encontrar justificativas para tratamento sanitário, independentemente da vontade do doente, quando, por exemplo, o estado de saúde do indivíduo contenha em si potencialidade para lesar terceiros. Há, em tal caso, interesse público a ser protegido." (BODIN DE MORAES, Maria Celina. *Na medida da pessoa humana: Estudos de direito civil-constitucional*. Rio de Janeiro: Renovar, 2010. p.178.)

[322] Não é novidade no país a constatação de situações emergenciais, no âmbito da saúde pública, que exigiram medidas restritivas aos direitos à liberdade e autonomia privada. Vale recordar, por exemplo, a Revolta da Vacina ocorrida em 1904 no Rio de Janeiro e as medidas sanitárias tomadas pelo governo a fim de combater doenças graves. Em 2010, foi elaborado o Plano Brasileiro de Preparação para Enfrentamento de uma Pandemia de Influenza e foram adotadas medidas preventivas e repressivas para garantia de saúde pública em razão da H1N1. A lei 13.301/16 dispôs sobre a adoção de medidas de vigilância em saúde quando verificada situação de iminente perigo à saúde pública pela presença do mosquito transmissor do vírus da dengue, do vírus chikungunya e do vírus da zika. Além disso, alguns diplomas legais estabelecem a possibilidade de interdição voluntária de pessoas, com a restrição à liberdade pessoal em favor da proteção da saúde, como a lei 10.216/01 que prevê a internação involuntária das pessoas portadoras de transtornos mentais e a lei 11.343/06, que admite, em seu art. 23-A, § 3º, II, e § 5º, a internação involuntária dos dependentes de drogas. Fonte: OLIVEIRA, Rafael Carvalho Rezende. Direito Administrativo e coronavírus. *Migalhas*, 17 de março de 2020. Fonte: <https://www.migalhas.com.br/depeso/321892/direito-administrativo-e-coronavirus> Acesso em: 13.04.20.

[323] PERLINGIERI, Pietro. *Perfis do Direito Civil. Introdução ao Direito Civil Constitucional.* Rio de Janeiro: Editora Renovar, 2007. p. 120-121. DALSENTER, Thamis. Direito à saúde entre a liberdade e a solidariedade: os desafios jurídicos do combate ao novo coronavírus – COVID-19. *Migalhas*, 05 de março de 2020. Fonte: <https://www.migalhas.com.br/coluna/migalhas-de-vulnerabilidade/321211/direito-a-saude-entre-a-liberdade-e-a-solidariedade-os-desafios-juridicos-do-combate-ao-novo-coronavirus-covid-19> Acesso em: 13.04.20.

ponderações que envolvam direitos fundamentais e metas coletivas da sociedade.[324]

Seguindo, o artigo 6º da Lei nº 13.979 afirma que é obrigatório o compartilhamento, entre órgãos e entidades da administração pública federal, estadual, distrital e municipal, de *dados essenciais à identificação* de pessoas infectadas ou com suspeita de infecção pelo coronavírus, com a finalidade exclusiva de evitar a sua propagação, não havendo, porém, na lei, esclarecimentos sobre quais seriam esses dados e se, em seu bojo, estariam incluídos dados sensíveis. Além disso, a mencionada obrigação se estendeu às pessoas jurídicas de direito privado, quando os dados forem solicitados por autoridade sanitária. Dessa forma, empresas de transporte aéreo ou rodoviário devem comunicar informações pessoais requeridas pelas autoridades sanitárias, assim como hospitais privados e empregadores podem ser acionados para comunicar dados relativos a clientes e empregados que se encontrem nessas condições.

Diante dos parâmetros da autodeterminação informativa e do direito à proteção de dados pessoais muito se questionou: quais seriam os limites para a aplicação dessas normas? Até onde o interesse coletivo pode avançar sobre o individual? A relevância de se monitorar o número de infectados, as taxas de mortalidade e a ocupação dos hospitais mostra-se indiscutível para o controle da pandemia, porém, até que ponto, o controle exercido pode adentrar nossos corpos e dados? É preciso que a sociedade tenha uma visão crítica sobre essas estratégias e sobre as necessidades efetivas de

[324] Em dezembro de 2020, o STF entendeu que o Estado poderia determinar que a vacinação da população fosse obrigatória, inclusive contra a Covid-19, sendo afastadas medidas invasivas como, por exemplo, o uso da força para exigir a imunização. Afirmou-se que: "A vacinação compulsória não significa vacinação forçada, porquanto facultada sempre a recusa do usuário, podendo, contudo, ser implementada por meio de medidas indiretas, as quais compreendem, dentre outras, a restrição ao exercício de certas atividades ou à frequência de determinados lugares (...)". Na ocasião, foram analisadas duas ações diretas de inconstitucionalidade e um recurso extraordinário (ADIs 6.586 e 6.587 e ARE 1.267.879). Prevaleceram os entendimentos dos relatores, ministros Ricardo Lewandowski e Luís Roberto Barroso. A tese fixada, de repercussão geral, foi a seguinte: "É constitucional a obrigatoriedade de imunização por meio de vacina que, registrada em órgão de vigilância sanitária, (i) tenha sido incluída no programa nacional de imunizações; (ii) tenha sua aplicação obrigatória determinada em lei; (iii) seja objeto de determinação da união, estados e municípios, com base em consenso médico científico. Em tais casos, não se caracteriza violação à liberdade de consciência e de convicção filosófica dos pais ou responsáveis, nem tampouco ao poder familiar". Um ano depois, em dezembro de 2021, foi protocolada a ADPF 929, tendo como objeto ato da secretaria extraordinária de enfrentamento à covid-19, que determinou a realização da Consulta Pública SECOVID/MS nº 1, a partir de 23 de dezembro de 2021 até 02 de janeiro de 2022, acerca da vacinação contra a Covid-19 das crianças de 5 a 11 anos e a omissão do Poder Executivo Federal – União Federal, por não determinar a imediata vacinação de crianças e adolescentes. Em janeiro de 2022, foi iniciada a vacinação de crianças entre 05 e 11 anos.

monitoramento que expõem a privacidade e as informações das pessoas.[325] Embora tais medidas objetivem a tutela emergencial da saúde pública, é evidente o conflito entre a busca por maximizar a efetividade das políticas de vigilância, ainda que em prol do interesse público, com os limites estabelecidos por direitos e valores fundamentais, como a privacidade e a proteção de dados pessoais.[326]

Apesar dos diversos benefícios apresentados pela LGPD e pelas políticas que buscam a sua efetividade, no momento ainda se percebe baixa adequação das instituições à lei, bem como um aumento significativo de ataques cibernéticos e de vazamentos de dados. A LGPD toma corpo em um momento extremamente delicado para a sociedade: a pandemia de COVID-19.[327] Diante desse cenário, o debate em torno de tecnologias de vigilância e segurança, como reconhecimento facial, drones, *contact tracing* e mapas de calor, que tratam e utilizam bancos de dados sensíveis, tornou-se ainda mais importante, trazendo novas preocupações para os titulares dos dados e organizações públicas e privadas.

---

[325] Nesse sentido, vale recordar dois documentos do *European Data Protection Board* (EDPB): a) Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak; e b) Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak. Disponível em: <https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_en>Acesso em: 26.02.2021

[326] GABRIEL, Anderson de Paiva. TEFFÉ, Chiara Spadaccini de. Ferramentas tecnológicas e controle da pandemia. *Jota*, Rio de Janeiro, 14 jun. 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/juiz-hermes/ferramentas-tecnologicas-e-controle-da-pandemia-14062020> Acesso em: 31 jul. 2020. PAVÃO, Juliana Carvalho; ESPOLADOR, Rita de Cássia Resquetti Tarifa. A proteção de dados clínicos durante a pandemia da COVID-19: comentários à luz dos direitos da personalidade e dos referenciais bioéticos. *SCIENTIA IURIS*, Londrina, v. 25, n. 3, p. 125-140, nov. 2021. DOI: 10.5433/21788189.2021v25n3p125. Acesso em: 03 jan. 2022.

[327] "Ainda que tais medidas objetivem a tutela emergencial da saúde pública, é evidente o conflito entre a busca por maximizar a efetividade das políticas de vigilância, ainda que em prol do interesse público, com os limites estabelecidos por direitos e valores fundamentais como a privacidade e a proteção de dados pessoais. A *vexata quaestio* concerne à harmonização dos diversos direitos e interesses em jogo. Em nome da segurança e do interesse público, quais tipos de intervenções e ferramentas tecnológicas podem ser legitimamente implementadas? Como garantir que o banco de dados desenvolvido para a tutela da saúde da população não será direcionado a finalidades diversas e nem de longe tão nobres? Quais parâmetros normativos deverão ser usados para analisar os tratamentos de dados realizados tanto pelo setor público quanto pelo privado? Sem dúvidas, a desenfreada instituição de rígidos sistemas de controle sobre nossos corpos e dados, por meio de mecanismos de vigilância, irá influenciar sobremaneira o futuro da humanidade." (GABRIEL, Anderson de Paiva; TEFFÉ, Chiara Spadaccini de. Ferramentas tecnológicas e controle da pandemia. *Jota*, Rio de Janeiro, 14 jun. 2020.)

2.2.3.2 Dados genéticos

Os avanços na tecnologia genética e nos estudos sobre o genoma humano e o mapeamento genético têm implicações importantes para a saúde e o bem-estar dos indivíduos, ajudando os pesquisadores a compreender, prevenir e tratar diversas doenças, predisposições e características de ordem genética. Os testes genéticos para avaliar os riscos à saúde ou para determinar as relações biológicas levantam questões, porém, que afetam não apenas a privacidade e a proteção de dados de um indivíduo, mas também de grupos, visto que nossa composição genética é compartilhada, por exemplo, por outros membros da família.

A pesquisa genética abriu caminho para pesquisas médicas de longo alcance e aplicações biomédicas. Os dados genéticos podem ser usados para diagnóstico médico, prevenção de doenças e estudos de genética populacional. Como a herança genética de cada pessoa é específica, a ciência forense e o sistema judicial também utilizam tais dados para fins de identificação. Em consequência disso, o número de bancos de dados genéticos vem aumentando, sendo mantidos inclusive em nível nacional, como a Rede Integrada de Bancos de Perfis Genéticos (RIBPG), que se destina a subsidiar a apuração criminal e a identificação de pessoas desaparecidas.[328]

No Recurso Extraordinário 973.837, relatado pelo Min. Gilmar Mendes, debate-se a constitucionalidade da inclusão e manutenção de perfil genético de condenados por crimes violentos ou por crimes hediondos em banco de dados estatal. Discute-se, à luz do princípio da não autoincriminação e do Art. 5º, II, da Constituição Federal, a constitucionalidade do Art. 9º-A da Lei 7.210/1984, introduzido pela Lei 12.654/2012, que prevê a identificação e o armazenamento de perfis genéticos de condenados por

[328] "A lei nº 12.654/2012, de 28 de maio de 2012, determina que as informações genéticas contidas nos bancos de dados de perfis genéticos não poderão revelar traços somáticos ou comportamentais das pessoas, exceto determinação genética de gênero. De fato, o perfil genético é obtido a partir de regiões não-codificantes do DNA, sendo incapaz de revelar qualquer característica física ou de saúde. A única aplicação é a individualização. Os bancos de dados de perfis genéticos têm caráter sigiloso, sendo o acesso restrito e controlado. Desta forma, o administrador responde civil, penal e administrativamente caso permita ou promova a utilização dos bancos de perfis genéticos para fins diversos dos previstos em lei ou em decisão judicial. Os Administradores dos Bancos de Perfis Genéticos (BPG), dentre outras atribuições, zelam pela segurança e pela qualidade das informações armazenadas. A fim de garantir o sigilo, são utilizados dados dissociados do indivíduo, ou seja, dados não associados a uma pessoa identificável." (XIV Relatório da Rede Integrada de Bancos de Perfis Genéticos (Maio/2021). Disponível em: <https://www.justica.gov.br/sua-seguranca/seguranca-publica/ribpg/relatorio> Acesso em: 11.07.21.)

crimes violentos ou por crimes hediondos.[329] Adicionalmente, cabe indagar a compatibilidade de tal tratamento de dados genéticos com a LGPD e as salvaguardas que ela oferece à categoria dos dados sensíveis.

Neste campo, muitas pessoas temem que os dados genéticos sejam usados para fins contrários aos direitos humanos e às liberdades fundamentais. Já se verificou que o uso inadequado dessas informações pode acarretar discriminações ilícitas ou abusivas em face de seu titular, como também sua estigmatização, trazendo-lhe consequências tanto em âmbito familiar quanto profissional e social. Por tal razão, deve-se proteger de forma ampliada e diferenciada a intimidade genética e se garantir ao indivíduo a possibilidade de recusar a análise genética como regra.

De acordo com doutrina, é possível afirmar que:

> Os dados genéticos são únicos, pois apresentam informações genéticas do ser enquanto espécie. São estruturais por guardarem características especiais de um indivíduo diferenciando-o dos outros, tornando-o singular. São probabilísticos por apresentarem, de forma aproximada, as possibilidades do desenvolvimento de alguma enfermidade. E, por fim, são geracionais por informar a herança genética do indivíduo e a sua interligação genética com seus parentes. (HAMMERSCHMIDT, 2005, p. 17-20). Dados genéticos humanos podem gerar caracterizações sociais discriminatórias, com a distinção de indivíduos cuja análise genética identificou a possibilidade do desenvolvimento de doenças genéticas do restante da sociedade, sendo exemplo plausível o requerimento da análise genética para que o indivíduo exerça certa profissão ou assuma determinado cargo.[330]

---

[329] Dispõe o Art. 9º-A que: "Os condenados por crime praticado, dolosamente, com violência de natureza grave contra pessoa, ou por qualquer dos crimes previstos no art. 1º da Lei nº 8.072, de 25 de julho de 1990, serão submetidos, obrigatoriamente, à identificação do perfil genético, mediante extração de DNA - ácido desoxirribonucleico, por técnica adequada e indolor. § 1º A identificação do perfil genético será armazenada em banco de dados sigiloso, conforme regulamento a ser expedido pelo Poder Executivo. § 1º-A. A regulamentação deverá fazer constar garantias mínimas de proteção de dados genéticos, observando as melhores práticas da genética forense. § 2º A autoridade policial, federal ou estadual, poderá requerer ao juiz competente, no caso de inquérito instaurado, o acesso ao banco de dados de identificação de perfil genético. § 3º Deve ser viabilizado ao titular de dados genéticos o acesso aos seus dados constantes nos bancos de perfis genéticos, bem como a todos os documentos da cadeia de custódia que gerou esse dado, de maneira que possa ser contraditado pela defesa. § 4º O condenado pelos crimes previstos no **caput** deste artigo que não tiver sido submetido à identificação do perfil genético por ocasião do ingresso no estabelecimento prisional deverá ser submetido ao procedimento durante o cumprimento da pena. § 5º (VETADO). § 6º (VETADO). § 7º (VETADO). § 8º Constitui falta grave a recusa do condenado em submeter-se ao procedimento de identificação do perfil genético." O perfil genético extraído destes indivíduos será armazenado no Banco Nacional de Perfis Genéticos (BNPG). O BNPG foi instituído pelo Decreto nº 7.950/2013, responsável também por criar a Rede Integrada de Bancos de Perfis Genéticos (RIBPG), que "surgiu da iniciativa conjunta do Ministério da Justiça e Segurança Pública e das Secretarias de Segurança Pública Estaduais tendo por objetivo propiciar o intercâmbio de perfis genéticos de interesse da Justiça, obtidos em laboratórios de perícia oficial." Disponível: <https://www.justica.gov.br/sua-seguranca/seguranca-publica/ribpg> Acesso em: 30.06.21.

[330] TORQUATO-DE-OLIVEIRA-NAVES, Bruno; GOIATA, Sarah Rêgo. Direitos Humanos, patrimônio genético e dados genéticos humanos: crítica à doutrina dos dados genéticos como interesse difuso. *Rev.*

Em 1997, foi publicada a Declaração Universal do Genoma Humano e dos Direitos Humanos. Logo após, em 2003, a Declaração Internacional sobre Dados Genéticos Humanos[331], que dispõe que eles apresentam um *status* especial porque: (i) podem informar predisposições genéticas de indivíduos; (ii) podem ter um impacto significativo na família, incluindo a descendência, estendendo-se por gerações e, em alguns casos, por todo o grupo ao qual a pessoa pertence; (iii) podem conter informações relevantes cujo significado não seja necessariamente conhecido no momento da coleta das amostras biológicas; e (iv) podem ter significado cultural para pessoas ou grupos. Por essas razões, segundo a Declaração, deve ser dada a devida consideração à sensibilidade dos dados genéticos humanos, bem como ser estabelecido um nível apropriado de proteção para essas informações.

Outro ponto relevante é que as análises genéticas, por mais que se refiram à pessoa do titular dos dados, acabam ultrapassando a esfera individual, podendo recair em interesses de terceiros e em conflitos éticos. Por exemplo, imagine-se uma situação em que o titular dos dados não permite estudos a partir de suas informações genéticas, mas seus familiares demandam tomar conhecimento de eventuais doenças que tenham propensão. No mesmo caso, e se o cônjuge do titular do dado desejar que ele realize testes visando a ter ciência da futura carga genética de seus (possíveis) descendentes? Pessoas (jurídicas ou naturais) com quem o titular tenha algum tipo de vínculo podem solicitar acesso a dados genéticos ou a testes específicos relacionados? Essa questão mostra-se notadamente preocupante no ambiente de trabalho e na contratação de seguros e planos de saúde. Caso tal solicitação envolvesse a investigação de um crime, seria ela plausível em alguma medida? Por fim, quais devem ser os princípios e limites da pesquisa genética?

A Constituição Portuguesa consagra que "A lei garantirá a dignidade pessoal e a identidade genética do ser humano, nomeadamente na criação, desenvolvimento e utilização das tecnologias e na experimentação científica" (Art. 26º, item 3). No Brasil, ao tratar da identidade genética, decidiu o STF pela impossibilidade de óbices ao exercício do direito fundamental à busca da identidade genética:

Bioética y Derecho, Barcelona, n. 40, p. 63-81, 2017. Disponível em: <http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872017000200006&lng=es&nrm=iso>. Acesso em: 03.03. 2021.

[331] Disponível em: <http://portal.unesco.org/en/ev.php-URL_ID=17720&URL_DO=DO_TOPIC&URL_SECTION=201.html>. Acesso em: 03.03. 2021.

> (...) no núcleo essencial da dignidade da pessoa humana há de ser tido como presente o direito fundamental à identidade pessoal do indivíduo, que se desdobra, dentre outros aspectos, na identidade genética. A inserção de cada pessoa no mundo, para que possa realizar todas as suas potencialidades, é feita em função de sua história, projetando a autoimagem e a identidade pessoal a partir de seus dados biológicos inseridos em sua formação, advindos de seus progenitores. É com o conhecimento do estado de filiação que se fincam as premissas da atribuição à pessoa humana de reconhecimento e de distinção no cenário social, permitindo sua autodeterminação no convívio com os iguais[332].

A LGPD não apresenta definição para os dados genéticos, porém, o polêmico Decreto nº 10.046/19[333]-[334], em seu Art. 2º, IV, define atributos genéticos como "características hereditárias da pessoa natural, obtidas pela análise de ácidos nucleicos ou por outras análises científicas". Longe de apresentar definição completa para a categoria em questão, mostra-se relevante utilizar a experiência estrangeira na temática.

De acordo com o considerando 34 do GDPR, os dados genéticos deverão ser definidos como os dados relativos às características genéticas, hereditárias ou adquiridas de uma pessoa que resultem da análise de uma amostra biológica da mesma, nomeadamente da análise de cromossomas, ácido desoxirribonucleico (ADN) ou ácido ribonucleico (ARN) ou da análise de um outro elemento que permita obter informações equivalentes. Em seguida, no Art. 4º, 13, da norma europeia, dispõe-se que os dados

---

[332] STF. RE 363.889 DF, Rel. Min. Dias Toffoli, Tribunal Pleno, DJe: 16.12.2011. Trecho da ementa: "1. É dotada de repercussão geral a matéria atinente à possibilidade da repropositura de ação de investigação de paternidade, quando anterior demanda idêntica, entre as mesmas partes, foi julgada improcedente, por falta de provas, em razão da parte interessada não dispor de condições econômicas para realizar o exame de DNA e o Estado não ter custeado a produção dessa prova. 2. Deve ser relativizada a coisa julgada estabelecida em ações de investigação de paternidade em que não foi possível determinar-se a efetiva existência de vínculo genético a unir as partes, em decorrência da não realização do exame de DNA, meio de prova que pode fornecer segurança quase absoluta quanto à existência de tal vínculo. 3. Não devem ser impostos óbices de natureza processual ao exercício do direito fundamental à busca da identidade genética, como natural emanação do direito de personalidade de um ser, de forma a tornar-se igualmente efetivo o direito à igualdade entre os filhos, inclusive de qualificações, bem assim o princípio da paternidade responsável. 4. Hipótese em que não há disputa de paternidade de cunho biológico, em confronto com outra, de cunho afetivo. Busca-se o reconhecimento de paternidade com relação a pessoa identificada. (...)"
Sobre o tema, cf. BARBOZA, Heloisa Helena Gomes. A proteção da identidade genética. In: Agassiz Almeida Filho; Plínio Melgaré. (Org.). *Dignidade da pessoa humana. Fundamentos e critérios interpretativos*. São Paulo: Malheiros Editores Ltda, 2010. p. 83-100. MORAES, Maria Celina Bodin de. Recusa à realização do exame de DNA e direitos da personalidade, In: *Na medida da pessoa humana*. Estudos de direito civil constitucional, Rio de Janeiro: Ed. Renovar, 2010.

[333] Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.

[334] Em janeiro de 2021, o Conselho Federal da Ordem dos Advogados do Brasil ajuizou, no Supremo Tribunal Federal, a Ação Direta de Inconstitucionalidade 6649, contra o Decreto 10.046/2019 da Presidência da República. A ação foi distribuída, por prevenção, ao ministro Gilmar Mendes, relator da Arguição de Descumprimento de Preceito Fundamental 695, que questiona o mesmo decreto. Disponível em: <http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=459125> Acesso em: 27.02.21.

genéticos são os dados pessoais relativos às características genéticas, hereditárias ou adquiridas de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa e que resultem designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa.[335] [336]

Acerca do tema e suas questões, vale recordar também a Lei de Não Discriminação de Informações Genéticas (GINA) de 2008, que protege os norte-americanos de discriminações com base em suas informações genéticas tanto na área do seguro saúde quanto em relações de emprego. Dessa forma, por exemplo, a lei proíbe discriminações com base em informações genéticas quando se tratar de qualquer aspecto relacionado ao emprego, incluindo contratação, demissão, pagamento, atribuições de trabalho, promoções, dispensas, treinamento, benefícios adicionais ou qualquer outro termo ou condição de emprego.[337] Ainda que a LGPD apresente o princípio da não discriminação, com base na experiência acima, seria relevante um cuidado mais específico na legislação a respeito dos dados genéticos.

---

[335] Disponível em: <https://geneticdataprotection.com/>. Acesso em: 03.03. 2021.

[336] A "(...) medicina personalizada, ao utilizar testes genéticos, propõe um serviço exclusivo adaptado a cada organismo. Em que pese tais estudos genéticos apresentarem resultados mais assertivos de diagnósticos (além de possibilitar ações de medicina preventiva), o armazenamento e compartilhamento de dados genéticos, quando mal manipulados, podem desenvolver a categorização de riscos provenientes do perfil genético do indivíduo, culminando em uma "genetização da vida" e provocando a estigmatização de doenças. Estes fatores, consequentemente, tendem dar azo a condutas preconceituosas, tais como o reducionismo e determinismo genético, atingindo searas importantes da vida privada, como a familiar, a profissional, e até no que diz respeito à contratação de seguros e planos de saúde (RUARO; LIMBERGER, 2013)." (COLUSSI, Fernando Augusto Melo; SANTOS, Tomlyta Luz Velasquez dos. Novas tecnologias e liberdade de expressão na pesquisa científica: uma análise sobre a proteção de dados genéticos e de saúde. *Rev. de Biodireito e Direito dos Animais*, Porto Alegre, v. 4, n. 2, p. 01-21, Jul./Dez. 2018. p.08.)

[337] Para a Lei de Não Discriminação de Informações Genéticas, "Genetic information includes information about an individual's genetic tests and the genetic tests of an individual's family members, as well as information about the manifestation of a disease or disorder in an individual's family members (i.e. family medical history). Family medical history is included in the definition of genetic information because it is often used to determine whether someone has an increased risk of getting a disease, disorder, or condition in the future. Genetic information also includes an individual's request for, or receipt of, genetic services, or the participation in clinical research that includes genetic services by the individual or a family member of the individual, and the genetic information of a fetus carried by an individual or by a pregnant woman who is a family member of the individual and the genetic information of any embryo legally held by the individual or family member using an assisted reproductive technology." Disponível em: <https://www.eeoc.gov/genetic-information-discrimination> Acesso em: 03.03.21.

2.2.3.3 Dados biométricos

A biometria é a ciência de se estabelecer a identidade de alguém, a partir da medição e análise de seus atributos fisiológicos[338] ou comportamentais mensuráveis. No primeiro caso, são exemplos a impressão digital, o reconhecimento da íris, a identificação por retina, a definição dos traços do rosto, a arcada dentária, a geometria da mão e a altura da pessoa. As medidas fisiológicas geralmente oferecem o benefício de permanecer mais estáveis ao longo da vida de um indivíduo. No segundo caso, é possível mencionar: a forma como a pessoa digita, como anda, gestos característicos, dinâmica da assinatura (velocidade do movimento da caneta, acelerações, pressão exercida e inclinação), a altura que o indivíduo costuma segurar o celular, a forma com que ele movimenta o *mouse* do computador, a pressão que ele exerce no teclado ou na tela e, até mesmo, como corrige as palavras. Com o aprendizado de máquina e a inteligência artificial, é possível entender e analisar como uma pessoa se comporta no computador ou no celular, por exemplo.

Um importante elemento – conjugado com outros dados pessoais – para identificar a real identidade de um usuário é o seu comportamento. Especificamente no uso do celular, seu comportamento relacionado à localização. Esse tipo de biometria avalia os padrões de comportamento de localização do dispositivo do indivíduo para entender onde ele costuma passar a maior parte de seu tempo, locais que frequenta regularmente, onde passa a maior parte do horário comercial e, para aferir a residência, onde costuma permanecer durante a maior parte da noite. Dessa forma, eventual atividade realizada em localização dissonante à padrão ou esperada naquele momento poderá trazer um sinal de alerta de fraude à aplicação.

Dados biométricos oferecem meios de identificar e autenticar indivíduos de maneira confiável e rápida, com base em um conjunto de dados reconhecíveis e verificáveis, que são únicos e específicos sobre seus titulares. O corpo torna-se a senha, meio único e exclusivo de individualização da pessoa. Ao contrário dos dados sensíveis

[338] "They can be either morphological or biological. These mainly consist of fingerprints, the shape of the hand, of the finger, vein pattern, the eye (iris and retina), and the shape of the face, for morphological analyses. For biological analyses, DNA, blood, saliva, or urine may be used by medical teams and police forensics" (BIOMETRICS: authentication & identification (definition, trends, use cases, laws and latest news) - 2020 review. *Thales Group*. Disponível em: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics. Acesso em: 14 jun. 2020.)

mais voltados à expressão da pessoa na esfera pública, os dados biométricos – assim como os dados genéticos – não advém como regra de escolhas pessoais dos indivíduos.

A LGPD não apresenta definição para os dados biométricos, porém, o já mencionado Decreto nº 10.046/19, em seu Art. 2º, II, define atributos biométricos como "características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar."

Entende-se que o conceito de dados biométricos deve ser extraído tanto da doutrina e de estudos publicados por grupos específicos[339][340] quanto de normas estrangeiras.[341] [342] Nesse sentido, o GDPR em seu artigo 4º, 14, dispõe que são dados biométricos "dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos".[343]

---

[339] ARTICLE 29 DATA PROTECTION WORKING PARTY. Working document on biometrics. 01/08/2003 Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf> Article 29 Data Protection Working Party. Opinion 02/2012 on facial recognition in online and mobile services. 22/03/2012. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf> Article 29 Data Protection Working Party. Opinion 3/2012 on developments in biometric technologies. Adotada em 27 de abril de 2012. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf> Acesso em: 27.02.21

[340] PARLAMENTO EUROPEU. Person identification, human rights and ethical principles Rethinking biometrics in the era of artificial intelligence. Dezembro de 2021.

[341] O *California Consumer Privacy Act* (CCPA) entende informação biométrica como "(…) an individual's physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information." https://www.termsfeed.com/blog/ccpa-biometrics/

[342] Em Nova Iorque, entrou em vigor em julho de 2021 lei que aborda o tratamento de dados biométricos, trazendo limites para o seu uso pelo setor privado. Ela define o termo "biometric identifier information" como: "a physiological or biological characteristic that is used by or on behalf of a commercial establishment, singly or in combination, to identify, or assist in identifying, an individual, including, but not limited to: (i) a retina or iris scan, (ii) a fingerprint or voiceprint, (iii) a scan of hand or face geometry, or any other identifying characteristic.)." Disponível: <https://codelibrary.amlegal.com/codes/newyorkcity/latest/NYCadmin/0-0-0-42626> Acesso em: 15.07.21.

[343] Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679> Acesso em: 27.02.21. Encontramos a mesma definição no art. 3º, 13, da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho.

De acordo com o *Information Commissioner's Office* (ICO), se você processar fotografias digitais de pessoas, esses dados não serão automaticamente biométricos, mesmo que sejam usados para fins de identificação. Embora uma imagem digital possa permitir a identificação por meio de características físicas, ela só se tornará um dado biométrico se você realizar um "processamento técnico específico". Normalmente, isso envolve o uso dos dados da imagem para criar um modelo digital individual ou perfil, que, por sua vez, você usará para correspondência automática de imagens e identificação.[344]

Vistas comumente como um meio de identificação e autenticação, as informações biométricas vêm sendo tratadas para variados fins e contextos: de sistemas de reconhecimento facial e de voz, para permitir que funcionários acessem ambientes específicos ou encontrar pessoas procuradas pela polícia, a impressões digitais para liberar o acesso ao almoço em uma escola primária. À medida que a tecnologia avança, o uso de características humanas como informação continuará a representar desafios para as noções de privacidade e de proteção de dados pessoais. A confiabilidade das informações e sistemas biométricos vem sendo incrementada, sendo a biometria geralmente considerada forte e valiosa para fins de autenticação. Inclusive, sistemas de identificação multibiométrica vêm sendo amplamente adotados. Contudo, entender formas de melhor proteger tais dados e evitar tratamentos desproporcionais[345] ou ilícitos ainda são desafios que precisam ser mais bem trabalhados.[346]

---

[344] Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/#scd4> Acesso em: 27.02.21.

[345] Acerca da proporcionalidade e razoabilidade da aplicação de biometria, recorda-se ação judicial – proposta com a LGPD já em vigor - em que se questiona a obrigatoriedade do cadastramento biométrico facial para o uso do bilhete eletrônico "VEM Estudante" em Recife. Beneficiário da meia-entrada, o reclamante não consegue utilizar o transporte público por não ter feito cadastramento. Ao ser informado da necessidade do cadastramento, o estudante questionou o funcionário da empresa sobre a política de proteção de dados da empresa, que administra o sistema, e não foi informado sobre o regramento. (TJPE. Processo nº 0060336-35.2020.8.17.2001. 18ª Vara Cível da Capital)

[346] "À medida que, através de sensores biométricos, cada vez mais dados fluírem de seu corpo e seu cérebro para máquinas inteligentes, será fácil para corporações e agências do governo conhecer você, manipular você e tomar decisões por você. Mais importante ainda, eles serão capazes de decifrar os mecanismos profundos de todos os corpos e cérebros, e com isso adquirir o poder de fazer a engenharia da vida. Se quisermos evitar que uma pequena elite monopolize esses poderes, que parecem divinos, e se quisermos impedir que a humanidade se fragmente em castas biológicas, a questão chave é: quem é dono dos dados? Os dados de meu DNA, meu cérebro e minha vida pertencem a mim, ao governo, a uma corporação ou ao coletivo humano?" (HARARI, Yuval Noah. *21 lições para o século 21*. 1.ed. Companhia das Letras: 2018, p. 94-95) Harari prossegue: "Num nível ainda mais profundo, sensores biométricos e interfaces cérebro-computador diretas visam a erodir a fronteira entre máquinas eletrônicas e corpos orgânicos e, literalmente, entrar debaixo de nossa pele. Quando os gigantes de tecnologia

Caso que vale recordar se deu em 2018, quando o Instituto Brasileiro de Defesa do Consumidor (Idec)[347] e outras entidades ingressaram com Ação Civil Pública contra a ViaQuatro, concessionária da Linha Amarela do metrô de São Paulo, devido à coleta de dados pessoais pelas "portas interativas" das estações. O projeto "Portas Digitais", anunciado em abril pela ViaQuatro, filmava as reações dos passageiros à publicidade veiculada nas portas dos vagões, coletando as emoções, sem prévio consentimento dos consumidores, com o objetivo de vender anúncios de forma mais eficiente. A empresa promoveu a implantação de portas interativas em algumas das estações de metrô, buscando reconhecer o gênero, a faixa etária e as emoções dos usuários expostos à publicidade veiculada (inclusive comercial).[348] Os autores da ação pleitearam a condenação da ré (i) a não utilizar dados biométricos ou qualquer outro tipo de identificação dos consumidores e usuários do transporte público, sem consentimento do usuário; e (ii) ao pagamento de indenização pela utilização indevida da imagem dos consumidores e pelos danos coletivos em valor não inferior a R$ 100.000.000,00.

Em 07 de maio de 2021, foi proferida sentença de mérito sobre o caso, em que se afirmou ser inegável que a conduta da requerida violava, patentemente, o direito à imagem dos consumidores usuários do serviço público, as disposições acerca da proteção especial conferida aos dados pessoais sensíveis, além dos direitos básicos do consumidor, notadamente à informação e à proteção com relação às práticas comerciais abusivas. Diante disso, o pedido para a ré não utilizar dados biométricos ou qualquer outro tipo de identificação dos usuários do transporte público, sem a comprovação do devido consentimento do consumidor, foi julgado procedente. A magistrada destacou

---

adquirirem compreensão completa do corpo humano, poderão acabar manipulando todo o nosso corpo da mesma maneira que manipulam nossos olhos, dedos e cartões de crédito." (HARARI, Yuval Noah. *21 lições para o século 21*. 1.ed. Companhia das Letras: 2018, p. 105)

[347] Em junho de 2021, o Idec notificou o grupo Raia Drogasil, dono da rede Droga Raia, para explicar sobre a coleta e uso da biometria de clientes. Afirmou-se que consumidores foram barrados de aproveitar promoções caso não cadastrassem a digital. O instituto também enviou carta à Associação Brasileira de Farmácias (Abrafarma) para saber se outras empresas estariam seguindo os passos da Droga Raia. Segundo reportagem, "A notificação de caráter extrajudicial à Raia Drogasil exige que a empresa pare com a coleta de digital e CPF e explique qual a finalidade de coleta de dados. As 12 perguntas feitas pelo Idec, contidas na advertência, fazem parte de uma investigação do instituto sobre as ações da rede de drogarias. Ele quer saber o porquê do cadastro da biometria de consumidores. O que motiva o Idec são denúncias de membros cadastrados e relatos nas redes sociais de pessoas que foram impedidas de conseguir desconto em itens sob a condição de cadastrar o dado, que é sensível segundo a Lei Geral de Proteção de Dados." Disponível em: <https://idec.org.br/idec-na-imprensa/idec-notifica-raia-drogasil-dono-da-droga-raia-sobre-biometria-digital> Acesso em: 06.07.21

[348] TJSP. Processo nº 1090663-42.2018.8.26.0100 da 37ª Vara Cível do Foro Central Cível da Comarca de São Paulo. Julgado em 07 de maio de 2021. Estudo sobre o caso pode ser encontrado em: <https://irisbh.com.br/publicacoes/parecer-idec-vs-viaquatro/> Acesso em: 01.03.21

que, caso deseje readotar as práticas tratadas nos autos, deverá a requerida obter o consentimento prévio dos usuários, mediante informação clara e específica sobre a captação e o tratamento dos dados, com adoção das ferramentas pertinentes.

A possibilidade de reconhecimento facial e de detecção facial e a utilização - com evidente finalidade comercial - das imagens captadas dos usuários do metrô sem o consentimento ou cientificação dos usuários mostram-se, segundo a magistrada, bastante reprováveis, atingindo a moral e os valores coletivos. Levou-se em conta também as garantias adicionais que a LGPD oferece aos dados sensíveis, bem como o fato de na estação circularem, além de adultos, crianças e adolescentes.

A sentença trata com precisão a problemática, porém se mostra relevante questionar se a base legal do consentimento seria suficiente e adequada para legitimar o tratamento de dados pessoais no caso. Para ser aplicado no trato de dados sensíveis, o consentimento deverá ser livre, informado e dado de forma específica e destacada, para finalidades específicas (Art.11, I, da LGPD). O transporte por meio do metrô é importante e, muitas vezes, essencial para muitas pessoas, não podendo elas optarem por outro meio. Tem um custo acessível e facilita o acesso a diversos locais. Diante disso, não parece possível obter um consentimento realmente livre dos usuários do serviço, tendo em vista a impossibilidade da maioria de dizer “não” e optar por outro meio. Além disso, a finalidade do tratamento mostra-se pouco legítima, apresentando um viés estritamente comercial e patrimonial. Não há, por exemplo, um interesse público significativo que embase a coleta.

Ao final, determinou-se que a requerida se abstenha de captar as imagens, sons e quaisquer outros dados pessoais dos consumidores usuários, através das câmeras ou outros dispositivos envolvendo os equipamentos instalados na Linha 4 Amarela do metrô sem o consentimento prévio dos consumidores. Além disso, foi estabelecido que, caso deseje readotar as práticas tratadas nos autos, a requerida deverá obter o consentimento prévio dos usuários mediante informação clara e específica sobre a captação e o tratamento dos dados, com a adoção das ferramentas pertinentes. Adicionalmente, a requerida foi condenada a pagar indenização por danos morais coletivos no valor de R$100.000,00, a ser revertido para o Fundo de Defesa de Direitos Difusos.

Dados biométricos permitem a identificação precisa de uma pessoa natural, sem a necessidade de se realizar múltiplos cruzamentos de dados. Havendo a coleta e o registro de dados biométricos desde o nascimento[349] será possível o rastreio, o monitoramento e uma profunda análise das pessoas pelos setores público e privado.[350] Mais do que unificar documentos, será possível implementar sistemas sofisticados de vigilância e controle sob a população, bem como desenvolver perfis e analisar emoções, o que certamente traz à tona um cenário bastante preocupante de intensos rastreios e discriminações.

Vale destacar, aqui, tecnologias que permitem o reconhecimento de emoções faciais (*Facial Emotion Recognition* - FER). Elas são usadas para analisar sentimentos de pessoas naturais, a partir de diferentes fontes, como fotos e vídeos. As expressões faciais são formas de comunicação não verbal, fornecendo importantes recursos para a análise das emoções humanas. Há anos, decodificar tais expressões de emoção tem sido um interesse de pesquisa no campo da psicologia. Recentemente, a elevada difusão de câmeras, os avanços tecnológicos no campo do tratamento de dados biométricos e a ampliação do uso de inteligência artificial e *machine learning* têm desempenhado um papel de destaque no refinamento da mencionada tecnologia. Entretanto, a complexidade das expressões faciais e as amplas possibilidades de uso da tecnologia aumentam cada vez mais os riscos de lesão à privacidade e aos dados sensíveis.[351]

---

[349] A Portaria nº 248, de 2 de fevereiro de 2018, do Ministério da Saúde, dispõe que: "As Declarações de Nascidos Vivos - DNV, a que se refere a alínea "h" do inciso XIX do caput, deverão ser vinculadas ao registro biométrico do recém-nascido e de sua mãe, na forma de ato conjunto das Secretarias de Vigilância em Saúde e de Atenção à Saúde."

[350] ABBAS DA SILVA, L.; FRANQUEIRA, B. D.; HARTMANN, I. A. O que os olhos não veem, as câmeras monitoram: reconhecimento facial para segurança pública e regulação na América Latina. *Revista Digital de Direito Administrativo*, v. 8, n. 1, p. 171-204, 2021. SIMÃO, Bárbara; FRAGOSO, Nathalie; ROBERTO, Enrico. *Reconhecimento Facial e o Setor Privado*: Guia para a adoção de boas práticas. InternetLab/IDEC, São Paulo, 2020.

[351] "FER analysis comprises three steps: a) face detection, b) facial expression detection, c) expression classification to an emotional state (Figure 1). Emotion detection is based on the analysis of facial landmark positions (e.g. end of nose, eyebrows). Furthermore, in videos, changes in those positions are also analysed, in order to identify contractions in a group of facial muscles (Ko 2018). Depending on the algorithm, facial expressions can be classified to basic emotions (e.g. anger, disgust, fear, joy, sadness, and surprise) or compound emotions (e.g. happily sad, happily surprised, happily disgusted, sadly fearful, sadly angry, sadly surprised) (Du, Tao, and Martinez 2014). In other cases, facial expressions could be linked to physiological or mental state of mind (e.g. tiredness or boredom)." (VEMOU, Konstantina; HORVATH, Anna. TechDispatch #1/2021 - Facial Emotion Recognition. Publicado em 26 de maio de 2021. Disponível em: <https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-12021-facial-emotion-recognition_en> Acesso em: 05.08.21.)

A fonte das imagens que servem como entrada para os algoritmos varia de câmeras de vigilância até câmeras colocadas perto de telas de publicidade em lojas ou inseridas em dispositivos pessoais (como celulares). O reconhecimento de emoções faciais pode ser combinado com identificação biométrica. Sua precisão é ampliada quando conjugado com tecnologia que analisa diferentes tipos de fontes, como voz, texto, dados de saúde e/ou padrões de fluxo sanguíneo inferidos da imagem.

Verifica-se uma ampla gama de aplicações para as referidas tecnologias:[352] prestação de serviços personalizados; análise do comportamento do cliente e direcionamento de publicidade; cuidados de saúde, como detectar autismo ou doenças neurodegenerativas, prever transtornos psicóticos e observar as condições dos pacientes durante o tratamento; ajudar na tomada de decisões de recrutadores em processos seletivos; monitorar o humor e a atenção dos funcionários; monitorar a atenção dos alunos; e detectar envolvimento na aprendizagem online. No campo da segurança pública, por exemplo, podem ser utilizadas em detectores de mentira e no controle inteligente de fronteiras, para analisar imagens de cenas de um crime e para detectar e reduzir reclamações de seguros fraudulentas.[353] Além de questões relacionadas à segurança pública[354], persecução criminal e prevenção do terrorismo, nos últimos tempos, vem crescendo o debate acerca do estabelecimento de bancos de dados biométricos para a identificação dos cidadãos, para fins de validação de identidades, e como meio para a concessão de benefícios e auxílios governamentais. Recorda-se, aqui, a Lei n° 13.444/2017, que criou a Identificação Civil Nacional (ICN), "com o objetivo de identificar o brasileiro em suas relações com a sociedade e com os órgãos e entidades

---

[352] VEMOU, Konstantina; HORVATH, Anna. TechDispatch #1/2021 - Facial Emotion Recognition. Publicado em 26 de maio de 2021.

[353] Recomenda-se a leitura de: Andalibi, Nazanin, and Justin Buss. 2020. "The Human in Emotion Recognition on Social Media: Attitudes, Outcomes, Risks." In *Proceedings of the 2020 Chi Conference on Human Factors in Computing Systems*, 1–16. CHI '20. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3313831.3376680. Barrett, Lisa Feldman, Ralph Adolphs, Stacy Marsella, Aleix M. Martinez, and Seth D. Pollak. 2019. "Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements." *Psychological Science in the Public Interest* 20 (1): 1–68. https://doi.org/10.1177/1529100619832930. Jacintha, V, Judy Simon, S Tamilarasu, R Thamizhmani, K Thanga yogesh, and J. Nagarajan. 2019. "A Review on Facial Emotion Recognition Techniques." In *2019 International Conference on Communication and Signal Processing (Iccsp)*, 0517–21. IEEE. https://doi.org/10.1109/ICCSP.2019.8698067. Rhue, Lauren. 2018. "Racial Influence on Automated Perceptions of Emotions." *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3281765.

[354] A Lei nº 13.964/19, conhecida como lei anticrime, em seu art. 12, autorizou a criação, no Ministério da Justiça e Segurança Pública, do Banco Nacional Multibiométrico e de Impressões Digitais. Dessa forma, na Lei nº 12.037/09, encontra-se disposto que: "Art. 7º-C. Fica autorizada a criação, no Ministério da Justiça e Segurança Pública, do Banco Nacional Multibiométrico e de Impressões Digitais."

governamentais e privados." Sua base de dados contará com diversas informações, inclusive a base de dados biométricos da Justiça Eleitoral. O objetivo do programa é cadastrar as pessoas para que sejam identificadas com segurança tanto nas relações com organismos públicos quanto particulares. Busca-se que, a partir da validação dos dados biométricos na base da ICN, o cidadão possa usufruir de serviços antes disponíveis apenas no atendimento presencial de órgãos federais, como o INSS e a Receita Federal.[355] O registro de dados biométricos em cadastros de órgãos públicos vem se mostrando uma tendência, sendo possível mencionar exemplos na Índia[356], China e Estados Unidos.[357] Entretanto, no caso de uma violação ou incidente de segurança envolvendo dados biométricos, isso criará uma situação bastante grave: atribuições físicas, como impressões digitais, não podem ser substituídas como meras senhas numéricas. Justamente por isso, recursos de segurança deverão ser ampliados e garantidos, sendo incluídos meios de criptografia, avaliações de impacto e auditorias técnicas. Ao considerar soluções tecnológicas, os agentes devem optar, inicialmente, por medidas que sejam menos invasivas e limitadoras de direitos fundamentais.

2.2.4 Dados referentes à vida sexual

A LGPD quando tratou da sensibilidade de dados pessoais relativos à vida sexual não especificou em detalhe para quais informações estava reservando uma proteção ampliada. A partir de análises que levam em conta o reconhecimento de direitos e a trajetória percorrida pelas comunidades LGBTQIA+, bem como o contexto político e social brasileiro, costuma-se pleitear tutela, dentro dessa categoria, também

[355] TSE. Em 2021, TSE ampliou ações para implementar a Identificação Civil Nacional (ICN). Publicado em 23 de dezembro de 2021. Disponível em: <https://www.tse.jus.br/imprensa/noticias-tse/2021/Dezembro/em-2021-tse-ampliou-acoes-para-implementar-a-identificacao-civil-nacional-icn> Acesso em: 20.02.22.
[356] Disponível em: <https://uidai.gov.in/> Acesso em 01.03.21.
[357] Cf. DOERING, Victor; SILVA, Alexandre Pacheco da. O tratamento de dados biométricos na LGPD: dilemas jurídicos e políticos de seu processamento. In: FILHO, Francisco; RAIS, Diogo (Coord.). *Direito público digital*. São Paulo: Thomson Reuters Brasil, 2020. p. 99-113.

para os dados referentes à orientação sexual e à identidade de gênero.[358] Isso porque o tratamento de tais dados pode provocar cenários de elevada discriminação e intensificar vulnerabilidades de determinados sujeitos. Dados pessoais relativos à vida sexual devem representar mais do que informações sobre a atividade sexual de uma pessoa e suas relações sexuais. Nesse sentido, observa-se que a Lei do Cadastro Positivo já trazia "orientação sexual" como informação sensível, em seu Art. 3º, par. 3º, II (Lei 12.414/11). Busca-se trazer proteção plena à intimidade, identidade e orientação sexual do ser humano, respeitando-se suas preferências, fantasias, desejos e singularidades.[359]

Entende-se por "identidade de gênero" o gênero com que a pessoa humana se identifica, independentemente de questões biológicas. Há quem se perceba, por exemplo, como homem, como mulher, como ambos ou mesmo como nenhum dos dois gêneros: como no caso do não binário[360] [361]. Cisgênero é aquele que se identifica com o

---

[358] "A empresa americana de headhunters Signium diz que a contratação de executivas mulheres por seus clientes cresceu mais de 50% nos últimos 12 meses em postos com remuneração anual de R$ 500 mil a R$ 1 milhão. Especializada na seleção de profissionais para vagas de presidentes, conselheiros e demais cargos para o alto escalão, a recrutadora diz que atingiu o resultado depois que decidiu abolir as informações pessoais dos candidatos (como idade, gênero e estado civil) nas apresentações aos contratantes." Disponível em: <https://www1.folha.uol.com.br/colunas/painelsa/2021/07/headhunter-diz-que-elevou-contratacao-de-mulheres-para-cargo-de-r-1-milhao-apos-ocultar-genero-e-estado-civil.shtml?utm_source=linkedin&utm_medium=social&utm_campaign=compli&origin=folha> Acesso em: 12.07.21

[359] Analisando-se o cenário europeu, afirma-se que: "Protection of a person's sex life is part of the protection of private and family life under Article 7 CFR and Article 8 ECHR, and Article 21(1) CFR protects against discrimination based on sexual orientation. The two categories 'data concerning a natural person's sex life' and 'sexual orientation' are closely connected but not identical. Sexual orientation refers to information concerning whether, for example, an individual is heterosexual, homosexual, bisexual, or of some other orientation. Data concerning a natural person's sex life is to be broadly construed to include not only this, but also information about sexual practices (for example, the consumption of pornography) as well as details on marital status and intimate personal details (for example, concerning change of gender or the use of contraception)." (GEORGIEVA, Ludmila; KUNER, Christopher. Article 9 Processing of special categories of personal data In: KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher. *The EU General Data Protection Regulation (GDPR): A Commentary.* 1.ed. Oxford University Press: 2020. p. 375.)

[360] "No exterior, vários países do continente europeu, como Grécia, Holanda e Dinamarca, mas também Nepal e Malta (pioneiro no tema) já reconhecem que, tal como entre o preto e o branco existe o cinza, entre homem e mulher existe um terceiro gênero (intergênero), permitindo que essas pessoas possam se registrar sob o gênero "diverso", uma categoria guarda-chuva que abrange inúmeras variações. Na Alemanha, o Tribunal Constitucional teve papel relevantíssimo no reconhecimento da identidade - e, consequentemente, da dignidade - dessas pessoas ao admitir pioneiramente, em 2017, a existência de uma terceira categoria de gênero entre o masculino e feminino, quebrando, dessa forma, o milenar sistema binário heteronormativo do ordenamento jurídico alemão." **(**FRITZ, Karina Nunes. Pessoa não-binária tem direito a ser tratada de forma neutra, diz juiz de Frankfurt - ainda há muito por fazer pela identidade e igualdade de gênero. Migalhas, artigo publicado em 8 de março de 2021. Disponível: <https://www.migalhas.com.br/coluna/german-report/341325/pessoa-nao-binaria-tem-direito-a-ser-tratada-de-forma-neutra> Acesso em: 10.03.21.)

[361] "A juíza de Direito Sandra Tamara Gayer M., de Foz de Iguaçu/PR, acatou pedido de pessoa não binária para determinar a alteração de gênero para "não determinado" em sua certidão de nascimento. O

mesmo gênero que lhe foi dado no nascimento. Por outro lado, o transexual ou transgênero[362] se identifica com um gênero diferente daquele que lhe foi dado ao nascer. [363] Dessa forma, considera-se homem transexual aquele nascido com o sexo feminino que se identifica como homem, enquanto são mulheres transexuais aquelas nascidas com o sexo masculino, mas que se identificam como mulheres. A transexualidade não se relaciona com a orientação sexual; refere-se à identidade de gênero.

Portanto, compreende-se que os órgãos sexuais e as demais características biológicas de uma pessoa não determinarão o gênero com o qual ela se identificará, sua orientação sexual ou performance de gênero.[364] A identidade de gênero é sentida pela experiência interna e individual de cada pessoa. Ela pode ou não corresponder ao sexo atribuído no nascimento. Depende também do senso pessoal a respeito do próprio corpo e pode envolver, por livre escolha, modificações na aparência e em outras expressões de gênero.

Já a "orientação sexual" encontra-se relacionada, em certa medida, com o gênero do(s) parceiro(s) com quem se desenvolve atração sexual e laços românticos. Refere-se ao que cada pessoa pensa e sente sobre si própria, sua afetividade e sexualidade, assim como por quem se sente atraída.[365] Tradicionalmente, entende-se que o heterossexual é quem tem atração por alguém de outro gênero. Já o homossexual é quem tem atração

---

nome da pessoa não binária também poderá ser alterado." Disponível em: <https://www.migalhas.com.br/quentes/356871/pessoa-nao-binaria-muda-registro-para-genero-nao-determinado> Acesso em: 20.02.22

[362] A Resolução CFM nº 2.265/2019 dispõe sobre o cuidado específico à pessoa com incongruência de gênero ou transgênero. Ela prevê a ampliação do acesso ao atendimento a essa população na rede pública e estabelece critérios para maior segurança na realização de procedimentos com hormonioterapia e cirurgias de adequação sexual. De acordo com seu artigo 1º, "Compreende-se por transgênero ou incongruência de gênero a não paridade entre a identidade de gênero e o sexo ao nascimento, incluindo-se neste grupo transexuais, travestis e outras expressões identitárias relacionadas à diversidade de gênero. § 1º Considera-se identidade de gênero o reconhecimento de cada pessoa sobre seu próprio gênero. (...) § 4º Considera-se travesti a pessoa que nasceu com um sexo, identifica-se e apresenta-se fenotipicamente no outro gênero, mas aceita sua genitália. § 5º Considera-se afirmação de gênero o procedimento terapêutico multidisciplinar para a pessoa que necessita adequar seu corpo à sua identidade de gênero por meio de hormonioterapia e/ou cirurgias." Prossegue a Resolução afirmando que: "Art. 2º A atenção integral à saúde do transgênero deve contemplar todas as suas necessidades, garantindo o acesso, sem qualquer tipo de discriminação, às atenções básica, especializada e de urgência e emergência."

[363] KONDER, Carlos Nelson de Paula. O alcance do direito à identidade pessoal no direito civil brasileiro. Pensar, Fortaleza, v. 23, n. 1, p. 1-11, jan./mar. 2018

[364] PRESGRAVE, Ana Beatriz Ferreira Rebello; HILDEBRAND, Cecília Rodrigues Frutuoso; PEIXOTO, Renata Cortez Vieira. Pais que dão à luz: como o direito brasileiro regulamenta o registro dos filhos de transgêneros? *IBDFAM*, publicado em: 24 de fevereiro de 2021. Disponível em: <https://ibdfam.org.br/artigos/1652/Pais+que+d%C3%A3o+%C3%A0+luz%3A+como+o+direito+brasileiro+regulamenta+o+registro+dos+filhos+de+transg%C3%AAneros%3F> Acesso em: 07.03.21

[365] Entende-se que as expressões "opção sexual" e "preferência sexual" seriam inadequadas, já que ninguém optaria ou escolheria, conscientemente, sua orientação sexual.

por alguém do mesmo gênero. Prosseguindo, é possível compreender o bissexual como uma pessoa que sente atração por mais de um gênero, enquanto o pansexual sente atração por pessoas, independentemente do sexo, do gênero ou de como se apresentam ao mundo. A assexualidade normalmente é definida como a ausência de desejo sexual por qualquer gênero. Contudo, mostra-se necessário observar que tais categorias não são estanques, havendo diversas possibilidades e composições viáveis, a depender do momento, desejos e complexidades dos sujeitos.

O movimento político e social de inclusão de pessoas de diversas orientações sexuais e identidades de gênero assim como as demandas, em âmbito jurídico, por maior visibilidade e garantia de direitos para as pessoas LGBTQIA+[366] não são recentes. Da igualdade material, constitucionalmente assegurada, aos direitos à identidade pessoal, nome e integridade psicofísica, muita luta foi travada e violências de toda a forma sofridas.

Nos últimos anos, os tribunais superiores vêm assegurando mais direitos a tais comunidades, como, por exemplo, em 2018, no julgamento da ADI 4.275 e do RE 670.422[367], em que o Supremo Tribunal Federal reconheceu que pessoas trans poderiam alterar seu prenome e classificação de gênero no registro civil, não se exigindo, para tanto, nada além da manifestação de vontade do indivíduo. Em seguida, o Provimento 73/2018 do Conselho Nacional de Justiça estabeleceu regras para a alteração do prenome e do gênero nos assentos de nascimento e casamento de pessoa *transgênero* no Registro Civil das Pessoas Naturais. As alterações poderão ser feitas sem a

[366] A sigla apresenta o seguinte significado: L = Lésbicas; G = Gays; B = Bissexuais; T = Transexuais ou transgêneros; Q = Queer; I = Intersexo; A = Assexual; e o + é utilizado para incluir outros grupos e variações de sexualidade e gênero, como os pansexuais.

[367] "Decisão: O Tribunal, por maioria e nos termos do voto do Relator, apreciando o tema 761 da repercussão geral, deu provimento ao recurso extraordinário. Vencidos parcialmente os Ministros Marco Aurélio e Alexandre de Moraes. Nessa assentada, o Ministro Dias Toffoli (Relator), reajustou seu voto para adequá-lo ao que o Plenário decidiu na ADI 4.275. Em seguida, o Tribunal fixou a seguinte tese: "i) O transgênero tem direito fundamental subjetivo à alteração de seu prenome e de sua classificação de gênero no registro civil, não se exigindo, para tanto, nada além da manifestação de vontade do indivíduo, o qual poderá exercer tal faculdade tanto pela via judicial como diretamente pela via administrativa; ii) Essa alteração deve ser averbada à margem do assento de nascimento, vedada a inclusão do termo 'transgênero'; iii) Nas certidões do registro não constará nenhuma observação sobre a origem do ato, vedada a expedição de certidão de inteiro teor, salvo a requerimento do próprio interessado ou por determinação judicial; iv) Efetuando-se o procedimento pela via judicial, caberá ao magistrado determinar de ofício ou a requerimento do interessado a expedição de mandados específicos para a alteração dos demais registros nos órgãos públicos ou privados pertinentes, os quais deverão preservar o sigilo sobre a origem dos atos". Vencido o Ministro Marco Aurélio na fixação da tese. Ausentes, neste julgamento, o Ministro Gilmar Mendes, e, justificadamente, a Ministra Cármen Lúcia (Presidente). Presidiu o julgamento o Ministro Dias Toffoli (Vice-Presidente). Plenário, 15.8.2018."

obrigatoriedade da comprovação da cirurgia de mudança de sexo ou de decisão judicial. Dessa forma, "toda pessoa maior de 18 anos completos habilitada à prática de todos os atos da vida civil poderá requerer ao ofício do RCPN a alteração e a averbação do prenome e do gênero, a fim de adequá-los à identidade autopercebida."[368] [369]

Recorda-se também que na Ação Direta de Inconstitucionalidade por Omissão (ADO) 26 e no Mandado de Injunção (MI) 4.733, julgados conjuntamente, o Supremo Tribunal Federal restringiu o direito à liberdade de expressão para que fossem tutelados direitos de minorias, criminalizando-se, por analogia aos crimes de preconceito de raça ou de cor (Lei 7.716/89), condutas discriminatórias dirigidas a homossexuais e a transexuais.[370] O ministro Gilmar Mendes entendeu que: "O que a nossa Constituição visa a coibir é a discriminação inferiorizante, a qual ela repudia com a alcunha de 'racismo'." Assim, foi proposto na ADO 26 que, até que sobrevenha lei emanada do Congresso Nacional destinada a implementar os mandados de criminalização definidos nos incisos XLI e XLII do Art. 5º da Constituição, as condutas homofóbicas e transfóbicas, que envolverem aversão odiosa à orientação sexual ou à identidade de gênero de alguém, por traduzirem expressões de racismo, ajustam-se, por identidade de razão e mediante adequação típica, aos preceitos primários de incriminação definidos na Lei nº 7.716/89, constituindo, também, na hipótese de homicídio doloso, circunstância que o qualifica, por configurar motivo torpe.[371]

---

[368] Disponível em: <https://www.cnj.jus.br/cnj-servico-como-fazer-a-troca-de-nome-e-genero-em-cartorios/> Acesso em: 07.03.21

[369] A recente Resolução CNJ nº 366, editada em 20 de janeiro de 2021, altera parcialmente a Resolução CNJ nº 348/2020, estabelecendo diretrizes e procedimentos a serem observados pelo Poder Judiciário, no âmbito criminal, com relação ao tratamento da população LGBTI que seja custodiada, acusada, ré, condenada, privada de liberdade, em cumprimento de alternativas penais ou monitorada eletronicamente.

[370] STF, ADO 26, rel. Min. Celso de Mello, julgamento em 13.6.2019. Ata de julgamento publicada no Dje de 1º.7.2019. STF, MI 4733, rel. Min. Edson Fachin, julgamento em 13.6.2019. Ata de julgamento publicada no Dje de 1º.7.2019.

[371] Levando em conta o julgamento da ADO/DF nº 26, doutrina destaca que: "A LGPD se baseia no conceito de origem racial, diretamente dependente do entendimento de o que é "raça." Se "raça", de acordo com o STF, "projeta-se para além de aspectos estritamente biológicos ou fenotípicos, pois resulta, enquanto manifestação de poder, de uma construção de índole histórico-cultural", outros "marcadores sociais da diferença" devem nele ser incluídos, na medida em que produzam sistemas de discriminação social e de dominação coletiva, à exemplo do que ocorre com a "identidade de gênero." Assim, demonstra-se a conexão entre identidade de gênero e o artigo 5º II, uma vez que dados de origem racial são dados sensíveis, de acordo com a LGPD." (FICO, Bernardo de Souza Dantas; SICUTO, Guilherme Hernandes; NÓBREGA, Henrique Meng. Lei Geral de Proteção de Dados para LGBTs: Identidade de gênero como dado sensível. *Justificando*. Publicado em 16 de junho de 2020. Disponível em: <https://www.justificando.com/2020/06/16/leigeral-de-protecao-de-dados-para-lgbts-identidade-de-genero-como-dado-sensivel/> Acesso em: 03.03.21.)

No plano internacional, em junho de 2011, o Conselho de Direitos Humanos adotou a resolução 17/19 – primeira resolução das Nações Unidas sobre direitos humanos, orientação sexual e identidade de gênero. Sua adoção abriu caminho para o primeiro relatório oficial das Nações Unidas sobre o assunto, o qual apresentou evidências de um padrão de violência sistemática e de discriminações dirigidas às pessoas, em todas as regiões, em razão de sua orientação sexual e identidade de gênero – como discriminações nas relações de emprego, na assistência médica e no acesso à educação, criminalização de condutas consideradas "inadequadas", ataques físicos seletivos e assassinatos.[372] Antes disso, porém, os *Princípios de Yogyakarta* (em referência à conferência havida nesta cidade da Indonésia em 2006, dirigida a otimizar a legislação internacional de direitos humanos sobre orientação sexual e identidade de gênero)[373] já afirmavam que "Todos os seres humanos nascem livres e iguais em dignidade e direitos. Todos os direitos humanos são universais, interdependentes, indivisíveis e inter-relacionados. A orientação sexual e a identidade gênero são essenciais para a dignidade e humanidade de cada pessoa e não devem ser motivo de discriminação ou abuso."[374] Seu artigo 2º dispõe que:

> Todas as pessoas têm o direito de desfrutar de todos os direitos humanos livres de discriminação por sua orientação sexual ou identidade de gênero. Todos e todas têm direito à igualdade perante à lei e à proteção da lei sem

[372] Alto Comissariado das Nações Unidas. *Nascidos livres e iguais:* Orientação Sexual e Identidade de Gênero no Regime Internacional de Direitos Humanos, Brasília, 2013.

[373] Princípios sobre a aplicação da legislação internacional de direitos humanos em relação à orientação sexual e identidade de gênero (Princípios de Yogyakarta). Disponível em: <http://www.clam.org.br/uploads/conteudo/principios_de_yogyakarta.pdf> Acesso em: 10.03.21 ALAMINO, F. N. P.; DEL VECCHIO, V. A. Os Princípios de Yogyakarta e a proteção de direitos fundamentais das minorias de orientação sexual e de identidade de gênero. *Revista da Faculdade de Direito, Universidade de São Paulo*, v. 113, p. 645-668, 2018. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/156674. Acesso em: 8 mar. 2021. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/principios-de-yogyakarta-protecao-e-direitos-lgbt-30102018>Acesso em: 10.03.21

[374] Em 2017, os Princípios de Yogyakarta receberam dez novos itens e foram elencadas novas obrigações por parte dos Estados em relação à aplicação do direito internacional sobre direitos humanos relacionados à orientação sexual, identidade de gênero, expressão de gênero e características sexuais. "The Yogyakarta Principles plus 10 (YP+10) aims to document and elaborate these developments through a set of Additional Principles and State Obligations. YP+10 should be read alongside the original 29 Yogyakarta Principles. Together, these documents provide an authoritative, expert exposition of international human rights law as it currently applies to the grounds of sexual orientation, gender identity, gender expression and sex characteristics" (Additional principles and state obligations on the application of international human rights law in relation to sexual orientation, gender identity, gender expression and sex characteristics to complement the yogyakarta principles (The Yogyakarta principles plus 10): https://yogyakartaprinciples.org/wp-content/uploads/2017/11/A5_yogyakartaWEB-2.pdf Acesso em: 10.03.21)

> qualquer discriminação, seja ou não também afetado o gozo de outro direito humano. A lei deve proibir qualquer dessas discriminações e garantir a todas as pessoas proteção igual e eficaz contra qualquer uma dessas discriminações. A discriminação com base na orientação sexual ou identidade gênero inclui qualquer distinção, exclusão, restrição ou preferência baseada na orientação sexual ou identidade de gênero que tenha como objetivos ou efeito de anular ou prejudicar a igualdade perante à lei ou proteção igual da lei, ou o reconhecimento, gozo ou exercício, em base igualitária, de todos os direitos humanos e das liberdades fundamentais. A discriminação baseada na orientação sexual ou identidade de gênero pode ser, e comumente é, agravada por discriminação decorrente de outras circunstâncias, inclusive aquelas relacionadas ao gênero, raça, idade, religião, necessidades especiais, situação de saúde e status econômico.

Dentro do direito europeu, a Convenção Europeia de Direitos Humanos desde 1950 já inclui, em seu Art. 14, proibição de discriminação, de forma que o gozo dos direitos e liberdades reconhecidos no documento deve ser assegurado sem quaisquer distinções, tais como as fundadas no sexo, na raça, cor, língua, religião, opiniões políticas ou outras, origem nacional ou social, a pertença a uma minoria nacional, a riqueza, o nascimento ou qualquer outra situação.[375] Mesmo que o texto trouxesse apenas referência ao elemento *sexo* (e nada relacionado à orientação sexual ou identidade de gênero), ele acabou sendo expandido pelo Tribunal Europeu de Direitos Humanos.[376] No primeiro caso[377], o Tribunal reconheceu que o mencionado art. 14

[375] A Carta dos Direitos Fundamentais da União Europeia (2000) também preceitua a não discriminação em seu art. 21: "É proibida a discriminação em razão, designadamente, do sexo, raça, cor ou origem étnica ou social, características genéticas, língua, religião ou convicções, opiniões políticas ou outras, pertença a uma minoria nacional, riqueza, nascimento, deficiência, idade ou orientação sexual."

[376] A tutela para a vida sexual e a orientação sexual de uma pessoa costuma se dar também com base no art. 8º da Convenção, que trata do direito ao respeito pela vida privada e familiar.

[377] "(...) ao proibir a discriminação baseada em orientação sexual, cabe menção ao paradigmático caso Salgueiro da Silva Mouta v. Portugal envolvendo a denúncia de um peticionário português que se casou e teve uma filha. Divorciou-se da mulher e, desde então, passou a viver uma relação homossexual com um homem. Houve a disputa judicial a respeito do poder parental, sendo que, em grau de recurso, a ex-mulher obteve o poder parental, com base em decisão que se fundamentou na homossexualidade do peticionário. A Corte Europeia condenou Portugal por afronta ao artigo 8º (respeito ao direito à vida privada e familiar) e ao artigo 14 (proibição de discriminação), sob o argumento de que teria ocorrido violação ao princípio da proporcionalidade. Enfatizou que a decisão da justiça portuguesa, ao embasar-se fundamentalmente na homossexualidade do peticionário para negar-lhe o direito ao poder parental, estava a adicionar critério não previsto em lei, em direta afronta ao princípio da proporcionalidade, por "inexistir uma relação razoável entre os meios utilizados e o fim perseguido". Entendeu a Corte Europeia que não havia necessidade de fixar indenização pecuniária no caso, sendo a decisão em si mesma justa reparação pelo dano sofrido pelo peticionário. Outro precedente emblemático enfrentado pela Corte Europeia, em decisão recente (2013), é o caso Eweida and others v. United Kingdom, que envolve a tensão entre o direito à liberdade religiosa e a proibição da discriminação em razão da orientação sexual. Os peticionários, sob fundamentação diversa, reclamaram à Corte, alegando que o direito interno do Reino Unido teria falhado em proteger adequadamente o direito à liberdade de manifestação de crença religiosa. No julgamento, a Corte Europeia afirmou que, muito embora o direito à liberdade de religião seja um dos fundamentos das sociedades pluralistas e democráticas, a manifestação de determinada crença deve ser limitada quando a expressão da fé colidir com os direitos das outras pessoas. Vale dizer, a Corte afirmou

vedava também discriminações em razão da orientação sexual do sujeito. O elenco de situações referidas nessa disposição teria um carácter meramente indicativo, e não taxativo.[378] No segundo, o Tribunal destacou que a transexualidade era uma noção abrangida pelo artigo 14, o qual continha uma lista não exaustiva de razões proibidas para serem utilizadas para tratamentos discriminatórios.[379]

Em 2011, na Convenção do Conselho da Europa para a Prevenção e o Combate à Violência contra as Mulheres e à Violência Doméstica (Convenção de Istambul), em seu artigo 4º, §3º, foram mencionados importantes conceitos, como orientação sexual e identidade de gênero, ao se prever que: "As Partes deverão aplicar o disposto na presente Convenção, em especial as medidas que visam proteger os direitos das vítimas, sem discriminação alguma baseada nomeadamente no sexo, no género, na raça, na cor, na língua, na religião, na opinião política ou outra, na origem nacional ou social, na pertença a uma minoria nacional, na fortuna, no nascimento, na orientação sexual, na identidade de género, na idade, no estado de saúde, na deficiência, no estado civil, no estatuto de migrante ou de refugiado ou qualquer outro." Ao longo dos anos, verifica-se que o reconhecimento de direitos a grupos LGBTQIA+ e o uso de conceitos fundamentais para um tratamento igualitário para as pessoas vêm sendo ampliados em caráter global. Nesse sentido, recorda-se ainda decisão da Corte Interamericana de Direitos Humanos (CIDH), que na Opinião Consultiva OC-24/7, de 24 de novembro de 2017, solicitada pela República de Costa Rica, expressamente asseverou que a orientação sexual, a identidade de gênero e a expressão de gênero são categorias protegidas pelo artigo 1.1 da Convenção Americana de Direitos Humanos, estando, portanto, vedada qualquer norma, ato ou prática discriminatória baseada na orientação sexual ou na identidade de gênero das pessoas (item 68). A Corte Interamericana asseverou que dentre os fatores que definem a identidade sexual e de gênero de uma pessoa se apresenta como prioridade o fator subjetivo sobre seus caracteres físicos ou

---

que em nome da liberdade religiosa não é admitida a violação de direitos; a liberdade de crença não pode suplantar o direito à livre manifestação da orientação sexual." (PIOVESAN, Flávia; SILVA, Sandro Gorski. Diversidade sexual e o contexto global: desafios à plena implementação dos direitos humanos LGBTI. *Quaestio Iuris*. vol. 08, nº. 04, Número Especial. Rio de Janeiro, 2015. p. 2613-2650.)

[378] Tribunal Europeu dos Direitos Humanos. Case of Salgueiro da Silva Mouta v. Portugal, no. 33290/96, de 21 de dezembro de 1999, Estrasburgo.

[379] Tribunal Europeu dos Direitos Humanos. Affaire P.V. c. Espagne, no. 35159/09, de 30 de novembro de 2010, Estrasburgo.

morfológicos. As novas tecnologias e os dispositivos conectados tratam de forma praticamente direta e ininterrupta dados pessoais. Diante dos riscos advindos desse cenário, mostra-se urgente promover uma tutela especial e bem estruturada de dados relativos à identidade de gênero, à orientação sexual e à vida sexual, pois, como demonstrado, seu tratamento muitas vezes possibilita discriminações ilícitas ou abusivas, trazendo efetivos prejuízos especialmente à comunidade LGBTQIA+.[380] Vale lembrar que, em diversos locais do mundo, a mera disponibilização de dados referentes à vida sexual de um indivíduo pode trazer sérios riscos à sua integridade[381], havendo, inclusive, previsões de pena de morte como punição por atos sexuais consensuais entre pessoas do mesmo sexo.[382]

Dados sobre a vida sexual, compreendidos de forma ampla, podem ser analisados e, até mesmo, inferidos a partir das mais diversas fontes e meios, alimentados tanto pelo próprio titular quanto por terceiros. Exemplos disso são as interações e os fluxos de informações extraídos de redes sociais; listas de compras de produtos e serviços; opções personalizadas marcadas em objetos eróticos; uso de aplicativos de relacionamento[383] que promovem conexão entre pessoas a partir de

---

[380] No início de 2020, a Senacon (Secretaria Nacional do Consumidor) afirmou que notificaria os aplicativos de encontros Tinder e Grindr para esclarecerem sobre um suposto compartilhamento ilegal de dados pessoais dos usuários, identificado pelo Conselho de Consumidores da Noruega no relatório *Out of Control*. De acordo com o estudo, o Grindr, destinado especificamente ao grupo LGBT, compartilharia dados de localização de usuários e informações pessoais como orientação sexual para outras empresas. Da mesma forma, o Tinder compartilharia dados de seus usuários com diversas empresas, como informações sobre o gênero do usuário e qual o gênero ele estaria interessado. Fonte: <https://g1.globo.com/economia/tecnologia/noticia/2020/01/15/ministerio-da-justica-vai-notificar-tinder-e-grindr-por-suposta-venda-ilegal-de-dados-pessoais-dos-usuarios.ghtml?utm_source=meio&utm_medium=email> Acesso em:15.08.21. Em 2018, recorda-se notícia que apontou que o Grindr estava repassando dados pessoais, inclusive sensíveis, de seus usuários para empresas parceiras. Dentre os dados repassados, estavam o status de Vírus da Imunodeficiência Humana (HIV), localização, e-mail e telefone da pessoa. Informação disponível em: <https://www.npr.org/sections/thetwo-way/2018/04/03/599069424/grindr-admits-it-shared-hiv-status-of-users> Acesso em: 15.08.21.

[381] ILGA World: Lucas Ramon Mendos, Kellyn Botha, Rafael Carrano Lelis, Enrique López de la Peña, Ilia Savelev and Daron Tan, *State-Sponsored Homophobia 2020: Global Legislation Overview Update*. Dezembro de 2020. Disponível em: <https://ilga.org/state-sponsored-homophobia-report> Acesso em: 07.03.21.

[382] Cf. COSTA, Ramon S. *Entre taps e direitos*: proteção de dados pessoais, privacidade e liberdade no aplicativo Grindr. Dissertação (Mestrado em Direito). Universidade Federal de Juiz de Fora. 185 p. 2020.

[383] O aplicativo *Happn* lançou um recurso para identificar de forma mais precisa seus usuários. Segundo seus termos de uso: "Todo happner pode solicitar a autentificação de seu perfil gratuitamente. Para fazer isso, basta ir na tela de edição de perfil e selecionar "Obter". O aplicativo pedirá que você faça um movimento com a cabeça enquanto olha para a tela. Uma vez concluída essa operação, os dados biométricos deste vídeo serão comparados com os dados das fotos do seu perfil. Se a verificação funcionar, o seu perfil será autentificado. Caso contrário, você terá que tentar novamente." Disponível em: <https://www.happn.com/pt-br/faq/articles/360015322037> Acesso em: 21.02.22

preferências de gênero e localização dos usuários; vibradores sexuais com opções personalizáveis e, inclusive, acesso à distância por meio de aplicativo[384]; e acessos realizados a sites de pornografia. Sites com conteúdo pornográfico costumam realizar, como regra, elevado rastreamento de dados de seus usuários, não apresentam políticas transparentes de privacidade e oferecem recursos escassos de segurança da informação.[385] Cenário esse que apenas se agrava quando se constata que, principalmente após o início da pandemia de coronavírus, as principais plataformas de pornografia têm registrado recordes históricos de acesso aos seus conteúdos.[386] Mesmo quando não questionam diretamente dados relacionados à vida sexual dos seus usuários, dependendo da forma como eles usarem o site e os serviços relacionados, suas informações pessoais poderão incluir informações que permitirão, com certa facilidade, tirar conclusões sobre sua vida sexual, gênero e orientação sexual.[387] Registros de navegação indicando quais gêneros pornográficos um usuário acessou e mensagens em chats eróticos identificando suas preferências sexuais são casos claros que evidenciam esses tipos de dados. Observa-se, inclusive, que é possível inferir preferências de gênero tão somente a partir das URLs acessadas.

Pergunta-se: tendo em vista a natureza de um site pornográfico, é possível separar dados pessoais de um usuário e tratá-los como dados não sensíveis? Nesse caso, seria possível entender que mesmo dados comuns sobre uma pessoa (como nº de cartão de crédito, CPF, RG, nome do usuário, dados de geolocalização e IP) deveriam ser considerados dentro de um tratamento sensível de

---

[384] TEFFÉ, Chiara A. Spadaccini de. Brinquedos sexuais e coleta de dados sensíveis: voyeurismo 3.0? *Medium ITS Rio*, maio de 2017. Disponível em: <https://feed.itsrio.org/brinquedos-sexuais-e-coleta-de-dados-%C3%ADntimos-voyeurismo-3-0-be570007bf1f > Acesso em 07.03.21

[385] MARIS, Elena; LIBERT, Timothy; HENRICHSEN, Jennifer R. Tracking Sex: The Implications of Widespread Sexual Data Leakage and Tracking on Porn Websites. *New Media & Society*, vol. 22, n. 11, Nov. 2020, p. 2018–2038. Disponível em: <https://doi.org/10.1177/1461444820924632> Acesso em: 07.03.21. No artigo, ao realizarem pesquisa, os autores afirmaram que: "Our analysis of 22,484 pornography websites indicated that 93% leak user data to a third-party. Tracking on these sites is highly concentrated by a handful of major companies, which we identify. We successfully extracted privacy policies for 3856 sites, 17% of the total. The policies were written such that one might need a 2-year college education to understand them. Our content analysis of the sample's domains indicated 44.97% of them expose or suggest a specific gender/sexual identity or interest likely to be linked to the user. We identify three core implications of the quantitative results: (1) the unique/elevated risks of porn data leakage versus other types of data, (2) the particular risks/impact for "vulnerable" populations, and (3) the complications of providing consent for porn site users and the need for affirmative consent in these online sexual interactions."

[386] Disponível em: <https://www.uol.com.br/universa/colunas/mayumi-sato/2021/02/21/pandemia-e-pornografia-60-tem-consumido-mais-e-vicio-preocupa.htm?cmpid=copiaecola> Acesso em: 07.03.21.

[387] Disponível em: <https://www.brasileirinhas.com.br/politica-de-privacidade.html> Acesso em: 07.03.21.

informações, uma vez que a sua presença na base de dados de sites pornográficos, por si só, já revelaria elementos de sua vida sexual?

Sobre o tema, o GDPR apresenta as seguintes expressões dentro do rol dos dados sensíveis (Art.9º): "dado relativo à vida sexual" e "orientação sexual", porém não traz referência direta acerca de proteção especial à identidade de gênero. Nos considerandos 71 e 75 da norma, encontra-se disposto que o tratamento de dados pessoais deve evitar efeitos discriminatórios sobre as pessoas naturais, sendo recordadas, aqui, as informações sobre a orientação sexual do sujeito e as relativas à sua vida sexual. Não há dúvidas de que o conceito de dado referente à vida sexual presente na LGPD precisará ser amplamente discutido pela doutrina. Mostra-se necessário tutelar nesta categoria mais informações do que aquelas relacionadas estritamente ao conjunto de comportamentos que concernem à satisfação da necessidade e do desejo sexual. Seu conteúdo deve ter como base estudos e documentos internacionais de proteção aos direitos humanos, bem como os postulados da metodologia do direito civil-constitucional, para que seja possível inserir em seu bojo tutelas ampliadas para grupos mais vulneráveis e historicamente discriminados.[388] Visa-se, assim, conferir especial proteção a "pessoas que são sistematicamente vitimadas em virtude de serem exatamente quem são, no livre exercício da orientação sexual e da identidade de gênero que é integrante do núcleo intangível de promoção da pessoa humana."[389] O tratamento discriminatório com fundamento na orientação sexual ou identidade de gênero deve receber resposta adequada do ordenamento, visando à eliminação e coibição de condutas atentatórias de direitos e liberdades

[388] "First, a data protection law must be addressed from a human rights perspective, protecting vulnerable communities, such as the LGBTQIA+ population. Second, a diversity-prone interpretation of a data protection law allows countries to restrain discriminatory or abusive data processing against minority groups. Third, sexual orientation should be considered sensitive personal data under the LGPD because "sexual life" encompasses "sexual orientation." Fourth, gender identity should be regarded as sensitive personal data according to Brazilian Supreme Court's jurisprudence defining "racism" and "race." Fifth, the fourth conclusion fully applies to sexual orientation. (FICO, Bernardo de Souza Dantas; SICUTO, Guilherme Hernandes; NÓBREGA, Henrique Meng. Does Brazil's LGPD recognize gender identity, sexual orientation as sensitive personal data? IAPP, publicado em 10 de março de 2021. Disponível em: <https://iapp.org/news/a/does-brazils-lgpd-recognize-gender-identity-and-sexual-orientation-as-sensitive-personal-data/> Acesso em: 10.03.21.)

[389] ZANGEROLAME, Flávia; ALMEIDA, Vitor. A seletividade sexual e a intolerância à diversidade: a silenciosa discriminação cotidiana como dano injusto, migalhas, 5 de julho de 2021. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-vulnerabilidade/348038/a-seletividade-sexual-e-a-intolerancia-a-diversidade> Acesso em: 06.07.21

fundamentais.[390] Dessa forma, defende-se a inserção dentro desta categoria de dados relativos à orientação sexual do sujeito e, a depender da estrutura do tratamento e da atividade desenvolvida, de dados sobre a identidade de gênero da pessoa, o que não exclui certamente outras questões relacionadas à sexualidade e à intimidade sexual.

Uma vez finalizado o capítulo 2, foi possível até o momento desenvolver estudo acerca da evolução e do conteúdo dos dados pessoais sensíveis, bem como das principais espécies de dados assim qualificados. Compreender quais informações são sensíveis é tarefa, por vezes, árdua, a qual demanda análise contextual e funcional dos dados tratados e de suas possíveis interações dentro do ambiente tecnológico. Como analisado, a depender inclusive das informações dispostas e de seus titulares será necessário aplicar, além de hipóteses mais restritas para o tratamento de dados, requisitos tecnológicos e de segurança da informação mais sofisticados e robustos, em razão da elevação dos riscos e dos possíveis danos. Parte-se, agora, para o capítulo 03 da tese, em que haverá a aplicação da lógica até então desenvolvida para o tratamento dos dados sensíveis conforme as normas da LGPD.

[390] "A visibilidade das minorias como corolário da representatividade e a exclusão de personagens homossexuais e transexuais das publicidades e produções audiovisuais, de um modo geral, é tema cujo enfrentamento deve ser feito em conjunto com a própria dinâmica do desenvolvimento da sociedade, em que a abertura para a pluralidade vai avançando na medida em que a busca pela igualdade se revela crescente nos espaços públicos e privados. A seletividade na restrição da veiculação das vivências da comunidade LGBTQIAP+ mostra-se em descompasso com a legalidade constitucional, em especial os valores existenciais prevalentes, passível de gerar danos extrapatrimoniais coletivos. (...)" (ZANGEROLAME, Flávia; ALMEIDA, Vitor. A seletividade sexual e a intolerância à diversidade: a silenciosa discriminação cotidiana como dano injusto, migalhas, 5 de julho de 2021. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-vulnerabilidade/348038/a-seletividade-sexual-e-a-intolerancia-a-diversidade> Acesso em: 06.07.21)

3. DISCIPLINA NORMATIVA APLICÁVEL PARA O TRATAMENTO DE DADOS SENSÍVEIS

Após desenvolver a categoria dos dados sensíveis, realçar a sua importância para o livre desenvolvimento e expressão da pessoa humana e discutir o seu conteúdo, busca-se no capítulo 03 analisar as normas relativas ao tratamento dos dados pessoais sensíveis e às bases legais aplicáveis a eles. Para tanto, inicialmente, será realizado estudo acerca das hipóteses de tratamento de dados pessoais na LGPD e da estrutura de aplicação da referida lei. Em seguida, a atenção será dirigida ao artigo 11 da LGPD, que traz o rol de bases legais para o tratamento de dados pessoais sensíveis. Por fim, será aprofundado estudo a respeito do tratamento de dados sensíveis de crianças e de adolescentes, levando-se em consideração a sua especial condição de pessoa em desenvolvimento, que deve ser tutelada de forma integral e com base em seu melhor interesse.

3.1 **Tratamento de dados pessoais: requisitos e características**

Qualquer pessoa que trate dados pessoais, seja ela natural ou jurídica, de direito público ou privado, inclusive na atividade realizada nos meios digitais, deverá ter uma

base legal para fundamentar os tratamentos realizados. Por base legal, entende-se a hipótese legal disposta nos artigos 7º ou 11, a qual pode ser complementada – a depender do caso concreto – pelas normas dos artigos 14 ou 23 da LGPD. Essas bases foram estipuladas de forma geral e variada, devendo eventuais detalhes e adequações serem especificados principalmente pela Autoridade Nacional de Proteção de Dados, pelo Legislativo, pelo Judiciário e pela doutrina.[391]

Ainda que seja possível utilizar mais de uma base legal para determinado tratamento de dados, é preciso buscar a base mais *adequada* e *segura* para a situação concreta, levando em conta práticas de mercado, orientações de especialistas, guias de autoridades responsáveis pela proteção de dados em âmbito estrangeiro e o equilíbrio entre os direitos dos titulares e as melhores opções para o desenvolvimento dos negócios. Mostra-se necessário que o agente de tratamento realize uma análise ponderada que considere riscos e benefícios ao selecionar a base.

Cabe recordar que a noção de "tratamento" disposta na LGPD engloba toda operação realizada com dados pessoais, como aquelas que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Há, assim, amplo rol de ações dispostas na lei dentro da ideia contida em tratamento de dados pessoais. Por consequência, todas essas ações deverão ser respaldadas por uma base legal. No momento de seleção da base legal, mostra-se relevante refletir acerca de algumas questões que envolvem o dado pessoal, seu titular e a forma de tratamento. Sobre isso, de forma didática, vale propor as seguintes perguntas:

a) A LGPD é aplicável ao tratamento em questão (Arts. 1º e 3º)? O tratamento se enquadra nas exceções previstas no Art. 4º da LGPD?
b) O titular do dado é uma criança, um adolescente ou um adulto?
c) O dado pessoal é sensível?

[391] Cf. TEFFÉ, Chiara Spadaccini de; VIOLA, M. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. *Civilistica.com*, v. 9, p. 1-38, 2020. VIOLA, M.; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11. In: Bruno Bioni, Laura Schertel Mendes, Danilo Doneda, Otavio Luiz Rodrigues Jr., Ingo Wolfgang Sarlet. (Org.). *Tratado de Proteção de dados pessoais*. 2. ed. Rio de Janeiro: Forense, 2022.

d) O agente de tratamento está enquadrado no capítulo IV da LGPD (que versa sobre o tratamento de dados pessoais pelo Poder Público)?

e) O dado pessoal foi coletado diretamente do titular ou foi obtido por meio de terceiro? Qual a sua origem? A obtenção foi lícita?

f) Qual a finalidade do tratamento de dados pessoais?

Entende-se que tanto o rol do Art. 7º (destinado ao tratamento de dados pessoais comuns) quanto o do Art. 11 (voltado ao tratamento de dados pessoais sensíveis) são primordialmente taxativos,[392] sendo complementados – a depender do caso – pelos artigos 14 e 23 da LGPD. No Art. 7º, é pacífico o entendimento de que todas as bases apresentam o mesmo peso e importância, o que, porém, não se verifica no Art. 11 da LGPD, já que, para certos autores, o consentimento ali apresentaria alguma preferência em face das demais bases. Outro fato relevante acerca das duas listas de bases legais é a ausência ou alteração de algumas bases relativas especialmente a contratos, legítimo interesse e tutela do crédito. Para melhor visualização da discussão, segue tabela com comparativo das bases legais:

Bases legais	**Art. 7º da LGPD**	**Art. 11 da LGPD**
Consentimento: manifestação livre, informada e inequívoca pela qual o titular	X	Consentimento dado, de forma específica e

[392] No regulamento europeu de proteção de dados (GDPR), utiliza-se a mesma sistemática para a aplicação das bases legais para o tratamento de dados pessoais: "The principle of 'lawful processing', which is one of several data protection principles under Article 5 GDPR, requires that every processing operation involving personal data must have a legal basis. Article 6(1) stipulates what may constitute such a legal basis. At the same time, it must be kept in mind that legally sound processing of personal data will necessitate fulfilling also all other of the core principles for processing personal data set out by Article 5(1). The list of legal grounds for processing contained in Article 6(1) must be understood as exhaustive and final – it can neither be supplemented nor otherwise amended by interpretation. As far as Member States' legislators are, at all, allowed to act under Article 6(1),1 all legislative activities must keep within the strict boundaries it sets. The elements in the list must be seen to be legally equal. There is no ranking between Article 6(1)(a) to (f) in the sense that one ground has normative priority over the others.3 However, in the private sector, consent (Article 6(1)(a)) may in practice play a salient role as a potential substitute whenever there is no contractual context, no detailed legal rules about a fitting legal basis, or the scope of 'legitimate interests of the controller or of a third party' is particularly difficult to assess. This may also be the reason why it was deemed necessary in the GDPR to define valid consent more extensively than the other legal grounds for processing and - compared to the DPD – to add two articles (Articles 7 and 8) dealing with specific aspects of consenting" (KOTSCHY, Waltraut. Lawfulness of processing. In: *2018 Draft commentaries on 10 GDPR articles* (from Commentary on the EU General Data Protection Regulation, OUP 2019). Oxford University Press, 2018, p. 37. Disponível em: <https://works.bepress.com/christopher-kuner/1/>. Acesso em: 22.07.19).

concorda com o tratamento de seus dados pessoais para uma finalidade determinada (Art.5º, XII)		destacada, para finalidades específicas
Cumprimento de obrigação legal ou regulatória pelo controlador	X	X
Administração Pública e políticas públicas	pela administração pública, para o tratamento e uso compartilhado de 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	tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos
Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;	X	X
Necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados	X	Sem correspondente
Exercício regular de direitos	para o exercício regular de direitos em processo judicial, administrativo ou arbitral	exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral
Proteção da vida ou da incolumidade física do titular ou de terceiro	X	X
Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária	X	X
Necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a	X	Sem correspondente

proteção dos dados pessoais		
Proteção do crédito, inclusive quanto ao disposto na legislação pertinente	X	Sem correspondente
Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.	Sem correspondente	X

Há autores que defendem a existência de uma outra base legal para o tratamento de dados pessoais no Art. 23 da LGPD[393], que seria voltada para a execução das competências legais ou o cumprimento das atribuições legais do serviço público.[394] Contudo, é possível compreender que o tratamento de dados pessoais para tais atividades já estaria contemplado, em grande parte, nas hipóteses relativas ao cumprimento de uma obrigação legal (Art. 7º, II, e Art. 11, II, 'a'), já que a atuação da Administração Pública decorre de um mandamento legal, e ao tratamento e uso compartilhado de dados necessários à execução de políticas públicas (Art. 7º, III, e Art. 11, II, 'b'). A previsão contida no Art. 23 traria apenas requisitos adicionais e específicos para o tratamento de dados pessoais quando realizado pelo poder público. Esse entendimento foi, inclusive, indicado em guia da ANPD sobre o tratamento de dados pessoais pelo poder público:

> O tratamento de dados pessoais pelo Poder Público deve se amparar em uma das hipóteses previstas no art. 7º ou, no caso de dados sensíveis, no art. 11 da LGPD. Esses dispositivos devem ser interpretados em conjunto e de forma sistemática com os critérios adicionais previstos no art. 23, que

[393] LGPD - "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: I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; II - (VETADO); e III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; (...)"

[394] MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. *Revista de Direito do Consumidor*, v. 120, p. 555, 2018.

> complementam e auxiliam a interpretação e a aplicação prática das bases legais no âmbito do Poder Público (...).[395]

Observa-se que a Administração Pública em determinados casos poderá utilizar outras bases legais, como, por exemplo, a proteção da vida ou da incolumidade física do titular ou de terceiro; o exercício regular de direitos em processo judicial, administrativo ou arbitral; a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; e a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária. Há questionamentos relevantes acerca das possibilidades e dos procedimentos para a eventual aplicação das bases legais do consentimento, diante da assimetria entre as partes e da própria natureza da função pública, e do legítimo interesse por parte da Administração.

De forma a evitar abusos no tratamento de dados (sensíveis ou não) e a garantir os direitos do titular, ele poderá revogar o seu consentimento (Art. 18, IX) ou pleitear o direito à oposição, que significa que o titular poderá se opor a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto na LGPD (Art. 18, §2º). Além disso, encontra-se positivado o direito à explicação (Art. 20), que dispõe que o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

Observa-se que, diante do disposto no Art. 4º da LGPD, suas normas não se aplicarão ao tratamento de dados pessoais (inclusive sensíveis):

a) Realizado por pessoa natural para fins exclusivamente particulares e não econômicos, como, por exemplo, uma lista de contatos inserida em agenda telefônica pessoal, no celular ou em formato físico; um álbum de fotos particular; anotações pessoais em um caderno; troca de correspondência íntima; lista de nomes de pessoas para permitir a entrada em condomínio edilício; manutenção de registro de dados

---

[395] ANPD. Guia Orientativo. *Tratamento de Dados Pessoais pelo Poder Público*. Janeiro/2022. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/no-dia-internacional-da-protecao-de-dados-anpd-publica-guia-orientativo-sobre-tratamento-de-dados-pessoais-pelo-poder-publico> Acesso em: 02.02.2022.

sensíveis de saúde de familiares para ajudar em caso de emergência; e diário pessoal contendo gostos e interesses de terceiros. Nesse caso, não há vantagem financeira ou uso profissional.

b) Realizado para fins exclusivamente jornalístico ou artísticos. Essa exceção visa a proteger a liberdade de expressão e a liberdade artística. Por maioria, o Plenário do Supremo Tribunal Federal decidiu que é inconstitucional a exigência do diploma de jornalismo e registro profissional no Ministério do Trabalho como condição para o exercício da profissão de jornalista (Recurso Extraordinário 511.961, julgado em 2009). No caso, é importante analisar se a empresa ou pessoa tem como objeto social ou atividade preponderante o jornalismo e se a notícia possui interesse público ou relevância social.[396]

c) Realizado para fins exclusivamente acadêmicos, aplicando-se a esta hipótese os Arts. 7º e 11 da LGPD. Aqui, não é hipótese de não aplicação da LGPD, mas sim de aplicação mitigada, visto que há referência aos artigos que trazem as bases legais de tratamento.

d) Realizado para fins exclusivos de: segurança pública; defesa nacional; segurança do Estado; ou atividades de investigação e repressão de infrações penais. Nesses casos, os tratamentos realizados envolvem interesse e segurança públicas. São atividades de competência do Poder Público.

e) Provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

Dispõe o §1º, do Art.4º, da LGPD, que 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

[396] Information Commissioner's Office (ICO). *Data protection and journalism*: a guide for the media. 2014. Disponível em: <https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf> Acesso em: 12.07.21. Até janeiro de 2022, estava aberta consulta na ICO para o projeto de código de práticas no jornalismo. Disponível em: <https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-the-draft-journalism-code-of-practice/> Acesso em: 21.02.22.

titular previstos nesta Lei. Adicionalmente, a Autoridade Nacional de Proteção de Dados emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais (§3º), sendo neste caso obrigatório elaborar o relatório.

Diante da previsão legal, uma comissão de juristas foi criada pelo presidente da Câmara (na época) para elaborar anteprojeto de legislação específica[397], que foi divulgado em novembro de 2020 e ficou conhecido como a "LGPD Penal". Esse anteprojeto busca oferecer parâmetros específicos e seguros para operações de tratamento de dados pessoais no âmbito de atividades de *segurança pública* e de *persecução criminal*, equilibrando tanto a proteção do titular contra abusos quanto o acesso de autoridades a todo potencial de ferramentas e plataformas para segurança pública e investigações.[398] Não cobre, portanto, toda a extensão de atividades do inciso III. [399]

A LGPD inspirou-se claramente no Regulamento europeu de proteção de dados. A norma europeia regulou o tratamento de dados para fins de segurança pública e persecução penal separadamente de seu marco normativo aplicável ao tratamento de dados pessoais como um todo (Regulamento 679/2016), havendo, assim, norma especial: a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, a qual estabelece regras específicas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e prevenção de ameaças à segurança pública. Como apresentado, a mesma escolha pela lei específica foi tomada

[397] Câmara dos deputados. Ato do Presidente, de 26 de novembro de 2019. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/conheca-a-comissao/criacao-e-constituicao/ato-de-criacao. Acesso em: 14.07.21.

[398] Exposição de motivos: Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. "Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais realizado por autoridades competentes para atividades de segurança pública e de persecução penal, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural."

[399] Na exposição de motivos do anteprojeto, afirmou-se que: "(...) há um enorme déficit de proteção dos cidadãos, visto que não há regulação geral sobre a licitude, a transparência ou a segurança do tratamento de dados em matéria penal, tampouco direitos estabelecidos ou requisitos para utilização de novas tecnologias que possibilitam um grau de vigilância e monitoramento impensável há alguns anos. Apesar do crescimento vertiginoso de novas técnicas de vigilância e de investigação, a ausência de regulamentação sobre o tema gera uma assimetria de poder muito grande entre os atores envolvidos (Estado e cidadão)."

na LGPD, em seu Art. 4º, par. 1º, para atividades estratégicas do Poder Público voltadas à proteção do Estado e dos cidadãos.[400]

Na LGPD, acerca do tratamento de dados para *fins exclusivos de segurança pública* (Art.4º, III, "a"), vale levantar algumas questões: o bem tutelado seria apenas a segurança pública em sentido estrito ou poderia ser alargado em um contexto próximo ao de interesse público? Questões de segurança nacional estão englobadas pelo Art. 4º, III, da LGPD? Como poderia ser aplicada a mencionada exceção para respaldar tratamentos de dados advindos de reconhecimento facial realizado pelo Estado? Quais seriam os limites se a mencionada tecnologia fosse fruto – como geralmente ocorre – de uma parceria com agente privado? [401] [402]

Pensando na última questão, o parágrafo 2º, do Art. 4º, destaca que é vedado o tratamento dos dados a que se refere o inciso III por pessoa jurídica de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à Autoridade Nacional e que deverão observar a limitação imposta no parágrafo 4º: "Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público", como é o caso da empresa pública.

Feitas essas considerações, sendo um tratamento de dados pessoais em que haja a aplicação da LGPD[403], deverá desde logo o agente indicar base legal pertinente para o

---

[400] Cf. FERGUSON, Andrew. *The Rise of Big Data Policing*: Surveillance, Race, and the Future of Law Enforcement. New York University Press, 2017. ANGWIN, Agoia; LARSON, Jeff; MATTU, Surya; KIRCHNER, Laure. Machine Bias: Risk assessments in criminal sentencing. *ProPublica*, publicado em maio de 2016. Disponível em: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> MAYSON, Sandra Gabriel. *Bias In, Bias Out*. University of Georgia School of Law Legal Studies, Research Paper No. 2018-35. Disponível em: <https://ssrn.com/abstract=3257004> Acesso em: 03.05.21.

[401] TEFFÉ, Chiara Spadaccini de; FERNANDES, Elora. Tratamento de dados sensíveis por tecnologias de reconhecimento facial: proteção e limites. In: Gustavo Tepedino; Rodrigo da Guia Silva. (Org.). *O Direito Civil na Era da Inteligência Artificial.* 1ed.São Paulo: Editora dos Tribunais, 2020, v. 1, p. 283-310.

[402] A título exemplificativo, recorda-se experimento promovido durante o Carnaval de 2019 no Rio de Janeiro pela Polícia Militar e empresa de telefonia. Os dados foram tratados pela Oi e houve aplicação de tecnologia da Huawei, quando algumas pessoas foram presas. Nesse caso, houve intenso debate sobre os dados coletados, a falta de transparência da empresa sobre determinados tratamentos realizados e a real efetividade da tecnologia (MARTINS, Helena. Reconhecimento Facial: a banalização de uma tecnologia controversa. *Le Monde Diplomatique Brasil*. 22 abr. 2020. Disponível em: https://diplomatique.org.br/reconhecimento-facial-a-banalizacao-de-uma-tecnologia-controversa/. Acesso em: 08 de maio 2020.)

[403] LGPD – "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

tratamento praticado, levando em conta especialmente os tipos de dados em questão, a idade do titular e sua natureza jurídica enquanto agente de tratamento (se privada ou pertencente ao setor público). Diante do recorte proposto para a presente tese, passa-se ao longo dos próximos títulos para o estudo aprofundado e crítico das bases legais relativas ao tratamento de dados pessoais sensíveis de adultos, adolescentes e crianças.

3.2 **Seleção da base legal mais adequada para o tratamento de dados sensíveis**

Dispõe a LGPD em seu artigo 11 que o tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; ou II – quando sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para as situações expressas nas alíneas desse artigo: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;[404] c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei de Arbitragem (Lei nº 9.307, de 23 de setembro de 1996); e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de

direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. (...) 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."

[404] Art. 11, II, §2º Nos casos de aplicação do disposto nas alíneas "a" e "b" do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.

saúde ou autoridade sanitária; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no Art. 9º da LGPD e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. Nessa situação, devem todos os cuidados já previstos para o tratamento dos dados ser aplicados de forma ainda mais intensa, já que para os dados sensíveis se espera um padrão ainda mais rigoroso de proteções técnica e jurídica. Em um tratamento específico em que haja mescla de dados pessoais sensíveis e não sensíveis deverá prevalecer, naturalmente, um critério de maior rigor, de forma que os tratamentos de dados respeitem a necessidade de uma base legal disposta no Art. 11 da LGPD.

Em leitura comparativa das bases legais, como apresentado acima, verifica-se que o artigo 11 mantém várias das bases já previstas no artigo 7º para o tratamento de dados pessoais, deixando de fora expressamente do tratamento de dados sensíveis as hipóteses de atendimento aos interesses legítimos do controlador ou de terceiro (Art. 7º, IX) e de proteção do crédito (Art. 7º, X)[405]. A base referente ao contrato recebe no artigo 11 novos contornos, podendo o tratamento de dados sensíveis se dar para o exercício regular de direitos, inclusive em contrato.

O legítimo interesse é hipótese legal que visa a possibilitar tratamentos de dados pessoais, por parte do controlador ou de terceiro, que estejam vinculados ao escopo de

[405] Recorda-se que, na Lei do Cadastro Positivo (Lei n. 12.414/11), os bancos de dados poderão conter informações de adimplemento do cadastrado, para a formação do histórico de crédito, nas condições estabelecidas nesta lei, *ficando proibidas as anotações de informações sensíveis ou excessivas*. Para a formação do banco de dados, somente poderão ser armazenadas informações objetivas, claras, verdadeiras e de fácil compreensão, que sejam necessárias para avaliar a situação econômica do cadastrado. A vedação do uso de dados sensíveis busca evitar a utilização discriminatória da informação e garantir o dever de respeito à privacidade do consumidor. Nesse sentido, no Recurso Especial 1.419.697 (DJe 17/11/2014), foi estabelecido que na avaliação do risco de crédito devem ser respeitados os limites estabelecidos pelo sistema de proteção do consumidor no sentido da tutela da privacidade e da máxima transparência nas relações negociais, como disposto no Código de Defesa do Consumidor e na Lei 12.414/11. Além disso, no tocante ao sistema *scoring* de pontuação, afirmou-se que, "Apesar de desnecessário o consentimento do consumidor consultado, devem ser a ele fornecidos esclarecimentos, caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem como as informações pessoais valoradas" (entendimento que motivou a Súmula 550 do STJ). Em seguida, destacou-se que não podem ser valoradas pelo fornecedor do serviço de *credit scoring* informações sensíveis, ficando caracterizado abuso do direito a utilização de informações sensíveis, excessivas, incorretas ou desatualizadas. Veja-se, a esse título, *Transparência e Governança nos algoritmos: um estudo de caso sobre o setor de birôs de crédito*. Disponível em: <https://itsrio.org/pt/publicacoes/transparencia-e-governanca-nos-algoritmos-um-estudo-de-caso/>Acesso em: 14.07.21

suas atividades e que encontrem justificativa legítima.[406] Há no caso relação relevante e apropriada entre o titular dos dados e o responsável pelo seu tratamento, como, por exemplo, em situações quando o titular é um cliente do controlador e este deseja aplicar ações de marketing direto. Diante da flexibilidade dessa base legal, as expectativas do titular dos dados têm peso especialmente relevante para a sua aplicação, devendo ser consideradas também a finalidade, a necessidade e a proporcionalidade da utilização dos dados no caso concreto.

Dessa forma, a existência de um interesse legítimo exige uma avaliação cuidadosa, incluindo se o titular dos dados pode razoavelmente esperar, no momento e no contexto da coleta dos dados, que o tratamento para esse fim possa ocorrer. Os interesses e direitos fundamentais do titular podem, em particular, prevalecer sobre o interesse do responsável pelo tratamento quando os dados pessoais forem tratados em circunstâncias em que os titulares não esperem um tratamento posterior.

Quanto mais invasivo, inesperado ou genérico for o tratamento, menor será a probabilidade de que seja reconhecido o legítimo interesse do controlador ou de terceiro no caso concreto. Incluem-se, aqui, dentre outras relações, tratamentos de dados pessoais em que a obtenção do consentimento do titular poderia atrasar — ou mesmo inviabilizar — a exploração regular das informações. Mostrar que há um interesse legítimo significa que o controlador (ou um terceiro) deve ter algum benefício ou resultado claro e específico com o tratamento, não sendo tal interesse ilegítimo, antiético ou ilegal. Não basta afirmar a existência de interesses vagos ou genéricos. [407]

---

[406] Análise do legítimo interesse extraída do seguinte artigo: TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11. In: BIONI, Bruno; DONEDA, Danilo; SARLET, Ingo Wolfgang; SCHERTEL, Laura; JUNIOR, Otavio Luiz Rodrigues (Coord.). *Tratado de Proteção de Dados Pessoais*. 1ª ed. Rio de Janeiro: Editora Forense, 2021.

[407] Como exemplos de legítima expectativa de tratamento dados, vale trazer o seguinte exemplo: "An individual uploads their CV to a jobs board website. A recruitment agency accesses the CV and thinks that the individual may have the skills that two of its clients are looking for and wants to pass the CV to those companies. It is likely in this situation that the lawful basis for processing for the recruitment agency and their clients is legitimate interests. The individual has made their CV available on a job board website for the express reason of employers being able to access this data. They have not given specific consent for identified data controllers, but they would clearly expect that recruitment agencies would access the CV and share with it their clients, indeed, this is likely to be the individual's intention. As such, the legitimate interest of the recruitment agencies and their clients to fill vacancies would not be overridden by any interests or rights of the individual. In fact, those legitimate interests are likely to align with the interests of the individual in circulating their CV in order to find a job." Outro exemplo a se mencionar seria: "An individual creates a profile on a social networking website designed specifically for professional networking. There is a specific option to select a function to let recruiters know that the individual is open to job opportunities. If the individual chooses to select that option, they would clearly

Exemplos de aplicação da base legal do legítimo interesse são: a) o tratamento de dados pessoais estritamente necessário aos objetivos de prevenção e controle de fraudes[408] ou para garantir a segurança da rede e da informação nos sistemas informáticos de determinada instituição;[409] b) fornecimento de imagens de câmeras de segurança para fins de seguro (a finalidade é a prevenção e controle das fraudes na esfera securitária, não havendo o tratamento de dados sensíveis); c) segurança e melhoria de produtos e serviços ao consumidor; d) tratamentos de dados de empregados para programas de retenção de talentos e iniciativas de bem-estar; e) no caso de uso de dados por uma empresa para fazer ofertas mais adequadas e personalizadas a seus clientes, usando apenas os dados estritamente necessários para tal (*marketing* direto); f) envio de e-mail com descontos específicos para os produtos buscados por determinado usuário ou com indicações de compras, tomando como base seu histórico de compras; g) lembrar ao usuário que ele deixou itens no carrinho online, mas não finalizou a compra; e h) reunião de informações – de forma e em ambientes lícitos – sobre determinado candidato em processos seletivos Em relação à base legal do legítimo interesse, dentro de uma abordagem prática, é comum o seu questionamento em

---

expect those who view their profile might use their contact details for recruitment purposes and legitimate interests may be available (subject to compliance with other legal requirements, and PECR in particular). However, if they choose not to select that option, it is not reasonable to assume such an expectation. The individual's interests in maintaining control over their data – particularly in the context of the PECR requirement for specific consent to receive unsolicited marketing messages – overrides any legitimate interests of a recruitment agency in promoting its services to potential candidates." Exemplos disponíveis em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/>. Acesso em: 27.09.21.

[408] "Algo bastante comum é a criação de perfis comportamentais dos consumidores para combater fraudes e incidentes de segurança, pelos quais se diagnosticam atividades que fogem do padrão para tratá-las como suspeitas. É por esse motivo que serviços de e-mail, rede social e instituições financeiras alertam seus clientes e, em muitos casos, bloqueiam automaticamente acessos e transações financeiras. Por exemplo, se o acesso a uma conta parte de um dispositivo diferente, se a compra supera valores e é realizada em locais que não aqueles usuais. Todos esses dados informam ações de combate a fraudes e incidentes de segurança" (BIONI, Bruno. *Proteção de dados pessoais*: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020, p. 241).

[409] Muitas empresas precisam tratar certos dados pessoais para cumprir com os padrões da indústria, requerimentos dos reguladores e outros requisitos relacionados à prevenção de fraudes e lavagem de dinheiro, como, por exemplo, instituições financeiras, bancos, empresas de cartão de crédito, seguradoras e outras organizações com negócios voltados para o consumidor. Entende-se que as instituições financeiras e as redes de pagamento devem processar dados pessoais de indivíduos para monitorar, detectar e prevenir fraudes. Em particular, as redes de pagamento estão em uma posição privilegiada para monitorar e detectar sinais de fraude nos participantes do ecossistema de pagamento. Elas podem alertar em tempo real as instituições financeiras de que uma transação de pagamento pode ser fraudulenta, para que elas possam notificar os titulares de cartões individuais afetados e / ou tomar uma decisão quanto a aprovar ou negar uma transação de pagamento. (Cf. Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR. Centre for Information Policy Leadership GDPR Implementation Project. Publicado em 19 de maio de 2017)

relações em que há a presença de algum dado sensível ou quando o controlador não tem contato direto com o indivíduo e não pode pedir seu consentimento ou, ainda, em questões que envolvem segurança, verificação e autenticação de pessoas. Os exemplos incluem o uso de circuito fechado ou interno de televisão, de reconhecimento facial por varejistas, para identificarem ladrões de lojas conhecidos, ou de impressões digitais para identificação de pagamento.

Na LGPD, a hipótese legal do legítimo interesse não foi disponibilizada para o tratamento de dados sensíveis, devendo a atividade ser encaixada nas demais bases legais dispostas no Art. 11 da lei, que traz entre elas o consentimento, a proteção da vida ou da incolumidade física do titular ou de terceiro[410], a possibilidade de tratamento para a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, o exercício regular de direitos em contrato e o cumprimento de obrigação legal ou regulatória pelo controlador.[411]

O legítimo interesse justamente por apresentar maior flexibilidade ao agente de tratamento vai apresentar algumas limitações para a sua aplicação, devendo ser

[410] Exemplo de aplicação: durante o período mais grave da pandemia de COVID-19, uma empresa decidiu retomar parcialmente as suas atividades presenciais na sede, havendo, para isso, o estabelecimento de uma série de medidas sanitárias e de segurança. Ela estabeleceu rotina de checagem de temperatura corporal por meio de um aparelho medidor específico. Diariamente, na entrada, um profissional designado "testava" todos os funcionários, medindo sua temperatura e comunicando o resultado a cada um individualmente. A temperatura era registrada em uma planilha simples, associada ao nome do funcionário, à data de coleta e ao horário de entrada. Se um funcionário apresentasse temperatura corporal elevada, ele seria impedido de entrar no prédio para trabalhar. Contestando a referida análise, funcionário apontou que nunca fora pedida a sua autorização expressa para a realização da testagem e que não lhe fora dada a opção de se opor à prática (opt-out). Além disso, destacou que a medição não era precisa, que não necessariamente a temperatura elevada seria um sinal de estar com COVID-19 e que seu afastamento do trabalho seria injustificado. Analisando o caso, entende-se que o empregador não poderia se valer do legítimo interesse para embasar o tratamento de dados realizado, visto que há dados sensíveis sendo coletados, quais sejam, dados de saúde. Outra observação relevante envolve a desnecessidade do armazenamento de tais dados de saúde conjugados com outros dados pessoais, visto que a suposta utilidade desses dados se perdia rapidamente. (BIONI, Bruno; KITAYAMA, Marina; RIELLI, Mariana. *O Legítimo Interesse na LGPD*: quadro geral e exemplos de aplicação. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021. p.43-44).

[411] "(...) o monitoramento de funcionários por seus empregadores faz parte da relação de subordinação que é própria do direito do trabalho, sendo "uma das formas do empregador exercer o seu poder diretivo sobre seus colaboradores". Dessa forma, não há que se falar em ilegitimidade do ponto de vista da legislação. O outro elemento que compõe o teste da legitimidade, a concretude da situação, depende do tipo de monitoramento que será empregado - em qualquer caso, ele deve ser especificado (em outras palavras, a finalidade não pode ser tão somente um "monitoramento" genérico). Um ponto de atenção que pode ser suscitado é o tratamento de dados pessoais sensíveis, pois ele não pode acontecer com base no legítimo interesse." (BIONI, Bruno; KITAYAMA, Marina; RIELLI, Mariana. O Legítimo Interesse na LGPD: quadro geral e exemplos de aplicação. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021. p.44).

realizado antecipadamente um teste de ponderação[412]. Busca-se, assim, balancear os direitos do titular e de quem faz uso de suas informações, verificando-se tanto se há um interesse legítimo de quem trata os dados quanto se estão sendo respeitadas as legítimas expectativas e os direitos e liberdades fundamentais dos titulares.[413]

O teste de balanceamento requer uma avaliação de risco x benefício específica ao contexto e a implementação de salvaguardas e garantias como parte da responsabilidade organizacional. Cada controlador é responsável por garantir que a aplicação da base do legítimo interesse para uma nova finalidade de tratamento atenda ao teste de balanceamento. Além disso, cada novo propósito de tratamento deve ser revisado novamente conforme o teste de balanceamento. Os deveres de informação e de transparência são aqui muito relevantes, devendo a transparência ser fornecida contextualmente, por diferentes métodos e em diferentes momentos ao longo do ciclo de vida das operações de tratamento.

A LGPD estabelece parâmetros, em um rol exemplificativo, para a utilização do legítimo interesse como requisito autorizativo para o tratamento de dados do titular, conforme se depreende de seu artigo 10:

> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: I - apoio e

[412] GRUPO DE TRABALHO DO ARTIGO 29 PARA A PROTEÇÃO DE DADOS. Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva 95/46/CE. Adotado em 9 de abril de 2014. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_pt.pdf>. Acesso em 14.08.19.

[413] Destaca-se que o *legitimate interest assessment* (LIA) apresenta quatro fases que devem ser cumpridas de modo a se verificar o preenchimento do requisito do legítimo interesse, sendo elas: (i) a avaliação dos interesses legítimos; (ii) o impacto sobre o titular do dado; (iii) o equilíbrio entre os interesses legítimos do controlador e o impacto sobre o titular; e (iv) salvaguardas desenvolvidas para proteger o titular dos dados e evitar qualquer impacto indesejado. Tratando da aplicação do legítimo interesse e do teste de ponderação, o Guide to the General Data Protection Regulation – desenvolvido pelo Information Commissioner's Office (ICO) do Reino Unido – afirma que: "It makes most sense to apply this as a test in the following order: Purpose test – is there a legitimate interest behind the processing? Necessity test – is the processing necessary for that purpose? Balancing test – is the legitimate interest overridden by the individual's interests, rights or freedoms? This concept of a three-part test for legitimate interests is not new. In fact the Court of Justice of the European Union confirmed this approach to legitimate interests in the Rigas case (C-13/16, 4 May 2017) in the context of the Data Protection Directive 95/46/EC, which contained a very similar provision. This means it is not sufficient for you to simply decide that it's in your legitimate interests and start processing the data. You must be able to satisfy all three parts of the test prior to commencing your processing". Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/#three_part_test>. Acesso em: 10.02.21.

> promoção de atividades do controlador; e II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei. §1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados. §2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse. §3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Dados pessoais, quando processados em grande escala e combinados com outros dados, podem levar a inferências e a resultados de caráter sensível. Diante disso, bases que dependem menos de uma interação direta com o titular e que apresentam maior flexibilidade, como é o caso do legítimo interesse, podem aumentar os riscos aos direitos e liberdades dos titulares, o que seria ainda mais preocupante caso houvesse a permissão para o tratamento de dados sensíveis. Em razão disso, a aplicação do legítimo interesse encontra parâmetros e restrições.

Nos últimos anos, diante da importância do tratamento de dados dentro da lógica das eleições e das manifestações políticas, a Autoridade Nacional de Proteção de Dados (ANPD) manifestou-se no sentido de afirmar que:

> O interesse do controlador será considerado legítimo quando não encontrar óbices legais, isto é, quando não for contrário às disposições da lei. Por exemplo, não há legítimo interesse das candidatas e dos candidatos, dos partidos políticos, das coligações e das federações na obtenção de dados custodiados pela administração pública ou por pessoa jurídica de direito privado, tendo em vista se tratar de prática vedada pela legislação eleitoral (art. 57-E, *caput*, da Lei nº 9.504/1997 e art. 31 da Res.-TSE nº 23.610/2019). Do mesmo modo, é vedada a venda, por pessoas físicas e jurídicas, de cadastros eletrônicos (art. 57-E, § 1º, da Lei nº 9.504/1997 e art. 31, § 1º, da Res.-TSE nº 23.610/2019), o que impede a caracterização do legítimo interesse. Tampouco há legítimo interesse na utilização de dados pessoais para envio de propaganda eleitoral por *telemarketing*, tendo em vista que é prática vedada pelo art. 34 da Res.-TSE n° 23.610/2019 e pelo Supremo Tribunal Federal (STF) na ADI nº 5.122. [414] [415]

[414] ANPD. *Guia orientativo: aplicação da Lei geral de proteção de dados pessoais (LGPD) por agentes de tratamento no contexto eleitoral* [recurso eletrônico]. Brasília: Tribunal Superior Eleitoral, 2021. p. 27.
[415] A ANPD traz hipótese exemplificativa em que é possível a coleta de dados pessoais em site de partido político: "**Coleta de dados de navegação para melhoria da experiência durante a navegação.** Partido Alpha coleta dados de navegação a partir do acesso de pessoas usuárias a seu *site* na internet com a finalidade de desenvolver ações de *melhoria da experiência durante a navegação*. Para tanto, serão coletados dados pessoais mediante a utilização de *cookies*, que serão utilizados para gerar informações sobre a navegação das pessoas usuárias. No exemplo, o partido deverá, em momento anterior à coleta, avaliar: a legitimidade do seu interesse; a proporcionalidade entre o interesse declarado e as legítimas

As campanhas políticas utilizam, cada vez mais, processos automatizados de tratamento de dados para apresentar propostas e se aproximarem de seus potenciais eleitores, o que deve ser feito, porém, estritamente conforme as normas da LGPD. Como apontado, o "tratamento irregular de dados pessoais e, em particular, de dados sensíveis, no âmbito das campanhas políticas, pode gerar impactos negativos sobre a lisura do processo eleitoral e sobre a igualdade de oportunidades entre candidatas e candidatos."[416] Dentro da categoria dos dados sensíveis, informações sobre opinião política e filiação à organização de caráter político vêm se mostrando muito relevantes, havendo grande busca pelo tratamento de dados pessoais de indivíduos filiados a partidos políticos e pela formação de perfis que indiquem a classificação da pessoa conforme sua opinião política. Dessa forma, segundo guia da ANPD:

> (...) quando há revelação ou identificação indireta de aspectos sensíveis relacionados à personalidade da pessoa titular, com o potencial de prejudicar ou restringir seus direitos e interesses, expondo informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, também se aplica o regime jurídico especial previsto na LGPD para os dados sensíveis. É o caso da identificação de convicção religiosa, origem racial ou opinião política de pessoa titular de dados a partir de outras informações não sensíveis, como o nome, o endereço e o perfil de consumo. Da mesma forma, um banco de dados de pessoas doadoras e voluntárias engajadas em uma campanha eleitoral, ainda que contenha apenas informações cadastrais e de contato da pessoa titular, pode revelar sua opinião política e ser considerado dado sensível, por exemplo, ao ser associado ao partido ou a candidata ou candidato responsável pela coleta das informações. [417]

---

expectativas da pessoa titular do dado; e a eventual existência de violação aos direitos e liberdades individuais da pessoa titular do dado, devendo, ainda, adotar salvaguardas para garantir o respeito aos direitos da pessoa titular. Além disso, o partido Alpha deve limitar a utilização dos dados pessoais à finalidade declarada, não podendo utilizá-los para outras finalidades, como o desenvolvimento de perfis de pessoas usuárias a partir dos hábitos de navegação. Caso o partido pretenda utilizar os dados pessoais para essa segunda finalidade, deverá, necessariamente, fazê-lo com fundamento em outra base legal, como o consentimento, ou realizar nova avaliação de legítimo interesse. Além disso, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados e o controlador deverá adotar medidas para garantir a transparência do tratamento." (ANPD. *Guia orientativo: aplicação da Lei geral de proteção de dados pessoais (LGPD) por agentes de tratamento no contexto eleitoral* [recurso eletrônico]. Brasília: Tribunal Superior Eleitoral, 2021. p.28-29)

[416] ANPD. *Guia orientativo: aplicação da Lei geral de proteção de dados pessoais (LGPD) por agentes de tratamento no contexto eleitoral* [recurso eletrônico]. Brasília: Tribunal Superior Eleitoral, 2021. p. 11

[417] ANPD. *Guia orientativo: aplicação da Lei geral de proteção de dados pessoais (LGPD) por agentes de tratamento no contexto eleitoral* [recurso eletrônico]. Brasília: Tribunal Superior Eleitoral, 2021. p. 11-12.

As novas e sofisticadas formas de tratar dados, conjugadas com as dinâmicas aplicações da inteligência artificial, podem potencialmente conduzir ao processamento de dados sensíveis ou contextualmente sensíveis, além de inferências e previsões bastante específicas sobre os gostos, personalidades e comportamentos de um indivíduo ou grupo. Dependendo da natureza, do impacto e da utilização dessas previsões, isso pode ser altamente invasivo para a privacidade e a proteção de dados das pessoas, ampliando discriminações ilícitas ou abusivas.

Por exemplo, os controladores podem ter um interesse legítimo em conhecer as preferências de seus clientes, para permitir que eles personalizem melhor suas ofertas e, em última instância, ofereçam produtos e serviços que atendam melhor às necessidades e desejos dos clientes. O mesmo raciocínio pode ser aplicado a outras formas de marketing direcionado, incluindo publicidade baseada na atividade online de uma pessoa. A publicidade direcionada deve ser considerada como estando dentro dos interesses legítimos dos controladores e de terceiros, desde que os dados sejam tratados de acordo com requisitos específicos, que o indivíduo que recebe a publicidade obtenha informações sobre como seus dados serão tratados e ele tenha controles significativos sobre tais tratamentos. O controlador também deve ser responsável por honrar as escolhas que os indivíduos fizeram sobre como seus dados serão usados em anúncios.[418][419]

Ainda, vale lembrar entendimento consolidado no ambiente europeu – por meio dos *Guidelines on consent under Regulation 2016/679*, publicados pelo *Article 29 Working Party*[420] em 2017 – acerca da seleção e interação da base legal do consentimento com as demais bases aplicáveis ao tratamento de dados pessoais. Se um controlador optar por selecionar a base do consentimento para qualquer parte do tratamento, ele deverá estar preparado para respeitar a escolha do titular e, inclusive, interromper essa parte do tratamento se este retirar seu consentimento. Em outras

[418] Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR. Centre for Information Policy Leadership GDPR Implementation Project. Publicado em 19 de maio de 2017.

[419] A publicidade é um dos principais modelos de negócio em serviços (aparentemente) gratuitos. A personalização do conteúdo e da oferta é um recurso central de muitos serviços. Sem personalização, muitos serviços perderiam negócios, pois seus clientes e usuários contam com a personalização como uma das propostas de valor do serviço. A evidência crescente mostra a importância dos anúncios direcionados para os modelos de negócios de muitos editores e anunciantes online e o fato de que anúncios relevantes podem criar efetivo valor para os indivíduos, ajudando-os a descobrir novos produtos, serviços e causas, bem como a evitar a sujeição a uma publicidade discriminatória.

[420] Disponível em: <https://ec.europa.eu/newsroom/article29/items/623051/en> Acesso em: 22.07.21

palavras, o controlador não poderá passar do consentimento para outras bases legais. Por exemplo, não se mostra adequado utilizar a base do legítimo interesse retrospectivamente para justificar um tratamento onde foram encontrados problemas com a validade do consentimento. Devido à necessidade de o controlador divulgar a base legal em que se baseia no momento inicial do tratamento dos dados, ele deverá ter decidido com antecedência qual base será aplicável.

Hipótese diversa seria no caso de o controlador utilizar base legal para o tratamento dos dados que não fosse o consentimento. Seria lícito – em certos casos – cumular as bases legais, assim como ocorre em algumas relações regidas pelo GDPR? Em determinadas situações práticas, por exemplo, é comum que o controlador transite entre o legítimo interesse e a execução de contrato. A possibilidade de identificação de mais de uma base legal para determinada operação de tratamento de dados pessoais tem encontrado respaldo em alguns documentos de autoridades europeias de proteção de dados.[421] [422] Todavia, caso o controlador considere que mais de uma base legal pode ser utilizada para legitimar o tratamento, ele deverá identificar e documentar todas elas

[421] No mesmo sentido parece ter se posicionado o Grupo de Trabalho do Artigo 29, ainda durante a vigência da Diretiva 95/46/CE, mas já após a aprovação do GDPR, em sua "Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS)" (Parecer 03/2017 sobre o tratamento de dados pessoais no contexto dos Sistemas de Transporte Inteligentes Cooperativos (STIC)), quando afirmou que: "Processing shall be lawful only if and to the extent that at least one of the following cases applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject."(Article 29 Working Party. Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS). Adopted on 4 October 2017. p.09. Disponível em: <https://ec.europa.eu/newsroom/article29/items/610171> Acesso em: 27.09.21).

[422] Esse posicionamento também vem sendo aceito por parte da doutrina, sob a condição de que controladores consigam demonstrar que todos os requisitos para as distintas bases legais indicadas sejam preenchidos: "(...) in practice, entities often based their processing activities on several legal bases. For example, where an entity processed personal data based on their necessity for the performance of a contract, said entity would often also obtain the data subject's consent. This preventive approach aimed at securing the lawfulness of the processing operations in case one or several of the used legal bases would lose their legitimacy. This approach can be upheld under the GDPR. However, entities should choose a primary legal permission among the available options. This is advisable as, under the Regulation, the conditions for obtaining valid consent, as well as those regarding other legal bases for processing, have been specified and tightened. Therefore, entities should—prior to processing—evaluate which legal basis might be most suitable for their processing activities. Under the principle of accountability (see Sect. 3.1), entities must be able to prove that the legal bases they use are fulfilled, e.g., when processing personal data based on their prevailing legitimate interests, entities must be able to demonstrate their interests, as well as the legitimacy of the latter" (VOIGT, Paul; BUSSCHE, Axel von dem. The EU General Data Protection Regulation (GDPR). A Practical Guide. Springer, 2017, p. 101).

desde o início de sua atividade. O Information Commissioner's Office (ICO) do Reino Unido afirma de maneira clara que:

> You might consider that more than one basis applies, in which case you should identify and document all of them from the start. You must not adopt a one-size-fits-all approach. No one basis should be seen as always better, safer or more important than the others, and there is no hierarchy in the order of the list in the UK GDPR. Several of the lawful bases relate to a particular specified purpose – a legal obligation, performing a contract with the individual, protecting someone's vital interests, or performing your public tasks. If you are processing for these purposes then the appropriate lawful basis may well be obvious, so it is helpful to consider these first.[423]

Em seguida, o ICO destaca que o agente de tratamento deve determinar com cuidado e adequadamente sua base legal antes de iniciar o tratamento dos dados pessoais.[424] Se ele descobrir posteriormente que a base escolhida é realmente inadequada, será difícil simplesmente trocar por uma diferente. Mesmo que uma base diferente pudesse ter sido aplicada desde o início, a mudança retroativa da base provavelmente será injusta com o titular do dado e levará a violações dos requisitos de responsabilidade e transparência.[425]

---

[423] Disponível: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/> Acesso em: 27.09.21. Tradução: Você pode considerar que mais de uma base se aplica. Nesse caso, você deve identificar e documentar todas elas desde o início. Você não deve adotar uma abordagem única. Nenhuma base deve ser vista como sempre melhor, mais segura ou mais importante do que as outras, e não há hierarquia na ordem da lista no RGPD do Reino Unido. Várias das bases legais estão relacionadas a uma finalidade específica: uma obrigação legal, a execução de um contrato com o indivíduo, a proteção dos interesses vitais de alguém ou a execução de suas tarefas públicas. Se você estiver tratando para esses fins, a base legal apropriada pode ser óbvia, portanto, é útil considerá-la primeiro.

[424] Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/> Acesso em: 27.09.21. "You need to include information about your lawful basis (or bases, if more than one applies) in your privacy notice. Under the transparency provisions of the UK GDPR, the information you need to give people includes: your intended purposes for processing the personal data; and the lawful basis for the processing. This applies whether you collect the personal data directly from the individual or you collect their data from another source. Read the 'right to be informed' section of this guide for more on the transparency requirements of the GDPR."

[425] O ICO apresenta o seguinte exemplo: "A company decided to process on the basis of consent, and obtained consent from individuals. An individual subsequently decided to withdraw their consent to the processing of their data, as is their right. However, the company wanted to keep processing the data so decided to continue the processing on the basis of legitimate interests. Even if it could have originally relied on legitimate interests, the company cannot do so at a later date – it cannot switch basis when it realised that the original chosen basis was inappropriate (in this case, because it did not want to offer the individual genuine ongoing control). It should have made clear to the individual from the start that it was processing on the basis of legitimate interests. Leading the individual to believe they had a choice is inherently unfair if that choice will be irrelevant. The company must therefore stop processing when the individual withdraws consent." (Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-

Portanto, é importante avaliar cuidadosamente qual base é apropriada e documentar isso. Pode ser possível que mais de uma base se aplique ao tratamento porque, por exemplo, o controlador tem mais de uma finalidade. Em sendo esse o caso, ele deverá deixar isso claro desde o início. Se houver uma mudança nas circunstâncias ou se ele tiver um propósito novo, poderá haver um bom motivo para revisar sua base legal e fazer uma mudança, quando precisará informar ao titular a questão e documentar a mudança.

3.2.1 Consentimento específico, destacado e para finalidades específicas

A base legal do consentimento para o tratamento de dados do titular representa instrumento de autodeterminação e livre construção da esfera privada. Quando aplicável, permite diferentes escolhas e configurações em ferramentas tecnológicas, garantindo ao indivíduo maior controle sobre os seus dados pessoais. Verifica-se no texto da LGPD cuidadosa caracterização do consentimento, definido como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada", seguindo a linha do GDPR e das normas mais atuais sobre o tema. Nesse sentido, entende-se que:

> O maior cuidado com o consentimento do titular mostra-se de grande relevância no cenário tecnológico atual, no qual se verifica a coleta em massa de dados pessoais, a mercantilização desses bens por parte de uma série de sujeitos e a ocorrência de situações de pouca transparência no que tange ao tratamento de dados. Diante desse cenário, defende-se que a interpretação do consentimento deverá ocorrer de forma restritiva, não podendo o agente estender a autorização concedida para o tratamento dos dados para outros meios além daqueles pactuados, para momento posterior, para fim ou contexto diverso ou, ainda, para pessoas distintas daquelas informadas ao titular. Além disso, o consentimento deverá ser manifestado pelo titular antes do tratamento da informação.[426]

No Art. 11, a primeira hipótese autorizativa para o tratamento de dados sensíveis refere-se ao consentimento do titular ou de seu responsável legal, que deverá ser dado

---

protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/> Acesso em: 27.09.21.)

[426] TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. O consentimento na circulação de dados pessoais. *Revista Brasileira de Direito Civil (RBDCivil)*, Belo Horizonte, v. 25, p. 83-116, jul./set. 2020.

de forma específica e destacada, para finalidades específicas. Segundo doutrina, a base legal do consentimento para o tratamento de dados sensíveis deverá ser enxergada "como um vetor para que haja mais *assertividade* do titular com relação a esses movimentos 'específicos' de seus dados".[427] A noção, no caso, aproxima-se da ideia de consentimento expresso, por exigir maior atuação do titular dos dados, além de cuidado mais elevado com o tratamento da informação pelo agente.[428]

Específico deve ser compreendido como um consentimento manifestado em relação a propósitos concretos e claramente determinados pelo controlador e antes do tratamento dos dados, havendo também aqui, e com mais ênfase, as obrigações de granularidade, que trazem em si configurações de privacidade personalizáveis. Dessa forma, o titular terá condições de optar (ou não) por determinado tratamento, produto ou serviço que envolva os seus dados pessoais, podendo, inclusive, manifestar consentimento específico para certo tipo de tratamento, excluindo outros que não considerar adequados.

Além de configurarem uma boa prática, as *granular privacy settings* permitem maior autonomia para o titular de dados, devendo ele ser informado sempre das consequências dos aceites e das negativas efetuadas. Inclusive, a LGPD estabelece que, se o tratamento dos dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer seus direitos enumerados no Art. 18 da Lei. Regula-se, assim, a lógica binária das políticas de tudo ou nada[429], em que o

---

[427] BIONI, Bruno, op. cit., p. 202. O autor apresenta a seguinte crítica em relação à adjetivação inserida pelo legislador nacional ao consentimento para o tratamento de dados sensíveis: "(...) sob o ponto de vista de técnica legislativa, teria sido melhor que a LGPD tivesse adotado o adjetivo *expresso*, tal como fez a GDPR (...). Esse qualificador é o que semanticamente representaria melhor esse nível de participação mais intenso do cidadão no fluxo dos dados. Apesar dessa diferença semântica, entre os qualificadores expresso e específico, a consequência normativa tende a ser a mesma. Isso porque o que está em jogo é reservar um tipo de autorização singular em situações igualmente singulares no que tange ao tratamento de dados, sendo esta a racionalidade que percorre a LGPD, a GDPR e parte das leis setoriais brasileiras de proteção de dados pessoais" (BIONI, Bruno, op. cit., p. 203).

[428] Cf. TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. O consentimento na circulação de dados pessoais. *Revista Brasileira de Direito Civil (RBDCivil)*, Belo Horizonte, v. 25, p. 83-116, jul./set. 2020.

[429] "On the internet, we encounter many take-it-or-leave-it choices regarding our privacy. Social network sites and email services typically require users to agree to a privacy statement or to terms and conditions – if people do not agree, they cannot use the service. Some websites use a tracking wall, a barrier that visitors can only pass if they agree to tracking by third parties. When confronted with such take-it-or-leave-it choices, many people might click 'I agree' to any request. It is debatable whether people have meaningful control over personal information if they have to consent to tracking to be able to use services or websites." "For instance, chat and email services often require users to agree to a data use policy – if people do not agree, they cannot use the service. An app might require access to the camera or the contact

usuário ou aceita todas as disposições e termos do serviço ou não pode utilizá-lo.[430]

Na prática, um número reduzido de pessoas tem habilidade de negociar ou a possibilidade concreta de rejeitar as condições impostas nos termos de serviço e políticas de privacidade de plataformas. Assim, ao invés de realmente concordar com o uso dos próprios dados, o que se verifica é a obediência do titular à vontade das empresas, o que facilita práticas de controle e de uso indiscriminado de dados pessoais.[431] Dessa forma, mostra-se necessário realizar mudanças significativas tanto na maneira pela qual o consentimento é implementado nos termos e políticas, quanto no desenho e arquitetura das plataformas.[432] *Destacado* pode ser interpretado no sentido de que é importante que o titular tenha pleno acesso ao documento que informará todos os fatos relevantes sobre o tratamento de seus dados pessoais, devendo tais disposições virem destacadas para que a expressão do consentimento ocorra conforme a lei. Além de se referir a dados determinados e haver declaração de vontade que esteja ligada à objetivo específico, a manifestação deverá vir em destaque no instrumento de declaração que autoriza o tratamento. Acerca do consentimento para o tratamento de dados sensíveis, Mulholland nos ensina que:

> Considera-se consentimento livre e esclarecido - para efeitos deste artigo, consentimento informado - a anuência, livre de vícios, do titular de dados, após acesso prévio, completo e detalhado sobre o tratamento dos dados, incluindo sua natureza, objetivos, métodos, duração, justificativa, finalidades,

---

list on an end-user's phone, while that access is unnecessary for providing the service. A 'smart' TV might listen to the sounds in people's living rooms, and might only work when people 'consent' to that. Internet of Things equipment may only work if people 'consent' to data collection for marketing." (BORGESIUS, Frederik J. Zuiderveen; KRUIKEMEIER, Sanne; BOERMAN, Sophie C.; HELBERGER, Natali. Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation. *European Data Protection Law Review*. 2017. Disponível em: https://www.ivir.nl/publicaties/download/EDPL_2017_03.pdf. Acesso em: 28 dez. 2018.)

[430] "Pode-se adotar todos os argumentos historicamente adotados para criticar a "liberdade" do consentimento, na presença de contextos nos quais existem condicionamentos tais que excluem uma real possibilidade de escolha. (...) o condicionamento deriva do fato de que a possibilidade de usufruir de determinados serviços, essenciais ou importantes, ou tidos como tais, depende não somente do fornecimento de determinadas informações por parte do usuário do serviço, mas também do fato de que tais informações (eventualmente com base no consentimento do interessado) podem posteriormente ser submetidas a outras elaborações. Este é o caso de todos os serviços obtidos através das novas mídias interativas, cujos gestores, por evidentes razões de ordem econômica, estão prontos a exercer forte pressão sobre os usuários para que estes autorizem a elaboração (e a eventual transmissão a terceiros) de "perfis" pessoais ou familiares baseados nas informações coletadas por ocasião do fornecimento dos serviços." (RODOTÀ, Stefano. cit., p.76)

[431] PEÑA, Paz; VARON, Joana. *O poder de dizer NÃO na Internet.* Coding Rights. Disponível em: https://medium.com/codingrights/o-poder-de-dizer-não-na-internet-17d6e9889d4a. Acesso em: 29 julho. 2019.

[432] Cf. TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. O consentimento na circulação de dados pessoais. *Revista Brasileira de Direito Civil (RBDCivil)*, Belo Horizonte, v. 25, p. 83-116, jul./set. 2020.

> riscos e benefícios, assim como de sua liberdade total para recusar ou interromper o tratamento de dados em qualquer momento, tendo o controlador ou operador a obrigação de informar ao titular dos dados, em linguagem adequada, não técnica, para que ele a compreenda (Konder, 2003, 61). Portanto, em havendo o consentimento informado prévio do titular dos dados pessoais sensíveis, o seu tratamento estará autorizado. O consentimento deve ser também qualificado pela finalidade do tratamento, isto é, a aquiescência para o tratamento de dados deve ser delimitada pelo propósito para o qual os dados foram coletados, sob pena de abusividade ou ilicitude do tratamento a gerar eventual responsabilidade do agente de tratamento.[433]

Em seguida, a autora destaca que:

> O fundamento do consentimento qualificado para o tratamento de dados sensíveis se deve, sobremaneira, à natureza existencial e fundamental dos conteúdos a que se referem. Podemos tomar emprestado o conceito utilizado pelo biodireito para delimitar o que estaria compreendido como consentimento específico e destacado, para finalidades específicas. Essa correlação pode ser feita justamente porque a área do biodireito, por se referir a interesses de natureza existencial, em sua essência, necessita de um cuidado específico por parte do Direito para que viabilize a plena autonomia da pessoa que, em casos de tratamento de dados sensíveis, pode ser considerada concretamente como vulnerável.[434]

Dizer que o consentimento também deverá ser *informado* significa que o titular do dado deverá ter ao seu dispor as informações necessárias e suficientes para avaliar corretamente a situação e a forma como seus dados serão tratados. A informação é fator determinante para a expressão de um consentimento livre e consciente, dirigido a certo tratamento e sob condições específicas. Exige a lei que ao cidadão sejam fornecidas informações transparentes, adequadas, claras e em quantidade satisfatória acerca dos riscos e implicações do tratamento de seus dados.

Na lógica do consentimento informado, o artigo 9º da LGPD dispõe que o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca da: (I) finalidade específica do tratamento; (II) forma e duração do tratamento, observados os segredos comercial e industrial; (III) identificação do controlador; (IV) informações de contato do controlador; (V) informações acerca do uso compartilhado de dados pelo

---

[433] MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. Migalhas, publicado em 22 de junho de 2020. Disponível em: <https://migalhas.uol.com.br/coluna/migalhas-de-vulnerabilidade/329261/dados-pessoais-sensiveis-e-consentimento-na-lei-geral-de-protecao-de-dados-pessoais> Acesso em: 02.11.20.

[434] MULHOLLAND, Caitlin. Op. Cit.

controlador e a finalidade; (VI) responsabilidades dos agentes que realizarão o tratamento; (VII) e direitos do titular, com menção explícita aos direitos contidos no artigo 18.[435] Na hipótese em que o consentimento é requerido, ele será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca. Quando o consentimento for necessário, havendo mudanças em relação à finalidade para o tratamento dos dados não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo este revogar o consentimento, caso discorde das alterações. Adicionalmente, observa-se que a utilização de opções pré-assinaladas de adesão será inválida. Da mesma forma, o silêncio ou a inatividade por parte do titular dos dados, bem como a mera utilização de um serviço, não deverão ser encarados como manifestação ativa de escolha. A *finalidade da coleta* dos dados deve ser previamente conhecida. O princípio em questão diz respeito à relação entre os dados colhidos e a finalidade perseguida pelo agente, apresentando relação também com o princípio da utilização não abusiva e com a recomendação de eliminação ou transformação em dados anônimos das informações que não sejam mais necessárias.[436] Tratando-se de dados sensíveis, a manifestação do consentimento será sempre para "finalidades específicas". Parte da doutrina encontra no Art. 11 da LGPD a existência de preferência à base legal do consentimento, levando em conta o tipo de dado em questão e a técnica legislativa utilizada, qual seja, a inserção de dois incisos no Art. 11, sendo o primeiro sobre o consentimento e o segundo dispondo que, sem o fornecimento de consentimento do titular, poderá ocorrer o tratamento de dados sensíveis (apenas) nas hipóteses em que for indispensável para as sete situações ali estabelecidas nas alíneas.[437] Interpretação essa que já encontra crítica na doutrina:

[435] Art. 8º § 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.
[436] RODOTÀ, Stefano. cit., p. 59.
[437] Conforme dispõe a Lei Complementar nº 95, de 26 de fevereiro de 1998, em seu Art. 10, incisos II e IV, os textos legais serão articulados com observância dos seguintes princípios: "os artigos desdobrar-se-ão em parágrafos ou em incisos; os parágrafos em incisos, os incisos em alíneas e as alíneas em itens" e "os incisos serão representados por algarismos romanos, as alíneas por letras minúsculas e os itens por

> (...) tanto na hipótese de tratamento de dados sensíveis por meio do consentimento do titular quanto naquelas que se referem às demais situações que independem desta manifestação de autonomia, previstas nos incisos I e II do art. 11 da LGPD, reconhece-se na técnica legislativa utilizada uma posição de igualdade entre estas hipóteses, e não a de prevalência do consentimento.[438]

Acerca do uso do consentimento, o Information Commissioner's Office (ICO) traz o seguinte exemplo: uma academia apresenta um sistema de reconhecimento facial para permitir que os membros acessem suas instalações. Ela exige que todos os membros concordem com o reconhecimento facial como condição de entrada no local, não havendo outra maneira de acessar a academia. No caso, entende-se que esse consentimento não será válido e livre, pois os membros não terão uma escolha real. Se eles não consentirem, não poderão acessar a academia. Embora o reconhecimento facial possa oferecer alguns benefícios no trato da segurança e conveniência, ele não se mostra necessário para fornecer acesso às instalações de uma academia de ginástica. Inclusive, em raros casos, este tipo de local apresenta sistema robusto de proteção de dados, que envolva sofisticadas ferramentas técnicas.

No entanto, se a academia oferecer uma alternativa, como a escolha entre o acesso por reconhecimento facial ou por meio de um cartão de membro ou senha, o consentimento poderá ser considerado livre e válido. Dessa forma, a academia poderá contar com a base legal do consentimento, que deverá ser dado de forma específica e destacada, para o processamento das varreduras faciais biométricas dos membros que indicarem que preferem tal opção.[439]

A expressão do consentimento livre implica uma verdadeira escolha e controle para o titular dos dados. Se ele não puder exercer uma verdadeira escolha, se se sentir coagido a dar o consentimento ou sofrer consequências negativas injustificadas caso não consinta, então o consentimento não será válido. De acordo com entendimento do *European Data Protection Board*[440], a noção de

---

algarismos arábicos". Há, portanto, na técnica legislativa uma formalidade e uma hierarquia a serem obedecidas.

[438] MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei geral de Proteção de Dados Pessoais. *Revista do Advogado*, n. 144, nov. 2019, p. 47-53, p. 52.

[439] Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/#conditions1> Acesso em: 01.11.20.

[440] EUROPEAN DATA PROTECTION BOARD. Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679. Versão 1.1. Adotada em 4 de maio de 2020. p.08. Disponível em:

desequilíbrio e a assimetria informacional entre o responsável pelo tratamento e o titular dos dados devem ser cuidadosamente consideradas, assim como a vulnerabilidade de alguma das partes. Em termos gerais, qualquer elemento que constitua pressão ou influência inadequada sobre o titular dos dados e que o impeça de exercer livremente a sua vontade tornará o consentimento inválido.

É possível destacar três ocasiões em que as disparidades e a posição de vulnerabilidade de uma das partes geram um "desequilíbrio de poder": o tratamento de dados pelo poder público e nas relações de trabalho e de consumo. Isso ocorre, muitas vezes, em decorrência da posição hierarquicamente superior do controlador e de seu poderio econômico. Diante disso, sendo adequado e possível, um recurso seria o emprego de outras bases legais, diversas ao consentimento, em razão da dificuldade de sanar a assimetria existente.[441]

Na *Opinion 2/2017 on data processing at work* [442] afirma-se, por exemplo, que empregados dificilmente estarão em posição de fornecer ou de recusar uma solicitação de consentimento, em razão da relação *empregado x empregador*. Dentre os motivos para esse paradigma do regime protetivo frente à base legal do consentimento, pode-se citar a limitação que advém do poder decisório do titular de dados. Na hipótese, por mais que o legislador tenha tido cautela ao abordar a necessidade de informação sobre o tratamento de dados e os direitos do titular, ainda pode persistir dificuldade – por parte do empregado – de efetuar um processo de tomada

---

<https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en> Acesso em: 19.07.21. Sobre a questão, o documento traz exemplo interessante: "Exemplo 1: Uma aplicação para telemóvel de edição de fotografias solicita aos utilizadores que ativem a localização por GPS para fins de prestação dos serviços. A aplicação também os informa de que utilizará os dados recolhidos para efeitos de publicidade comportamental. Nem a geolocalização nem a publicidade comportamental em linha são necessárias para a prestação do serviço de edição de fotografias, indo além da concretização do serviço principal prestado. Uma vez que os utilizadores não podem utilizar a aplicação sem darem o seu consentimento para estes efeitos, o consentimento não pode ser considerado livre."

[441] É necessário observar que: "Os desequilíbrios de poder não são exclusivos das autoridades públicas e dos trabalhadores, também podem ocorrer noutras situações. Tal como foi realçado pelo GT29 em vários pareceres, o consentimento só pode ser válido se o titular dos dados puder exercer uma verdadeira escolha e não existir qualquer risco de fraude, intimidação, coação ou consequências negativas importantes (p. ex. custos adicionais substanciais) se o consentimento for recusado. O consentimento não será dado livremente nos casos em que exista qualquer elemento de obrigatoriedade, pressão, incapacidade de exercício da livre vontade." EUROPEAN DATA PROTECTION BOARD. Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679. Versão 1.1. Adotada em 4 de maio de 2020. p.11. Disponível em: <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en> Acesso em: 19.07.21.

[442] *Opinion 2/2017 on data processing at work.* Disponível em: http://ec.europa.eu/newsroom/document.cfm?doc_id=45631. Acesso em: 26 de julho de 2021.

de decisão genuíno a respeito do fluxo de seus dados pessoais.

Ao analisar o contexto laboral, mostra-se flagrante o desequilíbrio contratual existente entre empregador e empregado, bem como a relação de dependência do último. Assim, é necessário reconhecer que, por receio de represálias e considerando a manutenção do emprego, o empregado irá fornecer praticamente todo e qualquer tipo de consentimento para o controlador. Portanto, é "improvável que um trabalhador responda livremente ao pedido de consentimento do empregador para, por exemplo, ativar sistemas de controlo como a observação do local de trabalho através de câmaras ou preencher formulários de avaliação".[443] Contudo, isso não significa que os empregadores nunca poderão utilizar o consentimento como base legal. Pode haver situações em que seja possível ao empregador demonstrar que o consentimento foi dado livremente. Imagine, por exemplo, que uma equipe de filmagem pretende filmar determinada parte de um escritório. O empregador solicita o consentimento de todos os trabalhadores que se sentam na referida área do escritório para serem filmados, uma vez que podem aparecer em segundo plano nas filmagens. No caso, os trabalhadores que não quiserem ser filmados não serão de forma alguma penalizados, podendo ser colocados em um outro local de trabalho equivalente, enquanto durar a filmagem.[444] Orienta-se que: "Atendendo ao desequilíbrio de poder entre empregadores e empregados, estes só podem dar o seu consentimento livremente em circunstâncias excepcionais, quando o ato de dar ou recusar o consentimento não produza quaisquer consequências negativas."[445] [446] [447]

---

[443] EUROPEAN DATA PROTECTION BOARD. Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679. Versão 1.1. Adotada em 4 de maio de 2020. p.10. Disponível em: <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en> Acesso em: 19.07.21.

[444] EUROPEAN DATA PROTECTION BOARD. Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679. Versão 1.1. Adotada em 4 de maio de 2020. p.10. Disponível em: <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en> Acesso em: 19.07.21.

[445] EUROPEAN DATA PROTECTION BOARD. Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679. Versão 1.1. Adotada em 4 de maio de 2020. p.10. Disponível em: <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en> Acesso em: 19.07.21.

[446] Nos seus considerandos (42) e (43), o GDPR apresenta restrições quanto à base legal do consentimento, não o considerando válido diante de relações com manifesto desequilíbrio entre o titular dos dados pessoais e o agente responsável pelo seu tratamento: "Não se deverá considerar que o consentimento foi dado de livre vontade se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado."

Por vezes, em alguns contextos, evitar a base legal do consentimento pode gerar uma proteção mais efetiva dos dados pessoais, especialmente diante de relações assimétricas *(imbalance of power*) com elevado potencial de risco de abuso de poder[448]. Nesse sentido, o consentimento não pode ser entendido como uma base legal válida diante do evidente desequilíbrio entre o titular de dados e o responsável pelo seu tratamento, como acontece nas relações de trabalho.[449] Seguindo, portanto, o entendimento europeu, entende-se que a utilização da base do consentimento para o tratamento de dados pessoais, sobretudo sensíveis, nas relações trabalhistas, deverá ser evitada. Sobre a questão, dispõe o considerando 43 do GDPR que:

> A fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa. Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução.

Quando o responsável pelo tratamento for uma autoridade pública, há dúvidas acerca da possibilidade de utilização do consentimento, uma vez que existe

---

[447] Por exemplo, a concessão de plano de saúde empresarial ou tratamento de dados sensíveis de candidatos em processos seletivos que apliquem ações afirmativas dirigidas a minorias para corrigir distorções no mercado de trabalho.

[448] Com base nesse entendimento, a Autoridade Helênica de Proteção de Dados, na decisão 26/19 - *Greek SA* x *PWC*, multou a empresa PWC em 150 mil Euros pela utilização indevida da base legal do consentimento para tratar dados de seus funcionários. (EDPB. *Company fined 150,00 euros for infringements of the GDPR*. 2019. Disponível em: <https://edpb.europa.eu/news/national-news/2019/company-fined-150000-euros-infringements-gdpr_en> Acesso em: 25.06.21).

[449] Recentemente, motoristas da empresa norte-americana Amazon alegaram estar sendo coagidos pela empresa a assinar um formulário de "consentimento biométrico", sob pena desligamento. "Amazon delivery drivers nationwide have to sign a "biometric consent" form this week that grants the tech behemoth permission to use AI-powered cameras to access drivers' location, movement, and biometric data. If the company's delivery drivers, who number around 75,000 in the United States, refuse to sign these forms, they lose their jobs. The form requires drivers to agree to facial recognition and other biometric data collection within the trucks they drive." (GURLEY, Lauren. Amazon Delivery Drivers Forced to Sign 'Biometric Consent' Form or Lose Job. VICE, 2021. Disponível em: <https://www.vice.com/en/article/dy8n3j/amazon-delivery-drivers-forced-to-sign-biometric-consent-form-or-lose-job> Acesso em 25.5.21).

frequentemente um desequilíbrio de poder na relação entre o responsável pelo tratamento e o titular dos dados. De toda forma, a utilização do consentimento como fundamento jurídico para o tratamento dos dados pelas autoridades públicas não se encontra totalmente excluída, sendo possível, por exemplo, segundo o *European Data Protection Board* (EDPB), nas seguintes situações:

a) Um município local está planejando realizar obras de manutenção rodoviária. Uma vez que essas obras podem perturbar o trânsito durante muito tempo, o município oferece aos cidadãos a oportunidade de se registarem em uma lista de correio eletrônico para receberem atualizações sobre a evolução das obras e os atrasos previstos. O município deixa bem claro que não existe obrigação de participar e solicita o consentimento para utilizar os endereços de correio eletrônico (exclusivamente) para este fim. Os cidadãos que não derem o seu consentimento não deixarão de se beneficiar de qualquer serviço essencial do município nem deixarão de exercer qualquer direito, podendo dar o seu consentimento livremente. Todas as informações sobre as obras de manutenção rodoviária também estarão disponíveis no site do município.

b) Uma faculdade pública solicita aos estudantes consentimento para utilizar as suas fotografias numa revista estudantil impressa. O consentimento nessa situação seria uma verdadeira escolha, desde que não fosse negado aos estudantes o ensino ou os serviços a que têm direito e eles pudessem recusar a utilização das referidas fotografias sem ficarem prejudicados.

Outro tema de grande relevância acerca do consentimento e dos desafios para a sua aplicação é a sua exigência de forma contínua nas relações e as possibilidades de manipulação da real vontade do usuário. Sobre esse tema, a EDPB destaca o seguinte ponto:

> 87. No contexto digital, muitos serviços necessitam de dados pessoais para funcionar, daí que os titulares dos dados recebam diariamente vários pedidos de consentimento que exigem respostas através de cliques ou do deslizar do dedo. Esta situação pode resultar num certo «cansaço» em relação aos cliques: quando aparecem demasiadas vezes, o efeito de alerta dos mecanismos de consentimento começa a diminuir.
> 88. Resulta daqui que as questões ligadas ao consentimento começam a deixar de ser lidas. Esta situação constitui um risco particular para os titulares dos dados, uma vez que, tipicamente, o consentimento é solicitado para ações que, em princípio, são ilícitas sem o seu consentimento. O RGPD imputa aos

> responsáveis pelo tratamento o dever de desenvolver formas de dar resposta a esta questão.[450]

Nesse sentido, já se afirmou que o oferecimento excessivo de controle e possibilidades de escolha ao titular podem sobrecarregá-lo, causando um efeito negativo: ele não será capaz de gerenciar adequadamente as suas decisões quanto aos seus dados.[451] Haveria, assim, uma "fadiga do consentimento"[452], especialmente nas plataformas digitais.

Entende-se que o consentimento não deverá ser compreendido como um mecanismo de imputação de responsabilidade inteiramente sobre os ombros dos titulares, tendo em vista que os agentes também detêm responsabilidades no que concerne à garantia da proteção de dados pessoais. Além disso, os valores incorporados à tecnologia devem ser compatíveis com as expectativas sociais.

O consentimento deve ser visto como um processo, que envolve os dois polos da relação, sendo segmentado em etapas, diante dos qualificadores atribuídos a ele pela lei: informado, livre, inequívoco e dado de forma específica e destacada (quando se tratar de dado sensível). Há uma valorização da função dos agentes de tratamento, que são responsáveis por garantir que cada fase ocorra de acordo com a lei, de modo a obter um

---

[450] EUROPEAN DATA PROTECTION BOARD. Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679. Versão 1.1. Adotada em 4 de maio de 2020. p.22. Disponível em: <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en> Acesso em: 19.07.21.

[451] CHATELLIER, Régis *et al*. *Shaping choices in the digital world*. From dark patterns to data protection: the influence of UX/UI design on user empowerment. CNIL, 2019, p. 30.

[452] "(...) a cultura do consentimento está em cheque, especialmente porque o fenômeno da fadiga do consentimento vai além do simples cansaço da pessoa em face das centenas de políticas de privacidade diferentes. No ambiente online, o desinteresse e a falta de engajamento das pessoas ao ato de consentir sobre o fluxo de dados preponderam, seja porque os temas são bem complexos e explicados de maneira truncada que dificultam a compreensão, ou ainda em virtude da excessiva quantidade de cliques que a pessoa tem que fornecer para acessar os mais diversos conteúdos ou serviços. Nesse sentido, no âmbito do consentimento coletado para fins de processamento de dados com base em cookies, pesquisas conduzidas na União Europeia apontam que o consentimento não é informado e muitas vezes causa confusão nos indivíduos sobre a extensão daquela autorização." Como uma das formas de contornar esta situação, recorda-se "(...)o estabelecimento do chamado "one-stop shop" (balcão único), não confundido aqui com as questões de competência de autoridades nacionais de proteção de dados no contexto europeu. O conceito é bastante simples: a titular de dados encontrará todos os controles sobre a sua privacidade e as maneiras de exercê-los em um único link, canal ou página. Dessa maneira, consegue ter acesso a todas as informações sobre seus dados pessoais, além de alterar suas configurações e preferências, ou revogar eventual consentimento dado anteriormente. Um exemplo de sucesso das iniciativas de "one-stop shop" pode ser encontrado no Check-Up de Privacidade do Google." (VENTRE, Giovanna; CASTELLANO, Ana Carolina Heringer. O dilema do consentimento e a sobrecarga informacional. Jota, publicado em 28 de julho de 2021. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/dilema-consentimento-sobrecarga-informacional-lgpd-28072021> Acesso em: 28.07.21)

aceite válido ao final do processo, sendo o design um dos meios para se garantir que isso ocorra.

Contudo, da mesma forma que o design pode ser utilizado como instrumento para reforçar os direitos dos titulares, ele também pode servir como uma forma de enganá-los, através por exemplo de interfaces maliciosas (*dark patterns*). Design e consentimento estão relacionados seja de maneira positiva, quando as práticas de design são utilizadas para melhorar a capacidade das pessoas de tomarem decisões conscientes, seja negativamente, quando se busca enganá-las por meio de práticas de design abusivas ou que visem a conduzi-las a decisões não vantajosas.[453]

Interfaces maliciosas são inseridas no design de produtos e serviços para influenciar as tomadas de decisão das pessoas.[454] Muitas vezes, contam ainda com outros elementos, como os vieses cognitivos. Segundo Harry Brignull, "Dark Patterns are tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something."[455] Um elemento essencial de sua caracterização é a intenção de manipular a percepção e, consequentemente, a atuação do usuário, estrutura essa bastante preocupante se utilizada em tratamentos que envolvem dados sensíveis. São exemplos de práticas assim consideradas: (i) usar linguagem confusa, como os duplo-negativos; (ii) forçar os usuários a clicar ou a ouvir os motivos pelos quais não devem enviar uma solicitação de cancelamento antes de confirmar sua solicitação; (iii) obrigar o usuário a acessar uma política de privacidade para encontrar a opção de se descadastrar; (iv) estabelecer para o descadastro uma quantidade de cliques muito superior em relação à quantidade de cliques para se cadastrar; e (v) exigir que o titular entregue mais dados pessoais a fim de possibilitar o descadastro[456][457].

---

[453] CHATELLIER, Régis *et al*. *Shaping choices in the digital world*. From dark patterns to data protection: the influence of UX/UI design on user empowerment. CNIL, 2019, p. 41.

[454] NOUWENS, Midas. LICCARDI, Illaria. VEALE, MIchale, *et al*. Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. Disponível em: <https://iapp.org/resources/article/dark-patterns-after-the-gdpr-scraping-consent-pop-ups-and-demonstrating-their-influence/> Acesso em: 22.07.21

[455] Brignull mantém um site sobre o tema onde são listados os principais tipos de interfaces maliciosas: <https://www.darkpatterns.org>. Acesso em: 27 de jun. de 2021.

[456] VICENT, James. California bans 'dark patterns' that trick users into giving away their personal data. The Verge, 16 de mar. de 2021. Disponível em: <https://www.theverge.com/2021/3/16/22333506/california-bans-dark-patterns-opt-out-selling-data>. Acesso em: 03 de jul. de 2021.

[457] MERKEL, Jeremy. Dark Patterns Come to Light in California Data Privacy Laws. The National Law Review, vol. XI, n. 183, 02 de jul. de 2021. Disponível em: < https://www.natlawreview.com/article/dark-patterns-come-to-light-california-data-privacy-laws>. Acesso em: 03 de jul. de 2021.

De forma a inibir tais recursos, mostra-se relevante desenvolver uma regulamentação que verse sobre boas práticas na utilização do design, havendo inclusive a participação de especialistas em psicologia no debate. Nesse cenário, designers atuam como "arquitetos de escolhas" e são capazes de determinar como o indivíduo poderá exercer seu poder de decisão[458]. Apresentar boas e seguras interfaces é um recurso precioso, tendo em vista as diversas possibilidades quando o assunto é usar elementos gráficos e cognitivos para atender ao melhor interesse dos titulares de dados.[459] Além disso, para lidar com essa questão, recomenda-se também a conscientização das pessoas e o estímulo à discussão sobre o tema, pois, uma vez que elas tenham consciência do uso desses mecanismos para influenciar suas decisões, mais atentas ficarão, saindo de um comportamento meramente passivo para uma postura mais ativa nas redes.

3.2.2. Cumprimento de obrigação legal ou regulatória pelo controlador

É lícito tratar dados sensíveis para o cumprimento de obrigação legal ou regulatória pelo controlador, como, por exemplo, obrigações trabalhistas[460] e deveres oriundos da lei anticorrupção. Salvo melhor juízo, podemos incluir também aqui a figura do operador, bem como obrigações oriundas de Códigos de Ética profissionais, portarias do Ministério da Justiça e resoluções[461] de entidades consolidadas, como um

[458] CHATELLIER, Régis *et al*. *Shaping choices in the digital world*. From dark patterns to data protection: the influence of UX/UI design on user empowerment. CNIL, 2019, p. 41-42.

[459] "Ao colocar o titular no centro dessa relação a fim de lhe conferir maior poder sobre o uso de seus dados, a LGPD se aproxima de outra área do conhecimento, User Experience (UX ou experiência do usuário). Nesse sentido, ao analisar cookie banners, é latente a necessidade de engajar profissionais com conhecimento específico no tema, uma vez que são capazes de melhor traduzir um comando legal ao titular de dados, ao mesmo tempo em que se alinha à estratégia da empresa para obtenção de melhores taxas de consentimento, equilibrando os interesses que compõem essa relação. No universo *web*, o consentimento costuma ser obtido em websites por meio de banners na página inicial com opções sobre o uso de *cookies* para diferentes fins, como permitir análise comportamental, publicidade direcionada ou aferir o desempenho do site. Tal tarefa é desempenhada por *Consent Management Platforms* (CMPs), ferramentas que atuam não apenas mostrando o banner ao usuário do website, mas também obtendo e registrando a opção feita sobre o tratamento de dados." (SUNDFELD, Philippe; FERNANDES, Maria Luiza**.** LGPD e UX: um equilíbrio para o consentimento. Jota, publicado em 16 de julho de 2021. Disponível em: < https://www.jota.info/opiniao-e-analise/artigos/lgpd-e-ux-um-equilibrio-para-o-consentimento-16072021> Acesso em: 22.07.21)

[460] Exemplo: obrigatoriedade de exame médico (art.168, CLT); situações em que a lei permite o empregado deixar de comparecer ao serviço sem prejuízo do salário (art. 473, CLT); e dados relativos à filiação sindical para fins de desconto da contribuição sindical (art. 545, 578 e 579, da CLT).

[461] Como a resolução nº 466/2012 do Conselho Nacional de Saúde (CNS), que trata de pesquisas e testes em seres humanos; e a resolução da diretoria colegiada - RDC nº 9, de 20 de fevereiro de 2015, da

Conselho de determinada profissão ou especialidade. Obrigações contratuais não se encontram abrangidas por essa base legal.

Por exemplo, os setores de seguros e de saúde e o mercado financeiro estão submetidos a várias normas legais e regulatórias, devendo cumprir obrigações que eventualmente poderão exigir o tratamento de dados pessoais (inclusive sensíveis) de seus clientes. Além disso, pessoas jurídicas de direito privado que operam planos de assistência à saúde submetem-se à Lei 9.656/98 e à regulação da Agência Nacional de Saúde (ANS), a qual dispõe de resoluções normativas que versam sobre privacidade e proteção de dados.[462]

Como exemplo de obrigação legal, recorda-se que os dados de prontuários médicos deverão ser tratados conforme as disposições legais positivadas na Lei 13.787/18[463]:

> Art. 6º Decorrido o prazo mínimo de 20 (vinte) anos a partir do último registro, os prontuários em suporte de papel e os digitalizados poderão ser eliminados. § 1º Prazos diferenciados para a guarda de prontuário de paciente, em papel ou digitalizado, poderão ser fixados em regulamento, de acordo com o potencial de uso em estudos e pesquisas nas áreas das ciências da saúde, humanas e sociais, bem como para fins legais e probatórios. § 2º Alternativamente à eliminação, o prontuário poderá ser devolvido ao paciente. § 3º O processo de eliminação deverá resguardar a intimidade do paciente e o sigilo e a confidencialidade das informações. § 4º A destinação final de todos os prontuários e a sua eliminação serão registradas na forma de regulamento. § 5º As disposições deste artigo aplicam-se a todos os prontuários de paciente, independentemente de sua forma de armazenamento, inclusive aos microfilmados e aos arquivados eletronicamente em meio óptico, bem como aos constituídos por documentos gerados e mantidos originalmente de forma eletrônica.

Nesse tema, é possível citar também a Resolução do Conselho Federal de Medicina n. 1.605/09, que dispõe que o médico não pode, sem o consentimento do paciente, revelar o conteúdo do prontuário ou ficha médica, bem como a Resolução do CFM n. 1.821/07, a qual aprova as normas técnicas concernentes à digitalização e

---

Agência Nacional de Vigilância Sanitária – ANVISA, que dispõe sobre o Regulamento para a realização de ensaios clínicos com medicamentos no Brasil.

[462] "Conhecer o ambiente legal e regulatório para o desenvolvimento de suas atividades econômicas é uma diretriz segura que deve orientar não apenas hospitais e operadoras de planos de saúde mas também clínicas, prestadores de saúde, laboratórios, indústria farmacêutica e empresas de inovação em saúde, como as health techs. Setores altamente regulados como o setor de saúde precisam ter uma especial atenção às bases legais que autorizam o tratamento de dados, tudo levando em consideração a entrega do melhor serviço de saúde ao titular." Disponível em: <https://www.conjur.com.br/2019-nov-12/lei-geral-protecao-dados-pessoais-atividades-setor-saude> Acesso em: 01.11.20.

[463] Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente.

uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde.[464]

Diante do contexto pandêmico, a Lei nº 13.979/2020[465], em seu artigo 6º, dispõe que é obrigatório o compartilhamento entre órgãos e entidades da administração pública federal, estadual, distrital e municipal de dados essenciais à identificação de pessoas infectadas ou com suspeita de infecção pelo coronavírus, com a finalidade exclusiva de evitar a sua propagação. A obrigação a que se refere o caput deste artigo estende-se às pessoas jurídicas de direito privado quando os dados forem solicitados por autoridade sanitária. O Ministério da Saúde manterá dados públicos e atualizados sobre os casos confirmados, suspeitos e em investigação, relativos à situação de emergência pública sanitária, resguardando o direito ao sigilo das informações pessoais.

Um tema que vem gerando discussão acerca da escolha da melhor base legal diz respeito à utilização de dados biométricos de empregados para controle de jornada[466] ou para acesso a áreas restritas de uma empresa. Há entendimento de que seria válida a utilização da biometria para fins de registro de ponto em cumprimento ao disposto no Art. 74, da CLT[467], e na Portaria 1.510/2009, do então Ministério do Trabalho e

---

[464] Vale destacar os seguintes artigos da resolução do CFM n. 1.821/07: "Art. 6° No caso de microfilmagem, os prontuários microfilmados poderão ser eliminados de acordo com a legislação específica que regulamenta essa área e após análise obrigatória da Comissão de Revisão de Prontuários da unidade médico-hospitalar geradora do arquivo. Art. 7º Estabelecer a guarda permanente, considerando a evolução tecnológica, para os prontuários dos pacientes arquivados eletronicamente em meio óptico, microfilmado ou digitalizado. Art. 8°Estabelecer o prazo mínimo de 20 (vinte) anos, a partir do último registro, para a preservação dos prontuários dos pacientes em suporte de papel, que não foram arquivados eletronicamente em meio óptico, microfilmado ou digitalizado."

[465] Dispõe sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019.

[466] O ponto eletrônico por biometria identifica o dado biométrico do empregado através de um leitor e registra o horário utilizando-se, como regra, da impressão digital. Já o registro de jornada por reconhecimento facial pode se utilizar até mesmo das câmeras de segurança do local para o cômputo da jornada, não sendo necessário um aparelho específico apenas para essa função (o empregado pode usar o seu celular ou um tablet, bastando se posicionar em frente ao aparelho e registrar a sua imagem). De forma menos usual, há também o registro por voz para o controle de ponto.

[467] CLT, Art. 74. O horário de trabalho será anotado em registro de empregados. §1º (Revogado). §2º Para os estabelecimentos com mais de 20 (vinte) trabalhadores será obrigatória a anotação da hora de entrada e de saída, em registro manual, mecânico ou eletrônico, conforme instruções expedidas pela Secretaria Especial de Previdência e Trabalho do Ministério da Economia, permitida a pré-assinalação do período de repouso. §3º Se o trabalho for executado fora do estabelecimento, o horário dos empregados constará do registro manual, mecânico ou eletrônico em seu poder, sem prejuízo do que dispõe o caput deste artigo. § 4º Fica permitida a utilização de registro de ponto por exceção à jornada regular de trabalho, mediante acordo individual escrito, convenção coletiva ou acordo coletivo de trabalho.

Emprego[468], por ser a forma mais fidedigna de atestar a autenticação do lançamento dos horários e da autoria, estando assegurada pela base legal do Art. 11, II, "a", da LGPD.[469] Enquanto a utilização da biometria para o controle de acesso de funcionários a áreas restritas da empresa estaria legitimada na base legal do Art. 11, II, "g", do mesmo diploma legal. Ainda que as bases legais sugeridas não sejam o consentimento, deve-se ter bem claro que estamos diante de dados sensíveis, cujo tratamento é diferenciado pela própria legislação. Assim, certo é que não pode haver desvio na finalidade do uso desses dados e deve o controlador zelar pela segurança dessas informações.

Observa-se, porém, que o tema não está pacificado e requer maiores reflexões. Isso porque se pode questionar a "indispensabilidade" da biometria diante da possibilidade de utilização de sistemas alternativos menos intrusivos para as finalidades desse tratamento, tais como cartão magnético particular, utilização de senha de acesso às dependências da empresa ou medidas organizacionais de segurança.[470]

Além de ser uma base legal que consta tanto no rol do art. 7º quanto no rol do art. 11, o cumprimento de obrigação legal ou regulatória pelo controlador permite a conservação de dados pessoais após o término de seu tratamento, na forma do art. 16, inciso I, da LGPD.

---

[468] O artigo 74, da CLT, permite o controle manual, mecânico ou eletrônico, enquanto a Portaria 1.510/2009 do MTE disciplina o registro eletrônico de ponto e a utilização do Sistema de Registro Eletrônico de Ponto. Há, ainda, a portaria nº 373, de 25 de fevereiro de 2011, que dispõe sobre a possibilidade de adoção pelos empregadores de sistemas alternativos de controle de jornada de trabalho.

[469] "Conquanto seja possível, de fato, assinalar a jornada por outros meios diversos da biometria, não há meio tão eficaz quanto este para assegurar a integridade dos horários lançados nos respectivos registros e a autoria. E a fidedignidade desses registros é essencial e extremamente saudável para ambas as partes, evitando alegações de desvirtuamento da jornada pela existência, por exemplo, de controle paralelo e permitindo a justa e real apuração do saldo de horas. O tratamento do dado biométrico para fins de jornada estaria, assim, assegurado pelo cumprimento de obrigação legal pelo controlador (art. 11, II, a, da LGPD). Além disso, o registro biométrico também pode ser utilizado para outras formas de controle de acesso e segurança na empresa, o que também se legitimaria mesmo sem o consentimento do titular pela alínea "g" do mesmo dispositivo para "garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais"." (PINHEIRO, Iuri; BOMFIM, Vólia. A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho. Trabalho em Debate. Instituto Trabalho em Debate, 2020. Disponível em <http://trabalhoemdebate.com.br/artigo/detalhe/a-lei-geral-de-protecao-de-dados-e-seus-impactos-nas-relacoes-de-trabalho#sdfootnote17sym> Acesso em: 01.06.21.)

[470] Nesse sentido, a Autoridade Holandesa de Proteção de Dados impôs uma multa de 725.000 euros a uma empresa, por entender que o tratamento era excessivo ao exigir dos funcionários suas impressões digitais (*fingerprint data*) para fins de registro de presença e jornada. A empresa não estava autorizada a processar esses dados pessoais sensíveis, pois não se enquadrava em nenhuma das exceções legais. (*Company fined for processing employees' fingerprint data*. Abril de 2020. Disponível em: <https://autoriteitpersoonsgegevens.nl/en/news/company-fined-processing-employees%E2%80%99-fingerprint-data> Acesso em: 06.06.21).

3.2.3 Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos

Aborda-se, aqui, o tratamento de dados pessoais pela Administração Pública que sejam necessários à execução de políticas públicas previstas em leis ou regulamentos.[471] As políticas em questão podem envolver, por exemplo, saúde pública, prevenção de doenças, campanhas de vacinação, auxílios a cidadãos em situação de vulnerabilidade ou projetos voltados ao combate de discriminação dirigida a minorias.

Na redação do Art. 11, II, b, fala-se em "tratamento compartilhado de dados", expressão criticada pela doutrina especializada:

> (...) é necessário chamar atenção para a confusão terminológica do legislador quanto ao uso da expressão "tratamento compartilhado" no art. 11 da LGPD. Com efeito, a partir da leitura da lei, é possível compreender que o "uso compartilhado de dados", previsto no art. 5º, XVI, é uma modalidade de "tratamento" de dados, conforme definição do art. 5.º, X. Não faria sentido imaginar que a legislação tivesse pretendido limitar o tratamento de dados sensíveis pelo Poder Público à hipótese de uso compartilhado. Uma interpretação sistemática dos artigos em questão conduz, portanto, ao entendimento de que o art. 11 se refere tanto ao tratamento quanto ao uso compartilhado de dados sensíveis pelo Poder Público.[472]

Execução de políticas públicas é uma das justificativas para que o poder público realize tratamentos de dados.[473] Esse requisito encontra-se intimamente ligado à previsão estabelecida no artigo 23 da LGPD[474], que dispõe que o tratamento de dados

---

[471] Conferir: ANPD. Guia Orientativo. *Tratamento de Dados Pessoais pelo Poder Público*. Janeiro/2022.

[472] WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo poder público. In: Bruno Bioni, Laura Schertel Mendes, Danilo Doneda, Otavio Luiz Rodrigues Jr., Ingo Wolfgang Sarlet. (Org.). *Tratado de Proteção de dados pessoais*. 1ed.Rio de Janeiro: Forense, 2021. E-book.

[473] LGPD, 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. (...)

[474] "(...) o Estado desempenha um amplo rol de atividades de tratamento de dados que nem sempre podem ser compreendidas como políticas públicas. Atividades relacionadas ao pagamento de salários e gestão de servidores públicos, por exemplo, são claramente necessárias ao funcionamento da máquina estatal, mas dificilmente classificáveis como políticas públicas. Também atividades de fiscalização e sancionamento poderiam ser compreendidas como execução de políticas públicas apenas numa compreensão bastante

pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do Art. 1º da Lei 12.527/2011 (Lei de Acesso à Informação)[475] 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: a) sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; e b) seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais.

O tratamento de dados sensíveis pela Administração traz uma série de questões, especialmente em um momento de intensa coleta de dados de saúde e biométricos, bem como de uso crescente de tecnologias digitais por governos. Diante disso, primar pelos princípios constitucionais e de proteção de dados mostra-se fundamental para a garantia de direitos ao cidadão.

3.2.4 Realização de estudos por órgão de pesquisa

Pode-se também tratar dados sensíveis para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.[476] A

---

dilatada do termo. O deslinde dessa questão se dá pela leitura do *art. 23 da LGPD, que estabelece uma hipótese complementar para o tratamento de dados pelo Poder Público, ao acrescentar às previsões dos arts. 7.º e 11 o objetivo de "executar as competências legais ou cumprir as atribuições legais do serviço público".* Compreende-se, assim, que, no que tange às bases legais específicas para o tratamento de dados pessoais pelo Poder Público, a LGPD prevê duas hipóteses centrais: (i) execução de políticas públicas; e (ii) execução de competências legais ou atribuições legais do serviço público." (WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo poder público. In: Bruno Bioni, Laura Schertel Mendes, Danilo Doneda, Otavio Luiz Rodrigues Jr., Ingo Wolfgang Sarlet. (Org.). *Tratado de Proteção de dados pessoais*. 1ed.Rio de Janeiro: Forense, 2021. E-book.) (grifou-se)

[475] 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: 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.

[476] Cf. BARRETO, Maurício Lima; ALMEIDA, Bethania de Araujo; DONEDA, Danilo. Uso e Proteção de Dados Pessoais na Pesquisa Científica. *RDU*, Porto Alegre, Volume 16, n. 90, 2019, 179-194, nov-dez 2019.

referida disposição encontra-se com a mesma redação nos artigos 7º e 11 da LGPD.

É necessário observar que não será qualquer instituição que poderá utilizar esta base legal. Dispõe a lei, em seu Art. 5º, XVIII, que órgão de pesquisa representa "órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico". Como exemplos de órgão de pesquisa, pode-se recordar do Ipea - Instituto de Pesquisa Econômica Aplicada, do IBGE - Instituto Brasileiro de Geografia e Estatística e da Fiocruz - Fundação Oswaldo Cruz. A ausência de finalidade lucrativa para pessoa jurídica de direito privado cria parâmetro que impede que entidades de pesquisa privadas, como sociedades, possam se valer dessa base legal para tratar dados pessoais. Em relação à anonimização[477] — 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 —, entende a Lei que essa situação seria mais protetiva para os titulares, devendo ser sempre que possível garantida. Anonimizado é o dado que não identifica seu titular, ou seja, não apresenta mais relação direta ou indireta com seu titular. Uma vez anonimizado, o dado deixa de ser pessoal, segundo o Art. 12 da LGPD.[478]

[477] "Para proteger a privacidade dos indivíduos as bases de dados anonimizadas podem se valer de vários expedientes, como ocultar algumas informações, generalizar outras e assim por diante. Então ao invés de saber quem exatamente visitou o meu estabelecimento eu sei que essa pessoa é homem ou mulher e que tem uma idade entre 40-50 anos, só para continuar com o exemplo. Somando todas as entradas na base de dados eu consigo gerar uma visualização de quantos % do meu público é de cada faixa etária, gênero e assim por diante. Acontece que quanto mais informações eu jogo nessa base, mais fácil fica reidentificar a pessoa cujo dado foi anonimizado. Chegamos então em uma encruzilhada: como criar uma base de dados anonimizados que possa atingir o equilíbrio entre utilidade para quem se vale dela e ao mesmo tempo não saia por aí revelando a identidade de todo mundo? (...) para o dado ser considerado como anonimizado eu preciso olhar para dois fatores: um objetivo e outro subjetivo. Por fatores objetivos no conceito de "esforços razoáveis" a própria lei menciona "o custo e o tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis" (art. 12, §1º). Já os fatores subjetivos olham para quem fez o processo de anonimização e para quem está tentando quebrá-lo (SOUZA, Carlos Affonso. Eles sabem quem é você? Entenda o monitoramento de celulares na quarentena. Disponível em: <https://tecfront. blogosfera.uol.com.br/2020/04/17/eles-sabem-quem-e-voce-entenda-o-monitoramento-de-celulares-na-quarentena/>. Acesso em: 03.05.20).

[478] Considerando 26 do GDPR: "(...)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 anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não

Convém, no entanto, recordar crítica que afirma que o processo de anonimização seria, em verdade, circunstancial, podendo ser revertido em muitos casos a partir das novas técnicas e ferramentas tecnológicas. Seria, portanto, um equívoco acreditar que a anonimização ofereceria alto grau de proteção para os dados, tendo em vista as diversas possibilidades de cruzamento de informações e o contínuo desenvolvimento de tecnologias que visam a desanonimizar bases de dados pessoais, inclusive sensíveis.[479] Acerca da possibilidade de anonimização, destaca-se relevante posição doutrinária:

> (...) o ônus da determinação da possibilidade de anonimização de dados sensíveis recai necessariamente sobre o agente de tratamento de dados, no caso, os órgãos de pesquisa. Nessa hipótese, devem-se considerar o desconhecimento e a hipossuficiência do titular de dados em relação às técnicas de anonimização de dados existentes para estabelecer um padrão de segurança exigível. Portanto, parece necessário que seja regulado pela Autoridade Nacional de Proteção de Dados Pessoais qual o tipo de tecnologia de segurança e sistema de anonimização de dados que devem ser utilizados pelos agentes de tratamento, com fins de promover a ampla proteção dos dados sensíveis dos sujeitos que participam dos estudos levados a cabo pelos órgãos de pesquisa.[480]

Essa posição dialoga diretamente com o artigo 12, § 3º, da LGPD, o qual afirma que a Autoridade Nacional de Proteção de Dados 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.

Vale lembrar também que, de acordo com o Art. 13 da LGPD, na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a

---

possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação."

[479] Em perspectiva crítica, afirma-se que: "Interessa salientar que, em face dos processos de agregação de bases de dados e, portanto, de reidentificação, qualquer dado anonimizado é, em regra, um dado pessoal e, assim, as formas de discriminação podem igualmente sofrer alterações profundas, inclusive por vezes se tornando sutis e imperceptíveis ao cidadão comum. Oportunamente, deve-se clarificar que o termo identificável é, em regra, superável, tendo sido recepcionado pela LGPD no que diz respeito às formas de expressão da razoabilidade, ou seja, ao nível de investimento de tempo e de dinheiro envolvidos no processo de anonimização. De toda sorte, a pseudoanonimização, não custa mencionar, constitui um meio-termo entre o dado pessoal e o dado anomizado." (RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da lei geral de proteção de dados (LGPD) – Lei 13.709/2018. In: Bruno Bioni, Laura Schertel Mendes, Danilo Doneda, Otavio Luiz Rodrigues Jr., Ingo Wolfgang Sarlet. (Org.). *Tratado de Proteção de dados pessoais*. 1ed. Rio de Janeiro: Forense, 2021. E-book.)

[480] MULHOLLAND, C. O tratamento de dados pessoais sensíveis. In: Mulholland, Caitlin (Org.). *LGPD e o novo marco normativo no Brasil.* Porto Alegre: Arquipélago Editorial, 2020, v. 1, p. 142.

bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização[481] dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.[482] Acrescenta-se que a divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais. O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro. O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da Autoridade Nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.

Ainda sobre o tema, a LGPD assegura, expressamente, em seu artigo 16, II, que os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: "(...) II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais."

3.2.5 Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral

A norma traz a possibilidade de tratamento de dados sensíveis para o exercício regular de direitos tanto em relação a um contrato quanto em processo judicial, administrativo ou arbitral (nos termos da Lei nº 9.307, de 23 de setembro de 1996 - Lei de Arbitragem). O Art. 11 não replicou, portanto, a disposição do Art. 7º, V, que permite o tratamento de dados pessoais quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a

[481] Art. 13, § 4º, da LGPD: Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.
[482] Cf. EDPB. Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research. Adopted on 2 February 2021.

pedido do titular dos dados.[483]

Acerca das diferenças entre as bases legais no que concerne ao contrato, doutrina destaca:

> (...) quis o legislador impor maior grau de cautela aos agentes de tratamento. Assim, em vez de simplesmente transpor o texto do artigo 7º, V, e correr o risco de a base legal de execução de contrato ser aplicada de maneira extensiva, o legislador fez questão de frisar que o agente de tratamento deve identificar um direito concreto que exsurge do contrato e atrai a necessidade do tratamento. Na verdade, mais do que necessidade, no caso, a lei demanda que o tratamento seja essencial, dado o uso do termo "indispensável" no inciso II do artigo 11.[484]

Quanto ao exercício regular de direitos em contrato, recorda-se a situação de um seguro saúde ou seguro de vida necessitar coletar informações sensíveis, pois, sem o tratamento de tais dados, poderá não ser possível entregar a prestação que lhe compete decorrente da relação contratual, como o ressarcimento de despesas médicas no seguro saúde ou o pagamento de indenização por algum tipo de invalidez decorrente de acidente ou doença.[485] Afirma-se que, aqui, a seguradora não teria apenas o dever de cumprir a obrigação contratual, mas também o direito de adimpli-la.[486] Nesse sentido,

---

[483] Como, por exemplo, nas situações em que o titular adquira produtos ou serviços seus dados poderão ser tratados para essa finalidade específica (Art. 7º, V). A base também pode ser aplicada para levantamentos realizados por instituições financeiras em relação a determinada pessoa, anteriormente à concessão de crédito a ela. Após a solicitação efetuada pela pessoa, a instituição realizará análise de risco e de crédito. "Essa base legal tem especial importância para o setor de seguros, que necessita realizar análises preliminares para subsidiar a contratação (conhecimento do risco), como também para cumprir o contrato, como na hipótese da regulação de um sinistro, do fornecimento de assistência 24 horas, da inspeção de risco etc." (Guia de boas práticas do mercado segurador brasileiro sobre a proteção de dados pessoais. CNseg. p.26. Disponível em: <https://cnseg.org.br/data/files/A6/25/A2/F2/9B22571029E24F473A8AA8A8/GBPMS_ONLINE_ok.pdf >. Acesso em: 29.07.21)

[484] PALHARES, Felipe; PRADO, Luis; VIDIGAL, Paulo. *Compliance digital e LGPD*. São Paulo: Thomson Reuters Brasil, 2021. p.176.

[485] Guia de boas práticas do mercado segurador brasileiro sobre a proteção de dados pessoais. CNseg. p.31.

[486] Da mesma forma, a doutrina europeia tratando de dispositivo similar no GDPR reconhece a possibilidade de uma seguradora − com base no exercício regular de direitos decorrentes de um contrato − tratar dados de saúde de um segurado para verificar a regularidade de uma reclamação de indenização oriunda de um sinistro de seguros de pessoas. "Using sensitive data may also be necessary for a controller to establish, exercise or defend legal claims. Reliance on this criterion requires the controller to establish necessity. That is, there must be a close and substantial connection between the processing and the purposes. One example of an activity that would fall under this criterion is processing medical data by an insurance company in order to determine whether a person's claim for medical insurance is valid. Processing such data would be necessary for the insurance company to consider the claim brought by the claimant under their insurance policy" (USTARAN, Eduardo. *European Data Protection Law and Practice*. Portsmouth: IAPP, 2018, p. 88).

> (...) o requisito para tratamento de dados com base no exercício regular de direitos em sede contratual não se confunde com os interesses legítimos do controlador ou de terceiros. Como se trata de dados sensíveis, aqui a legislação **impõe um controle maior sobre o que efetivamente poderia contar como requisito que chancele o tratamento, incluindo a análise sobre**: ***(i)*** a existência de um direito envolvido no caso; ***(ii)*** se o exercício desse direito é regular (e não abusivo) e ***(iii)*** se esse direito decorre de uma relação contratual. (...) Não obstante, será possível se valer do exercício regular de um direito em sede contratual como base legal para o tratamento de dados em algumas hipóteses como, por exemplo, na prevenção e combate à fraude, porque prevenir e combater a fraude em seguros mais do que um direito da sociedade seguradora é um dever, como entidade encarregada de proteger a mutualidade representada por toda a massa de segurados e em decorrência de determinações legais e regulatórias específicas para essa finalidade.[487]

Acerca do exercício regular de direitos/de defesa em ações judiciais, entende-se que ele não deve se limitar a um processo judicial já em andamento, podendo tal hipótese de tratamento ser interpretada para abranger procedimentos judiciais futuros (para o seu estabelecimento ou em sede de defesa, dentro de critérios razoáveis e havendo justificativa plausível), para obtenção de orientação jurídica ou outra forma de defesa legal para exercício de direitos.[488] [489]

Essa base poderá ser utilizada para respaldar a guarda de dados, mesmo após o término de uma operação, para constituir eventual meio de prova de direitos e obrigações. Um parâmetro de tempo razoável para a guarda, em alguns casos, pode ser o prazo para exercício de determinada pretensão. Em um caso de constituição de prova, os dados pessoais deverão ser usados quando forem indispensáveis para a defesa do agente, levando em conta os princípios constitucionais do contraditório e da ampla defesa. Observa-se, portanto, cuidadosamente as situações de violação à boa-fé e de

---

[487] Guia de boas práticas do mercado segurador brasileiro sobre a proteção de dados pessoais. CNseg. p.31-32.

[488] Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/#conditions6> acesso em: 22.11.20

[489] "The processing of special categories of data which "is necessary for the establishment, exercise or defence of legal claims", whether in court proceedings or in an administrative or out-of-court procedure,425 is also allowed under the GDPR. In this case, processing must be relevant to a specific legal claim and its exercise or defence respectively, and may be requested by any one of the disputing parties. When acting in their judicial capacity, courts may process special categories of data within the context of resolving a legal dispute. Examples of these special categories of data processed in this context could include for example, genetic data when establishing parentage, or health status when part of the evidence concerns details of an injury sustained by a victim of crime." (Handbook on European data protection law 2018 edition. p.163.)

abuso do direito. É possível pedir ao juiz, em determinados casos, segredo de justiça para que o acesso aos dados fique limitado e protegido.

Vale recordar, aqui, exemplos desenvolvidos pela ICO para a presente base legal:

a) Um empregador está sendo processado por um de seus empregados após um acidente de trabalho. O empregador deseja transmitir os detalhes do acidente aos seus advogados para obter aconselhamento jurídico e se defender em reclamação judicial. As informações sobre o acidente incluem detalhes das lesões do indivíduo, que se qualificam como dados de saúde. Aqui, a presente base legal seria aplicável.

b) Um cabeleireiro realiza teste em cliente para verificar se ela terá alguma reação alérgica com a tintura que ele pretende aplicar em seu cabelo. O cabeleireiro registra quando o teste foi feito e os resultados. O cabeleireiro está, portanto, tratando dados de saúde sobre as alergias da cliente. Embora não haja nenhuma reclamação judicial em curso ou esperada, os objetivos no caso são estabelecer que o cabeleireiro está cumprindo o seu dever de cuidar da cliente e se defender em eventual ação judicial, no caso de haver alguma reação adversa.

3.2.6 Proteção da vida ou da incolumidade física do titular ou de terceiro

Em alguns casos, o tratamento de dados pessoais sensíveis pode proteger interesses individuais, relativos à vida e integridade do titular dos dados, e/ou coletivos, como, por exemplo, quando o tratamento for necessário para fins humanitários ou visando a tutelar questões de interesse público.

Em meio à pandemia da COVID-19, essa base legal mostrou-se de aplicação relevante na medida em que diferentes sujeitos da sociedade civil passaram a implementar estratégias para combater o coronavírus em seus ambientes privados, como, por exemplo, em prédios corporativos, indústrias ou estabelecimentos comerciais. O tratamento – devidamente fundamentado e apenas em situações necessárias – de determinados dados sensíveis dos titulares que frequentam tais ambientes passou a ser relevante para se limitar a possibilidade de proliferação da doença, representando uma medida de segurança.

Idealmente, a aplicação dessa base legal deve se dar nos casos em que for difícil obter o consentimento do titular dos dados, porque, por exemplo, ele se encontra inconsciente ou desaparecido. Exemplo: pessoa inconsciente é levada para um hospital (onde nunca esteve), após sofrer grave acidente. Nesse caso, o novo hospital precisará de pelo menos parte do histórico médico do paciente para atendê-lo de forma adequada. A partir dessa base legal, entende-se que poderá o médico que irá atendê-lo requisitar documentação a outro hospital onde o paciente já esteve ou ao médico de confiança dessa pessoa (se essa informação estiver disponível).

3.2.7 Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária

Diante da restrição quanto aos sujeitos que podem fazer uso desta base legal, resta claro que os principais controladores nesse contexto serão hospitais e outros agentes da área da saúde. Em relação à autoridade sanitária, recorda-se a Lei nº 9.782/99, que define o Sistema Nacional de Vigilância Sanitária e cria a Agência Nacional de Vigilância Sanitária.

Podemos trazer os seguintes questionamentos a respeito da base legal: quem seriam os profissionais de saúde[490] e quais serviços[491] seriam considerados de saúde? Um plano de saúde, por exemplo, poderá utilizar de forma ampla tal base legal? A tutela da saúde nesse dispositivo seria especificamente da pessoa a quem esses dados dizem respeito ou poderia envolver uma coletividade ou grupo específico?

O cuidado com a mencionada base deve existir entre outras razões porque, a partir da solicitação de exames ou da análise de dados de saúde, é possível ter em mãos

[490] Profissionais da saúde são, por exemplo, médicos, enfermeiros, nutricionistas, fisioterapeutas, terapeutas ocupacionais, biólogos, biomédicos, farmacêuticos, odontólogos, fonoaudiólogos, psicólogos, assistentes sociais, profissionais da educação física e médicos veterinários. Fonte: CGPNI: Coordenação Geral do Programa Nacional de Imunizações, janeiro de 2021. Informado pelo Grupo de Vigilância Estadual.

[491] Lei nº 8.080, de 19 de setembro de 1990 - Dispõe sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes e dá outras providências. Art. 1º Esta lei regula, em todo o território nacional, as ações e **serviços de saúde**, executados isolada ou conjuntamente, em caráter permanente ou eventual, por pessoas naturais ou jurídicas de direito Público ou privado.

situações muito sensíveis sobre determinada pessoa e terceiros que com ela tenham relação, bem como praticar discriminações ilícitas ou abusivas.

De acordo com o "Código de Boas Práticas: Proteção de Dados para Prestadores Privados de Serviços em Saúde", publicado em 2021 pela Confederação Nacional de Saúde (CNSaúde), para a adequada utilização dessa base legal mostra-se necessário cautela, pois seu conceito não se aplica indiscriminadamente a todas as etapas da prestação de serviços de saúde. Ainda que todo o setor de saúde atue pelo menos indiretamente para o benefício da saúde do paciente, a referida base legal somente será aplicável nos "procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridade sanitária", não podendo ser aplicável a qualquer processamento de dados do setor da saúde. No documento, sugere-se que sua utilização seja realizada à luz do conceito de tutela da saúde presente no Artigo 9(2)(h) e Artigo 9(3) do GDPR, que dispõem respectivamente que:

> Se o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, para o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito da União ou dos Estados-Membros ou por força de um contrato com um profissional de saúde, sob reserva das condições e garantias previstas no nº 3;[492]
> (...)
> 3. Os dados pessoais referidos no nº 1 podem ser tratados para os fins referidos no nº 2, alínea h), se os dados forem tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional, nos termos do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade ao abrigo do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes.[493]

Dessa forma, conforme o "Código de Boas Práticas", será necessário verificar quais tratamentos são realizados no âmbito das *atividades fim* dos prestadores (medicina

[492] Artigo 9(2)(h) do GDPR (…) "processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;"

[493] Artigo 9(3) do GDPR "Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies."

preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde) e se os dados foram tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de *sigilo profissional*.

Como exemplos, são destacados usos da base legal em casos de: "acesso e manuseio das informações do prontuário médico por profissionais de saúde envolvidos no tratamento do paciente que são obrigados ao sigilo profissional"; "utilização do prontuário médico para gerar diagnósticos com auxílio de softwares"; e "acessar informações do prontuário médico por profissional da saúde obrigado ao sigilo profissional em caso de risco de vida". Por outro lado, o "acesso e manuseio de informações do prontuário médico por profissionais não obrigados ao sigilo profissional" devem ser realizados com o consentimento do usuário ou por obrigação legal ou regulatória.

Ainda, no "Código de Boas Práticas" entende-se que, em relação às bases legais dos principais tipos de tratamentos de dados envolvendo exames laboratoriais, será necessário utilizar as bases do Art. 11. Diante disso,

> No caso da "coleta das amostras ou das imagens"; "encaminhamento da amostra ou da imagem para o setor responsável pela análise clínica"; "emissão de laudo diagnóstico"; "divulgação do resultado para o paciente"; "armazenamento dos resultados", quando realizados por profissional de saúde obrigado ao sigilo médico, a base legal aplicável é a tutela da saúde.[494]

Recorda-se que, durante o tratamento de um paciente, o profissional de saúde pode precisar compartilhar informações com colegas da profissão para dirimir dúvidas ou obter uma segunda opinião sobre determinado diagnóstico ou outras finalidades diretamente relacionadas à tutela da saúde do paciente. Sobre a situação, o "Código de Boas Práticas" esclarece que:

> (...) um clínico geral pode necessitar do auxílio de um neurologista para diagnosticar determinados sintomas, ou quer discutir um caso específico com outro colega da mesma área, e, para isso, circula dados do seu paciente em meios de comunicação. Caso algum dado que permita a identificação do paciente seja divulgado, ou mesmo os exames dele sejam compartilhados, o

[494] Código de Boas Práticas: Proteção de Dados para Prestadores Privados de Serviços em Saúde. p. 66. Documento disponível em: <http://cnsaude.org.br/baixe-aqui-o-codigo-de-boas-praticas-protecao-de-dados-para-prestadores-privados-de-saude/> Acesso em: 27.07.21.

> caso atrai a incidência da LGPD, devendo estar embasado em uma base legal que permita tal compartilhamento.[495]

A interpretação da referida base legal conforme a visão do GDPR parece uma proposta bastante interessante e que apresenta mais garantias à pessoa humana. O setor de saúde possui grande fluxo de dados sensíveis, devendo contar com proteções adicionais e maior segurança jurídica e técnica.

3.2.8 Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos

No lugar da hipótese relativa ao legítimo interesse (que não se aplica quando no tratamento houver dados sensíveis), o Art. 11, II, "g", trouxe base mais específica, que visa à prevenção de fraudes e a garantir a segurança do titular, restando vinculada aos interesses dos titulares e determinadas entidades.

Como exemplo de aplicação, aponta-se a seguinte situação: instituições bancárias e empregadores podem tratar dados biométricos para a prevenção de fraudes, sem o consentimento dos titulares dos dados, a fim de confirmar que é o empregado autorizado que está entrando em área de acesso restrito da empresa ou que é determinado cliente que está realizando uma transação bancária relevante. Ainda, é possível tratar dados sensíveis a partir dessa base legal em um contexto em que se necessite prevenir fraudes em processos de identificação ou de confirmação de identidade por meio de aplicativos utilizados em smartphones, como, por exemplo, para a criação de uma conta digital. Da mesma forma, pode-se utilizar essa base para a coleta de dados biométricos de colaborador para acesso a sistemas financeiros da empresa. Outra situação seria o pedido para atendimento médico-hospitalar, com a utilização de seguro ou de plano de assistência à saúde, que o segurado/beneficiário colocasse seu polegar em um leitor biométrico para confirmar sua identidade, a fim de evitar que outra pessoa utilizasse a cobertura securitária em seu lugar.

Na aplicação da referida base, é necessário observar em síntese quatro questões:

---

[495] Código de Boas Práticas, op.cit., p. 76.

a) O tratamento deve ocorrer visando a garantir a prevenção à fraude e a segurança do titular. Por consequência, o tratamento também oferecerá maior segurança ao controlador.

b) O tratamento do dado sensível será em processos de identificação e autenticação de cadastro do titular em sistemas eletrônicos.

c) No tratamento deverão ser resguardados os direitos mencionados no Art. 9º da LGPD.[496]

d) No tratamento em questão, é necessário observar cuidadosamente eventual lesão ou situação indevida que envolva direitos e liberdades fundamentais do titular e exija a proteção de seus dados pessoais. Assim como ocorre na utilização da base legal do legítimo interesse[497], caso os direitos e liberdades fundamentais do titular devam prevalecer no caso concreto, esta base legal não poderá ser utilizada.

A respeito da aplicação dessa base, parece equivocado realizar seu emprego quando for possível identificar a pessoa natural com outros dados pessoais (não sensíveis) e/ou através de ferramentas específicas, havendo, então, níveis próximos de segurança e o alcance da finalidade pretendida. É importante, aqui, que se tenha certeza de que os dados que serão tratados a partir dessa hipótese legal sejam realmente indispensáveis para se alcançar a prevenção de fraudes e a proteção da segurança do titular na utilização de serviços/bens relevantes. Sua utilização, como regra, será para contextos especiais em que seja necessário maior segurança para a correta identificação e autenticação do titular de dados. Além disso, deve-se observar – com maior vigor – as hipóteses legais e o período de conservação dos dados sensíveis tratados.

Diante da possibilidade de uso de reconhecimento facial para algumas atividades públicas e privadas, mostra-se necessário discutir com maior profundidade o uso de dados biométricos, bem como se a imagem de uma pessoa natural (contida em fotos ou

---

[496] Art. 9º O titular tem direito **ao acesso facilitado às informações sobre o tratamento de seus dados**, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: I - finalidade específica do tratamento; II - forma e duração do tratamento, observados os segredos comercial e industrial; III - identificação do controlador; IV - informações de contato do controlador; V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VI - responsabilidades dos agentes que realizarão o tratamento; e VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei. (...) (grifou-se)

[497] LGPD - "Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: (...) IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;"

captada em vídeo) pode ser considerada um dado pessoal sensível. Conforme dispõe o considerando 51 do *General Data Protection Regulation* (GDPR), o tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que elas serão apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular. Em adição ao considerando, mostra-se necessário observar também no caso concreto o contexto, os dados revelados pela imagem e a finalidade de seu tratamento.

Além de questões biométricas, considerando-se que uma imagem pode revelar, em alguns casos, dados de origem étnica ou racial, de saúde, de orientação sexual ou questões religiosas de determinada pessoa natural, é possível defender seu enquadramento, em determinados contextos e diante de certos usos, como um dado pessoal sensível. Além disso, se a finalidade do processamento da imagem (e demais dados adicionados) se relacionar com a obtenção de informações sensíveis, isso acarretará a aplicação das normas especiais relacionadas.[498]

3.2.9 Compartilhamento de dados sensíveis pelo setor privado

Voltando para os parágrafos do Art. 11 da LGPD, a comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com o objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da Autoridade Nacional de Proteção de Dados, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências (Art.11, §3º). A LGPD não dispôs, porém, se e em que condições o próprio titular poderia obter vantagem econômica a partir do compartilhamento dos seus dados sensíveis de saúde, o que vem sendo bastante discutido no setor da saúde e em novos negócios.[499]

Segundo a Lei (Art.11, §4º), é vedada a comunicação ou o uso

[498] Observa-se que a questão já foi abordada e aprofundada nos capítulos 1 e 2 da presente tese de doutorado.

[499] Sugere-se, aqui, a análise do projeto My Health My Data: <http://www.myhealthmydata.eu/why-mhmd/> Acesso em: 27.07.21. ROTHBARTH, Renata. Monetização de dados de saúde à luz da LGPD: interpretação do artigo 11, §3º. In: DALLARI, Analluza Bolivar; MONACO; Gustavo Ferraz de Campos (Org.). *LGPD na saúde*. São Paulo: Revista dos Tribunais, 2021. p. 299.

compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com o objetivo de obter vantagem econômica, *exceto* nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: I - a portabilidade de dados quando solicitada pelo titular; ou II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo[500].

Nesse caso, a noção de "em benefício dos interesses dos titulares de dados" mostra-se bastante aberta e traz uma série de discussões por se tratar de situação em que haverá a comunicação ou o uso compartilhado entre controladores de dados sensíveis referentes à saúde com o objetivo de obter vantagem econômica. Quem determinará se realmente há um benefício preponderante? Sobre o parágrafo em questão, afirma-se que "(...) o que o legislador quis evitar com a vedação ao compartilhamento dos dados de saúde foi, especialmente, a compra e venda mascarada de bases de dados com essas informações sensíveis e a discriminação na formação de preços de planos de saúde em razão dos conhecimentos obtidos por meio desses dados."[501] Recorda-se que a portabilidade dos dados representa um dos direitos do titular[502]. Ela possibilita que o titular, junto ao controlador, possa obter as suas informações pessoais de forma estruturada e de modo que possam ser transmitidas e reutilizadas em diferentes serviços. Ela permite que eles movam, copiem ou transfiram dados pessoais facilmente de um ambiente para outro, de forma segura e protegida, sem afetar sua usabilidade. O direito se aplica apenas às informações que o indivíduo forneceu ao controlador.[503] Estando de

---

[500] "(...) é de rigor que as operadoras de planos de saúde e outros prestadores de serviços de saúde recebam esses dados para que possam realizar as atividades para as quais são contratadas, como realizar o pagamento pelos serviços prestados e pelos eventuais insumos médicos utilizados durante o atendimento." (PALHARES, Felipe. Vantagem econômica no compartilhamento de dados de saúde: interpretação do artigo 11, § 4º, da LGPD. In: DALLARI, Analluza Bolivar; MONACO; Gustavo Ferraz de Campos (Org.). *LGPD na saúde*. São Paulo: Revista dos Tribunais, 2021. p. 310.)

[501] PALHARES, Felipe. Vantagem econômica no compartilhamento de dados de saúde: interpretação do artigo 11, § 4º, da LGPD. In: DALLARI, Analluza Bolivar; MONACO; Gustavo Ferraz de Campos (Org.). *LGPD na saúde*. São Paulo: Revista dos Tribunais, 2021. p. 309.

[502] LGPD - "Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: (...) V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;"

[503] Sobre portabilidade, a ICO apresenta o seguinte material: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/> Acesso em: 28.07.21.

posse de seus dados e de seu histórico, o titular pode obter similar contratação em concorrente, por exemplo, exercendo assim sua livre opção.[504] Na LGPD, o direito à portabilidade não inclui dados que foram anonimizados.[505]

Enfim, o § 5º do Art. 11 dispõe que é vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários. Esse dispositivo deve ser lido em consonância com o que dispõe a Lei 9.656/1998 (que versa sobre os planos e seguros privados de assistência à saúde) e seu Art. 14, o qual estabelece que, em razão da idade do consumidor, ou da condição de pessoa portadora de deficiência, ninguém pode ser impedido de participar de planos privados de assistência à saúde.[506]

Essa vedação não parece completamente nova para o setor da Saúde Suplementar, pois na Resolução Normativa n. 195, de 14 de julho de 2009, a Agência Nacional de Saúde Suplementar (ANS) já coibia tal prática, estabelecendo, em seu Art. 16, que para vínculo de beneficiários aos planos privados de assistência à saúde coletivos por adesão ou empresarial não serão permitidas quaisquer outras exigências que não as necessárias para ingressar na pessoa jurídica contratante. O setor de Saúde

---

[504] Um doente de uma clínica privada Y vai mudar-se para outra clínica X. O doente solicita à clínica Y, que possui arquivos eletrônicos a seu respeito, que lhe forneça os seus dados pessoais num formato estruturado de leitura automática, a fim de poder transmitir os mesmos aos profissionais de saúde pertinentes na clínica X. A clínica Y deve fornecer-lhe os seus dados pessoais num formato aberto de uso corrente. Ao selecionar o formato dos dados, a organização deve ter em consideração o modo como o formato irá afetar ou prejudicar o direito da pessoa a reutilizar os dados. Por exemplo, o fornecimento, a um doente, de versões em PDF do seu processo poderá não ser suficiente para garantir a reutilização fácil dos dados em questão.

[505] LGPD – "Art. 18, § 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador."

[506] "Esse dispositivo, porém, deve ser lido em consonância com o que dispõe a Lei nº 9.656/98 (que versa sobre os planos e seguros privados de assistência à saúde) e aqui merece ser feita uma distinção entre seleção de riscos e análise de risco para fins de subscrição e precificação. A Lei nº 9.656/98 veda a seleção de riscos, ou seja, a possibilidade de recusa de oferecimento de cobertura a determinado proponente, porém a mesma lei reconhece a possibilidade de precificação e de análise de riscos para fins de subscrição ao admitir que, na presença de doença preexistente, deverá ser ofertada ao proponente a cobertura parcial temporária ou o agravo do prêmio durante o período no qual seria aplicável a cobertura parcial temporária. Portanto, é nessa linha que deve ser interpretado esse dispositivo da LGPD. Logo, é fundamental que se ponha em perspectiva que nem toda discriminação é prejudicial e ilícita, como não é, por exemplo, aquela diretamente relacionada a subsidiar a contratação de um seguro" (Guia de boas práticas do mercado segurador brasileiro sobre a proteção de dados pessoais. CNseg. p.14.). "Portanto, seleção de riscos para fins de não oferecimento de cobertura em seguro saúde é vedada pelo dispositivo em questão, mas não a análise de risco para fins de precificação (agravo do prêmio) ou para o estabelecimento de cobertura parcial temporária, no caso de identificação de preexistência de alguma doença, o que, como consequência, autoriza o tratamento de dados sensíveis referentes à saúde do beneficiário ou do segurado para essas finalidades" (p. 34).

Suplementar, o qual apresenta consolidada regulação, dispõe de normas que disciplinam todo o processo de contratação de planos privados, o que mostra a importância de um diálogo consistente entre a LGPD e a legislação setorial. [507]

A ANS determina[508] que para a contratação de planos privados de assistência à saúde o contratante (beneficiário) apresente uma Declaração Pessoal de Saúde, por meio da qual deverá informar sobre as doenças ou lesões de que saiba ser portador ou sofredor e das quais tenha conhecimento no momento da contratação ou adesão contratual, para que a operadora possa verificar a necessidade de aplicação de carência, agravo ou cobertura parcial temporária. Não são permitidas perguntas sobre hábitos de vida, sintomas ou uso de medicamentos.

Faz parte do contrato de seguro o cálculo de risco, notadamente porque tal cálculo poderá pautar o preço da contraprestação a ser quitada pelo segurado. Nesse sentido, a Súmula Normativa nº 27/2015 da ANS dispõe que é vedada a prática de seleção de riscos pelas operadoras de planos de saúde na contratação de qualquer modalidade de plano privado de assistência à saúde. Portanto, resta vedada a não concretização da proposta de contratação de plano de saúde, em virtude de seleção de risco, em qualquer tipo de contratação. Levando isso em conta, entende-se que o parágrafo 5º, do Art.11, da LGPD "(...)não pretendeu extinguir a análise de risco com base em dados de saúde, mas somente proibir a seleção de risco que possa acarretar a exclusão de segurados ou a não contratação com pessoas que sejam classificadas como de risco alto."[509] [510] Uma proteção diferenciada aos dados

[507] Em relação ao parágrafo 5º, do art. 11, da LGPD, afirma-se que ele "Não significa uma vedação completa a que as operadoras realizem estudos populacionais, avaliando o comportamento de carteiras para o fim de aplicar uma precificação justa e adequada para cada grupo, coletivamente considerado. Significa, apenas, que as operadoras não realizarão tratamento de dados pessoais para aceitar ou excluir titular de sua carteira (...)." Disponível: <https://www.conjur.com.br/2019-nov-12/lei-geral-protecao-dados-pessoais-atividades-setor-saude> Acesso em: 02.11.20.

[508] Resolução normativa nº 162, de 17 de outubro de 2007 - Art. 9º Na contratação de planos privados de assistência à saúde, o conteúdo da declaração do beneficiário a respeito de seu estado de saúde e de possíveis DLP, que servirão de base para aplicação da regra contida no art. 11 da Lei nº 9.656 de 1998, deverão observar o disposto nesta Resolução.

[509] Disponível em: <https://opiceblum.com.br/em-quais-momentos-a-area-da-saude-utiliza-dados-pessoais/> Acesso em: 28.07.21.

[510] "De forma expressa na Lei Geral de Proteção de Dados Pessoais (LGPD), está proibido que as operadoras de saúde se utilizem de uma investigação do histórico do paciente para limitar acesso, contratação, bem como a exclusão de eventuais benefícios em razões da vida pregressa do beneficiário. Pois bem, ocorre que no âmbito da Lei 9.656/1998, que regulamenta os planos de saúde no Brasil, há a autorização legal para que as operadoras fixem um período de exclusão de cobertura em razão de doenças preexistentes. (...) De certo, a indicação de uma DLP no momento da contratação está inserida no dever de transparência e boa-fé contratual, pois a omissão de dados essenciais na prestação do serviço poderá

sensíveis – considerando-se sua relação com a tutela da dignidade da pessoa humana – mostra-se obrigatória seja em qual setor que ocorra o tratamento. A partir dessas informações, é possível conhecer com elevada precisão indivíduos, assim como criar cenários de discriminações ilícitas ou abusivas em face do titular do dado. Além disso, como visto, há dados potencialmente sensíveis e tratamentos realizados com fins de se obter ou inferir informações sensíveis sobre a pessoa, que exigem igualmente tutela especial pelo ordenamento.

3.2.10 Tratamento de dados públicos sensíveis

Quando a LGPD aborda os dados públicos, ela dispõe sobre duas categorias: a) dados tornados manifestamente públicos pelo titular; e b) "dados pessoais cujo acesso é público". A disposição legal sobre ambas se encontra nos parágrafos do Art.7º da lei. Importa ressaltar que a lei não tratou de forma específica os dados públicos de caráter sensível, trazendo, aparentemente, apenas duas normas gerais para o tratamento de dados pessoais considerados públicos.

Diante disso, cabe indagar: teria a LGPD unificado a forma como deverão ser tratados os dados públicos (sendo eles sensíveis ou não) ou todos os dados sensíveis, sendo públicos ou não, deveriam sempre ser tratados com base em uma das hipóteses legais do Art. 11? Verifica-se, então, que além do debate sobre que tipos de dados pessoais devem, de fato, ser considerados públicos, há também dúvidas acerca do

---

desequilibrar a expectativa econômica das partes. (...) Portanto, é dever legal do beneficiário trazer essa informação no momento da contratação; mas acaso este se omita, pode a operadora de saúde atuar para comprovar a prática ilícita do consumidor. Surge então um grande embaraço trazido pela LGPD, pois proíbe as operadoras de saúde de utilizar o histórico do paciente; porém, esse ônus lhe é imposto por outra norma, qual seja, pelo artigo 11 da Lei nº 9.656/1998. Como então compatibilizar a LGPD (que proíbe a utilização de dados relativos à saúde) com a Lei dos Planos de Saúde (que exige que o plano de saúde comprove a doença preexistente)? (...) não se pode cogitar que a LGPD não trouxe nenhuma barreira instransponível para a operadora de saúde apurar o histórico do beneficiário; e tampouco é uma ferramenta que inviabiliza o acesso a qualquer documento ou histórico do paciente. A nova lei coloca, nesse sentir, uma vedação clara, direta e objetiva nos objetivos dessa investigação. A pretensão da operadora de saúde somente será legítima se os dados colhidos para a verificação do conhecimento prévio do consumidor ou beneficiário dessa doença preexistente foi realizada unicamente para fins de satisfazer o artigo 11 da Lei 9.656/1998." (PSCHEIDT, Kristian Rodrigo. A relação entre a LGPD e a apuração da boa-fé contratual. Conjur, publicado em 07 de dezembro de 2020. Disponível em: <https://www.conjur.com.br/2020-dez-07/pscheidt-relacao-entre-lgpd-boa-fe-contratual> Acesso em: 28.07.21.)

seu tratamento lícito quando forem também sensíveis. Diante disso, mostra-se relevante tanto um maior cuidado doutrinário sobre o tema quanto uma manifestação da Autoridade Nacional de Proteção de Dados, para que esclareça dúvidas e detalhe a questão. No caso de dispensa da exigência do consentimento previsto no Art.7º, §4º, para os dados "tornados manifestamente públicos pelo titular",[511] os agentes de tratamento continuarão obrigados a observar os direitos do titular e os princípios previstos na Lei. Assim como na hipótese dos dados de acesso público[512], aqui deve ser considerado o contexto em que a informação foi disponibilizada e a finalidade do tratamento pretendido. Deve haver compatibilidade entre o seu uso e as circunstâncias pelas quais tal informação foi tornada pública pelo titular, tendo em vista a ressalva disposta na lei, que não autoriza seu uso indiscriminado. Esses tipos de dados, ainda que sejam considerados públicos, não deixam de ser pessoais, sendo necessário considerar sempre os princípios da LGPD, especialmente a finalidade, a adequação e a necessidade, em sua circulação e o que justifica sua disponibilização.[513]

A proteção dos dados públicos em todo o processo que envolve sua circulação e tratamento caminha ao encontro das novas formas de expressão da pessoa humana e de tutela dos dados sensíveis. Nesse sentido, destaca-se relevante reflexão:

> A necessidade de proteção foi dilatada para além das informações relacionadas à esfera íntima da pessoa, compreendidas como aquelas que o interessado excluiria de qualquer tipo de circulação (RODOTÀ, 2008). Se é possível conceber um "núcleo duro" da privacidade, a partir de informações que tradicionalmente remetem a uma necessidade de sigilo, ganha cada vez mais relevância as informações que têm uma potencialidade discriminatória, mas não podem ser confinadas na esfera privada, porque integram a esfera pública, constituindo as convicções que a pessoa deve poder manifestar publicamente e que formam, portanto, a sua identidade pública (RODOTÀ, 2008). Não obstante, a origem racial ou étnica da pessoa, abrangente de uma noção de pertencimento ao respectivo grupo social, constituem dados

[511] LGPD - Art. 7º, § 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.

[512] LGPD - Art. 7°, § 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.

[513] A doutrina oferece dois exemplos de utilização que esclarecem as possibilidades desses dados: "(...) a princípio, terceiros não poderiam usar dados de uma rede social, mesmo que de perfis públicos, para fins de *marketing*. As circunstâncias pelas quais tais dados foram tornados públicos pelo seu próprio titular deram-se para uma outra finalidade, que é a de se relacionar com quem integra o seu círculo social. Por outro lado, a princípio, seria compatível o uso de dados de perfis públicos de uma rede profissional (*e.g.*, Linkedin) por terceiros, como *headhunters*, para aproximar seus usuários às vagas profissionais de seu eventual interesse. Esse uso é compatível com a finalidade não só da plataforma em si, como, principalmente, a razão pela qual tais dados são públicos" (BIONI, Bruno. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 271).

> sensíveis que não podem circunscrever a sua tutela a uma reserva privada. (...) É com a finalidade de garantir a plenitude à esfera pública que são determinadas rigorosas condições para a circulação dos dados sensíveis, assegurando, paradoxalmente, segundo Rodotà (2008), um forte estatuto privado. É neste sentido que os riscos conexos ao uso das informações levaram ao reconhecimento da autodeterminação informativa como um direito fundamental, e não apenas de um sigilo, a partir da tendência de tutelar uma série de "posições individuais e coletivas relevantes no âmbito da informação"(RODOTÀ, 2008, p. 96). [514]

Uma questão relevante em torno da expressão dados "tornados manifestamente públicos pelo titular" é a sua interpretação: ela diz respeito à intenção prévia do usuário quando tornou públicos seus dados (ou seja, ele tinha clara ciência de que estava tornando públicos alguns dados pessoais) ou se refere ao aspecto público que os dados atingiram em virtude da divulgação/disponibilização feita pelo titular? Diante da lógica da lei, parece que os dois fatores devem ser conjugados na análise.[515] A ciência do titular sobre a publicização de seus dados, por meio da disponibilização, revela-se condição para que o tratamento deles, sem prévio consentimento, seja autorizado pela LGPD. Como exemplos de dados assim considerados, vale recordar os dados publicados no perfil do titular em uma rede social, bem como aqueles veiculados em uma página na rede criada pela própria pessoa. A exceção do §4º, do Art. 7º, não deverá servir para fins amplos e irrestritos.

Os dados devem ter sido "manifestamente" tornados públicos, o que requer um ato afirmativo por parte do titular dos dados e que ele perceba que esse será o resultado. Já se afirmou que o tratamento de dados no contexto da videovigilância não pode se basear na norma que regula o tratamento de dados pessoais tornados manifestamente públicos pelo titular. O mero fato de entrar no alcance de uma câmera não implica que o titular dos dados pretende tornar públicas até mesmo informações pessoais sensíveis sobre ele.

---

[514] KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. Dados Sensíveis na Lei Geral de Proteção de Dados Pessoais: mecanismos de tutela para o livre desenvolvimento da personalidade. Orientador: Sergio Marcos Carvalho de Ávila Negri. Dissertação (mestrado acadêmico) - Universidade Federal de Juiz de Fora, Faculdade de Direito. Programa de Pós-Graduação em Direito, 2019. p. 43.

[515] "On the other hand, such data would have to be made public by the data subject, and more than that, manifestly made public, so as to indicate that they wish and expect such data to be further processed. No need to mention that all other provisions, including the principles and the Article 6, still apply, and also the personal data may be processed only if the purpose of the processing could not reasonably be fulfilled by other means" (FOITZIK, Piotr. Publicly available data under the GDPR: Main considerations. Disponível em: <https://iapp.org/news/a/publicly-available-data-under-gdpr-main-considerations/>. Acesso em: 01.08.21)

Sobre a questão, o Information Commissioner's Office apresenta algumas questões para se verificar se determinado dado pessoal pode ser considerado como tendo sido tornado manifestamente público por seu titular: a) Quem tornou os dados públicos: foi o próprio indivíduo ou outra pessoa? b) Em que contexto o referido dado foi tornado público: em razão de uma entrevista, de o titular ter se candidatado a um cargo público ou de ele ter publicado conteúdo em suas mídias sociais? c) O indivíduo deliberadamente tomou as medidas que tornaram públicos esses dados ou foi algo acidental e não intencional? d) O indivíduo entendeu que sua ação significa que seus dados pessoais serão considerados públicos?[516]

Necessário analisar também a segunda categoria de dados públicos: "dados pessoais cujo acesso é público", como aqueles cuja publicação é obrigatória por lei, como o fato de alguém ser proprietário de um imóvel, sócio de uma empresa ou casado. Outro exemplo é a consulta de CPFs no site da Receita Federal com o propósito de mera confirmação da titularidade para operações financeiras. De acordo com o § 3º, do Art.7º, a tratamento dos referidos dados deverá considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

[516] A respeito dessa hipótese legal, vale ressaltar interpretação da ICO: "The term 'manifestly made public' is not defined by the UK GDPR. But it clearly assumes a deliberate act by the individual. It's not enough that it's already in the public domain – it must be the person concerned who took the steps that made it public. **Example** A security breach means that information about an individual's health condition is publicly available from an organisation's website. Clearly, making their special category data public was not a deliberate act on the part of the individual. Therefore this condition would not apply to any processing of health data obtained from the website. **Example** The political affiliations of a member of parliament are technically special category data (these are 'political beliefs'). However these are clearly a matter of public knowledge and the individual has actively chosen to make these public by standing for election as a member of parliament. You need to be confident that it was the individual themselves who actively chose to make their special category data public and that this was unmistakably a deliberate act on their part. There is a difference between assenting to or being aware of publication, and an individual actively making information available. For example, by blogging about their health condition or political views. You might also find it hard to show that someone has manifestly made information public if, for example, they made a social media post for family and friends but default audience settings made this public. You should therefore be very cautious about using this condition to justify your use of special category data obtained from social media posts. To be manifestly made public, the data must also be realistically accessible to a member of the general public. The question is not whether it is theoretically in the public domain (eg in a publication in a specialist library, or mentioned in court), but whether it is actually publicly available in practice. Disclosures to a limited audience are not necessarily 'manifestly public' for these purposes. In particular, information is not necessarily public just because you have access to it. The question is whether any hypothetical interested member of the public could access this information. You cannot use this condition to justify publication of previously unpublished data. It only applies to information which is already public." Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/#conditions5> Acesso em: 01.08.21.

Nesse sentido, afirmou o legislador que o tratamento posterior dos dados pessoais (públicos) a que se referem os §§ 3º e 4º do Art. 7º poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei (§7º).

Nos dois casos mostra-se relevante discutir acerca da necessidade de se aplicar uma base legal para tratar tais dados. Na hipótese do § 4º (dados tornados manifestamente públicos pelo titular), pode-se entender que não haveria necessidade de uma nova base legal para o tratamento desses dados, já que se trataria de hipótese autorizativa para o tratamento de dados sem o consentimento de seu titular.[517-518] Por outro lado, no caso do § 3º (dados pessoais cujo acesso é público), o enquadramento em uma das bases legais autorizativas contidas no rol do Art. 7º ou do Art. 11 se mostraria adequado. Entende-se não ser razoável admitir que dados disponíveis publicamente possam ser tratados sem uma base legal específica, pois isso seria o mesmo que autorizar que qualquer informação publicada, por exemplo, por força de uma obrigação legal, pudesse ser utilizada para uma finalidade distinta sem que o novo controlador precisasse demonstrar que existia uma base legal que autorizava o tratamento. Tanto é que o referido § 3º não dispensa a exigência de consentimento como faz o § 4º.[519]

De forma geral, dispôs a Lei que eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas

---

[517] Essa previsão, aliás, encontra semelhança no art. 9º, § 2º, alínea 'e' do GDPR, que reconhece como possível base legal para o tratamento de dados pessoais - no caso do GDPR dados sensíveis - quando tiverem sido manifestamente tornados públicos pelo seu titular. Isso não quer dizer, contudo, que basta que o dado pessoal tenha sido, por exemplo, disponibilizado online por seu titular. Para que um dado seja considerado como tornado manifestamente público pelo seu titular, deve restar inequívoco que ele pretende e espera que seus dados pessoais sejam tratados ulteriormente. Além disso, como previsto no próprio § 4º do Art. 7º da LGPD, devem ser observados os direitos do titular e os princípios previstos na LGPD.

[518] Neste sentido, já se afirmou que "salvo engano, referida regra seria uma válvula de escape a todas as hipóteses autorizadoras do art. 7º, e não apenas àquela do inciso I (consentimento), como seu texto dá a entender. A regra do §4º do citado artigo, a bem da verdade, poderia ser tratada como uma outra hipótese permissiva, pois o controlador que atua sob a regra excepcional acima não precisaria justificar suas atividades em nenhuma das demais hipóteses autorizadoras do art. 7º da LGPD, conforme entendo." (MOREIRA, André de Oliveira Schenini. A exceção dos dados pessoais tornados manifestamente públicos pelo titular na LGPD. Migalhas, publicado em 07 de janeiro de 2019. Disponível em: <https://www.migalhas.com.br/depeso/293745/a-excecao-dos-dados-pessoais-tornados-manifestamente-publicos-pelo-titular-na-lgpd> Acesso em: 01.08.21.)

[519] LGPD - Art. 7º (...) § 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.

na Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular (Art. 7º, § 6º).

Em diálogo com o tema abordado, recorda-se que o sistema de proteção de dados da LGPD relaciona-se com a Lei de Acesso à Informação (Lei Federal nº 12.527/2011 - LAI) e com princípios constitucionais, considerando-se que todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado (Art.5º, XXXIII, da CF/88). A LAI busca promover diretrizes como: publicidade como preceito geral e sigilo como exceção; divulgação de informações de interesse público, independentemente de solicitações; utilização de meios de comunicação viabilizados pela tecnologia da informação; fomento ao desenvolvimento da cultura de transparência na administração pública; e desenvolvimento do controle social da administração pública.[520]

Diante disso, parece surgir um aparente conflito normativo: enquanto a LAI tem como pilar os princípios da transparência e da publicidade da Administração Pública, a LGPD trata da proteção da privacidade e dos dados pessoais dos cidadãos, por meio de

[520] "Com efeito, ao dispor sobre o tratamento de dados pessoais pelo Poder Público (arts. 23 a 30), a LGPD não utiliza, em momento algum, as palavras "segredo" ou "sigilo". Em sentido diverso, a lei expressamente reforça e amplia as obrigações de transparência de entidades e órgãos públicos, ao determinar, por exemplo, a publicação de informações relativas ao tratamento de dados pessoais em veículos de fácil acesso (art. 23, I). Na mesma linha, o art. 25 estabelece que "os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas […] à disseminação e ao acesso das informações pelo público em geral", norma de teor semelhante ao art. 8º, § 3º, III, da LAI. Por sua vez, a LAI confere especial proteção ao tratamento de informações pessoais no setor público, conceito este (art. 4º, IV) similar ao de dado pessoal na LGPD (art. 5º, I). Daí a restrição de seu acesso a agentes autorizados e a possibilidade de sua divulgação apenas nas hipóteses previstas em lei ou mediante consentimento do titular (art. 31, § 1º). Além disso, a LAI já previa a responsabilização de agentes públicos ou particulares pelo "uso indevido" de informações pessoais (art. 31, § 2º), norma que pode ser interpretada em consonância com o princípio da finalidade e seus desdobramentos, conforme estabelecidos pela LGPD. (...)" Sobre a harmonização das normas, o autor afirma: "Será necessário, por exemplo, reavaliar processos internos e contratos com entidades privadas, questionar a necessidade de coleta ou de publicação de determinados dados pessoais e adotar medidas adicionais de prevenção e segurança que minimizem os riscos de acidentes e acessos não autorizados. Ademais, deve-se reconhecer a limitação da tradicional e rígida distinção entre dados públicos e sigilosos. Isso porque a LGPD demanda a adoção de medidas de proteção ao longo de todo o processo de tratamento, isto é, desde a coleta inicial até o término de sua utilização, independentemente do conteúdo ou do grau de publicidade conferido aos dados pessoais. Por conseguinte, mesmo dados pessoais a que se atribua publicidade são protegidos pela lei, devendo ser observados os direitos do titular, bem como a "finalidade, boa-fé e o interesse público que justificaram a sua disponibilização" (art. 7º, §§ 3º e 4º, LGPD)." (CARVALHO, Lucas Borges de. A LGPD e o acesso à informação pública: dado pessoal é dado sigiloso? Jota, publicado em 16 de dezembro de 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/lgpd-informacao-publica-16122020> Acesso em: 02.08.21)

medidas de prevenção e de segurança, buscando assegurar tratamentos com base legal delimitada e finalidade determinada. Entende-se, porém, que não haveria uma incompatibilidade entre a LAI e a LGPD, ainda que alguns casos concretos requeiram ponderação de valores, diante dos bens e direitos apresentados.[521]

3.3 Tratamento de dados sensíveis de crianças e de adolescentes

Conforme os mecanismos de comunicação e de interação online avançam, o ambiente digital vem se tornando cada vez mais relevante na vida das pessoas. Especialmente após o início da pandemia de COVID-19, diversas operações e atividades foram intensificadas ou migraram para o referido ambiente, como o ensino em escolas, universidades e cursos, serviços governamentais, parte do comércio e ferramentas de entretenimento e jogos. Não há dúvidas de que a Internet, em razão das potencialidades e recursos que oferece, apresenta novas oportunidades para a realização dos direitos de crianças e adolescentes. Além disso, o acesso permanente a tecnologias digitais pode ajudá-los a realizar uma série de direitos civis, políticos, culturais, econômicos e sociais. Contudo, diante dos diversos sujeitos que nela interagem e das sofisticadas formas de tratamento de dados disponíveis, ela apresenta também riscos de violação ou abuso a direitos dos menores.[522]

O acesso a conteúdos que estimulam violência, automutilação[523] ou o uso de drogas, o vazamento de imagens íntimas[524], o tratamento

[521] Cf. BUCAR, Daniel. Administração Pública e Lei Geral de Proteção de Dados. *In:* SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (coord.). *Caderno Especial:* Lei Geral de Proteção de Dados (PGPD). São Paulo: Revista dos Tribunais, 2019. p. 153-165. LANGENEGGER, Natalia; GOBBATO, Andréa. Compatibilização da Lei de Acesso à Informação com a Lei Geral de Proteção de Dados Pessoais: desafios no âmbito do Poder Judiciário. *Revista do Advogado*, São Paulo, v. 39, n. 144, p. 141-148, nov. 2019. MATOS, Ana Carla Harmatiuk; RUZYK, Carlos Eduardo Pianovski. Diálogos entre a Lei Geral de Proteção de Dados e a Lei de Acesso à Informação. *In:* FRAZÃO, Ana; OLIVA, Milena Donato; TEPEDINO, Gustavo (coord.). *Lei Geral de Proteção de Dados Pessoais*: e suas repercussões no Direito brasileiro. São Paulo: Revista dos Tribunais, 2019. p. 199-218.

[522] Cf. LATERÇA, Priscilla Silva; FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (Coords.). *Privacidade e Proteção de Dados de Crianças e Adolescentes*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021. E-book.

[523] TEFFÉ, Chiara Spadaccini de. Desafio da Baleia Azul: o que se sabe até agora. ITS FEED, 25 abr. 2017. Disponível em: <https://feed.itsrio.org/desafio-da-baleia-azul-o-que-se-sabe-at%C3%A9-agora-b4b85ae77a56> Acesso em 04.06.21.

indevido de dados pessoais, o *cyberbullying* e o aliciamento sexual são exemplos de riscos significativos a menores na rede. A relação das crianças e dos adolescentes com a Internet é marcada pela *conectividade* e pela *mobilidade* no acesso à rede, sendo o *smartphone* um dos principais dispositivos para a sua conexão. Inclusive, ele foi responsável muitas vezes por manter os menores conectados e acompanhando as aulas escolares em lares brasileiros. Segundo pesquisa realizada em 2019, considerando o total de usuários de 9 a 17 anos, 83% assistiram a vídeos, programas, filmes ou séries na Internet; 76% pesquisaram na Internet para trabalhos escolares; e 68% utilizaram redes sociais.[525] Mostra-se, assim, necessário analisar os diversos instrumentos de proteção a crianças e adolescentes e destacar a importância de um uso ético e responsável da Internet. Neste sentido, promover uma *educação digital* de qualidade para pais, professores e menores resultará em um melhor uso da rede, capaz de oferecer mais benefícios aos sujeitos. Adicionalmente, é importante manter canais para um *diálogo aberto* com os menores, de forma que eles se sintam seguros para tirar dúvidas e relatar situações de abuso que estejam sofrendo.

O controle e a *mediação parental* – necessários para a orientação de menores no uso da rede – devem ser aplicados em intensidades compatíveis com as idades da criança e do adolescente, respeitando seus graus de autonomia e discernimento, bem como seus processos de aquisição gradual de competências e entendimentos.[526] Os riscos e oportunidades relacionados com o envolvimento dos menores no ambiente digital mudam a depender de sua idade e estágio de desenvolvimento. Sendo possível e seguro, entende-se adequado conferir espaços de liberdade e privacidade para o menor, para que desenvolva sua autonomia e comunicação, tendo os seus pontos de vista devidamente considerados. O *design* de medidas apropriadas a cada idade deve ser informado pelas mais atualizadas pesquisas e práticas nos campos da educação e da

---

[524] TEFFÉ, Chiara Spadaccini de. Exposição não consentida de imagens íntimas: como o Direito pode proteger as mulheres? In: Nelson Rosenvald; Rafael Dresch; Tula Wesendonck (Org.). *Responsabilidade civil*: novos riscos. 1ed.Indaiatuba: Foco, 2019. p. 91-113.

[525] Resumo Executivo - Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil - TIC Kids Online Brasil 2019. Novembro de 2020. p.04. Disponível em: <https://cetic.br/pt/publicacao/resumo-executivo-pesquisa-sobre-o-uso-da-internet-por-criancas-e-adolescentes-no-brasil-tic-kids-online-brasil-2019/> Acesso em: 05.06.21

[526] O comentário n.25 acerca dos direitos da criança no ambiente digital foi importante embasamento teórico para o presente artigo. Committee on the Rights of the Child. General comment No. 25 (2021) on children's rights in relation to the digital environment. 2 March 2021. Disponível em: <https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC%2fC%2fGC%2f25&Lang=en> Acesso em: 05.06.21.

tecnologia. Observa-se também que as referidas considerações devem ser equilibradas com a importância de os menores exercerem seus direitos em ambientes apoiados, assim como com a gama de experiências e circunstâncias individuais.

Outros instrumentos igualmente relevantes, a depender da idade e da maturidade, são: a realização de atividades em conjunto com os pais, o estabelecimento de determinadas limitações quanto ao tempo de uso de tecnologias, a utilização de ferramentas e filtros para restringir atividades dos menores online e o monitoramento de interações diversas realizadas na Internet. Um adequado controle parental atrelado a uma educação digital de cunho emancipatório, pautada em responsabilidade e diálogo aberto, mostram-se essenciais para a proteção de crianças e adolescentes.[527]

O uso de dispositivos digitais não deve ser um substituto para as necessárias interações entre crianças e seus pais e crianças e seus colegas de escola. Além disso, verifica-se a importância de se prestar atenção aos efeitos da tecnologia nos primeiros anos de vida da criança, momento de grande relevância para o seu desenvolvimento cerebral e quando o ambiente social, em particular as relações com os pais e cuidadores, revela-se crucial para moldar seu desenvolvimento cognitivo, emocional e social. O ambiente digital deve apoiar e promover um engajamento seguro e equitativo dos menores, sendo relevante o desenvolvimento de políticas e ações que visem a uma efetiva *inclusão digital*. Caso isso não ocorra, as desigualdades existentes provavelmente aumentarão e outras poderão surgir, como no acesso à educação e à informação. O *direito a não discriminação* deve garantir que crianças e adolescentes tenham um acesso de qualidade ao ambiente digital. Neste sentido, mostram-se relevantes políticas públicas que facilitem o acesso a dispositivos conectados, uma internet aberta e serviços digitais. Além disso, com base no direito a não discriminação, deve-se proteger crianças e adolescentes de dados tendenciosos, falsos ou parciais, de tratamentos indevidos ou ilícitos de informações, além da criação de perfis voltados ao direcionamento de publicidade.[528]

---

[527] Parágrafo extraído de: TEFFÉ, Chiara Spadaccini de. Proteção de dados de crianças e adolescentes. *Revista do Advogado*, v. 39, 2019.

[528] Adicionalmente, o comentário n.25 acerca dos direitos da criança no ambiente digital afirma que: "The Committee calls upon States parties to take proactive measures to prevent discrimination on the basis of sex, disability, socioeconomic background, ethnic or national origin, language or any other grounds, and discrimination against minority and indigenous children, asylum-seeking, refugee and migrant children, lesbian, gay, bisexual, transgender and intersex children, children who are victims and survivors of trafficking or sexual exploitation, children in alternative care, children deprived of liberty and children in

Todas as ações direcionadas a crianças e adolescentes devem necessariamente visar ao seu *melhor interesse*, como, por exemplo, no fornecimento, regulação, design, gestão e uso do ambiente digital. O reconhecimento e a tutela de sua *hipervulnerabilidade*[529] ou vulnerabilidade agravada[530] podem ser inferidos do artigo 227 da Constituição Federal, o qual dispõe acerca do *princípio da prioridade absoluta* aos direitos da criança e do adolescente.[531] Caminha, assim, o Direito buscando harmonizar o respeito à capacidade e autodeterminação da pessoa e a necessária proteção jurídica que deve ser conferida a determinados grupos, para que gozem plenamente de seus direitos fundamentais. Longe de uma ótica paternalista, busca-se garantir efetividade e aplicação direta às normas constitucionais.[532]

A construção da doutrina da *proteção integral e prioritária* das crianças e dos adolescentes, segundo a qual tais "pessoas em desenvolvimento" devem receber total amparo e proteção do sistema

---

other vulnerable situations. Specific measures will be required to close the gender-related digital divide for girls and to ensure that particular attention is given to access, digital literacy, privacy and online safety."

[529] A construção da noção de hipervulnerabilidade pelos Tribunais parece estar associada à ideia de que as pessoas assim qualificadas se encontram em situação de maior desigualdade e, por essa razão, carentes de maior proteção. Nesse sentido, Cláudia Lima Marques explica que a noção foi desenvolvida "como um corolário positivo da proibição de discriminação, logo do princípio da igualdade (um dever ser), e mandamento de pleno desenvolvimento da personalidade, diretamente ligada, pois, a nossa visão de dignidade da pessoa humana." (MARQUES, Cláudia Lima. O diálogo das fontes como método da nova teoria geral do direito: um tributo a Erik Jayme. In.: _____ (coord.). *Diálogo das fontes:* do conflito à coordenação de normas no direito brasileiro novo regime das relações contratuais. São Paulo: RT, 2012, p.17-66, p. 46-47.) "Quanto à pergunta sobre se os hipervulneráveis são apenas os mencionados no texto constitucional (crianças, adolescentes, idosos e portadores de deficiência), parece-me cedo para responder de forma definitiva. A diferença está em que os hipervulneráveis mencionados nas normas constitucionais se beneficiam do mandamento de proteção constitucional (com efeitos e força normativa no direito privado), enquanto, por exemplo, os doentes e analfabetos são hipervulneráveis cuja proteção especial dependerá da atuação ativa do Judiciário e das especificidades do caso concreto (por exemplo, conhecimento pelo parceiro contratual de sua condição agravada de vulnerabilidade, tipo de contrato, onerosidade ou gratuidade deste, etc.)." (MARQUES, Cláudia Lima. O diálogo das fontes como método da nova teoria geral do direito: um tributo a Erik Jayme. In.: _____ (coord.) *Diálogo das fontes*: do conflito à coordenação de normas no direito brasileiro novo regime das relações contratuais. São Paulo: RT, 2012, p.17-66, p. 48.)

[530] MIRAGEM, Bruno. *Curso de Direito do Consumidor.* 3ed. São Paulo: RT, 2012, p.102.

[531] Art. 227. É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão.

[532] "10. Configura dano moral coletivo ofensa a direitos coletivos ou difusos de caráter extrapatrimonial associados a sujeitos ou bens vulneráveis e hipervulneráveis - pessoas com deficiência, consumidor, criança e adolescente, idoso, meio ambiente, ordem urbanística, entre outros." (STJ. REsp 1.793.332/MG, Rel. Ministro Herman Benjamin, Segunda Turma, DJe 26/08/2020)

jurídico[533], remonta à *Declaração dos Direitos da Criança* adotada pela Assembleia-Geral das Nações Unidas no ano de 1959.[534] Posteriormente, em 1989, através da *Convenção das Nações Unidas sobre os Direitos da Criança*[535], houve a ampliação dos direitos da criança no cenário internacional. Este documento considerou como criança todo ser humano com menos de 18 anos de idade, salvo quando, em conformidade com a lei aplicável à criança, a maioridade seja alcançada antes. A referida Convenção foi ratificada pelo Brasil em 1990 e influenciou diretamente a elaboração do *Estatuto da Criança e do Adolescente* (Lei 8.069/90 - ECA), que em seus artigos 3º e 4º destaca que todas[536] as crianças (pessoa até doze anos de idade incompletos) e adolescentes (aquela entre doze e dezoito anos de idade incompletos) gozam dos direitos fundamentais inerentes à pessoa humana, sem prejuízo da proteção integral de que trata esta Lei, sendo assegurados a eles todas as oportunidades e facilidades, a fim de lhes facultar o desenvolvimento físico, mental, moral, espiritual e social, em condições de liberdade e de dignidade.[537] Ato contínuo, o ECA dispõe que a criança e o adolescente têm direito à liberdade, ao respeito e à dignidade como *pessoas humanas em processo de desenvolvimento* e como

[533] STJ. REsp 1.587.477. Quarta Turma. Rel. Min. Luis Felipe Salomão, DJe 27/08/2020.

[534] Princípio II - A criança gozará de proteção especial e disporá de oportunidade e serviços, a serem estabelecidos em lei por outros meios, de modo que possa desenvolver-se física, mental, moral, espiritual e socialmente de forma saudável e normal, assim como em condições de liberdade e dignidade. Ao promulgar leis com este fim, a consideração fundamental a que se atenderá será o interesse superior da criança. (Declaração dos Direitos da Criança, 1959).

[535] Disponível em: <https://www.unicef.org/brazil/convencao-sobre-os-direitos-da-crianca> Acesso em: 05.06.21.

[536] Art. 3°, parágrafo único: "Os direitos enunciados nesta Lei aplicam-se a todas as crianças e adolescentes, sem discriminação de nascimento, situação familiar, idade, sexo, raça, etnia ou cor, religião ou crença, deficiência, condição pessoal de desenvolvimento e aprendizagem, condição econômica, ambiente social, região e local de moradia ou outra condição que diferencie as pessoas, as famílias ou a comunidade em que vivem."

[537] Recorda-se também a Lei nº 13.257, de 8 de março de 2016, chamada de *Marco Legal da Primeira Infância*: "Art. 1º Esta Lei estabelece princípios e diretrizes para a formulação e a implementação de políticas públicas para a primeira infância em atenção à especificidade e à relevância dos primeiros anos de vida no desenvolvimento infantil e no desenvolvimento do ser humano, em consonância com os princípios e diretrizes da Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente) ; altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente); altera os arts. 6º, 185, 304 e 318 do Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal) ; acrescenta incisos ao art. 473 da Consolidação das Leis do Trabalho (CLT), aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943 ; altera os arts. 1º, 3º, 4º e 5º da Lei nº 11.770, de 9 de setembro de 2008 ; e acrescenta parágrafos ao art. 5º da Lei nº 12.662, de 5 de junho de 2012 . Art. 2º Para os efeitos desta Lei, considera-se primeira infância o período que abrange os primeiros 6 (seis) anos completos ou 72 (setenta e dois) meses de vida da criança. Art. 3º A prioridade absoluta em assegurar os direitos da criança, do adolescente e do jovem, nos termos do art. 227 da Constituição Federal e do art. 4º da Lei nº 8.069, de 13 de julho de 1990 , implica o dever do Estado de estabelecer políticas, planos, programas e serviços para a primeira infância que atendam às especificidades dessa faixa etária, visando a garantir seu desenvolvimento integral."

sujeitos de direitos civis, humanos e sociais garantidos na Constituição e nas leis (Art. 15). O direito ao respeito consiste na inviolabilidade da integridade física, psíquica e moral da criança e do adolescente, abrangendo a preservação da imagem, da identidade, da autonomia, dos valores, ideias e crenças, dos espaços e objetos pessoais (Art. 17). A lei não menciona expressamente a proteção de dados pessoais dos menores, porém, diante da ampla tutela aplicada, é possível afirmar que o referido direito se encontra contemplado. Observa-se também que eles têm direito à informação, cultura, lazer, esportes, diversões, espetáculos e produtos e serviços que respeitem sua condição peculiar de pessoa em desenvolvimento (Art. 71). Isso é especialmente relevante quando consideramos os novos dispositivos conectados e os serviços disponibilizados na rede, como *games*, mídias sociais e aplicativos interativos.

A tutela diferenciada das crianças e adolescentes em qualquer relação na qual participem justifica-se exatamente por lhes faltar o completo discernimento, radicando nesse ponto a *ratio* protetiva. Contudo, deve-se ressaltar que não se trata apenas de uma proteção adequada ao estágio de desenvolvimento em que crianças e adolescentes se encontram, mas de uma proteção prospectiva, a fim de garantir a dignidade deles hoje e no futuro.[538] Temos, nos últimos tempos, a geração mais observada de toda a história. Cada vez mais, o *rastro digital* de menores vem sendo iniciado mais cedo e de forma ampliada, seja por meio de aplicativos para serem usados pelas mães durante a gestação, seja por meio de postagens realizadas pelos próprios pais, em mídias sociais, ainda quando são nascituros ou já nascidos.

Diante disso, cabe salientar a questão do *oversharenting*: hábito de os pais postarem constantemente e de forma intensa imagens e informações na Internet sobre os menores que estão sob sua responsabilidade. Abarca também situações em que os pais fazem a gestão da vida digital de seus filhos na internet, criando perfis em nome das crianças em redes sociais e postando sempre informações sobre sua rotina. Com isso, verifica-se que a intensa exposição dos filhos feita pelos pais vem causando uma verdadeira mudança na caracterização da infância, de forma que a nova geração já cresce com responsabilidades, anseios e expectativas de

[538] Pietro Perlingieri apresenta a definição de igual dignidade social em duas perspectivas convergentes: "como o instrumento que confere a cada um o direito ao respeito inerente à qualidade de homem, assim como a pretensão de ser colocado em condições idôneas a exercer as próprias aptidões pessoais." (PERLINGIERI, Pietro. *Perfis do direito civil*: introdução ao direito civil-constitucional. Rio de Janeiro: Renovar, 1997, p.37.)

uma vida adulta. Ocorre também, nesse cenário, a divulgação da família e dos filhos menores pelos chamados influenciadores digitais, os quais conjugam tal exposição com a divulgação de marcas e serviços. Recomenda-se, portanto, que antes da publicação de conteúdos que envolvam menores, os responsáveis reflitam criticamente acerca das consequências de suas ações. Além disso, mostra-se relevante incluí-los no processo decisório sobre o que vai ser postado sobre eles, de forma a educá-los sobre privacidade, consentimento e como se portar nas redes sociais.[539] *Oversharenting* pode trazer sérios impactos emocionais e subjetivos às crianças. Dentro das consequências negativas, é possível elencar: bullying em ambientes coletivos; invasão de senhas, falsificação de identidade e fraudes variadas; dificuldade de conseguir vaga de estágio ou mesmo crédito em instituições bancárias; e ser alvo de manipulação (política, comercial ou para qualquer fim de controle). Há, inclusive, uma preocupação acerca das consequências (presentes e futuras) da construção de uma memória pública e de um registro amplo de eventos e momentos que envolvam diretamente menores de idade.

Outro tema que permeia os debates envolve a *Internet dos brinquedos*, com bonecas, bichinhos de pelúcia e robôs conectados e inteligentes.[540] Ela se insere no amplo universo da Internet da Coisas (*Internet of Things* - IOT), que representa a integração de objetos físicos e virtuais em redes conectadas à Internet, permitindo que "coisas" tratem uma enorme quantidade de dados em nuvem, sendo possível o gerenciamento de dispositivos, mesmo à distância, para aumentar a eficiência de sistemas e processos. Cada vez mais, percebe-se a incorporação da IOT na vida de adultos, adolescentes e crianças. Relógios, geladeiras, leitores de digitais, vibradores sexuais, detectores de movimento, câmeras, peças de vestuário e brinquedos já se encontram conectados à Internet e presentes nas casas e corpos das mais diversas pessoas, enquanto empresas coletam dados sobre movimentos, preferências e hábitos de seus usuários, que não têm, por vezes, nem mesmo plena capacidade civil.

---

[539] STEINBERG, Stacey. *Growing Up Shared*: How Parents Can Share Smarter on Social Media-and What You Can Do to Keep Your Family Safe in a No-Privacy World. Sourcebooks, 2020. PLUNKETT, Leah A. *Sharenthood*: Why We Should Think before We Talk about Our Kids Online. The MIT Press, 2019. EBERLIN, Fernando Büscher von Teschenhausen. Sharenting, liberdade de expressão e privacidade de crianças no ambiente digital: o papel dos provedores de aplicação no cenário jurídico brasileiro. *Revista Brasileira de Políticas Públicas.* Brasília, v. 7, nº 3, 2017 p. 255-273.

[540] Cf. TEFFÉ, Chiara Spadaccini de; SOUZA, Carlos Affonso. Infância conectada: direitos e educação digital. In: Comitê Gestor da Internet no Brasil. (Org.). Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil: TIC kids online Brasil 2017. 1ed.São Paulo: Comitê Gestor da Internet no Brasil, 2018, v. 1, p. 31-40.

Dentro da *Internet of Toys*, despontam questões acerca: a) da falta de transparência e informação sobre o tratamento de dados de menores; b) do compartilhamento expressivo de dados com terceiros; c) da ausência de adequação das instituições à LGPD e às boas práticas internacionais em proteção de dados; d) de tratamentos indevidos de informações pessoais de terceiros que se encontram na residência, como pais, visitantes e amigos, sendo o brinquedo, por vezes, considerado um verdadeiro dispositivo de vigilância; e) da exposição excessiva da intimidade e de dados sensíveis do menor, a partir da coleta de informações, da interação realizada e das respostas oferecidas pela criança; e f) da qualidade do conteúdo que é direcionado a quem interage com os dispositivos, tendo em vista a possibilidade de inserção de publicidade implícita de bens durante as interações dos brinquedos com as crianças. Adicionalmente, ainda na seara relativa à proteção de dados, há sérias preocupações acerca da segurança e da proteção da integridade dos menores. Questiona-se, por exemplo: como fica a responsabilidade dos agentes em casos de incidentes de segurança e de danos? Quais padrões éticos e boas práticas eles deveriam adotar? Como mapear e sanar riscos e vulnerabilidades? O hackeamento de dispositivos, a reidentificação de dados anonimizados, o rastreamento de indivíduos e o *profiling* mostram-se presentes em diversas estruturas de tratamento de dados de crianças e adolescentes. Por fim, destaca-se também o impacto que a relação com o brinquedo conectado pode gerar nas formas de comunicação, interação e expressão das crianças.[541] Outro

[541] "Como regra, a comunicação estabelecida com esses dispositivos é pouco complexa e, muitas vezes, realizada na forma de comandos, sendo desnecessário utilizar expressões como "por favor" e "obrigado" (Lemos, 2017). Isso poderia influenciar negativamente as formas de expressão das crianças, prejudicando a sua interação com outros seres humanos. Em última instância, a diversão se transformou em um processo de criação de bases de dados. Quantas vezes a criança acessou o brinquedo? Quais informações ela trocou com ele? Quem tem acesso a essa comunicação e onde os dados são armazenados? O que pode ser feito com eles, além de melhorar a performance do brinquedo e do jogo? Existe um debate complexo sobre o consentimento dos pais e responsáveis para o tratamento de dados pessoais de seus filhos. Ainda que os pais tenham consentido com o uso do brinquedo e instalado um aplicativo que permite que eles controlem a brincadeira, há aspectos nebulosos nessa relação que precisam ser melhor debatidos. O que acontece se uma outra criança brincar junto e se comunicar com a boneca ou jogo? Enquanto cada vez mais brinquedos e jogos se conectam à rede, mais cedo as crianças também passam a utilizar a Internet. Duas certezas provenientes desse cenário são a transformação das práticas de diversão e os desafios constantes para a proteção da privacidade e dos dados pessoais." (TEFFÉ, Chiara Spadaccini de; SOUZA, Carlos Affonso. Infância conectada: direitos e educação digital. In: Comitê Gestor da Internet no Brasil. (Org.). Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil: TIC kids online Brasil 2017. São Paulo: Comitê Gestor da Internet no Brasil, 2018, v. 1, p. 31-40.)

tema que vale recordar envolve o uso de mídias sociais por menores.[542] [543]Como regra, as principais mídias sociais estabelecem, nos termos de uso apresentados no Brasil, a idade mínima de 13 anos para a abertura de contas e a utilização de seus serviços. Essa determinação tem como base norma norte-americana que considera criança o indivíduo com menos de 13 anos de idade: o *Children's Online Privacy Protection Act* de 1998 (COPPA). Para a Europa, a idade mínima estabelecida nas redes sociais costuma ser a de 16 anos[544] , tendo em vista que alguns países ainda vêm se adequando ao GDPR. O artigo 8º da norma europeia dispõe, em síntese, que, quando for aplicável o artigo 6º, n. 1, "a"[545], que traz a base legal do consentimento, quanto à oferta direta de serviços da sociedade da informação para crianças, o tratamento dos dados pessoais delas será legal quando tiverem pelo menos 16 anos de idade. Caso a criança tenha menos de 16 anos, o tratamento só será lícito se o consentimento for dado ou autorizado pelos titulares da autoridade parental. Contudo, destaca-se que os Estados-Membros poderão estabelecer idade menor para os efeitos referidos, desde que não inferior a 13 anos.[546]

Tanto a LGPD quanto o GDPR determinam que o responsável pelo tratamento

---

[542] Cf. TEFFÉ, Chiara Spadaccini de; FERNANDES, Elora. Contratação em redes sociais e proteção de dados de crianças e adolescentes. In: ROQUE, André Vasconcelos; OLIVA, Milena Donato. *Direito na era digital:* aspectos negociais, processuais e registrais. Salvador: Juspodivm, 2022. p.97-122.

[543] "Segundo a TIC Domicílios 2020, 64% da população de 10 a 17 anos reportou possuir uma conta no Instagram. A tendência de aumento da plataforma já havia sido identificada na pesquisa TIC Kids Online Brasil, na qual o Instagram apresentava o maior crescimento em relação à posse de perfil pela população de 9 a 17 anos (passou de 36%, em 2016, para 45%, em 2018). De maneira inédita, a TIC Domicílios 2020 investigou a posse de perfil no TikTok, reportado por 46% da população de 10 a 17 anos. A proporção foi expressivamente superior aos que possuíam perfil no Snapchat (18%) e no Twitter (14%). Ainda que o WhatsApp (86%) e o Facebook (61%) sejam as plataformas em que a população investigada mais possui perfil, o Instagram (35%) e o TikTok (27%), plataformas cujas funcionalidades centrais estão no compartilhamento e acesso a vídeos, foram reportados como as redes sociais mais utilizadas." (Resumo Executivo TIC Kids Online Brasil 2020 Edição COVID-19 – Metodologia adaptada. Publicado em 25 de novembro de 2021. p.06)

[544] Como exemplo, vale recordar os termos de uso do WhatsApp: "Se você reside em um país do Espaço Econômico Europeu (que inclui a União Europeia) ou em qualquer outro país ou território incluído (coletivamente, Europa), deve ter pelo menos 16 anos (ou mais, se for exigido em seu país) para se cadastrar e usar o WhatsApp. Se você reside em qualquer outro país, e não nos países pertencentes à Região Europeia, você deve ter pelo menos 13 anos (ou mais, se for exigido em seu país) para se cadastrar e usar o WhatsApp." Disponível em: <https://faq.whatsapp.com/general/security-and-privacy/minimum-age-to-use-whatsapp/?lang=pt_br> Acesso em: 05.06.21.

[545] Artigo 6.º Licitude do tratamento 1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações: a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas; (...)

[546] No estudo *The GDPR child's age of consent for data processing across the EU – one year later (July 2019)* foram apresentadas as idades mínimas estabelecidas por alguns países europeus para um menor consentir com o tratamento de seus dados por serviços da sociedade da informação. Disponível em: <https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=3017751> Acesso em: 05.06.21.

deverá promover todos os esforços razoáveis para verificar se o consentimento foi dado ou autorizado pelo titular das responsabilidades parentais sobre a criança, tendo em conta a tecnologia disponível.[547] O uso de linguagem clara e acessível para os menores nas plataformas também é sempre recordado.[548]

Em junho de 2021, uma mudança na política de privacidade da mídia social *TikTok*, nos EUA, [549] mostrou-se bastante preocupante, ao dispor inclusive sobre o tratamento de dados sensíveis biométricos:

> Podemos coletar informações sobre as imagens e áudio que fazem parte de seu Conteúdo de Usuário, como a identificação dos objetos e cenários que aparecem, a existência e localização dentro de uma imagem de características e atributos de rosto e corpo, a natureza do áudio e o texto das palavras faladas em seu Conteúdo do Usuário. Podemos coletar essas informações para habilitar efeitos especiais de vídeo, moderação de conteúdo, classificação demográfica, recomendações de conteúdo e anúncios e outras operações sem identificação pessoal. Podemos coletar identificadores biométricos e informações biométricas conforme definido nas leis dos Estados Unidos, como impressões faciais e de voz, de seu Conteúdo de Usuário. Quando exigido por lei, buscaremos suas permissões exigidas antes de qualquer coleta.[550]

---

[547] "The GDPR contains a number of specific protections for children's data protection rights, including the specific provisions in Article 8 GDPR, setting out the conditions applicable to obtaining a **child's consent** in relation to **information society services**.10 It should be noted, however, that consent is not the only possible legal basis for the processing of children's personal data, and controllers should assess on a case-by-case basis which is the most appropriate legal basis for any proposed processing. Where such services are offered directly to a child, and the controller seeks to rely on consent as a legal basis, the child's must be at least 16 years old to consent independently, or, if the child is younger, the holder of parental responsibility must have given or authorised the consent. Whilst Article 8(1) does allow for Member States to set the age at a lower level (between 13 and 16), the 2018 Act has maintained the age cut-off for consent to such services at 16 years old in Ireland. In cases involving children under 16, controllers must make **reasonable efforts to verify** that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology." (Autoridade de proteção de dados irlandesa. Guidance Note: Legal Bases for Processing Personal Data. December 2019. p. 09.)

[548] "Additional protection is granted to this type of personal data since children are less aware of the risks and consequences of sharing data and of their rights. Any information addressed specifically to a child should be adapted to be **easily accessible, using clear and plain language**. For most online services **the consent of the parent or guardian** is required in order to process a child's personal data on the grounds of consent up to a certain age. This applies to social networking sites as well as to platforms for downloading music and buying online games. The age threshold for obtaining parental consent is established by each EU Member State and can be between 13 and 16 years. (…) Companies have to make reasonable efforts, taking into consideration available technology, to check that the consent given is truly in line with the law. (…) Preventive or counselling services offered directly to children are exempted from the requirement for parental consent as they seek to protect a child's best interests." Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-personal-data-about-children-be-collected_en> Acesso em: 05.06.21.

[549] A idade mínima para utilização da mídia social nos EUA é de 13 anos. No Brasil, o mesmo critério etário é utilizado.

[550] "**Image and Audio Information.** We may collect information about the images and audio that are a part of your User Content, such as identifying the objects and scenery that appear, the existence and location within an image of face and body features and attributes, the nature of the audio, and the text of the words spoken in your User Content. We may collect this information to enable special video effects,

Parece que tal prática já era realizada pela empresa, restando agora de alguma forma expressa em sua política, na busca por oferecer uma aparente transparência ao usuário. Contudo, pouco se informa acerca de como será o desenvolvimento do tratamento de tais informações e quais leis poderão embasar eventual processamento. Há ainda preocupação de que as referidas informações sejam utilizadas para práticas comerciais mais agressivas.[551]

No momento pandêmico, o uso de redes sociais foi substancialmente alargado em razão de trends virais, desafios, filtros e práticas de unboxing, o que motivou, inclusive, que crianças buscassem tais plataformas, mesmo diante da vedação de sua presença nos termos de uso. Como evitar que crianças acessem serviços e conteúdos inadequados para a sua idade em mídias sociais? Quais mecanismos podem ser utilizados para se verificar a idade real do sujeito?[552] Sugere-se, por exemplo, a implementação de medidas de verificação de idade: como fazer uma pergunta que uma criança não seria capaz de responder; solicitar que o menor forneça o e-mail de seus pais, para que eles manifestem o consentimento por escrito; solicitar o número de determinados documentos do menor e de seu responsável (como o CPF e o número de um cartão de crédito); e analisar o hábito de navegação do sujeito para verificar se é compatível com a idade que diz ter. Contudo, será a idade de 13 anos já adequada para o uso desacompanhado de mídias sociais? Proibir ou controlar diretamente o uso seria a solução? As referidas questões desafiam pesquisadores e pais,

---

for content moderation, for demographic classification, for content and ad recommendations, and for other non-personally-identifying operations. We may collect biometric identifiers and biometric information as defined under US laws, such as faceprints and voiceprints, from your User Content. Where required by law, we will seek any required permissions from you prior to any such collection." Disponível em: <https://www.tiktok.com/legal/privacy-policy> Acesso em: 28.07.21.

[551] Disponível em: <https://canaltech.com.br/apps/tiktok-podera-coletar-dados-biometricos-dos-usuarios-inclusive-rostos-e-voz-186559/> Acesso em: 28.07.21.

[552] "The ongoing debate around age assurance is often centred around restricting access to the internet for children and young people. But done properly, age assurance can drive the development of new products and services to create a richer and more diverse digital ecosystem in which children (one in three internet users) are a recognised user group. (…) Rather than viewing it as simply restricting access, we should be looking at age assurance as a chance to invite children into a digital world that offers them greater privacy, freedom from commercial pressures, content and information in formats and language that they like, protection from misinformation or material that promotes harmful activities (such as suicide, self-harm or disordered eating), alongside supporting digital services in their legal duty not to provide children with age restricted contact and content." (But how do they know it is a child? Age Assurance in the Digital World. 5Rights Foundation. Março de 2021. Disponível: <https://5rightsfoundation.com/in-action/but-how-do-they-know-it-is-a-child-age-assurance-in-the-digital-world.html> Acesso em: 11.06.21)

devendo ser analisadas caso a caso, conforme as características, a autonomia e o discernimento do menor. As diversas e dinâmicas relações desenvolvidas na Internet, que envolvem tratamentos de dados e, por vezes, sua monetização e utilização para fins comerciais, nem sempre são adequadamente compreendidas por adolescentes. Além disso, durante a adolescência o sujeito não goza ainda de plena capacidade civil (a menos que seja emancipado aos 16 anos), o que traz questionamentos acerca da validade do consentimento manifestado em termos de uso, contratos e ferramentas online. Isso nos faz refletir sobre o processo de tomada de decisões na Internet e a respeito das escolhas jurídicas para a proteção da criança e do adolescente, compreendidos em caráter concreto e dentro de sua multiplicidade. Não se pode cair no equívoco de um excessivo formalismo, sob pena de prejudicarmos desproporcionalmente novos modelos de negócio e relações relevantes para a dinâmica comunicacional do ser humano. A análise do discernimento e da maturidade do sujeito se mostra fundamental, pois, ainda que o critério etário seja importante, ele não deverá ser em todos os casos único e absoluto.

Como apresentado no capítulo 1, dados sensíveis poderão alcançar diferentes níveis de sensibilidade, a depender da informação em si que guardam e/ou do titular a quem dizem respeito, impactando em graus de intensidade diversos a esfera íntima ou secreta de seu titular. Excelentes exemplos para se pensar em dados altamente sensíveis são dados biométricos de crianças e dados de saúde de menores de idade com deficiência[553], os quais além de serem sensíveis dizem respeito a sujeitos hipervulneráveis e destinatários de tutela integral. Neste caso, o melhor interesse e o dever de cuidado impõem grau de zelo maior com tais dados pessoais.

Para ilustrar, recorda-se interessante caso ocorrido em 2019 em que a Autoridade de Proteção de Dados Sueca[554] multou um município em aproximadamente 20.000 euros por usar tecnologia de reconhecimento facial para monitorar a frequência de alunos em escola.[555] No norte da Suécia, uma escola conduziu

[553] Sugere-se a leitura de caso que envolveu multa aplicada pela Autoridade de Proteção de Dados da Noruega ao município de Rælingen. Disponível em: <https://www.datatilsynet.no/en/news/2020/final-decision-administrative-fine-for-ralingen-municipality/> Acesso em: 06.06.21

[554] Fonte: <https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en> Acesso em: 06.06.21.

[555] Recomenda-se a leitura da Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools), adotada em 11 de fevereiro de 2009. Disponível em: <

um projeto piloto aplicando reconhecimento facial para monitorar a frequência dos alunos. O teste foi realizado em uma turma da escola por um período limitado. A Autoridade sueca concluiu que o teste violava disposições do GDPR e aplicou a referida multa. Entendeu que a escola havia tratado dados biométricos ilegalmente e que deveria ter realizado uma avaliação de impacto adequada, além de consulta prévia à Autoridade. A escola baseou o tratamento na base legal do consentimento, mas a Autoridade considerou que essa não era uma base válida, dado o claro desequilíbrio entre o titular dos dados e o responsável pelo tratamento.

Em 2020, o Presidente do Gabinete Polaco de Proteção de Dados Pessoais aplicou uma multa de 20.000 PLN por violação que consistia no tratamento de dados biométricos de menores para a utilização de cantina escolar.[556] A escola estava tratando categorias especiais de dados (dados biométricos) de 680 crianças, quando, na verdade, poderia usar outros recursos menos invasivos para identificar os alunos. Por essa violação, uma multa administrativa foi imposta à Escola Primária nº 2 em Gdansk. Além disso, foram ordenados o apagamento dos dados pessoais relativos às impressões digitais das crianças e a cessação de qualquer nova coleta de dados. Foi apurado que a escola utilizava um leitor biométrico na entrada da cantina escolar que identificava as crianças para verificar o pagamento da taxa de alimentação. Ela obtinha os dados e os tratava com base no consentimento por escrito dos pais ou responsáveis legais. A solução estava em vigor desde 1 de abril de 2015. No ano letivo 2019/2020, 680 alunos utilizaram o leitor biométrico, enquanto quatro alunos usaram sistema de identificação alternativo. Ressaltou-se que o tratamento de dados biométricos não era essencial para se atingir o objetivo de identificar o direito de uma criança ao almoço. A escola poderia realizar a identificação por outros meios que não interferissem tanto na privacidade da criança. Inclusive, de forma alternativa, a própria escola possibilitava a utilização dos serviços da cantina por meio de cartão eletrônico ou através da indicação do nome e do número do contrato. Contudo, de acordo com o regulamento, os alunos que não possuíam identificação biométrica deveriam aguardar no final da fila até que todos os alunos com a referida

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp160_en.pdf> Acesso em: 06.06.21.

[556] Fonte: <https://edpb.europa.eu/news/national-news/2020/fine-processing-students-fingerprints-imposed-school_en> Acesso em: 06.06.21.

identificação entrassem na cantina. Na opinião da Autoridade, tais regras introduziam um tratamento desigual aos alunos e sua diferenciação era injustificada, pois favorecia claramente os alunos com identificação biométrica. Além disso, a utilização de dados biométricos, tendo em conta a finalidade para a qual eram processados, era significativamente desproporcional.

O Presidente da Autoridade destacou que os menores necessitam de especial proteção para os seus dados pessoais. O sistema biométrico identifica características que não estão sujeitas a alterações, como no caso dos dados dactiloscópicos. Devido ao caráter único e permanente dos dados biométricos, eles devem ser usados com o devido cuidado. Os dados biométricos são únicos à luz dos direitos e liberdades fundamentais e, portanto, requerem proteção especial. Seu possível vazamento pode resultar em um alto risco para os direitos e liberdades das pessoas naturais.

Aplicar uma proteção ainda maior a dados sensíveis de crianças e adolescentes requer uma série de instrumentos jurídicos e técnicos, além do estabelecimento de boas práticas. Contar com o comprometimento de instituições públicas e privadas no tema também é de suma importância, havendo tanto a aplicação de severas sanções, por descumprimento das normas de proteção de dados, quanto a adequada orientação dos agentes por meio da publicação de guias e instruções. Nesse sentido, vale recordar os posicionamentos já estabelecidos pela Autoridade irlandesa de proteção de dados[557] e pela Autoridade do Reino Unido (Information Commissioner's Office - ICO)[558]. Em junho de 2021, a Autoridade Francesa de Proteção de Dados (*Commission Nationale de l'Informatique et des Libertés* - CNIL) publicou oito recomendações para a proteção de menores[559], quais sejam: a) supervisionar a capacidade dos menores de agir online; b) incentivar os menores a exercerem seus direitos; c) apoiar os pais na educação digital; d) obter o consentimento de um dos pais para menores de 15 anos; e) promover ferramentas de controle parental que respeitem a privacidade e o melhor interesse da criança; f) fortalecer a informação e os direitos dos menores por design; g) verificar a idade da criança e o consentimento dos pais com

[557] Fonte: <https://www.dataprotection.ie/en/dpc-guidance/blogs/the-children-fundamentals> Acesso em: 06.06.21.

[558] Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/executive-summary/> Acesso em: 06.06.21

[559] Disponível em: <https://www.cnil.fr/fr/la-cnil-publie-8-recommandations-pour-renforcer-la-protection-des-mineurs-en-ligne> Acesso em: 11.06.21.

respeito à sua privacidade; e h) oferecer garantias específicas para proteger os interesses da criança. Aplicações tanto de inteligência artificial quanto que envolvem o tratamento de dados de crianças e adolescentes necessitam ser desenvolvidas a partir de orientações que considerem princípios e valores éticos, além de haver a proteção aos direitos humanos inserida no desenho de todo o sistema. Ações alinhadas à lógica do *privacy by design* devem sempre ser tomadas no desenvolvimento de tecnologias, sendo incluídas também avaliações prévias de impacto e medidas técnicas e organizacionais de prestação de contas.

No cenário brasileiro, quando se advoga pela ampliação das bases legais para o tratamento de dados pessoais de crianças e adolescentes, o relatório de impacto à proteção de dados pessoais[560] representa documento essencial para a tutela do melhor interesse dos menores. Como se depreende da leitura do artigo 14 da LGPD, o consentimento[561] é uma das bases legais para o tratamento de dados de crianças e adolescentes, mas não a única. Entende-se que podem ser aplicadas, além das normas do Art. 14[562], as disposições dos artigos 7º e 11 da LGPD, com algumas limitações, quando, respectivamente, se tratar dado pessoal de caráter geral e dado pessoal sensível de criança ou adolescente. Diante da redação dos parágrafos 1º e 3º do Art. 14, ampliar as bases legais para o tratamento de dados de crianças pode parecer uma tese mais arriscada para alguns agentes, tendo em vista que as referidas disposições, ao mencionarem estritamente crianças, poderiam sinalizar uma possível restrição das hipóteses legais de tratamento para esses sujeitos. Por outro lado, tal situação não envolve diretamente a figura do adolescente, o qual apenas é mencionado no *caput* do art. 14 da LGPD. O pilar central e inegociável será sempre o *melhor interesse da criança e do adolescente*.[563] Contudo,

[560] O tema será analisado no capítulo 4 da tese.

[561] Sobre o consentimento e suas polêmicas ver: TEFFÉ, Chiara Spadaccini de. Proteção de dados de crianças e adolescentes. *Revista do Advogado*, v. 39, 2019.

[562] "Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente. § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. (...) § 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo." Observa-se que tanto o parágrafo 1º quanto o 3º mencionam apenas "crianças".

[563] Cf. TEIXEIRA, Ana Carolina Brochado; RETTORE, Anna Cristina de Carvalho. O princípio do melhor interesse no ambiente digital. In: LATERÇA, Priscilla Silva; FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (Coords.). *Privacidade e Proteção de Dados de Crianças e*

levando em conta as práticas de agentes públicos e privados, bem como a experiência europeia positivada no GDPR, expandir o rol de bases legais mostra-se uma tese possível e por vezes necessária, ainda que se ressalve a aplicação do legítimo interesse e da tutela do crédito. Nessa lógica, já se afirmou que tal entendimento:

> (...) pode ser facilmente verificado no tratamento de dados de crianças e adolescentes no âmbito de políticas públicas (Art. 7º, III, da LGPD), pela Administração Pública, visando-se a promover sua saúde e educação. Outros exemplos encontram-se no tratamento de dados para o cumprimento de obrigação legal ou regulatória pelo controlador (inciso II), no necessário tratamento de dados para a proteção da vida ou da incolumidade física (inciso VII) e para a tutela da saúde (inciso VIII), bases legais que, definitivamente, podem ser utilizadas para garantir o melhor interesse e proteção. (...) Ainda que o presente entendimento não seja pacífico e encontre várias polêmicas, defende-se que o art. 14 da LGPD traria, em si, especificidades quanto ao consentimento como base legal, mas não um rol extremamente restrito para o tratamento de dados de crianças. Dessa forma, como complemento às hipóteses de autorização legal para o tratamento de dados, afirma-se, no parágrafo 3º, do artigo 14, que poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o parágrafo 1º, do mencionado artigo, quando: a) a coleta for necessária para contatar os pais ou o responsável legal, devendo os dados serem utilizados uma única vez e sem armazenamento; ou b) para a proteção da criança. Porém, em nenhum caso, esses dados poderão ser repassados a terceiros sem o consentimento de que trata o § 1º.[564]

Acerca da base legal do consentimento, disposta no par. 1º do Art. 14, mostra-se necessário tecer algumas considerações. Na lei, em relação às crianças, afirma-se que o tratamento dos dados pessoais desses sujeitos deverá ser realizado com o consentimento específico e em destaque dado por, pelo menos, um dos pais ou pelo responsável legal, devendo esse consentimento ser também livre, informado e direcionado a tratamento de dados pessoais para finalidade determinada. Diante disso, o consentimento dado por sujeito fora do requisito legal ou pela própria criança não poderá ser admitido. Optou a lei por oferecer tutela destacada à criança, sujeito hipervulnerável e absolutamente incapaz, o qual deve ser representado sob pena de nulidade absoluta do ato praticado.

Adolescentes. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021. Edição do Kindle. MULHOLLAND, Caitlin; PALMEIRA, Mariana. As bases legais para tratamento de dados de crianças e adolescentes. In: LATERÇA, Priscilla Silva; FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (Coords.). *Privacidade e Proteção de Dados de Crianças e Adolescentes*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021. Edição do Kindle.

[564] Cf. TEFFÉ, Chiara Spadaccini de; FERNANDES, Elora. Contratação em redes sociais e proteção de dados de crianças e adolescentes. In: ROQUE, André Vasconcelos; OLIVA, Milena Donato. Direito na era digital: aspectos negociais, processuais e registrais. Salvador: Juspodivm, 2022.p.97-122.

Como visto, o par. 1º não menciona o adolescente, criando, assim, dúvida se o consentimento manifestado por ele sem assistência ou representação deveria ser considerado válido, como hipótese de capacidade especial, ou se simplesmente o legislador teria optado por não tratar do tema, por já existir legislação geral sobre a matéria no Código Civil (artigos 3º, 4º e 1.634, VII).

A priori, parece que o legislador pretendeu reconhecer validade ao consentimento manifestado diretamente pelo adolescente no que concerne, especificamente, ao tratamento de seus dados pessoais (quando a base legal adotada para o caso for o consentimento).[565] Como já afirmado, "Tomando-se como base a realidade da utilização da internet e das mídias sociais, que têm entre seus usuários milhares de adolescentes, é possível que se tenha optado por considerar jurídica hipótese fática dotada de ampla aceitação social."[566] Recorda-se, inclusive, que tanto o Código Civil quanto o Estatuto da Criança e do Adolescente trazem em suas normas disposições que valorizam a vontade dos menores e oferecem hipóteses de capacidade especial a eles.[567] Em sentido contrário[568], parte da doutrina entende que levando em conta as normas do Código Civil e a doutrina do melhor interesse, tanto para o tratamento de dados de criança quanto de adolescente, seria necessário ocorrer a manifestação do consentimento de, pelo menos, um dos pais ou responsável legal. No caso de adolescentes entre 16 e 18 anos, seria necessário o consentimento dele e de seu responsável.[569]

---

[565] Cf. TEPEDINO, Gustavo; OLIVA, Milena Donato. Tratamento de dados de crianças e adolescentes na LGPD e o sistema de incapacidades do Código Civil. In: LATERÇA, Priscilla Silva; FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (Coords.). *Privacidade e Proteção de Dados de Crianças e Adolescentes*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021. Edição do Kindle.

[566] TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. O consentimento na circulação de dados pessoais. *Revista Brasileira De Direito Civil*, v. 25, p. 83-116, 2020.p.109-110

[567] Exemplos de flexibilização do regime das incapacidades no ECA: art. 16, II; art. 28, §§1º e 2º; art. 100, XII; art. 111, V; e art. 161, §3º. Além desses exemplos, pode-se citar o próprio Código Civil, em seu art. 1.740, III. Existem também atos e negócios que os relativamente incapazes podem praticar, mesmo sem assistência, como se casar, exigindo-se autorização de ambos os pais ou de seus representantes legais; elaborar testamento; servir como testemunha de atos e negócios jurídicos; e ser eleitor.

[568] TEIXEIRA, Ana Carolina Brochado; RETTORE, Anna Cristina de Carvalho. A autoridade parental e o tratamento de dados pessoais de crianças e adolescentes. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Revista dos Tribunais, 2019. HENRIQUES, Isabella; PITA, Marina; HARTUNG, Pedro. A proteção de dados pessoais de crianças e adolescentes. In: Bruno Bioni, Laura Schertel Mendes, Danilo Doneda, Otavio Luiz Rodrigues Jr., Ingo Wolfgang Sarlet. (Org.). *Tratado de Proteção de dados pessoais*. 1ed. Rio de Janeiro: Forense, 2021. Ebook.

[569] "(...) ainda que o §1º não mencione os adolescentes, não faria sentido deixá-los desprovidos da igual e devida proteção, sob pena de se violar as garantias constitucionais dessas pessoas. Há que se defender,

Acerca da aplicação das demais bases legais dispostas na LGPD aos menores, há corrente que apresenta interessante entendimento, buscando conciliar uma perspectiva de ampliação das bases legais (por meio do Art. 11 da LGPD) com o Art. 14 da Lei:

> (...) a hipótese do art. 14, §1º, da LGPD, de consentimento parental, é semelhante à hipótese de consentimento de titular adulto prevista na regra para o tratamento de dados pessoais sensíveis do art. 11, I, da LGPD, no que diz respeito a suas características de ser específico e destacado – além, é claro, de livre, informado e inequívoco, como previsto no art. 5.º, XII, da LGPD. Há, com efeito, uma equivalência entre tais dispositivos legais (...) Diante dessa similitude de condições, é possível que se entenda que as outras hipóteses que dispõem sobre o tratamento de dados pessoais sensíveis, previstas no inciso II do art. 11 da LGPD – que não a do consentimento, que possui previsão específica no art. 14, § 1.º –, são válidas também para o tratamento de quaisquer dados pessoais de crianças e adolescentes, mesmo que não sejam considerados sensíveis nos termos da definição do art. 5.º, II, da LGPD, e contanto que haja observância ao melhor interesse dessas pessoas. Isso porque, no referido dispositivo, o legislador aumentou a proteção dos dados pessoais, por entender que dados pessoais sensíveis merecem maior cuidado, tal qual a criança e o adolescente por suas inerentes características.[570]

A referida corrente entende que, para fins de Direito, os dados pessoais de crianças e adolescentes serão sempre considerados sensíveis, visto que, por estarem em uma situação peculiar de desenvolvimento de suas capacidades, elas são mais vulneráveis e suscetíveis, inclusive às atividades de tratamento, manipulação e hiperexposição de dados pessoais. Dessa forma, além da hipótese de consentimento parental prevista no Art. 14, §1º, são também hipóteses legais para o tratamento de

---

nesse caso, a aplicação do Código Civil, a fim de se promover a integralidade de seus direitos. De fato, a proteção de dados pessoais, entendida enquanto parte do contrato civil, reforça a objeção à capacidade legal de crianças e de adolescentes consentirem quanto ao tratamento de seus dados, uma vez que, pelo exercício do poder familiar, compete a mães, pais e responsáveis representá-los até os 16 anos, nos atos da vida civil, e assisti-los, após essa idade, nos atos em que forem partes, suprindo-lhes o consentimento. Não se coadunaria, com efeito, com as garantias legais ao melhor interesse e à absoluta prioridade do adolescente que lhe fosse facultada a outorga de consentimento autônomo ilimitado para o tratamento de seus dados pessoais. Dessa forma, entende-se indispensável o consentimento parental ou de pessoa responsável legal para o tratamento de dados pessoais de crianças e de adolescentes de até 16 anos de idade, observando-se a forma prevista no referido 14, §1º, da LGPD, devendo, assim, o consentimento ser específico e em destaque. No caso de adolescentes entre 16 e 18 anos, será necessário o consentimento de ambos, não bastando o consentimento parental." (HENRIQUES, Isabella; PITA, Marina; HARTUNG, Pedro. A proteção de dados pessoais de crianças e adolescentes. In: Bruno Bioni, Laura Schertel Mendes, Danilo Doneda, Otavio Luiz Rodrigues Jr., Ingo Wolfgang Sarlet. (Org.). *Tratado de Proteção de dados pessoais*. 1ed. Rio de Janeiro: Forense, 2021. Ebook.)

[570] HENRIQUES, Isabella; PITA, Marina; HARTUNG, Pedro. A proteção de dados pessoais de crianças e adolescentes. In: Bruno Bioni, Laura Schertel Mendes, Danilo Doneda, Otavio Luiz Rodrigues Jr., Ingo Wolfgang Sarlet. (Org.). *Tratado de Proteção de dados pessoais*. 1ed. Rio de Janeiro: Forense, 2021. Ebook.

dados de crianças e adolescentes aquelas arroladas no Art. 11, II, da LGPD, que apresenta hipóteses mais restritas em relação à norma geral do Art. 7º. Há, portanto, pelo menos três correntes e possíveis interpretações para as bases legais aplicáveis ao tratamento de dados de crianças. De forma a ampliar as garantias no tratamento de dados de crianças e adolescentes, doutrina e autoridades de proteção de dados vêm afirmando a necessidade de os agentes desenvolverem relatórios de impacto à proteção de dados quando esses sujeitos estiverem envolvidos diretamente nas atividades de tratamento de dados, especialmente se houver o tratamento de informações sensíveis. Nessa lógica, a Agência Espanhola de Proteção de Dados destaca que precisarão de avaliação de impacto: tratamentos de dados de sujeitos vulneráveis ou em risco de exclusão social, incluindo dados de menores de 14 anos, maiores com algum grau de deficiência, pessoas que acedem a serviços sociais e vítimas de violência de gênero, bem como seus descendentes e pessoas que estão sob sua guarda e custódia.[571] Ela lista também diversos tratamentos que envolvem dados pessoais sensíveis.

O *Age appropriate design: a code of practice for online services*, publicado pela ICO, dispõe acerca da avaliação de impacto à proteção de dados. Segundo o código, deve-se realizar um DPIA (*Data Protection Impact Assessment*) [572] para avaliar e mitigar os riscos aos direitos e liberdades das crianças que provavelmente terão acesso aos serviços ali mencionados. Afirma-se também que o agente deverá levar em consideração as diferentes idades, capacidades e necessidades de desenvolvimento dos menores, além de se certificar de que seu DPIA seja elaborado em conformidade com o referido código. Orientações que devem, sem dúvida, ser aplicadas no cenário brasileiro. O contexto tecnológico atual – dinâmico e hiperconectado

[571] "Tratamientos de datos de sujetos vulnerables o en riesgo de exclusión social, incluyendo datos de menores de 14 años, mayores con algún grado de discapacidad, discapacitados, personas que acceden a servicios sociales y víctimas de violencia de género, así como sus descendientes y personas que estén bajo su guardia y custodia." Fonte: <https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf> Acesso em: 06.06.21.

[572] "A DPIA is a defined process to help you identify and minimize the data protection risks of your service – and in particular the specific risks to children who are likely to access your service which arise from your processing of their personal data. You should begin a DPIA early in the design of your service, before you start your processing. It should include these steps: Step 1: identify the need for a DPIA Step 2: describe the processing Step 3: consider consultation Step 4: assess necessity and proportionality Step 5: identify and assess risks arising from your processing Step 6: identify measures to mitigate the risks Step 7: sign off, record and integrate outcomes." (Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/2-data-protection-impact-assessments/> Acesso em: 06.06.21.)

– traz diversas oportunidades e recursos para as crianças e adolescentes, auxiliando inclusive na promoção de seus direitos. Contudo, os riscos enfrentados e as diversas situações de tratamento indevido de dados trazem consigo desafios para a tutela dos referidos sujeitos. Ameaças à integridade física, psíquica ou moral, a hiperexposição de dados pessoais e a discriminação, a modulação e a manipulação de comportamentos e a publicidade infantil são exemplos de impactos negativos e problemas concretos enfrentados pelos menores. Diante disso, como apresentado, a LGPD trouxe uma série de direitos, orientações e garantias para a proteção de crianças e adolescentes, nos meios físico e digital, as quais deverão ser conjugadas com a doutrina do melhor interesse e a proteção integral, havendo a ampla participação dos mais variados sujeitos que atuam em sociedade.

4. SEGURANÇA E BOAS PRÁTICAS COM DADOS SENSÍVEIS

No quarto capítulo, busca-se finalizar o estudo funcional dos dados sensíveis, por meio da análise de questões relativas à segurança, cuidados específicos e boas práticas no tratamento de tais informações. Será oferecida especial ênfase à lógica do *privacy by design* em todo o ciclo de tratamento de dados e ao relatório de impacto à proteção de dados pessoais, documento relevante, e por vezes fundamental, em determinados tratamentos, realizados por sujeitos públicos e privados, que envolverem dados sensíveis. No tema da gestão de riscos serão abordadas algumas questões de ordem técnica – ainda que a presente tese se proponha a ser um texto integralmente jurídico –, diante da compreensão de que a temática necessita de uma aplicação de recursos multidisciplinares. Em seguida, serão desenvolvidas algumas orientações para a mitigação de incidentes de segurança, especialmente envolvendo dados sensíveis. Ao final, o estudo será dirigido aos artigos da LGPD referentes ao término do tratamento de dados e à conservação de informações pessoais sensíveis.

4.1 Cuidados específicos e boas práticas no tratamento de informações pessoais sensíveis

O tratamento de dados sensíveis impõe um padrão mais elevado de proteção e segurança para as informações, assim como um maior rigor nas técnicas empregadas para a sua circulação. Além de seguir estritamente normas e resoluções, as instituições

devem obedecer a todo o arcabouço regulatório pertinente à atividade desenvolvida e criar normas internas – como Códigos de Ética e Conduta –, visando a direcionar o comportamento de seus diretores, executivos e funcionários em torno de determinados valores e princípios, coibindo comportamentos negativos, desvios de conduta e inconformidades com as normas.[573] Cabe também promover interações entre *players* que desenvolvam atividades semelhantes e agentes de diferentes setores da sociedade, numa perspectiva multissetorial, para a troca e elaboração de boas práticas.

Nesse sentido, nas atividades de compliance[574] pertinentes à questão deve-se buscar uma aplicação ampla do *privacy by design*, a elaboração de relatórios de impacto, uma gestão eficiente de riscos, o desenvolvimento de planos de resposta a incidentes de segurança, a ampliação das áreas de segurança da informação e proteção de dados e o registro documental dos fluxos de dados[575], que detalhe todo o tratamento empregado, inclusive compartilhamentos, prazos de guarda e conservação, término da atividade e eliminação das informações.

A proteção de dados – especialmente os qualificados como sensíveis – e as normas jurídicas, técnicas e institucionais referentes à matéria podem ser percebidas como formas de: (I) conter os efeitos nefastos do capitalismo de vigilância e as manipulações[576] oriundas de grandes plataformas; (II) afastar os riscos

---

[573] ANTONIK, Luis Roberto. *Compliance, ética, responsabilidade social e empresarial*: uma visão prática. Rio de Janeiro: Alta Books, 2016.

[574] Doutrina destaca a importância do compliance, sendo ele responsável pela: "(...) estruturação de políticas e procedimentos corporativos que se traduzam em ações sistemáticas com o objetivo de atender ao cumprimento aos preceitos normativos, a permitir a prevenção do ato ilícito ou, caso tal não seja possível, minorar seus efeitos e sancionar eventuais responsáveis. Os programas de *compliance* relacionam-se à fixação de controles internos que, em reforço à regulação estatal, auxiliem os agentes econômicos a se manterem em conformidade com a lei (e, de forma mais ampla, também com suas políticas corporativas). Sua relevância aprofundou-se nas últimas décadas diante da ampliação do papel sancionador do Estado: paradoxalmente, ao mesmo tempo em que se os agentes econômicos passaram a se preocupar com as (cada vez mais elevadas) sanções aplicadas pelo Estado, passou-se a denotar que apenas essa perspectiva era incapaz de apresentar as soluções necessárias." (FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. Compliance de dados pessoais. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coords.). *A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Revista dos Tribunais, 2019. p. 683-684.)

[575] Mapeamento de todos os dados pessoais e operações de tratamento que envolvam tanto dados de usuários de produtos e/ ou serviços da organização quanto de não usuários, como funcionários, representantes de clientes, parceiros, fornecedores ou terceiros.

[576] "À medida que, através de sensores biométricos, cada vez mais dados fluírem de seu corpo e seu cérebro para máquinas inteligentes, será fácil para corporações e agências do governo conhecer você, manipular você e tomar decisões por você. Mais importante ainda, eles serão capazes de decifrar os mecanismos profundos de todos os corpos e cérebros, e com isso adquirir o poder de fazer a engenharia da vida. Se quisermos evitar que uma pequena elite monopolize esses poderes, que parecem divinos, e se quisermos impedir que a humanidade se fragmente em castas biológicas, a questão chave é: quem é dono

que determinadas aplicações com algoritmos podem oferecer às liberdades fundamentais; (III) trazer garantias às pessoas diante da opacidade e da ausência de *accountability* de muitas estruturas políticas e econômicas[577]; e (IV) impedir discriminações ilícitas ou abusivas em face de pessoas singulares e grupos.

Além de se preocupar com o cumprimento integral das normas relativas à proteção de dados, na forma do Art. 50 da LGPD, os controladores e operadores, no âmbito de suas competências, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. Tais regras deverão, inclusive, ser publicadas e atualizadas periodicamente.

Estar em conformidade significa alterar toda a cultura da instituição no que tange ao tema, observando de forma específica os princípios da LGPD (especialmente a responsabilidade e a prestação de contas, a segurança, a prevenção, a transparência e a não discriminação), bem como capacitar todos os sujeitos para que atuem conforme as normas que apresentam relevância jurídica. A conformidade é caracterizada "pelo compromisso com a criação de um sistema complexo de políticas, de controles internos e de procedimentos, que demonstrem que a empresa está buscando "garantir" que se mantenha em um estado de *compliance*."[578]

A adoção de um programa de compliance que tenha atenção aos tratamentos de dados realizados pela instituição mostra-se essencial para auxiliar no efetivo atendimento aos comandos da lei, de acordo com as particularidades de cada local, bem como para prevenir a ocorrência de violações aos direitos dos titulares, traduzindo de

---

dos dados? Os dados de meu DNA, meu cérebro e minha vida pertencem a mim, ao governo, a uma corporação ou ao coletivo humano?" (HARARI, Yuval Noah. *21 lições para o século 21*. 1.ed. Companhia das Letras: 2018, p. 109.)

[577] Cf. FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de dados. In: Gustavo Tepedino, Ana Frazão e Milena Donato Oliva (Org.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. 1ed. São Paulo: Thomson Reuters - Revista dos Tribunais, 2019, v. 1, p. 23-52.

[578] SAAVEDRA, Giovani Agostini. Compliance de dados. In: Bruno Bioni, Laura Schertel Mendes, Danilo Doneda, Otavio Luiz Rodrigues Jr., Ingo Wolfgang Sarlet (Org.). *Tratado de Proteção de dados pessoais*. 1ed.Rio de Janeiro: Forense, 2021, v. 1, p. 729.

forma concreta para as atividades cotidianas as premissas da LGPD.[579] Por exemplo, as regras de governança podem dispor sobre as hipóteses específicas em que o tratamento será considerado pela entidade como fundamentado em seu legítimo interesse (Art. 7º, X, da LGPD) ou em que hipóteses a instituição deverá realizar um relatório de impacto.

Um programa que envolva altas lideranças corporativas, tenha suporte financeiro adequado, ofereça autonomia e independência aos envolvidos e detecte e puna exemplarmente condutas contrárias às diretrizes adotadas contribui tanto para a boa reputação da empresa quanto para a criação de um ambiente de confiança com os titulares de dados (como clientes e parceiros), além de representar diferencial competitivo frente aos demais agentes que atuam no mesmo setor. Para tanto, devem ser reforçados canais de denúncia, comitês de ética, políticas de penalidades e auditorias, "para que se possa averiguar se as políticas e demais medidas do sistema de gestão de *compliance* de dados estão sendo aplicadas corretamente e se os envolvidos na gestão do sistema estão registrando adequadamente as evidências do sistema."[580]

Considerar aspectos éticos e boas práticas internacionalmente elogiadas e aplicadas no tratamento de dados é medida fundamental no programa implementado. Por meio de uma cultura de compliance proativo de dados, as instituições podem buscar uma transformação digital segura, assim como evitar os riscos associados à não conformidade regulatória, como, por exemplo, multas, restrições, perda da confiança do consumidor e de clientes e diminuição de oportunidades de negócios. A LGPD demanda novos modelos empresariais, sendo programas robustos de compliance e o gerenciamento ágil dos riscos essenciais para proteger as instituições e promover seu desenvolvimento. Nesse sentido, vale lembrar os princípios que compõem a sigla "ESG", que significa literalmente *environmental, social and corporate governance.* Ela é usada para se referir e mensurar

[579] "A expressão *Sistema de Gestão de Compliance* (*Compliance Management System*) foi cunhada pela International Organization for Standardization (ISO), por meio da norma ISO 19600. Conforme referido anteriormente, não há dúvida de que a proteção de dados e a tão difundida necessidade de "adequação à LGPD" nada mais são do que um elemento desse sistema mais amplo de gestão de *compliance*. (...) Uma das grandes novidades que as legislações recentes sobre proteção de dados trouxeram foi a adoção da sistemática de *compliance* como critério interno de conexão entre os vários institutos da legislação. O sistema de gestão de *compliance* de dados aparece nessa legislação como expressão do princípio da *accountability* e como meio de proteção dos direitos subjetivos/fundamentais de dados." (SAAVEDRA, op. cit. p.730-731)

[580] SAAVEDRA, op. cit. p.739.

as práticas ambientais, sociais e de governança de um negócio. Como exemplos[581], é possível afirmar que o pilar ambiental tem como foco a gestão das emissões de gases de efeito estufa e o consumo de recursos naturais (como água, energia, produção e descarte adequado de resíduos); o social analisa o relacionamento com os colaboradores, os valores da empresa, a diversidade no corpo de funcionários e campanhas externas; e o de governança trata de aspectos relacionados às políticas e práticas da empresa, à diversidade nos conselhos corporativos e às aplicações voltadas à ética, transparência e práticas anticorrupção. Percebe-se que tal cuidado beneficia, além do coletivo, a própria empresa, a qual se torna mais competitiva, tem melhor controle sobre os riscos e tende a alcançar melhores resultados no longo prazo.

Preocupar-se e atuar ativamente em tais setores representa, nos últimos tempos, critério relevante para o recebimento de investimentos e caminha ao encontro da lógica do "capitalismo de stakeholders", conceito que visa a debater qual papel os stakeholders podem desempenhar na busca de uma economia global mais sustentável, resiliente e inclusiva.[582] Klaus Schwab[583] propõe que as empresas busquem a criação de valores de longo prazo, ao invés de lucros de curto prazo, levando em consideração as necessidades de todas as partes interessadas e da sociedade em geral. Os governos devem cooperar para criar a maior prosperidade possível para seu povo, enquanto a sociedade civil e as organizações internacionais completam o diálogo com as partes interessadas, ajudando a equilibrar os interesses das pessoas e do planeta.

Assim, empresas comprometidas com a redução de seus impactos ambientais, com a construção de um ambiente socialmente responsável para

---

[581] COELHO, Nathália; LIMA, Antônio Pedro. ESG: por que essa sigla vai mudar o seu negócio daqui para a frente? Firjan, 19 de abril de 2021. Disponível em: <https://casafirjan.com.br/lab-de-tendencias/artigos-estudos-e-pesquisas/esg-por-que-essa-sigla-vai-mudar-o-seu-negocio-daqui> Acesso em: 04.05.21.

[582] "Em tempos em que os investimentos ESG estão em alta, a discussão sobre o que seria o capitalismo de *stakeholders* – que se preocupa não apenas com os acionistas, mas também com as demais partes interessadas, tais como consumidores, trabalhadores, meio ambiente, demais agentes econômicos e a sociedade como um todo – e qual deveria ser o interesse social das sociedades empresárias fica em maior evidência, até por refletir os propósitos da atividade econômica." (FRAZÃO, Ana. Capitalismo de stakeholders e investimentos ESG. *Jota*, publicado em 28 de abril de 2021.)

[583] Em 2021, na reunião anual do Fórum Econômico Mundial, debateu-se a questão do capitalismo de stakeholders, tema desenvolvido na obra *Stakeholder Capitalism: A Global Economy that Works for Progress, People and Planet*, do economista alemão Klaus Schwab, fundador e presidente-executivo do Fórum, e de Peter Vanham. Fonte: <https://www.weforum.org/agenda/2021/01/klaus-schwab-on-what-is-stakeholder-capitalism-history-relevance/> Acesso em: 02.05.21.

seus colaboradores e para a comunidade em seu entorno e com os melhores processos de administração vêm se destacando, por mostrarem o quanto são resilientes e sustentáveis. Sistemas de gestão de compliance comprometidos com as questões acima protegem a instituição, por exemplo, de incidentes de segurança, sanções, penalidades e do pagamento de elevadas indenizações impostas por autoridades.

4.1.1 Aplicação do *Privacy by Design* no tratamento de dados sensíveis

A lógica do *privacy by design* preconiza que a privacidade e a proteção de dados devem ser consideradas desde a concepção e durante todo o ciclo de vida de projetos, sistemas, serviços, produtos e processos que envolvam o tratamento de dados,[584] especialmente se eles forem sensíveis, devendo, por consequência, ser incluídas avaliações prévias de impacto, medidas técnicas e organizacionais adequadas e instrumentos de prestação de contas (*accountability*).[585] A privacidade por design garante que os dados pessoais sejam protegidos automaticamente em qualquer sistema de TI ou prática comercial. Mesmo se um indivíduo não questionar as práticas da instituição acerca da proteção de dados, suas informações permanecerão protegidas. Portanto, nenhuma ação será necessária por parte dele para proteger sua privacidade: isso por padrão será integrado de forma automática ao sistema.

O conceito de *Privacy by Design* (PbD) foi desenvolvido pela *Information and Privacy Commissioner de Ontário* (Canadá): Dr.ª Ann Cavoukian, nos anos 90. Entende-se que procedimentos de tratamento de dados são mais bem seguidos e

---

[584] CAVOUKIAN, Ann. *Operationalizing Privacy by Design*: A Guide to Implementing Strong Privacy Practices. Dez. 2012. CAVOUKIAN, Ann. *Privacy by Design*: The 7 Foundational Principles. Disponível em: <https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/> Acesso em: 09.04.21. EDPB. *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.* Adopted on 20 October 2020. Disponível em: <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en> Acesso em: 10.05.21. Norwegian Data Protection Authority. *Software development with Data Protection by Design and by Default*. Nov. 2017. Disponível em: <https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?print=true> Acesso em: 04.08.21.

[585] Conforme o considerando n. 78 do GDPR.

aplicados quando já estão integrados na tecnologia desde o seu início. Do ponto de vista técnico, recomenda-se a realização de, por exemplo, a minimização dos dados tratados, a anonimização ou pseudonimização de dados pessoais o mais cedo possível (quando viável), a aplicação de criptografia (se adequado), o uso de padrões ISO, a autenticação (verificação das identidades das partes comunicantes) e a utilização de ferramentas tecnológicas capazes de dar transparência aos critérios utilizados para a tomada de decisões.[586] Além disso, o controlador deverá aplicar as técnicas mais avançadas, a fim de garantir que esteja em condições de cumprir as suas obrigações legais e contratuais em matéria de proteção de dados.

Exemplos[587] de aplicação de *data protection by design* são: o uso de pseudonimização (substituição de material que permite identificação pessoal por identificadores artificiais) e criptografia (codificação de mensagens de forma que apenas as pessoas autorizadas possam lê-las). Nessa linha, uma excelente aplicação de *data protection by default* seria uma plataforma de mídia social definindo as configurações de perfil dos usuários dentro das opções mais favoráveis à privacidade, limitando por exemplo desde o início as possibilidades que terceiros terão de conhecer informações pessoais dispostas nos perfis dos usuários. Obviamente, os usuários poderão modificar tais configurações para compartilhar mais informações com terceiros e/ou de forma pública, mas isso será uma ação oriunda de sua vontade e escolha.

Como forma de ilustrar a positivação da lógica da *proteção de dados por design*, recorda-se o artigo 25 (1) do GDPR: levando em consideração o estado da técnica (estado da arte), o custo de implementação[588] e a natureza, escopo, contexto e finalidades do tratamento, bem como os riscos de probabilidade e severidade variados para os direitos e liberdades das pessoas físicas, o controlador deve, tanto no momento da determinação dos meios de tratamento quanto no momento do próprio tratamento, implementar medidas técnicas e organizacionais adequadas, tais como pseudonimização, que são concebidas para implementar princípios de proteção de dados, como a minimização, de uma forma eficaz e para integrar as salvaguardas

[586] *Handbook on European data protection law*. European Union Agency for Fundamental Rights and Council of Europe. Luxembourg: Publications Office of the European Union, 2018. p.184-185.
[587] European Commission. What does data protection 'by design' and 'by default' mean? Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en> Acesso em: 03.08.21.
[588] A mesma referência encontra-se no Art. 32 do GDPR.

necessárias no tratamento, a fim de cumprir os requisitos do presente regulamento e proteger os direitos das pessoas em causa.[589]

Em seguida, a *proteção de dados por padrão* encontra-se no artigo 25 (2) do GDPR: o responsável pelo tratamento deve implementar medidas técnicas e organizacionais adequadas para garantir que, por padrão, apenas sejam tratados os dados pessoais necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais coletados, à extensão do seu tratamento, ao período de armazenamento e à acessibilidade. Em particular, tais medidas devem assegurar que, por padrão, os dados pessoais não sejam disponibilizados a um número indefinido de pessoas.[590] Portanto, por *data protection by default*[591] se exige que o controlador garanta que trata apenas os dados necessários para atingir sua finalidade específica. Ele se vincula aos princípios da minimização dos dados e da limitação da finalidade. A proteção de dados, por padrão, significa que você precisa especificar esses dados antes do início do tratamento, informar as pessoas de maneira adequada e processar apenas os dados de que precisar para o seu propósito.[592]

---

[589] Trazendo críticas ao conteúdo e à redação do artigo 25 do GDPR: WALDMAN, Ari Ezra. Data Protection by Design? A Critique of Article 25 of the GDPR. *Cornell International Law Journal*, vol. 53, 2021. Disponível em: <https://ssrn.com/abstract=3773143> Acesso em: 04.08.21.

[590] Tradução livre do artigo 25 do GDPR. Em inglês: "*Article 25* **Data protection by design and by default** 1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. 2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. 3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article." Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=PT> Acesso em: 03.08.21

[591] ICO. Data protection by design and default. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/> Acesso em: 03.08.21.

[592] "(…) you must consider things like: adopting a 'privacy-first' approach with any default settings of systems and applications; ensuring you do not provide an illusory choice to individuals relating to the data you will process; not processing additional data unless the individual decides you can; ensuring that personal data is not automatically made publicly available to others unless the individual decides to make it so; and providing individuals with sufficient controls and options to exercise their rights." [592] (ICO. Data protection by design and default. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-

No Brasil, as referidas diretrizes foram expressamente positivadas no Art. 46 da LGPD, que dispõe que:

> 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.

No que concerne ao parágrafo 2º do Art. 46 da LGPD, que traz o conceito de *privacy by design*, Lemos e Branco destacam que:

> Busca-se, assim, a criação de confiança não apenas no método, no procedimento de coleta e de tratamento de dados, mas também na própria arquitetura do sistema. Objetiva-se com a chamada *privacy by design* dar ao usuário mais ferramentas de confiança na rede. (...) Não bastam o debate público, o esclarecimento social e a lei. É necessário estimular que a regulação de comportamento esteja intrinsecamente conectada às ferramentas usadas na coleta, tratamento e utilização dos dados pessoais.[593]

Em relação ao parágrafo 1º do Art. 46 da LGPD, os referidos autores bem esclarecem que:

> A LGPD, assim como o regulamento europeu, não identifica quais são essas medidas de segurança, técnicas e administrativas que devem ser adotadas desde a fase de concepção do produto ou do serviço até sua execução. E não poderia ser diferente. Afinal, quando a lei trata de tecnologia, o detalhamento técnico certamente levaria à obsolescência em pouco tempo. Caberá, assim, à Autoridade Nacional de Proteção de Dados identificar quais são os padrões mínimos a serem observados por todos a quem a norma se destina. Isso permitirá, ao menos em tese, a atualização periódica desses padrões,

---

protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/> Acesso em: 03.08.21.)

[593] LEMOS, Ronaldo; BRANCO, Sérgio. Privacy by design: conceito, fundamentos e aplicabilidade na LGPD. In: Bruno Bioni, Laura Schertel Mendes, Danilo Doneda, Otavio Luiz Rodrigues Jr., Ingo Wolfgang Sarlet. (Org.). *Tratado de Proteção de dados pessoais*. 1ed. Rio de Janeiro: Forense, 2021. E-book.

> deixando-os em conformidade com o estado da arte e alinhados a demandas mais recentes de proteção de dados pessoais dos indivíduos. [594]

O *design* das tecnologias, ou seja, como elas são dispostas e arquitetadas, influencia diretamente o comportamento das pessoas. A mensagem e os sinais emitidos pelo *design* afetam o relacionamento do ser humano com a tecnologia e as instituições, bem como o cálculo de risco elaborado. Além disso, ele afeta os custos e o tempo aplicado em uma transação, melhora a experiência em ferramentas e induz e manipula condutas. A partir dessas funções, verifica-se que *design* e poder estão profundamente conectados. Da mesma forma que o *design* tem o poder de melhorar a qualidade de vida das pessoas e gerar processos mais eficientes, os "empurrõezinhos"[595] por ele proporcionados podem também ser utilizados para fins não tão benéficos e, por vezes, enganosos ou abusivos.[596] Diante dessa lógica, de forma a orientar as organizações e suas operações práticas, o Information Commissioner's Office (ICO) desenvolveu interessante checklist[597] para analisar as condições de tratamento de dados pessoais aplicadas, devendo o controlador assinalar sim ou não para:

a) Consideramos as questões de proteção de dados como parte do projeto e da implementação de sistemas, serviços, produtos e práticas comerciais.

b) Tornamos a proteção de dados um componente essencial da funcionalidade central de nossos sistemas e serviços de processamento.

c) Antecipamos riscos e eventos que invadam a privacidade antes que eles ocorram e tomamos medidas para prevenir danos a indivíduos.

d) Só tratamos os dados pessoais de que necessitamos para o(s) nosso(s) propósito(s) e só os usamos para esses fins.

e) Asseguramos que os dados pessoais são protegidos automaticamente em qualquer sistema de TI, serviço, produto e / ou prática comercial.

---

[594] LEMOS, Ronaldo; BRANCO, Sérgio. Privacy by design: conceito, fundamentos e aplicabilidade na LGPD. In: Bruno Bioni, Laura Schertel Mendes, Danilo Doneda, Otavio Luiz Rodrigues Jr., Ingo Wolfgang Sarlet. (Org.). *Tratado de Proteção de dados pessoais*. 1ed. Rio de Janeiro: Forense, 2021. E-book.

[595] THALER, Richard H.; SUNSTEIN, Cass R. *Nudge*: Improving Decisions about Health, Wealth and Happiness. New Haven: Yale University Press, 2008.

[596] HARTZOG, Woodrow. *Privacy's Blueprint*: the battle to control the design of new technologies. Cambridge: Harvard University Press, 2018.

[597] ICO. Data protection by design and default. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/> Acesso em: 03.08.21.

f) Fornecemos a identidade e as informações de contato dos responsáveis pela proteção de dados.

g) Adotamos uma política de "linguagem simples" para todos os documentos públicos, para que os indivíduos entendam facilmente o que estamos fazendo com seus dados pessoais.

h) Fornecemos ferramentas para que as pessoas possam determinar como estamos usando seus dados pessoais e se nossas políticas estão sendo devidamente aplicadas.

i) Oferecemos fortes padrões de privacidade e controles amigáveis. Respeitamos as preferências do usuário.

j) Só usamos operadores[598] de dados que fornecem garantias suficientes de suas medidas técnicas e organizacionais para a proteção de dados por design.

k) Quando usamos outros sistemas, serviços ou produtos em nossas atividades de tratamento nos certificamos de usar apenas aqueles cujos designers e fabricantes levam em consideração as questões de proteção de dados.

l) Usamos tecnologias que aumentam a privacidade (*privacy-enhancing technologies* - PETs)[599] para nos auxiliar no cumprimento de nossas obrigações de proteção de dados.

Simone Van Der Hof e Eva Lievens [600] afirmam que a inclusão dos princípios de *data protection by default* e *data protection by design* no GDPR representa inovação regulatória que deve aumentar a proteção de crianças e adolescentes. Eles podem

[598] O controlador só deve usar e celebrar contratos com operadores que forneçam garantias suficientes para implementar medidas técnicas e organizacionais adequadas, de modo que o processamento cumpra os requisitos legais.

[599] "Privacy-enhancing technologies or PETs are technologies that embody fundamental data protection principles by minimising personal data use, maximising data security, and empowering individuals. A useful definition from the European Union Agency for Cybersecurity (ENISA) refers to PETs as: 'software and hardware solutions, ie systems encompassing technical processes, methods or knowledge to achieve specific privacy or data protection functionality or to protect against risks of privacy of an individual or a group of natural persons.' PETs link closely to the concept of privacy by design, and therefore apply to the technical measures you can put in place. They can assist you in complying with the data protection principles and are a means of implementing data protection by design within your organisation on a technical level." (ICO. Data protection by design and default. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/> Acesso em: 03.08.21.)

[600] VAN DER HOF, Simone; LIEVENS, Eva. The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data under the GDPR. *Communications law*, edited by Paul Wragg, vol. 23, n. 1, 2018, p. 33-43. Disponível em: <https://ssrn.com/abstract=3107660> Acesso em: 04.08.21

garantir que a proteção de dados se torne parte integrante dos sistemas de tratamento e fornecem oportunidades para integrar direitos de controle sobre os dados pessoais nas operações dos sistemas, tornando-os potencialmente mais transparentes e eficazes. Obviamente, o impacto desses princípios depende muito da maneira como eles serão implementados e, até que ponto, os responsáveis serão capazes e estarão dispostos a moldar com eficácia os arranjos de proteção de dados na arquitetura dos sistemas.

Alguns direitos dos titulares de dados, sendo manifestações expressas dos princípios de tratamento[601] aos quais o Artigo 25 do GDPR se refere, têm claramente uma importância particular em relação aos menores, como, por exemplo, o direito à transparência no tratamento de informações (Artigos 12, 13 e 14 do GDPR)[602], o direito de não ser submetido a criação de perfil[603] e o direito ao apagamento (Art. 17 do GDPR). Segundo as autoras[604], dada a vulnerabilidade da criança e do adolescente, o direito ao apagamento é considerado especialmente importante no que diz respeito aos dados pessoais tratados enquanto o titular ainda era menor.[605] O direito ao apagamento é baseado na ideia de que os indivíduos devem ter controle sobre seus dados pessoais e é frequentemente formulado com base no argumento da "ficha limpa": quaisquer que

[601] Como, por exemplo, legalidade, justiça e transparência; limitação de propósito; minimização de dados; precisão; limitação de armazenamento; e integridade e confidencialidade.

[602] Considerando n. 58 do GDPR: "(...) Uma vez que as crianças merecem proteção específica, sempre que o tratamento lhes seja dirigido, qualquer informação e comunicação deverá estar redigida numa linguagem clara e simples que a criança compreenda facilmente."

[603] "(...) under the GDPR, data subjects, in principle, have the right not to be subject to automated individual decision-making, including profiling (Article 22).31 Although Article 22 does not explicitly refer to children, Recital 71 states that '[s]uch a measure should not concern a child'. Given that it refers to 'measure' as 'evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her', we can assume that profiling is meant. As a consequence, *organisations need to distinguish between children and adults when profiling data subjects leading to decisions that produce legal effects or similarly significantly affects them, assuming that profiling is otherwise in compliance with data Protection regulation. Data processing processes can thus be designed in ways that automatically rule out personal data which holds attributes pertaining to persons under eighteen as well as refrain from applying the results of profiling processes to these persons.*" (VAN DER HOF, Simone; LIEVENS, Eva. The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data under the GDPR. *Communications law*, edited by Paul Wragg, vol. 23, n. 1, 2018, p. 33–43.) (grifou-se)

[604] VAN DER HOF, Simone; LIEVENS, Eva. The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data under the GDPR. *Communications law*, edited by Paul Wragg, vol. 23, n. 1, 2018, p. 33-43.

[605] De acordo com o considerando n. 65 do GDPR, este direito é relevante, em particular, quando o titular dos dados deu o seu consentimento quando menor, não estando totalmente ciente dos riscos envolvidos no tratamento, e posteriormente deseja remover esses dados pessoais, especialmente na Internet. O titular dos dados poderá - como regra - exercer tal direito, apesar de não ser mais menor.

sejam os erros durante a fase de crescimento, eles não devem assombrar a pessoa até a idade adulta.

Um relatório de impacto é uma ferramenta que o agente pode utilizar para identificar e reduzir os riscos à proteção de dados em suas atividades de tratamento. Ele também pode ajudá-lo a projetar processos mais eficientes para o tratamento de informações pessoais. É parte integrante da proteção de dados por design e por padrão, podendo determinar as medidas técnicas e organizacionais de que você precisa para garantir que seu tratamento esteja em conformidade com o ordenamento jurídico.

4.1.2 Hipóteses de desenvolvimento do relatório de impacto à proteção de dados pessoais

No Brasil, a LGPD dispõe acerca do relatório de impacto à proteção de dados pessoais[606] (RIPD), sendo ele reconhecido como boa prática, especialmente quando há alto risco no tratamento de dados, e instrumento de conformidade e prestação de contas em diversos tratamentos de dados. Ele faz parte do processo de gestão de riscos e evita a perda de confiança e reputação do agente de tratamento. Operações que envolvem dados sensíveis, especialmente dados genéticos, de saúde e biométricos, são comumente consideradas de alto risco, por exemplo.

A feitura do relatório não é, como regra, obrigatória[607] ao agente de tratamento nos fluxos de dados que realiza. Contudo, dispõe a LGPD que a Autoridade Nacional (ANPD) poderá determinar ao controlador que elabore relatório de impacto referente as suas operações de tratamento de dados, nos termos de regulamento editado pela própria,

---

[606] QUELLE, Claudia. Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability-and Risk-based Approach, *European Journal of Risk Regulation*, 9, p. 502-526. 2018. KORFF, Douwe. GDPR Requirements on Data Protection Impact Assessments & Methodologies for DPIAs. Jul. 2020. Disponível em: <https://ssrn.com/abstract=3656234 > Acesso em: 21.08.21.

[607] Caso em que o RIPD é obrigatório encontra-se disposto no Art.4º, § 3º, da LGPD, que dispõe que: A Autoridade Nacional de Proteção de Dados emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais. As hipóteses de tratamento de dados do inciso III envolvem segurança pública; defesa nacional; segurança do Estado; ou atividades de investigação e repressão de infrações penais.

observados os segredos comercial e industrial.[608] Segundo o Art. 55-J, XIII, compete à ANPD "editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar *alto risco* à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei".

Em razão disso, a ANPD promoveu no início de 2021 reunião técnica acerca da temática. Em última instância, o relatório encontra-se relacionado à avaliação e ao gerenciamento de riscos no tratamento de informações pessoais. Há, portanto, um debate necessário que envolve o que é risco, seus graus e em quais casos haverá obrigatoriedade da produção do relatório. Questiona-se: como será possível identificar previamente os riscos envolvidos na operação e, em seguida, classificá-los até o nível de alto risco? Não há uma indicação na LGPD sobre operações de tratamento que envolvam ou que possam implicar alto risco, restando à ANPD – que deverá analisar de forma contínua o assunto[609] e trazer diretrizes para o tema, além de rol exemplificativo de situações em que o documento deverá ser elaborado – e aos controladores, por meio de análise e classificação interna de riscos, desenvolverem métodos, parâmetros, métricas e matrizes de risco. Com isso, será possível preparar desde a avaliação de impacto até o relatório em si. Outra questão levantada na reunião versou sobre o porte da instituição que realiza o tratamento de dados.[610] Como regra, o porte não deverá ser utilizado como parâmetro principal para a definição de processo de alto risco nem ser determinante na análise acerca da obrigatoriedade de elaboração do relatório. O foco deve restar na natureza do processo de tratamento de dados, no alto risco envolvido, na qualidade das informações e nos titulares a quem esses dados dizem respeito.

Dentro dos moldes da LGPD, o relatório pode ser definido como a documentação do controlador que contém a descrição dos processos de tratamento de

[608] LGPD, "Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados."

[609] Nesse sentido, recorda-se o capítulo III "Do tratamento de alto risco" da Resolução CD/ANPD nº 2, de 27 de janeiro de 2022.

[610] ANPD. Resolução CD/ANPD nº 2, de 27 de janeiro de 2022 - Aprova o Regulamento de aplicação da Lei nº 13.709/18 para agentes de tratamento de pequeno porte.

dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como as medidas, salvaguardas e mecanismos de mitigação de risco adotados.[611] Ele deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação às medidas, salvaguardas e mecanismos de mitigação de riscos implementados.[612] Ele concretiza os princípios da segurança e prevenção, sendo de grande importância para o compliance do controlador. Entende-se que o documento deverá ser elaborado antes de a instituição iniciar o tratamento de dados: preferencialmente, na fase inicial do programa, projeto ou serviço que tem o propósito de usar esses dados.

Os casos previstos pela LGPD em que o RIPD deverá ou poderá ser solicitado são por exemplo: a) para tratamento de dados pessoais realizado para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (exceções previstas no inciso III do Art. 4º); b) alguns autores[613] entendem, a partir da combinação dos artigos 31 e 32 da LGPD[614] que, quando houver infração dela, em decorrência do tratamento de dados pessoais por órgãos públicos, o relatório também será necessário; c) a qualquer momento sob determinação da

[611] Este documento dialoga diretamente com a seguinte norma técnica: ABNT NBR ISO/IEC 29134:2020 - Tecnologia da informação - Técnicas de segurança - Avaliação de impacto de privacidade. Outra norma relevante no tema é: ABNT NBR ISO/IEC 29151:2020 - Tecnologia da informação - Técnicas de segurança - Código de prática para proteção de dados pessoais.

[612] A elaboração de um RIPD para todas as operações de tratamento de dados pessoais ou de um RIPD para cada projeto, sistema ou serviço deve ser avaliada de forma criteriosa por cada instituição. Por exemplo, uma instituição que realize tratamento de quantidade reduzida de dados, com poucos processos e serviços, pode optar por um RIPD único. Por outro lado, instituição que implemente vários processos e projetos que envolvam o tratamento de expressiva quantidade e diversidade de dados pessoais pode optar por elaborar RIPDs específicos, por ser mais adequado à sua realidade. Fonte: Guia operacional sobre o Relatório de Impacto de proteção de dados <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd> Acesso em: 10.05.21

[613] Guia operacional... op. cit.

[614] 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.

ANPD[615]; e d) quando o tratamento tiver como fundamento o legítimo interesse do controlador (Art. 10, §3º).[616]

Conforme orientação de Guia Operacional para adequação à LGPD[617], o qual aborda o relatório de impacto, é indicada a sua elaboração ou atualização sempre que existir a possibilidade de ocorrer impacto na proteção dos dados pessoais resultante de por exemplo: a) uma tecnologia, serviço ou outra nova iniciativa em que dados pessoais e dados sensíveis sejam ou devam ser tratados; b) rastreamento da localização dos indivíduos ou qualquer outra ação de tratamento que vise à formação de perfil comportamental de pessoa natural, se identificada (LGPD, Art. 12 §2º); c) tratamento de dado pessoal sobre "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (LGPD, Art. 5º, II); e d) tratamento de dados pessoais de crianças e adolescentes (LGPD, Art. 14). No cenário brasileiro, quando se advoga pela ampliação das bases legais para o tratamento de dados pessoais de crianças e adolescentes, o relatório de impacto representa documento essencial para a tutela do melhor interesse dos menores.

No RIPD, o encarregado deve ser consultado durante a sua elaboração, podendo contribuir acerca de pontos como: necessidade de realização do relatório, forma e metodologia para o desenvolvimento do documento, esclarecimentos acerca das salvaguardas (incluindo medidas técnicas e administrativas) a serem aplicadas para atenuar os eventuais riscos para os titulares de dados, orientação acerca da necessidade de se buscar a opinião de terceiros e viabilidade da atividade após a finalização do relatório[618]. Sendo possível e não havendo comprometimento desproporcional da segurança e do segredo dos controladores, em alguns casos será interessante realizar consulta para compreender a opinião e os interesses dos titulares afetados.

No que tange à mitigação dos riscos, é possível mencionar ações como:

---

[615] Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. (...)

[616] Mostra-se necessário distinguir o relatório de impacto à proteção de dados pessoais e o teste de balanceamento realizado antes da seleção da base legal do legítimo interesse para o tratamento de dados pessoais (Art. 7º, IX, LGPD).

[617] Guia operacional... op. cit.

[618] PALHARES, Felipe; PRADO, Luis; VIDIGAL, Paulo. *Compliance digital e LGPD.* São Paulo: Thomson Reuters Brasil, 2021. p.236.

eliminação ou minimização dos dados tratados, treinamento completo dos colaboradores e funcionários, elaboração de avisos de privacidade, desenvolvimento de contratos e termos contendo disposições específicas sobre proteção de dados com terceiros, operadores e funcionários e garantia dos direitos à revogação do consentimento e de oposição ao tratamento pelos titulares.

No Regulamento Geral Europeu de Proteção de Dados, o *Data Protection Impact Assessment* (DPIA) só será obrigatório em operações de tratamento de alto risco. Em seguida, o legislador optou por estabelecer alguns critérios para definir quando haverá a necessidade de realização de uma avaliação de impacto sobre a proteção de dados, verificando-se no Art.35 do GDPR um rol exemplificativo que dispõe sobre algumas atividades de tratamento que podem ensejar riscos elevados aos titulares:

> 1.Quando um tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, puder resultar em um *alto risco* para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento deve, antes do tratamento, efetuar uma avaliação do impacto das operações de tratamento previstas na proteção dos dados pessoais. Uma única avaliação pode abordar um conjunto de operações de processamento semelhantes que apresentam altos riscos semelhantes. Uma única avaliação pode abordar um conjunto de operações de processamento semelhantes que apresentam altos riscos semelhantes. 2. Ao efetuar uma avaliação de impacto sobre a proteção de dados, o responsável pelo tratamento solicita o parecer do encarregado da proteção de dados, nos casos em que este tenha sido designado. 3. A realização de uma avaliação de impacto sobre a proteção de dados a que se refere o n. 1 é obrigatória nomeadamente em caso de: a) Avaliação sistemática e completa dos aspetos pessoais relacionados a pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar; b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9º, n. 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10; ou c) monitoramento sistemático de áreas acessíveis ao público em larga escala. (...)[619]

[619] GDPR, **Article 35 - Data protection impact assessment** 1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks. 2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment. 3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of

Em outras palavras, o GDPR não exige a realização de um *Data Protection Impact Assessment* (DPIA) para todas as operações de tratamento que possam resultar em riscos para os direitos e liberdades das pessoas. A realização de uma DPIA só será obrigatória quando o tratamento "puder resultar em um *alto risco* para os direitos e liberdades das pessoas singulares".[620] Mas como determinar o que representa um "alto risco"? O GDPR e o Article 29 Working Party – conforme disposto nas *Guidelines on Data Protection Impact Assessment* (DPIA)[621] – fornecem alguns exemplos de situações que demandariam um DPIA:

a) Uma extensa avaliação das informações da pessoa, em que as decisões são tomadas com base no tratamento automático e na criação de perfis.

---

special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible area on a large scale. 4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68. 5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board. 6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union. 7. The assessment shall contain at least: (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned. 8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment. 9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations. 10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities. 11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

[620] Necessário interpretar o artigo em conjunto com os considerandos 89, 71, 75 e 91 do GDPR.

[621] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. Adopted on 4 April 2017. As last Revised and Adopted on 4 October 2017. Disponível em: <https://ec.europa.eu/newsroom/article29/items/611236> Acesso em: 23.08.21.

b) Tratamento de categorias especiais de dados (dados sensíveis – Art. 9º do GDPR) ou dados pessoais relacionados com condenações criminais ou infrações (Art. 10 do GDPR). Além dessas disposições do GDPR, algumas categorias de dados quando tratadas podem ser consideradas como suscetíveis de aumentar os riscos para os direitos e liberdades dos indivíduos. Isso porque estão ligadas a atividades privadas (como comunicações eletrônicas, cuja confidencialidade deve ser protegida) ou porque afetam o exercício de um direito fundamental (como dados de localização cuja coleta põe em questão a liberdade de circulação) ou porque a sua violação envolve claramente impactos graves na vida quotidiana do titular dos dados (como dados financeiros que podem ser utilizados para fraude de pagamento).

c) Monitoramento sistemático: tratamento usado para observar, monitorar ou controlar os titulares dos dados, incluindo dados coletados por meio de networks, ou "um monitoramento sistemático de uma área acessível ao público" (Artigo 35 (3) (c)). Esse tipo de monitoramento é um critério porque os dados pessoais podem ser coletados em circunstâncias nas quais os titulares podem não saber quem está coletando seus dados e como eles serão usados. Além disso, pode ser impossível para os indivíduos evitarem a sujeição a tal tratamento em espaços públicos (ou acessíveis ao público). Exemplo disso seria usar uma câmera colocada em uma via pública para registrar e monitorar o comportamento de motoristas.

d) Avaliação ou pontuação de indivíduos, incluindo perfis e previsões, especialmente de aspectos relativos ao desempenho da pessoa no trabalho, situação econômica, saúde, preferências ou interesses pessoais, confiabilidade ou comportamento, localização ou movimentos. Exemplos: 1) uma tecnologia que monitora o comportamento do usuário e usa essas informações para construir perfis de marketing; 2) instituição financeira que faz a triagem de seus clientes em um banco de dados de referência de crédito ou em um banco de dados que envolve combate à lavagem de dinheiro, terrorismo ou fraude; 3) empresa de biotecnologia que oferece testes genéticos diretamente aos consumidores para avaliar e prever riscos de doenças; e 4) empresa construindo perfis comportamentais ou de marketing com base no uso ou navegação em seu site.

e) Tomada de decisão automatizada com efeito legal ou significativo na vida dos indivíduos, como, por exemplo, um programa de computador que usa o

histórico de comportamento de condenados para determinar automaticamente se eles devem receber liberdade condicional. O tratamento mencionado pode levar à exclusão ou discriminação de indivíduos. O tratamento com pouco ou nenhum efeito sobre os indivíduos não atende a esse critério específico.

f) Dados da pessoa tratados em grande escala. O GDPR não define o que constitui grande escala, embora o considerando 91 forneça algumas orientações. Em qualquer caso, o WP29 recomenda que os seguintes fatores sejam considerados ao se determinar se o tratamento é realizado em grande escala: a) o número de titulares de dados em questão, seja como um número específico ou como uma proporção da população relevante; b) o volume de dados e/ou a gama de diferentes itens de dados sendo processados; c) a duração ou permanência da atividade de processamento de dados; e d) a extensão geográfica da atividade de processamento. Um exemplo pode ser uma rede social online com milhões de usuários.

g) Conjuntos de dados que foram combinados: como dados provenientes de duas ou mais operações de tratamento de dados realizadas para diferentes fins e / ou por diferentes controladores de dados, de uma forma que excederia as expectativas razoáveis do titular dos dados.

h) Dados relativos a titulares vulneráveis. Exemplo: menores de idade, empregados, segmentos mais vulneráveis da população que requerem proteção especial (pessoas com doenças mentais ou idosos, por exemplo) e, em qualquer caso, quando houver um desequilíbrio na relação entre a posição do titular dos dados e o controlador.

i) Uso inovador ou aplicação de novas soluções tecnológicas ou organizacionais, como, por exemplo, combinar o uso de impressão digital e reconhecimento facial para melhor controle de acesso a ambiente. Isso ocorre porque o uso de tal tecnologia pode envolver novas formas de coleta e uso de dados, possivelmente com um alto risco para os direitos e liberdades dos indivíduos. As consequências pessoais e sociais da implantação de uma nova tecnologia podem ser desconhecidas. Um DPIA ajudará o controlador a compreender e a tratar esses riscos. Por exemplo, certas aplicações de “Internet das Coisas” podem ter um impacto significativo na vida diária e na privacidade das pessoas, exigindo consequentemente um DPIA.

j) Quando o próprio tratamento "impede os titulares dos dados de exercerem um direito ou utilizarem um serviço ou contrato" (artigo 22 e considerando 91, ambos do GDPR). Isso inclui operações de tratamento que visam a permitir, modificar ou recusar o acesso dos titulares dos dados a um serviço ou a entrada em um contrato. Um exemplo disso é quando um banco verifica seus clientes em um banco de dados de referência de crédito para decidir se lhes oferece um empréstimo.

Quanto mais situações – como as narradas acima – estiverem presentes no tratamento, mais provável será que ele represente um alto risco para os direitos e liberdades dos titulares e, portanto, exija uma DPIA. Os critérios narrados – tratados expressamente nas *Guidelines on Data Protection Impact Assessment* – devem servir de parâmetros para a melhor compreensão e aplicação do relatório de impacto no contexto brasileiro.

Importante questão sobre o relatório de impacto envolve a necessidade ou não de sua publicação pelas instituições públicas e privadas. Questiona-se: em caso de publicação alguns elementos deveriam ou poderiam ser retirados da versão pública? Seria possível pensar em três versões do RIPD: uma versão pública (respeitando os segredos comercial e industrial), uma versão interna e uma versão para a ANPD e demais instituições? Não há na LGPD norma que imponha a publicação do relatório, cabendo à ANPD regulamentar essa questão. É possível, porém, pensar na publicização de uma versão do referido documento como uma boa prática em termos de prestação de contas e transparência,[622] permitindo a participação pública no debate relativo à definição dos riscos e às formas de tratamento de dados. No que concerne às instituições públicas, vale lembrar que a questão do relatório deverá ser analisada também

[622] Em setembro de 2020, o Banco Central do Brasil publicou relatório de impacto à proteção de dados pessoais. "Este documento demonstra, em linhas gerais, como os dados pessoais são coletados, tratados, usados, compartilhados, bem como as medidas adotadas para o tratamento dos riscos que possam afetar as liberdades civis e os direitos fundamentais dos titulares desses dados. Além disso, foram apresentadas informações que denotam o estágio atual de conformidade do BCB à LGPD. Este Relatório será revisto e atualizado anualmente ou sempre que a Instituição implementar qualquer tipo de mudança que afete o tratamento dos dados pessoais. O BCB preocupa-se em avaliar continuamente os riscos de tratamento de dados pessoais que surgem em consequência do dinamismo das transformações nos cenários tecnológico, normativo, político e institucional." Disponível em: <https://www.bcb.gov.br/content/acessoinformacao/lgpd_docs/relatorio_de_impacto_a_protecao_de_dados_pessoais.pdf> Acesso em: 21.08.21.

observando-se a Lei de Acesso à Informação e os princípios constitucionais da Administração Pública, como o da publicidade.[623]

Observa-se que, no Brasil, relatórios de impacto não são figuras desconhecidas. No Direito ambiental, há a previsão do Estudo de Impacto Ambiental (EIA) — instrumento da Avaliação de Impacto Ambiental (AIA) — para o planejamento ambiental, avaliação de impactos e delimitação de área de influência. Ele define mecanismos de compensação e de mitigação dos resultados em decorrência da implantação de atividades de grande potencial poluidor e modificação do meio ambiente, conforme o Art. 2º da Resolução Conama nº 01/86. As principais informações contidas no EIA, bem como sua conclusão, devem ser destacadas no Relatório de Impacto Ambiental (RIMA), em linguagem clara e objetiva, de modo a se compreender as vantagens e desvantagens do projeto, assim como todas as consequências ambientais de sua implementação. Respeitado o sigilo industrial, o RIMA será acessível ao público.

Recorda-se, ainda, a análise de impacto regulatório (AIR) definida no Art. 2º, inciso I, do Decreto nº 10.411/20[624], como: "procedimento, a partir da definição de problema regulatório, de avaliação prévia à edição dos atos normativos de que trata este Decreto, que conterá informações e dados sobre os seus prováveis efeitos, para verificar a razoabilidade do impacto e subsidiar a tomada de decisão". Ela é compreendida como instrumento que contribui significativamente para a melhoria da qualidade regulatória e representa apoio para decisão acerca de intervenção ou não em determinado setor. Pode ser conceituada como: "metodologia que sistematiza a análise do tema, a coleta e a análise dos dados; identifica alternativas comparando seus custos e benefícios; e aborda o impacto de cada alternativa."[625] Deve ter linguagem clara, mas técnica, com exaustiva abordagem sobre o tema, havendo tanto a participação dos grupos afetados no debate quanto a comunicação de seus resultados.

---

[623] Na Holanda, o governo realizou a publicação de relatórios relativos ao Google Workspace, em razão de seu uso. (**DPIA report** data processing in Google G Suite Enterprise (now: Google Workspace). Data de publicação: 9 de julho de 2020, com atualização em 12 de fevereiro de 2021. Status: público. Disponível em: <https://www.rijksoverheid.nl/documenten/publicaties/2021/02/12/google-workspace-dpia-for-dutch-dpa> Acesso em: 21.08.21.)

[624] Regulamenta a análise de impacto regulatório, de que tratam o art. 5º da Lei nº 13.874, de 20 de setembro de 2019, e o art. 6º da Lei nº 13.848, de 25 de junho de 2019.

[625] Guia para elaboração de análise de impacto regulatório (AIR). Secretaria de advocacia da concorrência e competitividade. 2021. p. 23. Disponível em: <https://www.gov.br/economia/pt-br/acesso-a-informacao/reg/noticias/seae-lanca-novo-guia-de-analise-de-impacto-regulatorio> Acesso em: 21.08.21.

Verifica-se, assim, que o relatório de impacto à proteção de dados pessoais e seu futuro regulamento dispõem de relevantes fontes e experiências para orientar a sua elaboração. É documento de grande relevância quando houver no tratamento de dados alto risco para os direitos, interesses e liberdades dos titulares, o que torna a sua feitura em situações que envolvem dados sensíveis uma estratégia bastante alinhada com os princípios da LGPD e boas práticas consagradas internacionalmente.

4.2 Gestão de riscos e mitigação de incidentes de segurança

Analisar e gerenciar riscos representam fundamentos para os sistemas de compliance, mostrando-se ações estratégicas e que devem estar presentes em todas as tomadas de decisão. A partir dessa prática, busca-se medir a probabilidade que uma ameaça tem de "explorar" determinada situação ou vulnerabilidade de uma instituição, trazendo perdas, danos e/ou prejuízos. Age-se na direção de identificar, prevenir, controlar e/ou minimizar possíveis riscos enfrentados pela organização, por meio de atividades coordenadas.

Durante o processo, mostra-se relevante definir critérios para analisar a importância dos riscos na estrutura da organização (havendo, então, o estabelecimento de matriz de risco), incluindo a definição de como a probabilidade, o impacto e os níveis de risco serão estimados, assim como para estabelecer diretrizes para avaliar e priorizar determinados riscos e selecionar as respostas mais apropriadas para tratá-los. Em seguida, sugere-se a implementação de procedimentos para monitorar a ocorrência de riscos e a eficácia das respostas adotadas, bem como para reportar às instâncias de governança o desempenho do processo de gestão e os aspectos que necessitam ser aperfeiçoados.[626] Todos os processos implementados deverão ser devidamente registrados. Recomenda-se também uma ampla comunicação sobre

[626] Tribunal de Contas da União. *10 passos para a boa gestão de riscos*. Brasília: TCU, Secretaria de Métodos e Suporte ao Controle Externo (Semec), 2018. p. 19. ENISA. European Union Agency for Network and Information Security. *Recommendations for a methodology of the assessment of severity of personal data breaches.* Working Document, December 2013. Disponível em: <https://www.enisa.europa.eu/publications/dbn-severity> Acesso em: 09.01.21. U.S. Department of Justice Cybersecurity Unit. *Best Practices for Victim Response and Reporting of Cyber Incidents*. Version 2.0 (September 2018).

assuntos relacionados a riscos, que deverá assegurar que tanto os responsáveis pela implantação do processo de gestão quanto as demais partes interessadas (internas e externas) compreendam o contexto, as decisões tomadas e as ações necessárias.

Com base em metodologias e melhores práticas no tema, doutrina destaca algumas etapas consideradas fundamentais:

> 1) conhecer a empresa; 2) conhecer seu ambiente legal e suas obrigações de *compliance*; 3) realizar entrevistas e análise de documentos; 4) fazer testes e checagem dos dados levantados; 5) identificar riscos e fatores de risco; 6) realizar avaliação de probabilidade; 7) desenvolver matriz de riscos; 8) realizar monitoramento. A avaliação de riscos conecta-se com o sistema de gestão de *compliance* de maneira essencial, dado que tanto o escopo quanto o projeto de implantação do sistema de gestão de *compliance* são construídos a partir da avaliação de riscos.[627]

Dentro de uma abordagem que avalie e faça a gestão de riscos[628], mostra-se necessário estabelecer um processo para ser utilizado quando da verificação de incidentes de segurança. Para tanto, cabe recordar alguns *frameworks* regulatórios baseados em melhores práticas e normas técnicas (como as normas da ISO: *International Organization for Standardization*)[629], que especificam requisitos e fornecem controles e diretrizes para a implantação e o desenvolvimento de sistemas de gestão de segurança da informação e de proteção de dados.

---

[627] SAAVEDRA, Giovani Agostini. Compliance de dados. In: Bruno Bioni, Laura Schertel Mendes, Danilo Doneda, Otavio Luiz Rodrigues Jr., Ingo Wolfgang Sarlet (Org.). *Tratado de Proteção de dados pessoais*. 1ed.Rio de Janeiro: Forense, 2021, v. 1, p. 729.

[628] A norma técnica ABNT NBR ISO 31.000 apresenta processo de gerenciamento bem delimitado. Além dela, mostra-se relevante também o estudo dos documentos desenvolvidos pelo COSO, *Committee of Sponsoring Organizations of the Treadway Commission*, que publicou em 2017 modelo de gestão de riscos chamado de *Enterprise Risk Management—Integrating with Strategy and Performance* (Gerenciamento de Riscos Corporativos integrado com a Estratégia e o Desempenho), buscando ressaltar a importância de se considerar os riscos tanto no estabelecimento da estratégia quanto na condução do desempenho.

[629] Cabe recordar algumas normas relevantes baseadas em melhores práticas: ABNT NBR ISO/IEC 27.001:2013 - Sistema de gestão de Segurança da Informação – Requisitos; ABNT NBR ISO/IEC 27.002:2013 - Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da Segurança da Informação; ABNT NBR ISO/IEC 27.005:2011 - Gestão de Riscos de Segurança da Informação; ABNT NBR ISO/IEC 27.003:2011 - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Orientações; ABNT NBR ISO/IEC 27701:2020 - Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes; ABNT NBR ISO/IEC 29100:2020 - Tecnologia da informação — Técnicas de segurança — Estrutura de Privacidade; ISO/IEC 27035-1:2016 - Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management; e ISO/IEC 27035-2:2016 - Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response.

Seguir tais orientações é relevante diante do mandamento legal (Art. 49 da LGPD) que dispõe que os sistemas utilizados para o tratamento de dados devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios[630] gerais previstos na LGPD e nas demais normas regulamentares. Conforme dispõe expressamente o Art. 47 da LGPD, os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término. Portanto, orienta-se que o agente atue no sentido de:

a) Designar um Comitê de Segurança da Informação, com experts das áreas técnica, jurídica e da comunicação, e implementar uma Política de Segurança da Informação[631], que estabeleça diretrizes sobre padrões e medidas técnicas internas de segurança.

b) Conscientizar os funcionários por meio de treinamentos e de campanhas de conscientização sobre suas obrigações e responsabilidades relacionadas ao tratamento de dados pessoais.

c) Criar um ambiente que incentive usuários de sistemas da empresa, como clientes, parceiros e funcionários, a informar incidentes e vulnerabilidades detectadas.

d) Controlar os acessos (em processos de autenticação, autorização e auditoria), como medida técnica para garantir que os dados sejam acessados somente por pessoas autorizadas.

---

[630] A LGPD traz em seu art. 6º, inciso VII, o Princípio da Segurança que preconiza a "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão".

[631] "A política de segurança da informação - PSI, consiste em um conjunto de diretrizes e regras que tem por objetivo possibilitar o planejamento, a implementação e o controle de ações relacionadas à segurança da informação em uma organização. 22. Essa política pode ser endereçada por organizações de qualquer porte e compreende uma boa prática para a gestão da segurança. Muito embora não seja obrigatória, a elaboração dessa política e sua implementação são incentivadas pela ANPD aos agentes de tratamento de pequeno porte porque evidenciam boa-fé e diligência na segurança dos dados pessoais sob sua custódia e fornecem as diretrizes para a gestão da segurança da informação. (...) a ANPD sugere que, quando possível, seja estabelecida pela organização uma política de segurança da informação, ainda que simplificada, com previsão de revisão periódica e que contemple controles relacionados ao tratamento de dados pessoais, como por exemplo, cópias de segurança; uso de senhas; acesso à informação; compartilhamento de dados; atualização de softwares; uso de correio eletrônico; uso de antivírus, entre outros." (ANPD. Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte Outubro/2021. p.08)

e) Gerenciar senhas adequadamente, usando autenticação multifator, e seguir o princípio do menor privilégio: os usuários de um sistema terão o menor nível de acesso necessário para a realização de suas atividades.

f) Gerenciar contratos, havendo a assinatura, inclusive, de termos de confidencialidade (*non-disclosure agreement*) com funcionários e parceiros, assim como aquisições, para que haja atenção à distribuição de funções e responsabilidades entre as partes. No caso de agentes que terceirizam os serviços de TI, recomenda-se que estabeleçam com os fornecedores contratos que incluam cláusulas de segurança da informação.

g) Desenvolver um Plano de Resposta a Incidentes de Privacidade e Remediação.

h) Quando possível, havendo o armazenamento de dados sensíveis, implementar soluções que dificultem a identificação do titular, como técnicas de pseudonimização e criptografia.

i) Trabalhar a segurança das comunicações internas e externas, diante de possíveis vulnerabilidades no processo de transmissão de dados ou informações, como, por exemplo, se houver troca de links maliciosos ou se o usuário receber algum arquivo infectado. Destaca-se, assim, a relevância de se utilizar conexões cifradas (com uso de TLS/HTTPS) ou aplicativos com criptografia fim a fim. Havendo dados sensíveis ou confidencias, sugere-se que os e-mails sejam cifrados ou, opcionalmente, que os arquivos sejam cifrados para envio. [632]

j) Gerenciar o tráfego de rede e manter programa de gerenciamento de vulnerabilidades, havendo o monitoramento da existência de novas versões e correções disponíveis em todos os sistemas e aplicativos.

k) Contratar provedores de serviço de computação em nuvem que observem e implementem as recomendações internacionais e as boas práticas de segurança da informação e proteção de dados.

O GDPR prevê, textualmente, o conceito de "violação de dados pessoais"

[632] ANPD. Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte Outubro/2021. p.14. "Outro cuidado importante é remover quaisquer dados sensíveis e outros dados pessoais que estejam desnecessariamente disponibilizados em redes públicas, por exemplo, o site da empresa. Caso o negócio da empresa envolva o tratamento de dados sensíveis (ex. serviços de saúde) recomenda-se criar um canal de acesso restrito para que o cliente acesse essas informações." (ANPD. Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte Outubro/2021. p.15)

(*personal data breach*), em seu artigo 4º, item 12, como "uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento".[633][634]

Uma violação pode ter uma série de efeitos adversos significativos sobre as pessoas, o que pode resultar em danos físicos, materiais ou imateriais. O GDPR explica que isso pode incluir perda de controle sobre os dados pessoais, limitação de direitos, discriminação, roubo de identidade ou fraude, perda financeira, reversão não autorizada de pseudonimização, danos à reputação e perda de confidencialidade de dados. Também pode incluir qualquer outra desvantagem econômica ou social significativa para esses indivíduos. Uma das obrigações mais importantes do controlador de dados é avaliar esses riscos para os direitos e liberdades dos titulares dos dados e implementar medidas técnicas e organizacionais adequadas para resolvê-los.

Acerca da gestão de incidentes de segurança da informação, a ISO/IEC 27701 afirma que convém que a organização estabeleça responsabilidades e procedimentos para a identificação e registro de violações de dados pessoais, assim como relativos à notificação para as partes envolvidas nas violações e autoridades, levando em conta regulamentações e/ou legislações aplicáveis. Segundo a Autoridade Nacional de Proteção de Dados (ANPD),

> Um incidente de segurança com dados pessoais é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais. (...) os agentes de tratamento de dados pessoais devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados

---

633 Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT> Acesso em: 04.10.21.

634 "In its Opinion 03/2014 on breach notification and in its Guidelines WP 250, WP29 explained that breaches can be categorised according to the following three well-known information security principles: "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data. "Integrity breach" - where there is an unauthorised or accidental alteration of personal data. "Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data." (EDPB. *Guidelines 01/2021 on Examples regarding Personal Data Breach Notification.* Adopted on 14 December 2021. Version 2.0)

> e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.[635] [636] [637]

Em caso de um incidente de segurança com dados pessoais, as primeiras medidas a se tomar são: a) avaliar internamente o incidente (sua natureza e tipo; quantidade de titulares de dados afetados; gravidade das consequências do incidente a eles; características especiais dos titulares - se são, por exemplo, menores de idade ou idosos; a facilidade de identificação dos titulares; espécies e quantidade de dados afetados; consequências concretas e prováveis do incidente; e características especiais do controlador - como controladores sujeitos a outros sigilos); b) comunicar ao encarregado da instituição; c) comunicar ao controlador, se você for o operador; d) o controlador comunicar[638] à ANPD e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares[639]; e e) elaborar documentação com a avaliação interna do incidente[640], medidas tomadas e análise de risco.[641]

---

[635] Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca> Acesso em: 10.05.21.

[636] "(...) assim como nem todo incidente de segurança necessariamente envolve vazamento de dados ou comprometimento de todos dos princípios da SI a um só tempo (confidencialidade, integridade, disponibilidade, não-repúdio, autenticidade, privacidade e legalidade), nem todo incidente de segurança, mesmo que envolva dados pessoais, necessariamente implica em responsabilização do agente de tratamento caso este comprove não ter sido negligente ou que a falha de segurança deu-se em virtude de algum fator alheio e aquém de seu controle." (BRAZ JR., Marcilio. Considerações sobre a notificação de incidente de segurança da informação no contexto da lei geral de proteção de dados (e além). *Migalhas*, 1 de fevereiro de 2019. Disponível em: <https://www.migalhas.com.br/depeso/295440/consideracoes-sobre-a-notificacao-de-incidente-de-seguranca-da-informacao-no-contexto-da-lei-geral-de-protecao-de-dados--e-alem> Acesso em: 13.05.21.)

[637] "Logo, sejam os "vazamentos" considerados espécie do gênero "incidente de segurança" - como sugere a ANPD - ou uma categoria sui generis de ilícito relativo a dados pessoais, fato é que sua ocorrência será determinada pela concretude danosa de natureza patrimonial, moral, individual ou coletiva (art. 42), catalisada pela irregularidade da atividade de tratamento, cuja aferição não deverá se pautar por qualquer espécie de culpa, mas pela identificação casuística das situações acidentais ou ilícitas (art. 46) que permitam concluir, a partir de circunstâncias objetivas (art. 44, I a III), que o tratamento realizado, em qualquer de suas etapas, até mesmo após o término (art. 47), não oferece a segurança esperada pelo titular (arts. 44, caput, e 49), e desde que o nexo causal não seja excepcionalmente afastado (art. 43)." (FALEIROS, José Luiz de Moura. O que é, afinal, um "vazamento" de dados? *Migalhas*, publicado em: 10 de setembro de 2021. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/351388/o-que-e-afinal-um-vazamento-de-dados> Acesso em: 04.10.21)

[638] "Enquanto pendente a regulamentação, recomenda-se que após a ciência do evento adverso e havendo risco relevante, a ANPD seja comunicada com a maior brevidade possível, sendo tal considerado a título indicativo o prazo de 2 dias úteis, contados da data do conhecimento do incidente." Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca> Acesso em: 10.05.21

[639] LGPD, "Art. 48 (...) § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo: I - a descrição da natureza dos dados pessoais afetados; II - as informações sobre os titulares envolvidos; III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; IV - os riscos relacionados ao incidente; V - os motivos da demora, no caso de a comunicação não ter sido imediata; e VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do

A ANPD recomenda que os controladores sejam cautelosos, de modo que ocorra a comunicação mesmo nos casos em que houver dúvida sobre a relevância dos riscos e danos envolvidos no caso. Eventual ou comprovada subavaliação dos riscos e danos por parte dos controladores poderá ser considerada descumprimento à LGPD.[642] Embora a responsabilidade e a obrigação pela comunicação à ANPD sejam do controlador, caso sejam apresentadas informações pelo operador, elas serão devidamente analisadas pela Autoridade.

Acerca da notificação, é necessário mapear os agentes internos e externos que deverão ser devidamente avisados, bem como designar previamente equipe interdisciplinar para atuar em tal situação. Recomenda-se também a elaboração de um plano de comunicação tanto interna quanto externa sobre o incidente de segurança, de forma a cumprir a lei, respeitar os direitos dos titulares e proteger a reputação e confiança depositada na empresa. Um seguro com cobertura específica para incidentes de segurança pode ser uma opção interessante, a depender da estrutura da instituição e da atividade desenvolvida.

Atuar de forma preventiva e proativa representa tarefa obrigatória para os agentes de tratamento, já que reduz não só o risco da ocorrência de um incidente, como

---

prejuízo. § 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como: I - ampla divulgação do fato em meios de comunicação; e II - medidas para reverter ou mitigar os efeitos do incidente. § 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los."

Acerca da gestão de incidentes de segurança da informação, a ISO/IEC 27701 afirma que a: "Notificação pode conter detalhes como: —— um ponto de contato onde mais informações podem ser obtidas; —— uma descrição da violação e a probabilidade das consequências; —— uma descrição da violação, incluindo o número de indivíduos envolvidos, bem como o número de registros relacionados; —— medidas tomadas ou planejadas para serem tomadas."

[640] A ISO/IEC 27701 afirma que, quando ocorrer uma violação a dados pessoais, convém que um registro seja mantido com informação suficiente para fornecer um relatório para propósitos forenses e/ou regulatórios, contendo: uma descrição do incidente; período de tempo; consequências do incidente; nome do relator; para quem o incidente foi reportado; passos tomados para resolver incidentes (incluindo a pessoa em questão e os dados recuperados); e o fato de que um incidente resultou em indisponibilidade, perda, divulgação ou alteração de dados. O registro também deve incluir uma descrição do dado pessoal comprometido e, se as notificações forem realizadas, os espaços tomados para notificar aos titulares, agências regulatórias e/ou clientes.

[641] Cf. SOUZA, Carlos Affonso; PADRÃO, Vinicius. Incidentes de segurança e dever de notificação à luz da Lei Geral de Proteção de Dados Pessoais. *In:* SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (coord.). *Caderno Especial*: Lei Geral de Proteção de Dados (PGPD). São Paulo: Revista dos Tribunais, 2019.

[642] No final de 2021, foram publicados pela ANPD materiais de segurança da informação voltados aos agentes de tratamento de pequeno porte. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-guia-de-seguranca-para-agentes-de-tratamento-de-pequeno-porte> Acesso em: 08.01.22.

também minimiza substancialmente vulnerabilidades e prejuízos. Diante de um incidente, há um somatório de prejuízos operacionais com danos reputacionais e financeiros, situação tal que pode se mostrar muito lesiva tanto aos titulares de dados quanto para a instituição. Adicionalmente, cabe ressaltar que uma substancial adoção de medidas de segurança pode significar argumento relevante para questionar eventuais sanções impostas pela ANPD e reduzir indenizações estabelecidas pelo Poder Judiciário.

4.3 Término do tratamento de dados e conservação de dados sensíveis

Diante da principiologia da LGPD, é possível afirmar que os dados deverão ser conservados durante o mínimo de tempo possível, observando-se os princípios da transparência, finalidade e necessidade. Este período deve levar em conta os motivos pelos quais o agente precisa efetuar o tratamento dos dados e ter respaldo em uma base ou hipótese legal da LGPD e/ou outras leis ou regulamentos, como, por exemplo, obrigações trabalhistas, fiscais ou antifraude. No momento de analisar a viabilidade ou necessidade de exclusão de um dado, o agente deverá considerar as bases legais de tratamento. Se a informação pessoal for essencial para que o serviço seja prestado ou houver um dever de conservação, por exemplo, pode ser que o dado não seja removido, enquanto gozar de tal qualidade.

A fim de garantir que os dados pessoais não sejam mantidos por mais tempo do que o necessário, o responsável pelo tratamento deve estabelecer prazos para o apagamento ou revisão dos dados conservados, desenvolver políticas de retenção e de eliminação de dados pessoais[643], adotar medidas técnicas e organizativas adequadas e

[643] Acerca do descarte de dados pessoais, a ISO 27701 dispõe que: "Convém que a organização tenha políticas, procedimentos e/ou mecanismos documentados para o descarte de DP. **Diretrizes para implementação**. A escolha das técnicas de descarte do DP depende de um número de fatores, uma vez que uma técnica de descarte difere nas suas propriedades e resultado (por exemplo, na granularidade da mídia física resultante, ou a capacidade para recuperar uma informação excluída de uma mídia eletrônica). Fatores a considerar ao escolher uma técnica de descarte apropriada incluem, porém não estão limitados a, a natureza e a abrangência do DP a ser descartado, se existe ou não um metadado associado ao DP, e as características físicas da mídia na qual o DP é armazenado. (...) Convém que a organização desenvolva e implemente uma política quanto ao descarte de DP e convém tornar esta política disponível

garantir que os dados que possuem são exatos e atualizados.[644] Todas as medidas razoáveis devem ser tomadas para garantir que os dados pessoais inexatos sejam retificados ou excluídos. Os dados pessoais devem ser tratados buscando-se garantir segurança e confidencialidade, de forma a se evitar acessos não autorizados ou utilizações indevidas dos dados.

Acerca do tema, o considerando 39 do GDPR afirma que deverá ser transparente para as pessoas que os dados pessoais que lhes dizem respeito são coletados, utilizados, consultados e/ou sujeitos a outros tratamentos e em que medida os dados pessoais são ou serão tratados. O princípio da transparência exige que as informações e comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, além de formuladas em uma linguagem clara e simples. Esse princípio preconiza que devem ser encaminhadas aos titulares a identidade do responsável pelo tratamento e seus objetivos, bem como informações para a garantia de um tratamento justo e transparente, no que diz respeito às pessoas naturais em causa e ao direito delas de obterem confirmação e comunicação das informações que estão sendo tratadas. As pessoas devem ser informadas sobre os riscos, regras, garantias e direitos em relação ao tratamento de dados, bem como acerca de como exercer os seus direitos em relação a um tratamento. Os fins específicos para os quais os dados pessoais serão tratados devem ser explícitos, legítimos e determinados no momento da coleta dos dados. Os dados pessoais devem ser adequados, relevantes e limitados ao necessário para os fins aos quais serão tratados. Deve-se, assim, assegurar que o período durante o qual os dados pessoais serão armazenados seja limitado ao mínimo possível. Observa-se que, na forma do artigo 9º da LGPD, o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva

---

para o cliente quando solicitado. Convém que a política cubra o período de retenção para DP antes do seu descarte, e depois do encerramento de um contrato, para proteger um cliente da perda de DP por meio de um lapso acidental de um contrato."

[644] Como exemplo, recorda-se: "A sua empresa/organização é uma agência de recrutamento e, para esse efeito, recolhe CV de pessoas que se encontram à procura de emprego e que lhe pagam uma taxa pelos seus serviços de intermediação. Planeia conservar os dados durante 20 anos e não toma medidas que prevejam a atualização dos CV. O período de conservação não parece ser proporcional à finalidade de encontrar emprego para uma pessoa a curto/médio prazo. Além disso, o facto de não solicitar atualizações dos CV a intervalos regulares torna algumas das pesquisas inúteis para o candidato a emprego após um determinado período de tempo (por exemplo, porque a pessoa pode entretanto ter adquirido novas qualificações)." Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_pt> Acesso em: 04.10.21

acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: I - finalidade específica do tratamento; II - forma e duração do tratamento, observados os segredos comercial e industrial; (...).[645]

A respeito do término do tratamento dos dados pessoais, de sua eliminação e possível conservação, a LGPD apresenta seção específica, que envolve dados pessoais sensíveis ou não e dialoga profundamente com o capítulo da lei referente aos direitos dos titulares.[646] Dispõe o Art. 15 da LGPD acerca das hipóteses para o término do tratamento de dados pessoais[647], ou seja, acerca das situações que ensejarão a sua eliminação/exclusão.[648] Na lei, fala-se em eliminação, e não em "apagamento" como o faz o GDPR, ao dispor sobre o *right to erase* (Art. 17 - Direito ao apagamento dos dados). As hipóteses do Art. 15 da LGPD, que não são cumulativas, poderão ser flexibilizadas pelas normas do Art.16, as quais serão mais a frente analisadas.

A primeira hipótese se dá com a verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada. O princípio da finalidade no caso é aplicado diretamente. Como exemplo, destaca-se que depois de um indivíduo cancelar seu plano

---

[645] Art. 8º, §6º, da LGPD: "Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração."

[646] É importante observar que o Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014) também dispõe sobre a questão, especialmente nos artigos: a) "Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: (...) X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais; (Redação dada pela Lei nº 13.709, de 2018)" b) "Art. 14. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet." c) "Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento. (...)" d) "Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda: I - dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7º; ou II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais."

[647] Art. 15 da LGPD: "O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses: I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; II - fim do período de tratamento; III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei."

[648] Por eliminação (Art.5º, XIV), entende-se a "exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado".

em uma academia, ela não precisará mais manter dados sensíveis dele referentes a acesso à unidade (como dado biométrico de impressão digital). Respeita-se, aqui, a função (para que serve) do tratamento de dados.

A segunda hipótese aborda o fim do período de tratamento, de forma que, cumprido o período especificado para o tratamento, os dados não mais poderão ser tratados. Esse período costuma ser apresentado, por exemplo, em políticas de retenção e descarte de dados pessoais, as quais apresentam basicamente o período máximo de retenção por categoria de registro, formas de controle de prazos e finalidades, descrição das atividades e formas de descarte.

A terceira traz a comunicação pelo titular, inclusive no exercício de seu direito de revogação do consentimento (conforme disposto no §5º, do Art. 8º, da LGPD[649]), resguardado o interesse público. No referido caso, há o pedido expresso de eliminação por parte do titular do dado, havendo, porém, a proteção ao interesse público. A mencionada hipótese traz questões como: havendo a revogação do consentimento para o tratamento o pedido de eliminação estará implícito? Quem poderá alegar a existência de interesse público? Quais parâmetros e critérios deverão ser demonstrados para que se demonstre o interesse público? A organização pode cobrar uma taxa em determinados casos para atender o pedido do titular? O que ele poderá fazer se a organização não responder ou se não estiver satisfeito com o resultado do procedimento? Em diálogo com o inciso III do Art.15, recorda-se o Art. 18 da LGPD que afirma que o titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei (inciso IV) e eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no Art. 16 desta Lei (inciso VI). Por fim, no inciso IV do Art.15, o término do tratamento de dados pessoais poderá ocorrer por determinação da Autoridade Nacional de Proteção de Dados (ANPD), quando houver violação ao disposto na LGPD. Isso complementa uma das possibilidades de sanção administrativa imposta pela ANPD, conforme dispõe o Art. 52, inciso VI: os agentes de tratamento de dados, em razão das

[649] Art. 8º, §5º, da LGPD: "O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei."

infrações cometidas às normas previstas na LGPD, ficam sujeitos à eliminação dos dados pessoais a que se refere a infração. Observa-se que, conforme o Art. 18, §6º, da LGPD, o responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional. Acerca do compliance para o término do tratamento de dados, Guedes e Meireles[650] ensinam que:

> O programa de compliance precisa ter regras expressas e muito claras para orientar como deve ocorrer o encerramento do tratamento de dados e como deve se dar o seu descarte, prevendo também as sanções para o caso de descumprimento. Com isso, o próprio programa poderá criar o *standard* de conduta que deverá ser sempre observado no encerramento do tratamento e, posteriormente, no momento em que haverá o descarte dos dados, prevenindo potenciais situações lesivas. Quanto mais precisas e claras forem as regras, mais efetivo será o programa; quanto mais suas regras e medidas preventivas forem observadas, menor será o risco de ocorrer algum incidente de segurança. (...) A ausência de normas de conduta que indiquem procedimentos para o término do tratamento de dados certamente poderá acarretar infrações à LGPD, na medida em que a eliminação constitui consequência resultante do próprio término. Assim, se no âmbito da gestão não for possível delimitar quando ocorre o término, também não haverá a eliminação dos dados, a configurar infração administrativa, além de outras sanções. [651]

Conforme guia publicado pela autoridade dinamarquesa de proteção de dados[652] sobre a minimização de dados e o direito ao apagamento, os controladores de dados devem desenvolver procedimentos de exclusão para sistemas onde os dados sejam tratados, bem como implementar procedimentos de acompanhamento para garantir a exclusão dos mesmos. Para fins de prestação de contas, os controladores podem manter registro das solicitações recebidas.

Além disso, a autoridade dinamarquesa destaca que os dados pessoais devem ser excluídos dos backups, se tecnicamente possível. Se isso não for, o controlador deve

---

[650] GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau. A importância do compliance para o término do tratamento de dados. In: Ana Frazão; Ricardo Cueva (Coord). *Compliance e políticas de proteção de dados.* São Paulo: Thomson Reuters Brasil, 2021. p.245-268.

[651] GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau. A importância do compliance para o término do tratamento de dados. In: Ana Frazão; Ricardo Cueva (Coord). *Compliance e políticas de proteção de dados.* São Paulo: Thomson Reuters Brasil, 2021. p.257-259.

[652] Disponível em: <https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/sikkerhed-/sletning/sletning-emne> Acesso em: 05.01.22.

garantir que os dados excluídos do sistema também sejam removidos se um backup for restabelecido. Portanto, pode ser necessário manter um registro das exclusões realizadas no sistema em operação, em relação ao momento em que o backup foi realizado. Esse registro não deve conter informações de identificação pessoal direta, mas pode indicar, por exemplo, que uma determinada linha de uma tabela foi excluída em um determinado momento.[653]

Nesse quadro, pergunta recorrente é: como provar a exclusão e o apagamento de dados pessoais? Sobre isso, é possível recordar algumas técnicas de "transparência de exclusão":[654] a) a autodeclaração por parte do agente de tratamento, baseada em sua boa-fé objetiva; b) o registro de metadados da operação com a adoção de medidas para que não seja editável; c) a apresentação de busca "inexistente" para pesquisa sobre o titular, ou seja, havendo pesquisa na base de dados com informações do titular não saem mais referências sobre ele; d) operação assistida e registro da operação de exclusão, o qual deve ser mantido de forma segura, para eventual questionamento judicial ou administrativo; e) registros descentralizados: um terceiro recebe metadados da operação e custodia; e f) contratação de uma eliminação certificada ou de um serviço de perícia ou consultoria para realizar ou acompanhar a exclusão. Na perícia, serão avaliados o ambiente, os processos de exclusão, as bases de dados, a eficácia do processo (levando em conta as tecnologias disponíveis), os registros da época e os indícios de eliminação ou não dos dados.

Dispondo acerca de orientações para agentes de tratamento de pequeno porte sobre segurança da informação, a ANPD destaca que:

> (...) sobre a eliminação de dados pessoais, sugere-se que em todas as mídias que contenham dados pessoais seja executado o método de formatar antes de descartá-las. Quando isso não for possível, como em CDs e DVDs, sugere-se que seja realizada a destruição física da mídia – o que também se aplica para destruição de papel e de mídia portátil para armazenar dados pessoais. 51. Além disso, para os agentes que fazem uso de serviço de terceiros para o descarte, seja de mídia ou registro de papel, sugere-se que seja estabelecido

[653] Afirma-se que, uma vez que o objetivo básico de um backup é ser capaz de recuperar dados, se os dados em um sistema forem perdidos, situações poderão surgir quando - após a exclusão de dados pessoais em um sistema em operação - houver dados pessoais correspondentes armazenados em uma cópia de segurança.

[654] Fonte obtida em aula de José Antonio Milagre. Disponível em: <https://www.youtube.com/watch?v=a6lryiVm998> Acesso em: 04.10.21

> um contrato de serviço com cláusulas de registro da destruição que for realizada.[655]

Por outro lado, acerca da conservação de dados pessoais, dispõe o artigo 16 da LGPD – de forma taxativa[656] e com hipóteses não cumulativas - que os dados serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, sendo autorizada a conservação para as finalidades a seguir.[657]

Em primeiro lugar, cumprimento de obrigação legal ou regulatória pelo controlador. Entende-se que, em tal caso, é possível também incluir o operador, bem como normas internacionais reconhecidas no país e boas práticas consolidadas. Em segundo lugar, estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais (conforme o artigo 12 da LGPD).

Em terceiro lugar, transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na LGPD (especialmente, portanto, os artigos 7º, 11 e 14). A última hipótese refere-se ao uso exclusivo dos dados pelo controlador, vedado seu acesso por terceiro, e desde que sejam anonimizados. Recorda-se que, uma vez anonimizado, o dado deixa de ser dado pessoal, não sendo mais as normas da LGPD diretamente aplicáveis, o que, em tese, permitiria que terceiros tivessem acesso aos dados integralmente anonimizados. O artigo 16 da lei não traz prazo específico para os casos acima, devendo o agente observar os princípios da LGPD.

CONCLUSÃO

[655] ANPD. Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte. Versão 1.0 – outubro/2021. p.14.

[656] GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau. A importância do compliance para o término do tratamento de dados. In: Ana Frazão; Ricardo Cueva (Coord). *Compliance e políticas de proteção de dados.* São Paulo: Thomson Reuters Brasil, 2021. p.252.

[657] Acerca da retenção de dados pessoais, a ISO 27701 dispõe que: **"**Convém que a organização não retenha DP por um tempo maior do que é necessário para os propósitos para os quais o DP é tratado. **Diretrizes para implementação.** Convém que a organização desenvolva e mantenha esquemas de retenção para as informações que ela guarda, considerando o requisito para retenção do DP por um tempo não maior do que é necessário. Convém que estes esquemas considerem requisitos legais, regulamentares e de negócio. Onde ocorrem conflitos com estes requisitos, uma decisão de negócio precisa ser tomada (com base em uma avaliação de riscos) e documentada no esquema apropriado."

No atual cenário tecnológico, marcado pela hiperconectividade e amplo uso de inteligência artificial, os dados pessoais devem necessariamente ser avaliados dentro de uma perspectiva dinâmica e contextual, que considere diversos fatores, possíveis inferências, sujeitos e tratamentos. Há cada vez mais formas de análise que podem identificar indivíduos, criar perfis e revelar dados sensíveis sobre eles e, inclusive, terceiros. A partir de informações pessoais é possível conhecer hábitos, comportamentos, gostos, preferências, descendência, estado de saúde e crenças de uma pessoa natural. Dados contam histórias, trazem conexões e permitem sofisticadas associações, o que impõe uma tutela ampla das informações pessoais e atualizada com os avanços científicos e tecnológicos.

Conforme crescem os graus de exposição dos indivíduos e de sua sujeição à vigilância de estruturas tecnológicas, públicas e privadas, verifica-se a relevância de se desenvolver instrumentos que coloquem os direitos fundamentais à proteção de dados e à privacidade em posição de preeminência, em face de situações estritamente patrimoniais. Nessa lógica, cabe destacar a importância de se analisar e conferir tutela ampliada a certas categorias de dados, especialmente os classificados como sensíveis, em razão da qualidade das informações que guardam e de seu uso em situações de discriminação ilícita ou abusiva, em face de seus titulares e grupos, ampliando estereótipos e segregações. A tutela de informações sensíveis mostra-se, portanto, vital para que a pessoa humana se realize integralmente e se relacione, com liberdade e em condições de igualdade, na sociedade. Representa, também, garantia de maior segurança aos dados e age impedindo práticas discriminatórias e de vigilância em massa.

Diante disso, a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/18) representa instrumento normativo fundamental para a proteção da dignidade da pessoa humana (Art.1º, III, da CRFB/88), devendo ser amplamente aplicada e colocada em prática pelas instituições. Em adição, devem ser estabelecidas políticas de compliance, normas setoriais e códigos de ética que envolvam os tratamentos de dados realizados, bem como a gestão dos riscos e das vulnerabilidades decorrentes. Além de amplo diálogo dentro das organizações, na busca por maior conscientização e capacitação na temática, normas técnicas deverão ser aplicadas de forma robusta e interações entre agentes promovidas, criando cenários interdisciplinares e multissetoriais. Todos os sujeitos deverão se adaptar a uma nova cultura de tutela de dados pessoais, cabendo

especialmente à doutrina, às entidades de defesa de interesses coletivos, ao Judiciário e à Autoridade Nacional de Proteção de Dados harmonizarem a interpretação e a aplicação da Lei.

O desenvolvimento de mecanismos jurídicos, técnicos e de governança destinados a regular o tratamento dos dados auxilia a evitar incidentes de segurança, usos indevidos e discriminações ilícitas ou abusivas em face do titular e/ou de um grupo. Além disso, tais mecanismos afastam práticas que possam prejudicar concretamente as liberdades e as garantias fundamentais. A depender da forma como os algoritmos são programados, as bases de dados selecionadas e os processos estabelecidos e valorados, o resultado do tratamento pode ampliar indevidamente assimetrias, preconceitos e desigualdades — situação essa violadora da Constituição Federal e de documentos internacionais de direitos humanos.

Na LGPD, foi estabelecido um modelo legislativo que privilegia a prevenção de danos à pessoa humana e a segurança no tratamento de dados pessoais, instituindo deveres e responsabilidades específicas aos agentes, além de amplo rol de princípios e direitos aos titulares, por meio de tutelas individuais e coletivas. A proteção de dados e a norma jurídica referente à matéria podem ser percebidas como formas de: (i) conter os efeitos nefastos do capitalismo de vigilância e as manipulações oriundas de grandes plataformas; (ii) afastar os riscos que determinadas aplicações com algoritmos podem oferecer aos direitos fundamentais; e (iii) trazer garantias às pessoas diante da opacidade e da ausência de *accountability* de diversas estruturas políticas e econômicas. As inferências e predições realizadas por meio de tratamentos de dados mostram-se bastante preocupantes, pois podem determinar ou influenciar destinos, desejos e classificações, inclusive, restringindo indevidamente o acesso a bens e a oportunidades, bem como ampliar cenários de discriminação e de desigualdades.

A LGPD entrou em vigor em um momento extremamente complexo para a sociedade brasileira: a pandemia mundial de COVID-19. Diante desse cenário, o debate em torno de medidas que utilizam dados pessoais sensíveis e ferramentas tecnológicas conectadas tornou-se ainda mais importante e trouxe novas preocupações para os titulares dos dados, organizações e países. Compreender, dentro do contexto normativo brasileiro, o que são dados sensíveis, como e em que hipóteses eles podem ser tratados e quais instrumentos de proteção deverão ser estabelecidas e garantidos parece

contribuição pertinente no presente momento, diante do início dos trabalhos de interpretação, aplicação e adequação à LGPD.

Para tanto, a presente conclusão será estruturada conforme as etapas de elaboração da tese, abordando questões essenciais para uma análise funcional da categoria dos dado sensíveis e das hipóteses de tratamento: a) estudo acerca da função, dos fundamentos e das espécies de dados sensíveis; b) disciplina normativa aplicável para o tratamento de dados sensíveis, havendo o estudo crítico das bases legais dispostas na LGPD em seus artigos 7º e 11, assim como do artigo 14 da norma, voltado a crianças e adolescentes; e c) segurança e boas práticas com dados sensíveis: aplicação do *privacy by design,* desenvolvimento do relatório de impacto, gestão de riscos, mitigação de incidentes de segurança, término do tratamento de dados e conservação de dados sensíveis.

Dados sensíveis: estudo acerca da função da categoria, seus fundamentos e espécies

A proteção ampliada dos dados sensíveis decorre especialmente da cláusula geral de tutela da pessoa humana, assim como de dois significativos princípios: o livre desenvolvimento da personalidade e a não discriminação. Quando se afirma a relevância do livre desenvolvimento da personalidade, entende-se que cada pessoa deve eleger o seu modo de vida, podendo desenvolver e expor, de forma ampla, seu projeto pessoal. Garante-se autonomia para que cada um constitua sua personalidade de forma livre, sem qualquer imposição ou interferência de terceiros, havendo tanto um direito à individualidade quanto à diferença. A proteção da integridade, igualdade e autonomia individual dar-se-á para além dos direitos positivados expressamente no ordenamento, cabendo também a pessoas e instituições respeitarem as expressões alheias e desenvolverem ambientes e políticas inclusivas e diversas.

Uma tutela ampliada dos dados sensíveis mostra-se especialmente relevante para a garantia de direitos e liberdades fundamentais, devendo ser protegidos de forma mais específica e cuidadosa pelas diversas estruturas normativas. Isso porque, em virtude da qualidade e da natureza das informações que trazem, seu tratamento ou eventual vazamento poderá gerar riscos significativos à pessoa humana, podendo ser fonte para

preconceitos e discriminações ilícitas ou abusivas. Na categoria, há informações que vão além da simples proteção da vida privada, representando meio para a defesa da igualdade material entre as pessoas. Resguarda-se também, aqui, conteúdo relacionado com a intimidade e a identidade da pessoa natural, conteúdo esse que, como regra, só cabe a ela desenvolver e atuar sobre. Diante das novas dinâmicas de poder e expressão, vêm sendo tuteladas na categoria também informações sensíveis que integram a esfera pública em que se encontra seu titular, constituindo as convicções que ele deve poder manifestar e que fazem parte de sua identidade pública.

A seleção sobre quais dados são sensíveis demonstra que a circulação de determinadas informações pode acarretar maior potencial lesivo aos seus titulares, em uma determinada configuração social e política. Diante disso, a compreensão sobre os mecanismos que devem ser empregados na tutela de dados sensíveis perpassa um entendimento substancial sobre as dinâmicas discriminatórias que estão articuladas nas sociedades. Mesmo com o avanço na garantia dos direitos fundamentais, grupos vulneráveis e minorias vêm sendo os mais perseguidos e violentados na sociedade brasileira, o que torna essencial e urgente a tutela ampliada dos dados sensíveis, assim como o questionamento efetivo de estruturas discriminatórias e opressivas de poder.

O Direito precisa ser mobilizado para a aplicação dos princípios da igualdade material e da não discriminação, impedindo a perversa utilização de informações de saúde e políticas, assim como de características étnico-raciais, sexuais ou de gênero, como mecanismos de exclusão e segregação de pessoas. Outro ponto de preocupação é o desenvolvimento contínuo de análises e de perfis comportamentais com tais dados, visando a direcionar e a personalizar, com elevada precisão, bens e serviços.

O princípio da não discriminação – relevante fundamento para a tutela ampliada dos dados sensíveis – aparece expressamente na LGPD por duas vezes: na primeira, no inciso IX do Art. 6º, que o conceitua como "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos", e na segunda, no § 2º do Art. 20, que prevê a possibilidade de a Autoridade Nacional de Proteção de Dados realizar auditoria para verificar aspectos discriminatórios em tratamento automatizado de dados pessoais.

Decisões que há pouco tempo eram tomadas exclusivamente por seres humanos vêm sendo delegadas – no todo ou pelo menos em parte – para sistemas automatizados, algoritmos de ranking e modelos de risco preditivo que, por sua vez, acabam

controlando questões relativas a, por exemplo, saúde, integridade, crédito, liberdade e emprego. Percebe-se, assim, o potencial das decisões automatizadas de violarem direitos fundamentais, se tomadas sem o cumprimento de determinados parâmetros éticos e constitucionais que garantam transparência, possibilidade de controle, segurança, participação do indivíduo no processo decisório que lhe diz respeito, bem como a correção e atualização dos dados. Nesse contexto, a LGPD previu o direito do titular dos dados de solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir seu perfil pessoal, profissional, de consumo e de crédito ou aspectos de sua personalidade.

O tratamento de dados sensíveis é inevitável no mundo contemporâneo e nem sempre terá por objetivo práticas negativas ou discriminatórias, podendo contribuir para a melhor organização de instituições e com o funcionamento de bens e serviços, gerando, então, resultados benéficos para os titulares de dados e grupos. Contudo, é imprescindível que tais dados sejam utilizados respeitando-se, estritamente, os princípios e limites impostos na Constituição Federal e na LGPD.

Diante dos fundamentos da categoria dos dados sensíveis, relacionados diretamente com a tutela da liberdade e da igualdade material, e de sua natureza intrinsecamente relacionada a aspectos existenciais e particulares da pessoa humana, entende-se que ela deverá ser compreendida em rol exemplificativo, o que, diga-se, não encontra qualquer óbice textual na LGPD. A lei estabelece, ainda, que o disposto no Artigo 11 – que apresenta as bases legais para o tratamento de dados sensíveis – aplica-se a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular (Art. 11, § 1º).

Como direito da personalidade, a proteção de dados pessoais é essencial à pessoa humana, necessária, irrenunciável e inalienável. A elasticidade do rol de dados sensíveis representa instrumento para efetivar formas de proteção também atípicas, pautadas no interesse ao livre exercício da vida e de relações. Uma previsão legal exaustiva dos dados sensíveis deixaria de fora manifestações e exigências da pessoa que exigem uma proteção ampliada. Na medida em que a criação da categoria de dados sensíveis justifica-se, entre outras razões, para proteger um tipo de informação que pode ocasionar práticas discriminatórias, ela pode abranger, por exemplo, dentro de certos

contextos e usos, outras informações pessoais para além daquelas tipificadas na LGPD como, por exemplo, origem social, dados financeiros, orientação sexual e identidade de gênero. Tal perspectiva deve levar em conta, porém, a necessidade de não ocorrer um alargamento excessivo e inadequado desta categoria especial, já que isso tanto limitaria alguns tratamentos de dados quanto poderia deixar a categoria com menos relevo no futuro.

Entende-se que a identificação dos dados sensíveis pode variar, a depender da forma como eles forem compreendidos em cada legislação, cultura e ambiente. A priori, parece que um grupo relativamente amplo de informações pessoais pode ser considerado sensível, especialmente diante de alguns tratamentos específicos realizados. Por consequência, os dados pessoais deverão ser avaliados considerando-se, por exemplo: (I) a natureza e as características da informação pessoal, além do contexto que determina seu tratamento; (II) interesses específicos do responsável pelo tratamento, assim como dos destinatários potenciais dos dados; (III) finalidade e propósito para os quais os dados serão tratados; (IV) condições do tratamento; (V) relações que podem ser estabelecidas com as demais informações disponíveis sobre o titular e/ou o grupo de que ele faz parte; (VI) as possibilidades tecnológicas atuais e futuras envolvendo dados; (VII) como a informação pode afetar o indivíduo a quem ela diz respeito e o livre desenvolvimento de sua personalidade; e (VIII) a potencialidade do tratamento do dado servir como instrumento de estigmatização ou discriminação ilícita ou abusiva da pessoa.

A combinação de vários conjuntos de dados pode aumentar a probabilidade de que conclusões de natureza sensível sejam alcançadas, mesmo quando isso não for aparente, ao se olhar para conjuntos de dados específicos de forma isolada. Em ambientes cada vez mais interconectados, isso pode envolver levar em consideração não apenas outros dados que possam estar em posse do controlador, mas também dados a que ele possa ter acesso em outro lugar e, inclusive, com terceiros. Outro fator que deve ser avaliado diz respeito às habilidades técnicas do controlador de dados (ou outros controladores em potencial). Isso incluirá a capacidade computacional e o *know-how* técnico disponíveis. Tendo em vista que tais fatores estão em constante evolução e que o acesso a conjuntos de dados complementares está sempre aumentando, o contexto específico de um tratamento deverá, como regra, ser compreendido de forma dinâmica.

Como apresentado, não se mostra possível definir de forma antecipada, absoluta e permanente os efeitos concretos de um tratamento de informações nem a real sensibilidade de um dado. Por exemplo, dados pessoais que pareçam não relevantes em determinado momento, que não façam referência a alguém diretamente ou, ainda, que não sejam formalmente sensíveis, uma vez transferidos, cruzados e/ou organizados, podem resultar em dados bastante específicos sobre determinada pessoa, trazendo informações, inclusive, de caráter sensível sobre ela.

Entende-se que, além de se realizar uma proteção mais ampla de dados considerados sensíveis, mostra-se necessário observar tal proteção também nos casos em que houver tratamento sensível de dados pessoais. Isso porque, com base estritamente em considerações a respeito da natureza dos dados tratados, nem sempre será possível predizer os efeitos que o tratamento poderá causar em seu titular ou em interesses coletivos *lato sensu*. Quando se pretender processar dados para se tirar conclusões sensíveis ou para produzir dados que possam revelar aspectos sensíveis, a proteção deverá ser ampliada, de acordo com a LGPD (Art. 11, § 1º), que preconiza que a proteção disposta em seu artigo 11 será aplicada, também, a qualquer tratamento de dados pessoais que revele dados sensíveis e que possa causar danos ao titular, ressalvado o disposto em legislação.

As novas e complexas formas de tratar dados vêm expandindo as possibilidades de classificação dos dados pessoais. Isso tem levado à defesa do estabelecimento de novas categorias, relações e tutelas. Diante dos avanços tecnológicos e científicos, até mesmo informações pessoais que tradicionalmente não eram classificadas como sensíveis podem causar tanto (a) um tratamento discriminatório ilícito ou abusivo quanto (b) a dedução ou a inferência de dados sensíveis como, por exemplo, histórico de compras, dados de geolocalização, dados financeiros, identidade de gênero, idade, CEP do domicílio, antecedentes e/ou processos criminais em andamento, alguns metadados etc. Em verdade, tendo em vista as diversas possibilidades de utilização e cruzamento de dados, bem como o oferecimento de ferramentas tecnológicas cada vez mais sofisticadas, mostra-se hoje difícil pensar em um dado pessoal que não seja potencialmente sensível.

Dados sensíveis podem alcançar diferentes níveis de sensibilidade, a depender da espécie de dado em questão, da informação em si que guarda e/ou do titular a quem

diz respeito, impactando em graus de intensidade diversos a esfera de seu titular. Quanto mais sensíveis forem as informações pessoais, maiores serão os riscos e os danos, se houver um incidente de segurança. Por tal razão, garantias específicas — jurídicas e técnicas — deverão ser implementadas e constantemente analisadas nos programas de compliance. Indaga-se, então, conforme provocado nesta tese, se não seria mais adequado, e inclusive necessário, criar categorias especiais de dados e, consequentemente, tutelas diferenciadas para eles, havendo níveis de segurança e de garantia ampliados. Nesse sentido, foi proposta na tese a defesa do desenvolvimento de uma nova categoria de dados especiais: os dados altamente sensíveis. Dentro da referida categoria, duas possibilidades de tratamento poderiam ser enquadradas: a) dados sensíveis relacionados a informações específicas de saúde, genéticas e biométricas; e b) determinados dados sensíveis de pessoas hipervulneráveis ou de vulnerabilidade agravada.

No segundo capítulo, foi desenvolvido estudo acerca das diversas espécies de dados pessoais considerados sensíveis, analisando-se seus conteúdos e quais informações tutelam. Definir tal ponto representa aspecto essencial e implica, em aspectos práticos, trabalhar em maior detalhe: gestão de riscos, bases legais aplicáveis para o tratamento de dados (valendo recordar que o Art. 11 da LGPD apresenta hipóteses mais restritas, conforme apresentado no capítulo 3), o desenvolvimento de relatórios de impacto e o incremento de mecanismos de proteção ampliada para dados sensíveis. A LGPD em seu Art. 5º, inciso II, trouxe espécies de dados pessoais considerados sensíveis, porém não esclareceu o que seriam dados sensíveis em termos conceituais, trouxe termos, por vezes, pouco precisos e não explicitou se o rol de tais dados seria taxativo ou exemplificativo, sendo a última opção defendida na presente tese.

A partir dos dados caracterizados como sensíveis na LGPD, de forma didática, buscou-se desenvolver ao menos quatro categorias: a) dados pessoais sensíveis sobre a origem racial ou étnica; b) dados pessoais sensíveis acerca de crenças e filiações: informações sobre convicções religiosas, opiniões políticas e filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político; c) dados pessoais sensíveis corporais: dados referentes à saúde, dados genéticos e dados biométricos; e d) dados pessoais sensíveis sobre a vida sexual. Para a análise de cada espécie, foram utilizados

especialmente recursos e orientações das normas do *General Data Protection Regulation,* assim como mencionadas aplicações concretas de cada uma, como, por exemplo, o prontuário eletrônico, a telemedicina, os aplicativos de controle menstrual, o uso de câmeras em transporte para fins de publicidade, o reconhecimento facial, a proteção de direitos de pessoa transgênero, os vibradores sexuais e o uso de dados por partidos políticos.

Dados sobre origem e crenças e dados relacionados a questões sexuais são especiais diante de históricas perseguições, discriminações e preconceitos em face de pessoas de determinadas origens raciais ou étnicas, com certas crenças ou posições políticas ou, ainda, que tenham determinada orientação sexual ou identidade de gênero. Os dados corporais, com o avanço da ciência e da tecnologia, apresentam uma sensibilidade também elevada, sendo diversas as suas aplicações e tratamentos. Atualmente, por exemplo, eles são fundamentais para alimentar sistemas de inteligência artificial, que irão colaborar com médicos em diagnósticos e em tratamentos de saúde (inclusive nas questões relativas à pandemia de COVID-19), na solução de investigações e de crimes e na implantação de tecnologias de vigilância e controle, como o reconhecimento facial e o *contact tracing*. Vale lembrar que, com o avanço da rede 5G e a disseminação da Internet das Coisas, os *wearables* tratam cada vez mais cedo e em grande volume informações sensíveis de pessoas naturais.

Disciplina normativa aplicável para o tratamento de dados sensíveis

No terceiro capítulo da tese, foi realizado estudo das normas relativas ao tratamento dos dados sensíveis e das bases legais aplicáveis a eles, havendo, inclusive, análise comparativa entre as bases dispostas nos artigos 7º e 11 da LGPD. Entende-se que qualquer pessoa que trate dados pessoais, seja ela natural ou jurídica, de direito público ou privado, deverá ter uma base para fundamentar os tratamentos realizados, ou seja, uma hipótese legal disposta no artigo 7º ou 11, a qual poderá ser complementada pelas normas dos artigos 14 ou 23 da LGPD.

Defendeu-se que, ainda que seja possível utilizar mais de uma base legal para determinado tratamento de dados, é preciso buscar a mais adequada e segura para a

situação concreta, levando-se em conta práticas de mercado, orientações de especialistas, guias de autoridades responsáveis pela proteção de dados, inclusive em âmbito estrangeiro, e o equilíbrio entre os direitos dos titulares e as melhores opções para o desenvolvimento dos negócios. Mostra-se necessário que o agente de tratamento realize uma análise ponderada que considere riscos e benefícios.

De forma a contribuir com os operadores do direito que atuam na área, buscou-se desenvolver raciocínio para a seleção da base legal em cada situação de tratamento, o qual deverá ser analisado de forma dinâmica e observando as suas características. Didaticamente, parece adequado refletir acerca das seguintes questões: a) A LGPD é aplicável ao tratamento? O tratamento se enquadra nas exceções previstas no Art. 4º da LGPD? b) O titular do dado é uma criança, um adolescente ou um adulto? c) O dado pessoal é sensível? d) O agente de tratamento está enquadrado no capítulo IV da LGPD (que versa sobre o tratamento de dados pessoais pelo Poder Público)? e) O dado pessoal foi coletado diretamente do titular ou foi obtido por meio de terceiro? Qual a sua origem? A obtenção foi lícita? f) Qual a finalidade do tratamento de dados pessoais?

Conforme pesquisa realizada para a tese, em relação ao Art. 7º da LGPD, é pacífico o entendimento de que todas as bases apresentam o mesmo peso e importância, o que, porém, não se verifica no Art. 11, já que, para certos autores, o consentimento ali apresentaria alguma preferência em face das demais bases. Outro fato relevante acerca das duas listas de bases legais é a ausência ou alteração de algumas bases relativas especialmente a contratos, ao legítimo interesse e à tutela do crédito, não havendo acertadamente, como destacado no texto, menção às duas últimas no rol de tratamento dos dados sensíveis, diante da natureza das informações e das possibilidades de discriminação ilícita ou abusiva com os dados. A base referente ao contrato recebe no Artigo 11 novos contornos, podendo o tratamento de dados sensíveis se dar para o exercício regular de direitos, inclusive em contrato.

Nessa situação, devem ser aplicados de forma ainda mais intensa todos os cuidados já previstos para o tratamento dos dados, uma vez que para os dados sensíveis se espera um padrão ainda mais rigoroso de proteções técnica, administrativa e jurídica. Em um tratamento específico em que haja mescla de dados pessoais sensíveis e não sensíveis deverá prevalecer, naturalmente, um critério de maior rigor, de forma que os

tratamentos de dados sempre respeitem a necessidade de uma base legal disposta no Art. 11 da LGPD.

Em relação à base legal do legítimo interesse, dentro de uma abordagem prática, é comum o seu questionamento em relações em que se verifica a presença de algum dado sensível ou quando o controlador não tem contato direto com o indivíduo e não pode pedir seu consentimento ou, ainda, em questões que envolvem segurança, verificação e autenticação de pessoas. Na LGPD, a referida hipótese não foi disponibilizada para o tratamento de dados sensíveis, devendo a atividade ser encaixada nas demais bases dispostas no Art. 11, que traz entre elas o consentimento; a proteção da vida ou da incolumidade física do titular ou de terceiros; a possibilidade de tratamento para a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos; o exercício regular de direitos em contrato; e o cumprimento de obrigação legal ou regulatória pelo controlador.

O legítimo interesse, justamente por apresentar maior flexibilidade ao agente de tratamento, apresenta algumas limitações para a sua aplicação, devendo ser realizado antecipadamente um teste de ponderação. Busca-se, assim, balancear os direitos do titular dos dados e de quem faz uso de suas informações, verificando-se tanto se há um interesse legítimo de quem trata os dados quanto se estão sendo respeitadas as legítimas expectativas e os direitos e liberdades fundamentais dos titulares.

Dados pessoais, quando processados em grande escala e combinados com outros dados, podem levar a inferências e a resultados de caráter sensível. Diante disso, bases que dependem menos de uma interação direta com o titular e que apresentam maior flexibilidade, se utilizadas sem garantias adequadas, podem não conseguir limitar os riscos aos direitos e liberdades dos titulares.

Acerca da seleção e interação da base legal do consentimento com as demais bases aplicáveis ao tratamento de dados, a partir de orientações interpretativas do GDPR, foram tecidas algumas observações. Se um controlador optar por selecionar a base do consentimento para qualquer parte do tratamento, ele deverá estar preparado para respeitar a escolha do titular e, inclusive, interromper essa parte do tratamento se este revogar seu consentimento. Por exemplo, não se mostra adequado utilizar a base do legítimo interesse retrospectivamente para justificar um tratamento em que foram

encontrados problemas com a validade do consentimento. Devido à necessidade de o controlador divulgar a base legal em que se fundamenta no momento inicial do tratamento dos dados, ele deverá ter decidido com antecedência qual base será aplicável.

Na LGPD, não parece haver restrição para que o controlador cumule bases legais em determinados tratamentos, sendo sugerido, porém, que aponte qual delas é a preponderante. Em determinadas situações práticas, por exemplo, é comum que o controlador transite entre o legítimo interesse e a execução de contrato. A possibilidade de identificação de mais de uma base legal para determinada operação de tratamento de dados tem encontrado respaldo em alguns documentos de autoridades europeias de proteção de dados, conforme apresentado. Pode ser possível também que mais de uma base se aplique ao tratamento porque, por exemplo, o controlador tem mais de uma finalidade. Se houver uma mudança nas circunstâncias ou se ele possuir um propósito novo, poderá haver um bom motivo para revisar sua base legal e fazer uma mudança, quando precisará informar ao titular a questão e documentar tal mudança.

No que concerne ao tratamento de dados públicos, os quais podem ser dados tornados manifestamente públicos pelo titular ou dados pessoais cujo acesso é público, importa ressaltar que a lei não tratou dessas espécies quando sensíveis, trazendo, aparentemente, apenas duas normas gerais, no Art.7º, para o tratamento de dados pessoais considerados públicos. A respeito do tema, a seguinte pergunta foi proposta: teria a LGPD unificado a forma como deverão ser tratados os dados públicos, sendo eles sensíveis ou não, ou todos os dados sensíveis, sendo públicos ou não, deveriam sempre ser tratados com base em uma das hipóteses legais do Art. 11?

Verifica-se, então, que além do debate sobre que tipos de dados pessoais devem, de fato, ser considerados públicos, há também dúvidas acerca do seu tratamento lícito quando forem também sensíveis. Diante disso, mostra-se relevante tanto um maior cuidado doutrinário sobre o tema quanto uma manifestação da Autoridade Nacional de Proteção de Dados, para que esclareça dúvidas e detalhe a questão.

Conforme os mecanismos de comunicação e de interação avançam, o ambiente digital vem se tornando cada vez mais relevante na vida das pessoas. Especialmente após o início da pandemia de COVID-19, diversas operações e atividades foram intensificadas ou migraram, ainda que provisoriamente, para o referido ambiente, como o ensino em escolas, universidades e cursos, serviços governamentais, atendimentos de

saúde, compras de bens e ferramentas de entretenimento e jogos. O acesso a recursos e a tecnologias digitais permite que crianças e adolescentes realizem uma série de direitos civis, políticos, culturais, econômicos e sociais. Contudo, diante das sofisticadas formas de tratamento de dados e da vulnerabilidade agravada desses sujeitos, os riscos de violação de informações e/ou de abusos tornam-se cada vez mais intensos.

Mostra-se, assim, necessário analisar diversos instrumentos para a proteção e a educação de crianças e adolescentes, assim como destacar a importância de um uso ético e responsável da rede. O controle e a mediação parental devem ser aplicados em intensidades compatíveis com as idades da criança e do adolescente, respeitando seus graus de autonomia e discernimento, e com seus processos de aquisição gradual de competências e entendimentos. Os riscos e oportunidades relacionados com o envolvimento dos menores no ambiente digital mudam a depender de sua idade e estágio de desenvolvimento.

Vale ressaltar, porém, que sendo possível e seguro entende-se adequado conferir espaços de liberdade e privacidade ao menor, para que desenvolva sua autonomia e comunicação, tendo os seus pontos de vista devidamente considerados. O *design* de medidas apropriadas a cada idade deve ser informado pelas mais atualizadas pesquisas e práticas nos campos da educação e da tecnologia. Observa-se também que as referidas considerações devem ser equilibradas com a importância de os menores exercerem seus direitos em ambientes apoiados, levando-se em conta suas experiências e circunstâncias individuais.

A construção das doutrinas do melhor interesse e da proteção integral e prioritária de crianças e adolescentes informam diretamente a tutela dos dados pessoais de tais sujeitos, devendo as garantias e cuidados serem ainda maiores quando se tratar de dados sensíveis. Essa orientação tem como fontes normativas diretas a Constituição Federal, o Estatuto da Criança e do Adolescente e a LGPD. Deve-se ressaltar que não se trata apenas de uma proteção adequada ao estágio de desenvolvimento em que crianças e adolescentes se encontram, mas de uma proteção prospectiva, a fim de garantir a dignidade deles hoje e no futuro.

Temos, hodiernamente, a geração mais observada e exposta de toda a história. O rastro digital de menores vem sendo iniciado cada vez mais cedo e de forma ampliada, seja por meio de aplicativos para serem usados pelas mães durante a gestação, seja por

meio de postagens realizadas pelos próprios pais, em mídias sociais, ainda quando são nascituros ou já nascidos. Questões como *oversharenting*, uso de dispositivos conectados na internet das coisas, acesso a mídias sociais por menores e *profiling* foram também mencionadas ao longo desta tese.

Aplicar uma proteção ainda maior a dados sensíveis de crianças e adolescentes requer uma série de instrumentos jurídicos e técnicos, além do estabelecimento de boas práticas. Contar com o comprometimento de instituições públicas e privadas no tema também é de suma importância, havendo tanto a aplicação de severas sanções por parte de autoridades administrativas e judiciais, por descumprimento das normas de proteção de dados, quanto a adequada orientação dos agentes por meio da publicação de guias e instruções. Como destacado, aplicações que envolvem o tratamento de dados de crianças e adolescentes necessitam ser desenvolvidas a partir de orientações que considerem princípios e valores éticos, além de haver a proteção aos direitos humanos inserida no desenho de todo o sistema. Ações alinhadas à lógica do *privacy by design* devem sempre ser tomadas no desenvolvimento de tecnologias, sendo incluídas também avaliações prévias de impacto e medidas técnicas e organizacionais de prestação de contas.

No cenário brasileiro, quando se advoga pela ampliação das bases legais para o tratamento de dados pessoais de crianças e adolescentes, o relatório de impacto à proteção de dados pessoais representa documento essencial para a tutela do melhor interesse dos menores. Como se depreende da leitura do Artigo 14 da LGPD, o consentimento é uma das bases legais para o tratamento de dados de crianças e adolescentes, mas não a única. Entende-se que podem ser aplicadas, além das normas do Art. 14, as disposições dos artigos 7º e 11 da LGPD, com algumas limitações, quando, respectivamente, se tratar dado pessoal de caráter geral e dado pessoal sensível de criança ou adolescente. Diante da redação dos parágrafos 1º e 3º do Art. 14, ampliar as bases legais para o tratamento de dados de crianças pode parecer uma tese mais arriscada para alguns agentes, tendo em vista que as referidas disposições, ao mencionarem estritamente crianças, poderiam sinalizar uma possível restrição das hipóteses legais de tratamento para tais sujeitos. Por outro lado, tal situação não envolve diretamente a figura do adolescente, o qual apenas é mencionado no *caput* do art. 14 da LGPD. O pilar central e inegociável será

sempre o melhor interesse da criança e do adolescente. Contudo, levando em conta as práticas de agentes públicos e privados, bem como a experiência europeia positivada no GDPR, expandir o rol de bases legais mostra-se uma tese possível e por vezes necessária, ainda que se ressalve a aplicação do legítimo interesse e da tutela do crédito.

Acerca da base legal do consentimento, disposta no parágrafo 1º do Art. 14, foram tecidas algumas considerações. Afirma-se na lei que, em relação às crianças, o tratamento dos dados pessoais desses sujeitos deverá ser realizado com o consentimento específico e em destaque dado por, ao menos, um dos pais ou pelo responsável legal, devendo esse consentimento ser também livre, informado e direcionado a tratamento de dados pessoais para finalidade determinada. Diante disso, o consentimento dado por sujeito fora do requisito legal ou pela própria criança não poderá ser admitido. Optou a lei por oferecer tutela destacada à criança, sujeito hipervulnerável e absolutamente incapaz, o qual deve ser representado sob pena de nulidade absoluta do ato praticado. Como visto, o parágrafo 1º não menciona o adolescente, criando assim dúvida se o consentimento manifestado por ele — sem assistência ou representação — deveria ser considerado válido, como hipótese de capacidade especial, ou se simplesmente o legislador teria optado por não tratar do tema, por já existir legislação geral sobre a matéria no Código Civil. A priori, parece que o legislador pretendeu reconhecer validade ao consentimento manifestado diretamente pelo adolescente no que concerne, especificamente, ao tratamento de seus dados pessoais (quando a base legal adotada para o caso for o consentimento). As questões acima – especialmente acerca da base legal aplicável e da emissão do consentimento pelo adolescente – encontram-se em amplo debate. Buscou-se na tese apresentar as principais correntes e propostas interpretativas para o Artigo 14 da LGPD, tão problemático em seus parágrafos. O contexto tecnológico atual – dinâmico e hiperconectado – traz diversas oportunidades e recursos para as crianças e adolescentes, auxiliando inclusive na promoção de seus direitos. Contudo, os riscos enfrentados e as diversas situações de tratamento indevido de dados trazem consigo desafios para a tutela dos referidos sujeitos. Ameaças às integridades física, psíquica e moral, a hiperexposição de dados pessoais, a discriminação, a modulação e a manipulação de comportamentos e a publicidade

infantil são exemplos de impactos negativos e problemas concretos enfrentados pelos menores. Diante disso, como apresentado, a LGPD trouxe uma série de direitos e garantias para a proteção de crianças e adolescentes, nos meios físico e digital, as quais deverão ser conjugadas com a doutrina do melhor interesse e a proteção integral, havendo a ampla participação dos mais variados sujeitos que atuam em sociedade.

Segurança e boas práticas com dados sensíveis

O tratamento de dados sensíveis impõe padrão mais elevado de proteção e segurança para as informações, assim como maior rigor nas técnicas empregadas para a sua circulação. Além de seguir estritamente normas e resoluções, as instituições devem obedecer a todo o arcabouço regulatório pertinente à atividade desenvolvida e criar normas internas – como Códigos de Ética e Conduta –, visando a orientar o comportamento de seus diretores, executivos e funcionários em torno de determinados valores e princípios. Cabe também promover interações entre *players* que desenvolvam atividades semelhantes e agentes de diferentes setores da sociedade, numa perspectiva multissetorial, para a troca e elaboração de boas práticas.

Nesse sentido, nas atividades de *compliance* pertinentes deve-se buscar uma aplicação ampla do *privacy by design*; a elaboração de relatórios de impacto à proteção de dados (RIPD); uma gestão eficiente de riscos; o desenvolvimento de planos de resposta a incidentes de segurança; a ampliação das áreas de segurança da informação e proteção de dados; e o registro documental dos fluxos de dados que detalhe todo o tratamento empregado, inclusive compartilhamentos, prazos de guarda e conservação, término das atividades e eliminação das informações.

A adoção de um programa de compliance que tenha atenção aos tratamentos de dados realizados pela instituição será essencial para auxiliar no efetivo atendimento aos comandos da lei, de acordo com as particularidades de cada local, bem como para prevenir a ocorrência de violações aos direitos dos titulares, traduzindo de forma concreta para as atividades cotidianas as premissas da LGPD. Um programa que envolva altas lideranças corporativas, tenha suporte financeiro adequado, ofereça autonomia e independência aos envolvidos e detecte e puna exemplarmente condutas

contrárias às diretrizes adotadas contribui tanto para a boa reputação da empresa quanto para a criação de um ambiente de confiança com os titulares de dados (como clientes e parceiros), além de representar diferencial competitivo frente aos demais agentes que atuam no mesmo setor. Nesse sentido, como lembrado, verifica-se a importância da incorporação dos princípios "ESG", que significam literalmente *environmental*, *social* e *corporate governance*, para a própria tutela de dados pessoais, seja no setor público ou privado.

Considerar aspectos éticos e boas práticas internacionalmente elogiadas e aplicadas no tratamento de dados é medida fundamental no programa implementado. Por meio de uma cultura de compliance proativo de dados, as instituições podem buscar uma transformação digital segura, assim como evitar os riscos associados à não conformidade regulatória, como, por exemplo, multas, restrições, perda da confiança do consumidor e de clientes e diminuição de oportunidades de negócios. A LGPD demanda novos modelos empresariais, sendo essenciais tanto programas robustos de compliance quanto o gerenciamento ágil dos riscos para proteger as instituições e promover seu desenvolvimento.

A lógica do *privacy by design* preconiza que a privacidade e a proteção de dados devem ser consideradas desde a concepção e durante todo o ciclo de vida de projetos, sistemas, serviços, produtos e processos que envolvam o tratamento de dados, especialmente se eles forem sensíveis, devendo, por consequência, ser incluídas avaliações prévias de impacto, medidas técnicas e organizacionais adequadas e instrumentos de prestação de contas (*accountability*). A privacidade por design garante que os dados pessoais sejam protegidos automaticamente em qualquer sistema de TI ou prática realizada. Após breve histórico do conceito e apresentação de sua relação com o *data protection by default*, foram destacados na tese alguns exemplos práticos que demarcam a sua relevância.

Na LGPD, a referida temática encontra-se adequadamente positivada em seu Artigo 46, devendo a sua interpretação ser enriquecida pela doutrina e orientações de autoridades de proteção de dados, como o Information Commissioner's Office (ICO) do Reino Unido. Adicionalmente, lembra-se que o *design* das tecnologias, ou seja, como elas são dispostas e arquitetadas, influencia diretamente o comportamento das pessoas. A mensagem e os sinais emitidos pelo *design* afetam o relacionamento do ser humano

com a tecnologia e com as instituições, bem como o cálculo de risco elaborado. Além disso, ele afeta os custos e o tempo aplicado em uma transação, melhora a experiência em ferramentas e induz e manipula condutas. A partir dessas funções, conforme apresentado, verifica-se que *design*, proteção de dados e privacidade encontram-se profundamente conectados.

Um relatório de impacto é uma ferramenta que o agente pode utilizar para identificar e reduzir os riscos à proteção de dados em suas atividades de tratamento. Ele também pode ajudá-lo a projetar processos mais eficientes para o tratamento de informações pessoais. É parte integrante da proteção de dados por design e por padrão, podendo determinar as medidas técnicas e organizacionais de que o agente precisa para garantir que seu tratamento esteja em conformidade com o ordenamento jurídico. Levando em conta a sua importância, na presente tese foram apresentados os seus elementos essenciais, definição e sugestões para a sua elaboração, especialmente quando houver, por exemplo, alto risco no tratamento de dados e ele envolver conjuntos complexos de dados sensíveis.

A feitura do relatório não é, como regra, obrigatória ao agente de tratamento nos fluxos de dados que realizar, havendo disposições legais específicas na lei. Contudo, dispõe a LGPD que a Autoridade Nacional poderá determinar ao controlador que elabore relatório de impacto referente às suas operações de tratamento de dados, nos termos de regulamento editado pela própria, observados os segredos comercial e industrial. O relatório encontra-se relacionado à avaliação e ao gerenciamento de riscos no tratamento de informações pessoais, sendo necessário debate multissetorial que discuta o que pode ser considerado risco, quais são os seus graus e em quais casos haverá obrigatoriedade da produção de um RIPD. Não há uma indicação objetiva na LGPD sobre operações de tratamento que envolvam ou que possam implicar alto risco, restando à ANPD – que deverá analisar o assunto e trazer diretrizes para o tema – e aos agentes de tratamento, por meio de análises e classificações internas de riscos, desenvolverem métodos, parâmetros e matrizes de risco. Com isso, será possível preparar desde a avaliação de impacto até o relatório em si.

Além de outras questões, o documento apresenta medidas, salvaguardas e mecanismos de mitigação de riscos implementados. Ele concretiza os princípios da segurança e da prevenção, sendo de grande importância para o compliance do

controlador. Entende-se que o documento deverá ser elaborado antes de a instituição iniciar o tratamento de dados: preferencialmente, na fase inicial do programa, projeto ou serviço que tem o propósito de usar esses dados. Seu estudo também foi apresentado em conjunto com as normas do GDPR relativas ao *Data Protection Impact Assessment* (DPIA), o qual só será obrigatório quando o tratamento puder resultar em um alto risco para os direitos e liberdades das pessoas naturais.

A respeito da gestão de riscos e da mitigação de incidentes de segurança, temas que dialogam diretamente com a área da segurança da informação e as normas técnicas da ISO, ainda que a presente tese seja um texto jurídico, entende-se que abordar as referidas questões mostra-se fundamental para a segurança e garantia dos dados sensíveis, ficando evidente sua interação com dimensões multidisciplinares. Analisar e gerenciar riscos representam fundamentos para os sistemas de compliance, sendo ações estratégicas e que devem estar presentes em todas as tomadas de decisão. A partir dessa prática, busca-se quantificar a probabilidade que uma ameaça tem de "explorar" determinada situação ou vulnerabilidade de uma instituição, trazendo perdas, danos e/ou prejuízos. Age-se na direção de identificar, prevenir, monitorar e controlar possíveis riscos enfrentados, por meio de atividades coordenadas.

Nesse sentido, indicou-se por exemplo a designação de um Comitê de Segurança da Informação, com experts das áreas técnica, jurídica e de comunicação; a implementação uma Política de Segurança da Informação e de um Plano de Resposta a Incidentes de Privacidade e Remediação; a criação de um ambiente que incentive usuários de sistemas da empresa, como clientes, parceiros e funcionários, a informar incidentes e vulnerabilidades detectadas; um controle mais rigoroso de acessos, senhas e autenticações; e a utilização de soluções que dificultem a identificação do titular do dado sensível, como técnicas de pseudonimização e criptografia.

Uma violação ou vazamento de dados sensíveis pode ter uma série de efeitos graves sobre seu titular, e inclusive terceiros, resultando em danos morais e materiais, além de discriminações e tratamento ilícitos. É, portanto, obrigação do controlador avaliar os riscos para os direitos e liberdades dos titulares e implementar medidas técnicas e organizacionais adequadas para resolvê-los.

Em relação aos incidentes de segurança com dados pessoais, a tese baseou-se diretamente em orientação publicada pela ANPD, a qual impõe aos agentes de

tratamento uma postura preventiva e proativa, visando a proteger integralmente os direitos dos titulares e minimizar substancialmente vulnerabilidades e prejuízos. Orienta-se que eles registrem e notifiquem adequadamente os sujeitos estabelecidos em lei a ocorrência de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares. A ANPD recomenda, inclusive, que os controladores sejam cautelosos, de modo que ocorra a comunicação mesmo nos casos em que houver dúvida sobre a relevância dos riscos e danos envolvidos no caso. Diante de um incidente, há um somatório de prejuízos operacionais com danos reputacionais e financeiros à instituição, os quais deverão ser considerados por ela no momento de contratação de pessoal e direcionamento de investimentos.

Diante da principiologia da LGPD, é possível afirmar que os dados deverão ser conservados durante o mínimo de tempo possível, observando-se os princípios da transparência, da finalidade e da necessidade. Este período deve levar em conta os motivos pelos quais o agente precisa efetuar o tratamento dos dados e ter respaldo em uma base ou hipótese legal da LGPD e/ou outras leis ou regulamentos, como, por exemplo, obrigações trabalhistas, fiscais ou antifraude. No momento de analisar a viabilidade ou necessidade de exclusão de um dado, o agente também deverá considerar as possibilidades legais.

A fim de garantir que os dados pessoais não sejam mantidos por mais tempo do que o necessário, o responsável pelo tratamento deve estabelecer prazos para o apagamento ou revisão dos dados conservados; desenvolver políticas de retenção e de eliminação de dados pessoais; adotar medidas técnicas e organizativas adequadas; e garantir que os dados que possuem são exatos e atualizados. Os dados pessoais devem ser tratados buscando-se garantir segurança e confidencialidade, de forma a se evitar acessos não autorizados ou utilizações indevidas dos dados.

A respeito do término do tratamento dos dados pessoais, de sua eliminação e possível conservação, a LGPD apresenta seção específica, que envolve inclusive dados pessoais sensíveis e dialoga profundamente com o capítulo da lei referente aos direitos dos titulares. Dispõe o Art. 15 da LGPD acerca das hipóteses para o término do tratamento de dados pessoais, ou seja, acerca das situações que ensejarão a sua eliminação/exclusão. Elas poderão ser flexibilizadas pelas normas do Art.16, as quais oferecem hipóteses taxativas para a conservação de dados. A interpretação das referidas

normas exige esforço interpretativo para que se mantenha dentro do escopo e principiologia da lei, devendo o agente empregar melhores práticas tanto em relação à forma dos procedimentos realizados quanto aos prazos.

Notas finais

A proteção de dados pessoais revela-se como direito fundamental, sendo condição para que o sujeito se realize e se relacione na sociedade. Como apresentado, tutelar dados sensíveis e tratamentos de caráter sensível significa proteger a pessoa contra discriminações abusivas ou ilícitas, assegurar igualdade material no seu tratamento e permitir o livre desenvolvimento da sua personalidade, levando-se em conta suas diferenças e características particulares.

Diante do atual cenário tecnológico, marcado pelo amplo uso de inteligência artificial e dentro de um contexto de web 4.0, não mais parece fazer sentido considerar um dado ou um conjunto de dados pessoais de forma isolada e estática, mas sim dentro de uma perspectiva dinâmica e funcional, que considere diversos fatores, sujeitos e possibilidades de tratamento. Há cada vez mais formas de análises que podem identificar indivíduos e revelar dados sensíveis sobre eles.

A consciência da importância do tema e a verificação da necessidade de contribuições sob a luz da metodologia do direito civil-constitucional fizeram-me trabalhar no desenvolvimento desta tese nos últimos quatro anos. A LGPD trouxe um novo e significativo referencial para a questão, cabendo à doutrina discutir a interpretação e aplicação da referida norma. Justamente com base nesse cenário, optei por não estabelecer um recorte mais específico, buscando compreender e oferecer primeiras reflexões acerca dos dados sensíveis em um ambiente hoje pautado por norma legal e que vive a emergência de uma grave pandemia, em que há a demanda pelo tratamento em massa de dados dessa natureza.

Entende-se, assim, que os dados sensíveis devem ser compreendidos dentro de um rol exemplificativo, considerando-se, inclusive, os diferentes níveis e intensidades de sensibilidade de cada informação, como forma de tutelar integralmente a dignidade

da pessoa humana e interesses tanto individuais quanto coletivos. Finalizo a tese retomando a referência que apresentei na epígrafe: o tratamento de dados pessoais deve ser concebido para servir ao ser humano, trazendo recursos, benefícios e interações que expandam a qualidade de vida das pessoas.

REFERÊNCIAS

ABBAS DA SILVA, L.; FRANQUEIRA, B. D.; HARTMANN, I. A. O que os olhos não veem, as câmeras monitoram: reconhecimento facial para segurança pública e regulação na América Latina. *Revista Digital de Direito Administrativo*, v. 8, n. 1, p. 171-204, 2021. Disponível em: <https://www.revistas.usp.br/rdda/article/view/173903> Acesso em: 27 fev. 2021.

ALAMINO, F. N. P.; DEL VECCHIO, V. A. Os Princípios de Yogyakarta e a proteção de direitos fundamentais das minorias de orientação sexual e de identidade de gênero. *Revista da Faculdade de Direito, Universidade de São Paulo, [S. l.]*, v. 113, p. 645-668, 2018. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/156674. Acesso em: 10.03.21

ALVARENGA, Rúbia Zanotelli de. Os direitos do trabalhador portador do HIV. *Revista Eletrônica Tribunal Regional do Trabalho do Paraná*. Curitiba, v. 3, n.27, p. 9-23, jan./fev. 2014.

ALVES, Fátima; ORTIGÃO, Isabel. Origem social e risco de repetência: interação raça-capital econômico. *Cadernos de Pesquisa*, v. 37, n. 130, p. 161-180, jan./abr. 2007.

ANDRADE, Vander Ferreira de. Limites e cautelas no uso de imagens gravadas por câmeras de condomínio e a responsabilidade correlata do síndico. *Migalhas*, publicado em 04 de setembro de 2020. Disponível em: <https://migalhas.uol.com.br/depeso/332871/limites-e-cautelas-no-uso-de-imagens-gravadas-por-cameras-de-condominio-e-a-responsabilidade-correlata-do-sindico> Acesso em: 20.01.21

ANGWIN, Agoia; LARSON, Jeff; MATTU, Surya; KIRCHNER, Laure. Machine Bias: Risk assessments in criminal sentencing. *ProPublica*, publicado em maio de 2016. Disponível em: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> Acesso em: 12.07.21.

ANPD. *Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte.* Outubro/2021.

ANPD. *Guia Orientativo Tratamento de Dados Pessoais pelo Poder Público.* Janeiro/2022.

ANPD. *Guia orientativo: aplicação da Lei geral de proteção de dados pessoais (LGPD) por agentes de tratamento no contexto eleitoral* [recurso eletrônico]. Brasília: Tribunal Superior Eleitoral, 2021.

ANTONIK, Luis Roberto. *Compliance, ética, responsabilidade social e empresarial*: uma visão prática. Rio de Janeiro: Alta Books, 2016.

ARAGÃO, Suéllyn Mattos de; SCHIOCCHET, Taysa. Lei Geral de Proteção de Dados: desafio do Sistema Único de Saúde. *RECIIS - Revista Eletrônica de Comunicação, Informação e Inovação em Saúde*, Rio de Janeiro, v. 14, n. 3, p. 692-708, jul./set. 2020.

ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. Adopted on 4 April 2017. As last Revised and Adopted on 4 October 2017. Disponível em: <https://ec.europa.eu/newsroom/article29/items/611236> Acesso em: 23.08.21.

ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 02/2012 on facial recognition in online and mobile services. 22/03/2012. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf> Acesso em: 27.02.21

ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools), adotada em 11 de fevereiro de 2009. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp160_en.pdf> Acesso em: 06.06.21.

ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 3/2012 on developments in biometric technologies. Adotada em 27 de abril de 2012. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf> Acesso em: 27.02.21

ARTICLE 29 WORKING PARTY. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. Bruxelas: Comissão Europeia, 2018.

ARTICLE 29 WORKING PARTY. Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS). Adopted on 4 October 2017. p.09. Disponível em: <https://ec.europa.eu/newsroom/article29/items/610171> Acesso em: 27.09.21.

ARTICLE 29 WORKING PARTY: Advice Paper on Special Categories of Data. Publicado em: 04 de abril de 2011. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/other-

document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf> Acesso em: 27.01.21

ARTICLE 29 WORKING PARTY. Opinion 2/2017 on data processing at work. Disponível em: http://ec.europa.eu/newsroom/document.cfm?doc_id=45631. Acesso em: 26 de julho de 2021.

BANISAR, David. *National Comprehensive Data Protection/Privacy Laws and Bills 2020*. Atualizado em 15 de dezembro de 2020). Disponível em: <https://ssrn.com/abstract=1951416>. Acesso em: 28.03.21

BARBOZA, Heloisa Helena Gomes. A proteção da identidade genética. In: Agassiz Almeida Filho; Plínio Melgaré. (Org.). *Dignidade da pessoa humana. Fundamentos e critérios interpretativos*. São Paulo: Malheiros Editores Ltda, 2010. p. 83-100.

BARBOZA, Heloisa Helena; PEREIRA, Paula Moura Francesconi de Lemos; ALMEIDA, Vitor. Proteção dos dados pessoais da pessoa com deficiência. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro.* São Paulo: Thomson Reuters: 2020.

BARRETO, Maurício Lima; ALMEIDA, Bethania de Araujo; DONEDA, Danilo. Uso e Proteção de Dados Pessoais na Pesquisa Científica. *RDU*, Porto Alegre, Volume 16, n. 90, 2019, 179-194, nov-dez 2019.

BARROSO, Luís Roberto. A dignidade da pessoa humana no direito constitucional contemporâneo: natureza jurídica, conteúdos mínimos e critérios de aplicação. Disponível em: <http://www.luisrobertobarroso.com.br/wp-content/uploads/2010/12/Dignidade_texto-base_11dez2010.pdf> Acesso em: 01.03.21.

BIONI, Bruno Ricardo. *Proteção de Dados Pessoais*: a função e os limites do consentimento. 2.ed. Rio de Janeiro: Editora Forense, 2020.

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

BIONI, Bruno; KITAYAMA, Marina; RIELLI, Mariana. *O Legítimo Interesse na LGPD*: quadro geral e exemplos de aplicação. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021.

BODIN DE MORAES, Maria Celina. *Danos à pessoa humana:* uma leitura civil-constitucional dos danos morais. Rio de Janeiro: Renovar, 2003. p. 107.

BODIN DE MORAES, Maria Celina. La tutela della persona umana in Brasile. *Civilistica.com*, Rio de Janeiro, a. 3, n. 2, jul.-dez./2014.

BODIN DE MORAES, Maria Celina. *Na medida da pessoa humana:* Estudos de direito civil-constitucional. Rio de Janeiro: Renovar, 2010.

BODIN DE MORAES, Maria Celina; CASTRO, Thamis Dalsenter Viveiros de. A autonomia existencial nos atos de disposição do próprio corpo. *Pensar*, Fortaleza, v. 19, n. 3, p. 779-818, set. /dez. 2014.

BORGESIUS, Frederik J. Zuiderveen; KRUIKEMEIER, Sanne; BOERMAN, Sophie C.; HELBERGER, Natali. Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation. *European Data Protection Law Review*. 2017. Disponível em: https://www.ivir.nl/publicaties/download/EDPL_2017_03.pdf. Acesso em: 28 dez. 2018.

BRAYNE, Sarah. *Predict and Surveil*: Data, Discretion, and the Future of Policing. 1.ed. Oxford University Press: 2020.

BRAZ JR., Marcilio. Considerações sobre a notificação de incidente de segurança da informação no contexto da lei geral de proteção de dados (e além). *Migalhas*, 1 de fevereiro de 2019. Disponível em: <https://www.migalhas.com.br/depeso/295440/consideracoes-sobre-a-notificacao-de-incidente-de-seguranca-da-informacao-no-contexto-da-lei-geral-de-protecao-de-dados--e-alem> Acesso em: 13.05.21.

BROWNE, Simone. *Dark Matters*: On the Surveillance of Blackness. Durham: Duke University Press Books, 2015.

BRUGINSKI, Márcia Kazenoh. Discriminação no trabalho: práticas discriminatórias e mecanismos de combate. Disponível em: <https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/90942/2015_bruginski_marcia_discriminacao_trabalho.pdf?sequence=1&isAllowed=y> Acesso em: 05.04.21.

BUCAR, Daniel. Administração Pública e Lei Geral de Proteção de Dados. *In:* SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (coord.). *Caderno Especial:* Lei Geral de Proteção de Dados (PGPD). São Paulo: Revista dos Tribunais, 2019. p. 153-165.

BURLE, Caroline; CORTIZ, Diogo. Mapeamento de princípios de inteligência artificial. Disponível em: <https://ceweb.br/publicacoes/mapeamento-de-principios-de-inteligencia-artificial/?page=1> Acesso em: 30.12.20

CALIMAN, Luciana. Os regimes da atenção na subjetividade contemporânea. *Arq. bras. psicol*., Rio de Janeiro, v. 64, n. 1, p. 02-17, abr. 2012.

CARVALHO, Lucas Borges de. A LGPD e o acesso à informação pública: dado pessoal é dado sigiloso? Jota, publicado em 16 de dezembro de 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/lgpd-informacao-publica-16122020> Acesso em: 02.08.21

CARVALHO, Lucas Borges de. A LGPD e o acesso à informação pública: dado pessoal é dado sigiloso? Jota, publicado em 16 de dezembro de 2020. Disponível em:

<https://www.jota.info/opiniao-e-analise/artigos/lgpd-informacao-publica-16122020> Acesso em: 02.08.21

CASTELLS, Manuel. *A Sociedade em Rede*. 21ª edição. Paz & Terra: 2013.

_____. Fim de milênio - A Era da Informação (vol. 3). 1ª edição. Paz e Terra: 2020.

CASTRO, Dayane Marciano de Oliveira; MANO, Janini Nogueira D'Alessandro; BARONOVSKY, Thainá. Dados pessoais bancários e financeiros são considerados dados sensíveis para a LGPD? *Migalhas*, publicado em 18 de agosto de 2021. Disponível em: <https://www.migalhas.com.br/depeso/350335/dados-pessoais-bancarios-sao-considerados-dados-sensiveis-para-a-lgpd> Acesso em 19.08.21.

CAVOUKIAN, Ann. *Operationalizing Privacy by Design*: A Guide to Implementing Strong Privacy Practices. Dez. 2012.

CAVOUKIAN, Ann. *Privacy by Design*: The 7 Foundational Principles. Disponível em: <https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/> Acesso em: 09.04.21.

CENTRE FOR INFORMATION POLICY LEADERSHIP. Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR. Centre for Information Policy Leadership GDPR Implementation Project. Publicado em 19 de maio de 2017.

CHATELLIER, Régis *et al*. *Shaping choices in the digital world*. From dark patterns to data protection: the influence of UX/UI design on user empowerment. CNIL, 2019.

CHENEY-LIPPOLD, John. *We are data. Algorithms and the making of our digital selves*. New York: New York University Press, 2017.

CITTON, Y. *The ecology of attention*. Malden: Polity Press, 2016.

CLERICI, Giovanna Bianchi. Corpo elettronico e tecnologie informatiche. Roma, 30 de janeiro de 2018. Disponível em: <https://www.garanteprivacy.it/documents/10160/0/Convegno+Uomini+e+Macchine+-+Intervento+di+Giovanna+Bianchi+Clerici.pdf/5156d23d-7a35-45fb-9b8d-f803a10426b3?version=1.0> Acesso em: 02.02.21.

CNSaúde. *Código de Boas Práticas*: Proteção de Dados para Prestadores Privados de Serviços em Saúde. 2021. Documento disponível em: <http://cnsaude.org.br/baixe-aqui-o-codigo-de-boas-praticas-protecao-de-dados-para-prestadores-privados-de-saude/> Acesso em: 27.07.21.

CNseg. Guia de boas práticas do mercado segurador brasileiro sobre a proteção de dados pessoais. 2019. Disponível em: <https://cnseg.org.br/publicacoes/guia-de-boas-

praticas-do-mercado-segurador-brasileiro-sobre-a-protecao-de-dados-pessoais.html>. Acesso em: 29.01.21

COE. Relatório Explicativo ao Protocolo que altera a Convenção para a Proteção das Pessoas no que diz respeito ao Tratamento Automático de Dados Pessoais publicado em 2018. Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223> Acesso em: 31.12.20.

COELHO, Nathália; LIMA, Antônio Pedro. ESG: por que essa sigla vai mudar o seu negócio daqui para a frente? Firjan, 19 de abril de 2021. Disponível em: <https://casafirjan.com.br/lab-de-tendencias/artigos-estudos-e-pesquisas/esg-por-que-essa-sigla-vai-mudar-o-seu-negocio-daqui> Acesso em: 04.05.21.

COLUSSI, Fernando Augusto Melo; SANTOS, Tomlyta Luz Velasquez dos. Novas tecnologias e liberdade de expressão na pesquisa científica: uma análise sobre a proteção de dados genéticos e de saúde. *Rev. de Biodireito e Direito dos Animais*, Porto Alegre, v. 4, n. 2, p. 01-21, Jul./Dez. 2018.

CORRÊA, Adriana Espíndola. O corpo digitalizado: um novo objeto para o direito. *Revista da Faculdade de Direito (UFPR),* v. 44, p. 77-94, 2006.

COSTA, Ramon S. *Entre taps e direitos*: proteção de dados pessoais, privacidade e liberdade no aplicativo Grindr. Dissertação (Mestrado em Direito). Universidade Federal de Juiz de Fora. 185 p. 2020.

COSTANZA-CHOCK, Sasha. *Design Justice.* Community-Led Practices to Build the Worlds We Need. The MIT Press: 2020.

CRARY, J. *24/7 – Capitalismo tardio e os fins do sono.* São Paulo: Cosac Naify, 2014.

DALESE, Pedro. Os dados pessoais sensíveis na era do Big Data. Migalhas, publicado em 03 de março de 2021. Disponível em: <https://www.migalhas.com.br/depeso/341100/os-dados-pessoais-sensiveis-na-era-do-big-data> Acesso em: 06.03.21

DALSENTER, Thamis. Direito à saúde entre a liberdade e a solidariedade: os desafios jurídicos do combate ao novo coronavírus – COVID-19. *Migalhas*, 05 de março de 2020. Fonte: <https://www.migalhas.com.br/coluna/migalhas-de-vulnerabilidade/321211/direito-a-saude-entre-a-liberdade-e-a-solidariedade-os-desafios-juridicos-do-combate-ao-novo-coronavirus-covid-19> Acesso em: 13.04.20.

DASTIN, Jeffrey. Amazon scraps secret AI recruiting tool that showed bias against women. Reuters, 10.11.2018. Disponível em: <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G>. Acesso em: 26.11.2020.

DAVENPORT, T; BECK, J. *The attention economy: understanding the new currency of business*. Boston: Harvard Business School Press, 2001.

DIRETIVA 2011/24/UE DO PARLAMENTO EUROPEU E DO CONSELHO de 9 de março de 2011 relativa ao exercício dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32011L0024> Acesso em: 21 jan. 2021.

DOERING, Victor; SILVA, Alexandre Pacheco da. O tratamento de dados biométricos na LGPD: dilemas jurídicos e políticos de seu processamento. In: FILHO, Francisco; RAIS, Diogo (Coord.). *Direito público digital*. São Paulo: Thomson Reuters Brasil, 2020. p. 99-113.

DONEDA et al. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. *Pensar*, Fortaleza, v. 23, n. 4, p. 1-17, 2018.

DONEDA, Danilo. *A proteção de dados pessoais nas relações de consumo*: para além da informação creditícia. Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010. p. 26-27

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

DONEDA, Danilo; MONTEIRO, Marília. Acesso à informação e privacidade no caso da Universidade Federal de Santa Maria. *Jota*. 2 jul. 2015. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/acesso-a-informacao-e-privacidade-no-caso-da-universidade-federal-de-santa-maria-02072015. Acesso em: 14 jun. 2020, n.p.

DUHIGG, Charles. How companies learn your secrets. *The New York Times*. 26 fev. 2012. Disponível em: <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp>. Acesso em: 31 maio 2020.

DWORKIN, Gerald. Paternalism, *The Stanford Encyclopedia of Philosophy* (Summer 2014 Edition), Edward N. Zalta (ed.). Disponível em: <http://plato.stanford.edu/archives/sum2014/entries/paternalism/> Acesso em: 01.03.21

EBERLIN, Fernando Büscher von Teschenhausen. Sharenting, liberdade de expressão e privacidade de crianças no ambiente digital: o papel dos provedores de aplicação no cenário jurídico brasileiro. *Revista Brasileira de Políticas Públicas.* Brasília, v. 7, nº 3, 2017 p. 255-273.

EDPB. Guidelines 01/2021 on Examples regarding Personal Data Breach Notification. Adopted on 14 December 2021. Version 2.0.

EDPB. Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak.

EDPB. Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak. Disponível em: <https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_en>Acesso em: 26.02.2021

EDPB. Guidelines 3/2019 on processing of personal data through video devices - version adopted after public consultation. Versão 2.0. Adotada em 29 de janeiro de 2020. Disponível em: <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en> Acesso em: 20.01.21.

EDPB. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. Adopted on 20 October 2020. Disponível em: <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en> Acesso em: 10.05.21.

ENISA. European Union Agency for Network and Information Security. *Recommendations for a methodology of the assessment of severity of personal data breaches.* Working Document, December 2013. Disponível em: <https://www.enisa.europa.eu/publications/dbn-severity> Acesso em: 09.01.21.

EUBANKS, Virginia. *Automating Inequality*: How High-Tech Tools Profile, Police, and Punish the Poor. St. Martin's Publishing Group, 2018.

EUROPEAN DATA PROTECTION BOARD. Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679. Versão 1.1. Adotada em 4 de maio de 2020. p.08. Disponível em: <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en> Acesso em: 19.07.21.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS AND COUNCIL OF EUROPE. *Handbook on European data protection law*. Luxembourg: Publications Office of the European Union, 2018.

FERNANDES, Dauney Oliveira. Direito humano à igualdade racial. *Lex Magister*. Disponível em: <https://www.lex.com.br/doutrina_27550329_DIREITO_HUMANO_A_IGUALDADE_RACIAL.aspx> Acesso em: 30.03.21.

FICO, Bernardo de Souza Dantas; SICUTO, Guilherme Hernandes; NÓBREGA, Henrique Meng. Lei Geral de Proteção de Dados para LGBTs: Identidade de gênero como dado sensível. *Justificando*. Publicado em 16 de junho de 2020. Disponível em: <https://www.justificando.com/2020/06/16/leigeral-de-protecao-de-dados-para-lgbts-identidade-de-genero-como-dado-sensivel/> Acesso em: 03.03.21.

FLORIDI, Luciano. Open Data, Data Protection, and Group Privacy. *Philos. Technol.* 27, 1–3, 2014. Disponível em: <https://doi.org/10.1007/s13347-014-0157-8> Acesso em: 23.12.20.

FOITZIK, Piotr. Publicly available data under the GDPR: Main considerations. Disponível em: <https://iapp.org/news/a/publicly-available-data-under-gdpr-main-considerations/>. Acesso em: 01.08.21

FORRESTER CONSULTING. The Cloud, Data, And AI Imperative for Healthcare. Hospital Readiness and Adoption Paths for Next-Generation Technologies. A Forrester Consulting Thought Leadership Paper Commissioned By IBM. February 2020.

FRANCK, Georg. The economy of attention. *Telepolis*, dezembro, 1999. Disponível em <https://www.heise.de/tp/features/The-Economy-of-Attention-3444929.html> Acesso em: 23.01.19.

FRAZÃO, Ana. Algoritmos e inteligência artificial, Jota, publicado em 15 de maio de 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/algoritmos-e-inteligencia-artificial-15052018> Acesso em: 09.01.21.

FRAZÃO, Ana. Capitalismo de stakeholders e investimentos ESG. *Jota*, publicado em 28 de abril de 2021.

FRAZÃO, Ana. Data-driven economy e seus impactos sobre os direitos de personalidade. *Jota*, publicado em 17 de julho de 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/data-driven-economy-e-seus-impactos-sobre-os-direitos-de-personalidade-17072018> Acesso em: 14.01.21

FRAZÃO, Ana. Discriminação algorítmica. Jota, publicado em 23 de junho de 2021. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/discriminacao-algoritmica-2-23062021?amp&fbclid=IwAR1oD_HSvSGJ1cDD9UsBMgHUIj8lmTxoohT5tQp1m8Vrjv5h8qv_NX5vW0k> Acesso em: 23.06.21

FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coords.). *A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Revista dos Tribunais, 2019. p. 23-52.

FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. *Lei Geral de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019.

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. Compliance de dados pessoais. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coords.). *A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Revista dos Tribunais, 2019.

FRAZAO, Ana; MULHOLLAND, Caitlin (Org.). *Inteligência Artificial e Direito*: Ética, Regulação e Responsabilidade - revisto e atualizado. 2. ed. São Paulo: Revista dos Tribunais, 2020.

FRITZ, Karina Nunes. Pessoa não-binária tem direito a ser tratada de forma neutra, diz juiz de Frankfurt - ainda há muito por fazer pela identidade e igualdade de gênero. Migalhas, artigo publicado em 8 de março de 2021. Disponível: <https://www.migalhas.com.br/coluna/german-report/341325/pessoa-nao-binaria-tem-direito-a-ser-tratada-de-forma-neutra> Acesso em: 10.03.21.

GABRIEL, Anderson de Paiva. TEFFÉ, Chiara Spadaccini de. Ferramentas tecnológicas e controle da pandemia. *Jota*, Rio de Janeiro, 14 jun. 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/juiz-hermes/ferramentas-tecnologicas-e-controle-da-pandemia-14062020> Acesso em: 31 jul. 2020.

GEORGIEVA, Ludmila; KUNER, Christopher. Article 9 Processing of special categories of personal data In: KUNER, Christopher; BYGRAVE, Lee; DOCKSEY, Christopher. *The EU General Data Protection Regulation (GDPR): A Commentary*. 1.ed. Oxford University Press: 2020.

GOLDHABER, M. The Attention Economy and the Net, 1997. Disponível em: <https://firstmonday.org/article/view/519/440> Acesso em 15.12.19.

GOMES, Orlando. Direitos da personalidade e responsabilidade civil. *Revista de direito comparado luso-brasileiro*. Rio de Janeiro, ano II, n. 2, 1983.

GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva 95/46/CE. Adotado em 9 de abril de 2014. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_pt.pdf>. Acesso em 14.08.19.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau. A importância do compliance para o término do tratamento de dados. In: Ana Frazão; Ricardo Cueva (Coord). *Compliance e políticas de proteção de dados.* São Paulo: Thomson Reuters Brasil, 2021. p.245-268.

GURLEY, Lauren. Amazon Delivery Drivers Forced to Sign 'Biometric Consent' Form or Lose Job. VICE, 2021. Disponível em: <https://www.vice.com/en/article/dy8n3j/amazon-delivery-drivers-forced-to-sign-biometric-consent-form-or-lose-job> Acesso em 25.5.21.

HARARI, Yuval Noah. *21 lições para o século 21*. 1.ed. Companhia das Letras: 2018.

HARTZOG, Woodrow. *Privacy's Blueprint*: the battle to control the design of new technologies. Cambridge: Harvard University Press, 2018.

HENRIQUES, Isabella; PITA, Marina; HARTUNG, Pedro. A proteção de dados pessoais de crianças e adolescentes. In: Bruno Bioni, Laura Schertel Mendes, Danilo Doneda, Otavio Luiz Rodrigues Jr., Ingo Wolfgang Sarlet. (Org.). *Tratado de Proteção de dados pessoais*. 1ed. Rio de Janeiro: Forense, 2021. Ebook.

HOF, Simone van der. I agree, or do I? A rights-based analysis of the law on children's consent in the digital world. *Wisconsin International Law Journal*, v. 34, n. 2, p. 409-445, 2016.

IBGE. Estatísticas de gênero: indicadores sociais das mulheres no Brasil. Coordenação de População e Indicadores Sociais. Rio de Janeiro: IBGE, 2021. Disponível em: <https://biblioteca.ibge.gov.br/index.php/biblioteca-catalogo?view=detalhes&id=2101784> Acesso em: 05.09.21.

ICO 2018: Investigation into the use of data analytics in political campaigns. Publicado em: 06 de novembro de 2018. Disponível em: <https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/> Acesso em: 01.04.21.

ICO. Data protection by design and default. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/> Acesso em: 03.08.21.

ICO. Information Commissioner's Office. Investigation into the use of data analytics in political campaigns. Investigation update. Publicado em 11 de julho de 2018. Disponível em: <https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/> Acesso em: 07.07.21.

IKAWA, Daniela. *Ações Afirmativas em Universidades.* Rio de Janeiro: Lumen Juris, 2008.

ILGA World: Lucas Ramon Mendos, Kellyn Botha, Rafael Carrano Lelis, Enrique López de la Peña, Ilia Savelev and Daron Tan, *State-Sponsored Homophobia 2020: Global Legislation Overview Update.* Dezembro de 2020. Disponível em: <https://ilga.org/state-sponsored-homophobia-report> Acesso em: 07.03.21.

INFORMATION COMMISSIONER'S OFFICE (ICO). *Data protection and journalism*: a guide for the media. 2014. Disponível em: <https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf> Acesso em: 12.07.21.

INSTITUTO DE LONGEVIDADE MAG. Preconceito etário traz falsas ideias sobre idosos no mercado de trabalho. 2021. Disponível em:

<https://institutodelongevidademag.org/longevidade-e-trabalho/carreira/preconceitos-idosos-no-mercado-de-trabalho> Acesso em: 05.09.21.

INTERNETLAB. *O que está em jogo no debate sobre dados pessoais no brasil?* Relatório final sobre o debate público promovido pelo ministério da justiça sobre o anteprojeto de lei de proteção de dados pessoais. Associação InternetLab de pesquisa em direito e tecnologia, 2016.

ITS RIO. *Transparência e Governança nos algoritmos: um estudo de caso sobre o setor de birôs de crédito*. Disponível em: <https://itsrio.org/pt/publicacoes/transparencia-e-governanca-nos-algoritmos-um-estudo-de-caso/>Acesso em: 14.07.21

JUNIOR, José Luiz de Moura Faleiros Junior, NOGAROLI, Rafaella. Telemedicina e proteção de dados: reflexões sobre a pandemia da COVID-19 e os impactos jurídicos da tecnologia aplicada à saúde. *Revista dos Tribunais*, vol. 1016, Jun./20.
JUNQUEIRA, Thiago. *Tratamento de Dados Pessoais e Discriminação Algorítmica nos Seguros.* Revista dos Tribunais, 2020.

KFOURI NETO, Miguel; NOGAROLI, Rafaella. Responsabilidade civil pelo inadimplemento do dever de informação na cirurgia robótica e telecirurgia: uma abordagem de direito comparado (Estados Unidos, União Europeia e Brasil). In: ROSENVALD, Nelson; MENEZES, Joyceane; DADALTO, Luciana (coords.). *Responsabilidade civil e medicina*. Indaiatuba: Foco, 2020. p. 159-185.

KNOP, M.; COLLARES, A. C. M. A influência da origem social na probabilidade de concluir os diferentes cursos de ensino superior. *Sociedade e Estado,* v. 34, n. 02, p. 351-380, 2019. Disponível em: https://periodicos.unb.br/index.php/sociedade/article/view. Acesso em: 2 abr. 2021.

KONDER, Carlos Nelson de Paula. O alcance do direito à identidade pessoal no direito civil brasileiro. Pensar, Fortaleza, v. 23, n. 1, p. 1-11, jan./mar. 2018

KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Org.). *A Lei Geral de Proteção de Dados Pessoais e Suas Repercussões no Direito Brasileiro*. Revista dos Tribunais: São Paulo, 2019.

KORFF, Douwe. GDPR Requirements on Data Protection Impact Assessments & Methodologies for DPIAs. Jul. 2020. Disponível em: <https://ssrn.com/abstract=3656234> Acesso em: 21.08.21.

KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. Dados Sensíveis na Lei Geral de Proteção de Dados Pessoais: mecanismos de tutela para o livre desenvolvimento da personalidade. Orientador: Sergio Marcos Carvalho de Ávila Negri. Dissertação (mestrado acadêmico) - Universidade Federal de Juiz de Fora, Faculdade de Direito. Programa de Pós-Graduação em Direito, 2019.

KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. Private traits and attributes are predictable from digital records of human behavior. *PNAS*, vol. 110, n. 15, abril/2013, p. 5802-5805. Disponível em: <https://doi.org/10.1073/pnas.1218772110> Acesso em: 19.01.21.

KOTSCHY, Waltraut. Lawfulness of processing. In: *2018 Draft commentaries on 10 GDPR articles* (from Commentary on the EU General Data Protection Regulation, OUP 2019). Oxford University Press, 2018, p. 37. Disponível em: <https://works.bepress.com/christopher-kuner/1/>. Acesso em: 22.07.19

KRAMER, Adam D. I.; GUILLORY, Jamie E.; HANCOCK, Jeffrey T. Experimental evidence of massive-scale emotional contagion through social networks. *PNAS*, vol. 111, n. 24, jun. 2014, p. 8788-8790. Disponível em: <https://doi.org/10.1073/pnas.1320040111> Acesso em: 19.01.21

KRUTZINNA, Jenny; TADDEO, Mariarosaria; FLORIDI, Luciano. Enabling Posthumous Medical Data Donation: A Plea for the Ethical Utilisation of Personal Health Data. In: KRUTZINNA, Jenny; FLORIDI, Luciano (Eds.) *The Ethics of Medical Data Donation*. Springer. 2019.p. 163-180.

LANGENEGGER, Natalia; GOBBATO, Andréa. Compatibilização da Lei de Acesso à Informação com a Lei Geral de Proteção de Dados Pessoais: desafios no âmbito do Poder Judiciário. *Revista do Advogado*, São Paulo, v. 39, n. 144, p. 141-148, nov. 2019.

LATERÇA, Priscilla Silva; FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (Coords.). *Privacidade e Proteção de Dados de Crianças e Adolescentes*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021. E-book.

LEITE, Fábio. A liberdade de crença e o sacrifício de Animais em cultos religiosos. *Veredas do Direito*, Belo Horizonte, v.10, n.20, p.163-177, jul./dez. 2013.

LEMOS, Ronaldo; BRANCO, Sérgio. Privacy by design: conceito, fundamentos e aplicabilidade na LGPD. In: Bruno Bioni, Laura Schertel Mendes, Danilo Doneda, Otavio Luiz Rodrigues Jr., Ingo Wolfgang Sarlet. (Org.). *Tratado de Proteção de dados pessoais*. 1ed. Rio de Janeiro: Forense, 2021. E-book.

LEMOS, Ronaldo; BRANCO, Sérgio. Privacy by design: conceito, fundamentos e aplicabilidade na LGPD. In: Bruno Bioni, Laura Schertel Mendes, Danilo Doneda, Otavio Luiz Rodrigues Jr., Ingo Wolfgang Sarlet. (Org.). *Tratado de Proteção de dados pessoais*. 1ed. Rio de Janeiro: Forense, 2021. E-book.

LEONARDI, Marcel. Principais bases legais de tratamento de dados pessoais no setor privado. *In*: SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (Coords.). *Lei geral de proteção de dados*. São Paulo: RT, 2019.

LESSIG, Lawrence. The Law of the Horse: What Cyberlaw Might Teach, 113 *Harvard Law Review*, p. 501-549, 1999. Disponível em: https://cyber.harvard.edu/works/lessig/finalhls.pdf. Acesso em: 13 out. 2018.

LIMA, Maria Batista. Identidade étnico/racial no Brasil: uma reflexão teórico-metodológica. *Revista Fórum identidades*. Ano 2, Volume 3, p. 33-46, jan-jun. 2008.

MAIA, Roberta Mauro Medina. A natureza jurídica da titularidade dos dados pessoais. In: MULHOLLAND, Caitlin. *A LGPD e o novo marco normativo no Brasil*. Arquipélago, 2020.

MALLET, Estêvão. Igualdade, discriminação e direito do trabalho. *Revista da Faculdade de Direito, Universidade de São Paulo*, v. 103, p. 241-267, 2008. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/67804. Acesso em: 5 abr. 2021.

MARIS, Elena; LIBERT, Timothy; HENRICHSEN, Jennifer R. Tracking Sex: The Implications of Widespread Sexual Data Leakage and Tracking on Porn Websites. *New Media & Society*, vol. 22, no. 11, Nov. 2020, p. 2018–2038. Disponível em: <https://doi.org/10.1177/1461444820924632> Acesso em: 07.03.21.

MARQUES, Cláudia Lima. O diálogo das fontes como método da nova teoria geral do direito: um tributo a Erik Jayme. In.: _____ (coord.) *Diálogo das fontes:* do conflito à coordenação de normas no direito brasileiro novo regime das relações contratuais. São Paulo: RT, 2012, p.17-66.

MARQUES, Claudia Lima; MIRAGEM, Bruno. *O novo direito privado e a proteção dos vulneráveis.* 2. ed. São Paulo: Revista dos Tribunais, 2014.

MARTINS, Guilherme Magalhães; SOARES, Flaviana Rampazzo. Proteção de dados pessoais em e-saúde: seu confronto com a utilidade do fornecimento e uso de dados, em aplicativos para dispositivos móveis. *Revista de Direito do Consumidor*, vol. 130, jul.-ago. / 2020.

MATOS, Ana Carla Harmatiuk; RUZYK, Carlos Eduardo Pianovski. Diálogos entre a Lei Geral de Proteção de Dados e a Lei de Acesso à Informação. *In:* FRAZÃO, Ana; OLIVA, Milena Donato; TEPEDINO, Gustavo (coord.). *Lei Geral de Proteção de Dados Pessoais*: e suas repercussões no Direito brasileiro. São Paulo: Revista dos Tribunais, 2019. p. 199-218.

MAYER-SCHOENBERGER, V.; CUKIER, K. *Big Data*: a revolution that will transform how we live, work, and think. Londres: John Murray, 2013.

MAYSON, Sandra Gabriel. *Bias In, Bias Out*. University of Georgia School of Law Legal Studies, Research Paper No. 2018-35. Disponível em: <https://ssrn.com/abstract=3257004> Acesso em: 03.05.21.

MCCULLAGH, K. Data Sensitivity: Proposals for Resolving the Conundrum, *Journal of International Commercial Law and Technology* 2, 2007, p. 190–201.

MEDEIROS, M. S. de; BORGES, L.; FILHO, J. E. T. ; LUCENA, R. C. B. de . Limites e contradições do uso de tecnologias digitais em saúde no contexto da pandemia da

COVID-19 no Brasil. *Serviço Social e Saúde*, Campinas, SP, v. 20, n. 00, p. e021002, 2021. Disponível em: https://periodicos.sbu.unicamp.br/ojs/index.php/sss/article/view/8665391. Acesso em: 3 jan. 2022.

MEDON, Filipe. *Inteligência Artificial e Responsabilidade Civil*: autonomia, riscos e solidariedade. 1. ed. Salvador: JusPodivm, 2020. 448p.

MEJIAS, Ulises A.; COULDRY, Nick. Datafication. *Internet Policy Review*, 8(4). 2019. Disponível em: <https://policyreview.info/concepts/datafication>. Acesso em: 27 jul. 2021.

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. *Pensar*, Fortaleza, v. 25, n. 4, p. 1-18, out./dez. 2020.

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. *Revista de Direito do Consumidor*, v. 120, p. 555, 2018.

MERKEL, Jeremy. Dark Patterns Come to Light in California Data Privacy Laws. The National Law Review, vol. XI, n. 183, 02 de jul. de 2021. Disponível em: < https://www.natlawreview.com/article/dark-patterns-come-to-light-california-data-privacy-laws>. Acesso em: 03 de jul. de 2021.

MIRAGEM, Bruno. *Curso de Direito do Consumidor.* 3ed. São Paulo: RT, 2012.

MIRAGEM, Bruno; PETERSEN, Luiza. O contrato de seguro e a lei geral de proteção de dados. *Revista dos Tribunais*, vol.1018, agosto de 2020.

MIRANDA, Monique. *Classificação de raça, cor e etnia*: conceitos, terminologia e métodos utilizados nas ciências da saúde no Brasil, no período de 2000 a 2009. Dissertação de mestrado. Rio de Janeiro: 2010.

MORAES, Maria Celina Bodin de. *Na medida da pessoa humana*: estudos de direito civil. Rio de Janeiro: Renovar, 2010.

MORAES, Maria Celina Bodin de. Recusa à realização do exame de DNA e direitos da personalidade, In: *Na medida da pessoa humana*. Estudos de direito civil constitucional, Rio de Janeiro: Ed. Renovar, 2010.

MOREIRA, André de Oliveira Schenini. A exceção dos dados pessoais tornados manifestamente públicos pelo titular na LGPD. Migalhas, publicado em 07 de janeiro de 2019. Disponível em: <https://www.migalhas.com.br/depeso/293745/a-excecao-dos-dados-pessoais-tornados-manifestamente-publicos-pelo-titular-na-lgpd> Acesso em: 01.08.21.

MOREIRA, Rodrigo Pereira. *Direito ao Livre Desenvolvimento da Personalidade*. Juruá: 2016.

MULHOLLAND, C. O tratamento de dados pessoais sensíveis. In: Mulholland, Caitlin (Org.). *LGPD e o novo marco normativo no Brasil.* Porto Alegre: Arquipélago Editorial, 2020, v. 1.

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

MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. *Migalhas*, publicado em 22 de junho de 2020. Disponível em: <https://migalhas.uol.com.br/coluna/migalhas-de-vulnerabilidade/329261/dados-pessoais-sensiveis-e-consentimento-na-lei-geral-de-protecao-de-dados-pessoais> Acesso em: 02.11.20.

MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei geral de Proteção de Dados Pessoais. Revista do Advogado, n. 144, nov. 2019, p. 47-53.

MULHOLLAND, Caitlin. Os contratos de seguro e a proteção dos dados pessoais sensíveis. In: GOLDBERG, Ilan; JUNQUEIRA, Thiago (Coords.). *Temas Atuais de Direito dos Seguros*, Tomo I. São Paulo: Thomson Reuters. 2020.

MULHOLLAND, Caitlin; FRAJHOF, I. Entre as leis da robótica e a ética: regulação para o adequado desenvolvimento da Inteligência Artificial. In: Mafalda Miranda Barbosa; Felipe Braga Netto; Michael César Silva; José Luiz de Moura Faleiros Júnior. (Org.). *Direito Digital e Inteligência Artificial*: diálogos entre Brasil e Europa. 1ed.Belo Horizonte: Editora Foco, 2021, v. 1, p. 65-80.

MULHOLLAND, Caitlin; KREMER, Bianca. Responsabilidade civil por danos causados pela violação do princípio da igualdade no tratamento de dados pessoais. In: Rodrigo da Guia Silva; Gustavo Tepedino. (Org.). *O Direito Civil na era da inteligência artificial*. São Paulo: Revista dos Tribunais, 2020, p.565-584.

MULHOLLAND, Caitlin; PALMEIRA, Mariana. As bases legais para tratamento de dados de crianças e adolescentes. In: LATERÇA, Priscilla Silva; FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (Coords.). *Privacidade e Proteção de Dados de Crianças e Adolescentes*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021. Edição do Kindle.

MUNANGA, Kabengele. *Negritude*: usos e sentidos. 4.ed. Autêntica: 2019.

MUNANGA, Kabengele. *Rediscutindo a mestiçagem no Brasil:* identidade nacional versus identidade negra. 5. ed. Autêntica: 2019.

NEGRI, Sergio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. A normatividade dos dados sensíveis na lei geral de proteção de

dados: ampliação conceitual e proteção da pessoa humana. *Rev. de Direito, Governança e Novas Tecnologias*, Goiânia, v. 5, n. 1, p. 63-85, Jan/Jun. 2019.

NOBLE, Safiya Umoja. *Algorithms of Oppression*: How Search Engines Reinforce Racism. NYU Press, 2018.

NORWEGIAN DATA PROTECTION AUTHORITY. *Software development with Data Protection by Design and by Default*. Nov. 2017. Disponível em: <https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?print=true> Acesso em: 04.08.21.

NOUWENS, Midas. LICCARDI, Illaria. VEALE, Michale, *et al*. Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. Disponível em: <https://iapp.org/resources/article/dark-patterns-after-the-gdpr-scraping-consent-pop-ups-and-demonstrating-their-influence/> Acesso em: 22.07.21

OBERMEYER, Ziad. Et al. Dissecting racial bias in an algorithm used to manage the health of populations. *Science*, 25.10.2019: Vol. 366, Issue 6464, pp. 447-453. Disponível em: <https://science.sciencemag.org/content/366/6464/447>. Acesso em: 01.12.2020.

OECD, *A Caminho da Era Digital no Brasil*, OECD Publishing, Paris, 2020. Disponível em: <https://doi.org/10.1787/45a84b29-pt.> Acesso em: 18.12.20.

OECD. The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines. *OECD Digital Economy Papers*, n. 176, OECD Publishing, Paris, 2011, p. 31-32. Disponível em: <https://doi.org/10.1787/5kgf09z90c31-en> Acesso em: 03.01.21

OLIVA, Milena. GUIA, R. Notas sobre o compliance no direito brasileiro. *Revista quaestio iuris*, v. 11, p. 2708-2729, 2018.

OLIVA, Milena; Silva, Jeniffer. Discriminação algorítmica nas relações de consumo. Migalhas, publicado em 23 de fevereiro de 2021. Disponível em: <https://www.migalhas.com.br/depeso/340680/discriminacao-algoritmica-nas-relacoes-de-consumo> Acesso em: 03.07.21

OLIVEIRA, Rafael Carvalho Rezende. Direito Administrativo e coronavírus. *Migalhas*, 17 de março de 2020. Fonte: <https://www.migalhas.com.br/depeso/321892/direito-administrativo-e-coronavirus> Acesso em: 13.04.20.

O'NEIL, Cathy. *Weapons of Math Destruction*: How Big Data Increases Inequality and Threatens Democracy. Crown: 2016.

ONU. Alto Comissariado das Nações Unidas. *Nascidos livres e iguais:* Orientação Sexual e Identidade de Gênero no Regime Internacional de Direitos Humanos, Brasília, 2013.

ONU. Convenção sobre os Direitos da Criança. *Comentário geral nº 25 sobre os direitos das crianças em relação ao ambiente digital.* 2021. Disponível em: <https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx> Acesso em: 26.01.21

ONU. Data Strategy of the Secretary-General for Action by Everyone, Everywhere with Insight, Impact and Integrity. 2020. Disponível em: <https://un.org/en/content/datastrategy/images/pdf/UN_SG_Data-Strategy.pdf>. Acesso em: 28 jun. 2021.

PALHARES, Felipe. Vantagem econômica no compartilhamento de dados de saúde: interpretação do artigo 11, § 4º, da LGPD. In: DALLARI, Analluza Bolivar; MONACO; Gustavo Ferraz de Campos (Org.). LGPD na saúde. São Paulo: Revista dos Tribunais, 2021.

PALHARES, Felipe; PRADO, Luis; VIDIGAL, Paulo. *Compliance digital e LGPD.* São Paulo: Thomson Reuters Brasil, 2021.

PASQUALE, Frank. *The black box society*. Cambridge: Harvard University Press. 2015.

PASQUALOTTO, Adalberto; SOARES, Flaviana. Consumidor hipervulnerável: análise crítica, substrato axiológico, contornos e abrangência. *Revista de Direito do Consumidor*, vol. 113, p. 81-109, Set.-Out./2017.

PAVÃO, Juliana Carvalho; ESPOLADOR, Rita de Cássia Resquetti Tarifa. A proteção de dados clínicos durante a pandemia da COVID-19: comentários à luz dos direitos da personalidade e dos referenciais bioéticos. *SCIENTIA IURIS*, Londrina, v. 25, n. 3, p. 125-140, nov. 2021.

PEÑA, Paz; VARON, Joana. *O poder de dizer NÃO na Internet.* Coding Rights. Disponível em: https://medium.com/codingrights/o-poder-de-dizer-não-na-internet-17d6e9889d4a. Acesso em: 29 julho. 2019.

PENA, Sérgio Danilo Junho; BIRCHAL, Telma de Souza. A inexistência biológica versus a existência social de raças humanas: pode a ciência instruir o etos social? *Revista USP*, nº 68, fevereiro de 2006, p. 10-21.

PERLINGIERI, Pietro. *O Direito Civil na legalidade constitucional.* Rio de Janeiro: Renovar, 2008.

PERLINGIERI, Pietro. *Perfis do Direito Civil. Introdução ao Direito Civil Constitucional.* Rio de Janeiro: Editora Renovar, 2007.

PINHEIRO, Iuri; BOMFIM, Vólia. A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho. Disponível em: <http://trabalhoemdebate.com.br/artigo/detalhe/a-lei-geral-de-protecao-de-dados-e-seus-impactos-nas-relacoes-de-trabalho> Acesso em: 14.07.21.

PINTO, Carlos Alberto da Mota. *Teoria Geral do Direito Civil*, 4ª Ed. atualizada por António Pinto Monteiro e Paulo Mota Pinto, Coimbra: Coimbra Editora, 2005.

PINTO, Paulo Mota. A influência dos direitos fundamentais sobre o direito privado português. In. MONTEIRO, António Pinto; NEUNER, Jörg; SARLET, Ingo (Orgs.). *Direitos fundamentais e direito privado:* uma perspectiva de direito comparado. Coimbra: Almedina, 2007.

PINTO, Paulo Mota. O direito ao livre desenvolvimento da personalidade. In: CANOTILHO, José Joaquim Gomes (coordenador). *Portugal-Brasil ano 2000*. Coimbra: Coimbra, 1999.

MIRANDA, Felipe Arady. O direito fundamental ao livre desenvolvimento da personalidade. *Revista do Instituto do Direito Brasileiro.* Ano 2, n. 10, p. 11175-11211. Lisboa, 2013.

PIOVESAN, Flávia; SILVA, Sandro Gorski. Diversidade sexual e o contexto global: desafios à plena implementação dos direitos humanos LGBTI. *Quaestio Iuris*. vol. 08, nº. 04, Número Especial. Rio de Janeiro, 2015. p. 2613-2650.

PLUNKETT, Leah A. *Sharenthood*: Why We Should Think before We Talk about Our Kids Online. The MIT Press, 2019.

POMPEU, Márcio. A LGPD como condição para as *healthtechs* captarem investimentos. Conjur, publicado em 11 de março de 2021. Disponível em: <https://www.conjur.com.br/2021-mar-11/pompeu-lgpd-condicao-healthtechs-captarem-investimentos#_ftn1> Acesso em: 17 de março de 2021.

PRESGRAVE, Ana Beatriz Ferreira Rebello; HILDEBRAND, Cecília Rodrigues Frutuoso; PEIXOTO, Renata Cortez Vieira. Pais que dão à luz: como o direito brasileiro regulamenta o registro dos filhos de transgêneros? *IBDFAM*, publicado em: 24 de fevereiro de 2021. Disponível em: <https://ibdfam.org.br/artigos/1652/Pais+que+d%C3%A3o+%C3%A0+luz%3A+como+o+direito+brasileiro+regulamenta+o+registro+dos+filhos+de+transg%C3%AAneros%3F> Acesso em: 07.03.21

EUROPEAN COMMISSION. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM/2017/010 final - 2017/03 (COD). Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010> Acesso em: 01.01.21

PSCHEIDT, Kristian Rodrigo. A relação entre a LGPD e a apuração da boa-fé contratual. Conjur, publicado em 07 de dezembro de 2020. Disponível em: <https://www.conjur.com.br/2020-dez-07/pscheidt-relacao-entre-lgpd-boa-fe-contratual> Acesso em: 28.07.21.

QUELLE, Claudia. Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability-and Risk-based Approach, *European Journal of Risk Regulation*, 9, p. 502-526. 2018.

QUINN, Paul; MALGIERI, Gianclaudio. The Difficulty of Defining Sensitive Data – the Concept of Sensitive Data in the EU Data Protection Framework. *Brussels Privacy Hub Research Paper*, publicado em 16 de outubro de 2020. Disponível em: <https://ssrn.com/abstract=3713134> Acesso em: 02.01.21

RAO, Dattaraj Jagdish; MANE, Shraddha. Digital Twin approach to Clinical DSS with Explainable AI. 2019. Disponível em: <https://arxiv.org/ftp/arxiv/papers/1910/1910.13520.pdf>. Acesso em: 28 jun. 2021

REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679> Acesso em: 21 jan. 2021.

RIBEIRO, Darcy. *O Povo Brasileiro.* Companhia de Bolso, 2006.

RIBEIRO, Djamila. Pequeno manual antirracista. São Paulo: Companhia das Letras, 2019.

RIOS, Roger Raupp. Tramas e interconexões no Supremo Tribunal Federal: Antidiscriminação, gênero e sexualidade. *Rev. Direito Práx.*, Rio de Janeiro, v. 11, n. 2, p. 1332-1357, abril. 2020. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S2179-89662020000201332&lng=en&nrm=iso> Acesso em: 28.12.20.

RIOS, Roger Raupp; LEIVAS, Paulo Gilberto Cogo; SCHÄFER, Gilberto. Direito da antidiscriminação e direitos de minorias: perspectivas e modelos de proteção individual e coletivo. *Rev. direitos fundam. democ.*, v. 22, n. 1, p. 126-148, jan./abr. 2017.

RODOTÀ, Stefano. *A vida na sociedade da vigilância – a privacidade hoje.* Coord. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RODOTÀ, Stefano. Costruzione del corpo, XXI Secolo. 2009. Disponível em: <http://www.treccani.it/enciclopedia/costruzione-del-corpo_(XXI_Secolo)/> Acesso em: 01.03.21.

RODOTÀ, Stefano. *Il diritto di avere diritti.* Roma-Bari: Laterza, 2012.

RODOTÀ, Stefano. *Il mondo nella rete*: Quali i diritti, quali i vincoli. Roma: Laterza & Figli – Gruppo Editoriale L'Espresso, 2019.

RODOTÀ, Stefano. Salviamo il corpo. Trecho de discurso proferido em conferência sobre "Transformações do corpo e dignidade da pessoa", Roma, 04 de maio de 2005. Disponível em: <https://www.privacy.it/archivio/rodo20050504.html> Acesso em: 02.02.21

RODRIGUES, Alexandre; SANTOS, Priscilla. A ciência que faz você comprar mais. *Galileu*. out. 2012. Disponível em: <http://revistagalileu.globo.com/Revista/Common/0,,EMI317687-17579,00-A+CIENCIA+QUE+FAZ+VOCE+COMPRAR+MAIS.html> Acesso em: 31 maio 2020.

RODRIGUES, Marco Antonio dos Santos; HIBNER, Davi Amaral. Parâmetros para a proteção de dados pessoais em tempos de pandemia. *Revista de Direito e as Novas Tecnologias*, vol. 8/2020, Jul - Set / 2020.

ROTHBARTH, Renata. Monetização de dados de saúde à luz da LGPD: interpretação do artigo 11, §3º. In: DALLARI, Analluza Bolivar; MONACO; Gustavo Ferraz de Campos (Org.). LGPD na saúde. São Paulo: Revista dos Tribunais, 2021.

RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da lei geral de proteção de dados (LGPD) – Lei 13.709/2018. In: Bruno Bioni, Laura Schertel Mendes, Danilo Doneda, Otavio Luiz Rodrigues Jr., Ingo Wolfgang Sarlet. (Org.). *Tratado de Proteção de dados pessoais*. 1ed. Rio de Janeiro: Forense, 2021. E-book.

SAAVEDRA, Giovani Agostini. Compliance de dados. In: Bruno Bioni, Laura Schertel Mendes, Danilo Doneda, Otavio Luiz Rodrigues Jr., Ingo Wolfgang Sarlet (Org.). *Tratado de Proteção de dados pessoais*. 1ed.Rio de Janeiro: Forense, 2021, v. 1.

SARLET, Ingo. Precisamos da previsão de um direito fundamental à proteção de dados no texto da CF? *Conjur*, publicado em 4 de setembro de 2020. Disponível em: <https://www.conjur.com.br/2020-set-04/direitos-fundamentais-precisamos-previsao-direito-fundamental-protecao-dados-cf> Acesso em: 26.12.20.

SCHREIBER, Anderson. *Direitos da Personalidade.* 2. ed. São Paulo: Atlas, 2013.

SCHULMAN, Gabriel. Tecnologias de telemedicina, Responsabilidade Civil e Dados Sensíveis. O princípio ativo da Proteção de Dados pessoais do paciente e os efeitos colaterais do coronavírus. *Coronavírus e Responsabilidade Civil.* Foco: Indaiatuba, 2020, p. 335-354.

SCHULMAN, Gabriel; CAVET, Caroline Amadori. As violações de dados pessoais na telemedicina: tecnologia, proteção e reparação ao paciente 4.0. In: *Debates Contemporâneos em Direito Médico e da Saúde.* São Paulo, RT, 2020. p. 145-174.

SCHULMAN, Gabriel; PEREIRA, Paula Moura. Futuro da saúde e saúde do futuro: impactos e limites reais da inteligência artificial. In: TEPEDINO, Gustavo; GUIA, Rodrigo da (Org.). *O Direito Civil na era da inteligência artificial.* São Paulo: RT, 2020, p. 165-182.

SIMÃO, Bárbara; FRAGOSO, Nathalie; ROBERTO, Enrico. *Reconhecimento Facial e o Setor Privado*: Guia para a adoção de boas práticas. InternetLab/IDEC, São Paulo, 2020.

SKINNER-THOMPSON, Scott. *Privacy at margins*. Cambridge: Cambridge University Press, 2020.

SOLOVE, Daniel J. The Myth of the Privacy Paradox (January 29, 2021). 89 *George Washington Law Review* 1 (2021). Disponível em: <https://ssrn.com/abstract=3536265> Acesso em: 02.02.21.

SOUZA, Carlos Affonso. Eles sabem quem é você? Entenda o monitoramento de celulares na quarentena. Disponível em: <https://tecfront. blogosfera.uol.com.br/2020/04/17/eles-sabem-quem-e-voce-entenda-o-monitoramento-de-celulares-na-quarentena/>. Acesso em: 03.05.20

SOUZA, Carlos Affonso. Segurança e Sigilo dos Dados Pessoais: primeiras impressões à luz da Lei nª 13.709/18. In: Gustavo Tepedino; Ana Frazão; Milena Donato. (Org.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro*. 1ed.São Paulo: Revista dos Tribunais, 2019, v. 1, p. 417-440.

SOUZA, Carlos Affonso; PADRAO, V. Incidentes de segurança e dever de notificação à luz da Lei Geral de Proteção de Dados Pessoais. In: Carlos Affonso Souza; Eduardo Magrani; Priscilla Silva. (Org.). *Lei Geral de Proteção de Dados (LGPD).* 1ed.São Paulo: Revista dos Tribunais, 2019, v. 1, p. 213-226.

SOUZA, Carlos Affonso; PADRÃO, Vinicius. Incidentes de segurança e dever de notificação à luz da Lei Geral de Proteção de Dados Pessoais. *In:* SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (coord.). *Caderno Especial*: Lei Geral de Proteção de Dados (PGPD). São Paulo: Revista dos Tribunais, 2019.

SOUZA, Carlos Affonso; PERRONE, C.; MAGRANI, Eduardo. O Direito à Explicação entre a experiência europeia e a sua positivação na LGPD. *Tratado de Proteção de Dados Pessoais.* 1ed.Rio de Janeiro: Forense, 2020, v. 1, p. 243-270.

SOUZA, Maria de Fátima Marinho de. Dos dados à política: a importância da informação em saúde. *Epidemiol. Serv. Saúde*, Brasília, v.17, n.1, p. 5-6, mar. 2008. Disponível em: <http://scielo.iec.gov.br/scielo.php?script=sci_arttext&pid=S1679-49742008000100001&lng=pt&nrm=iso>. Acesso em: 21 jan. 2021.

STEINBERG, Stacey. *Growing Up Shared*: How Parents Can Share Smarter on Social Media-and What You Can Do to Keep Your Family Safe in a No-Privacy World. Sourcebooks, 2020.

SUNDFELD, Philippe; FERNANDES, Maria Luiza**.** LGPD e UX: um equilíbrio para o consentimento. *Jota*, publicado em 16 de julho de 2021. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/lgpd-e-ux-um-equilibrio-para-o-consentimento-16072021> Acesso em: 22.07.21

TEFFÉ, Chiara A. Spadaccini de. Brinquedos sexuais e coleta de dados sensíveis: voyeurismo 3.0? *Medium ITS Rio*, maio de 2017. Disponível em: <https://feed.itsrio.org/brinquedos-sexuais-e-coleta-de-dados-%C3%ADntimos-voyeurismo-3-0-be570007bf1f > Acesso em 07.03.21

TEFFÉ, Chiara Antonia Spadaccini de. *A tutela da imagem da pessoa humana na internet:* da identificação do dano à sua compensação. 2016. 226 f. Dissertação (Mestrado em Direito Civil) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2016.

TEFFÉ, Chiara Spadaccini de. A saúde na sociedade da vigilância: como proteger os dados sensíveis? *Migalhas*. Publicado em: 14 abr. 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-vulnerabilidade/324485/a-saude-na-sociedade-da-vigilancia-como-proteger-os-dados-sensiveis. Acesso em: 31 maio 2020.

TEFFÉ, Chiara Spadaccini de. Dados sensíveis de crianças e adolescentes: aplicação do melhor interesse e tutela integral. In: LATERÇA, Priscilla Silva; FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (Coords.). *Privacidade e Proteção de Dados de Crianças e Adolescentes*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021. E-book.

TEFFÉ, Chiara Spadaccini de. Desafio da Baleia Azul: o que se sabe até agora. ITS FEED, 25 abr. 2017. Disponível em: <https://feed.itsrio.org/desafio-da-baleia-azul-o-que-se-sabe-at%C3%A9-agora-b4b85ae77a56> Acesso em 04.06.21.

TEFFÉ, Chiara Spadaccini de. Exposição não consentida de imagens íntimas: como o Direito pode proteger as mulheres? In: Nelson Rosenvald; Rafael Dresch; Tula Wesendonck (Org.). *Responsabilidade civil*: novos riscos. 1ed.Indaiatuba: Foco, 2019. p. 91-113.

TEFFÉ, Chiara Spadaccini de. LGPD em programas de compliance: vantagem competitiva e aderência às práticas ESG. Jota, publicado em 10 de junho de 2021. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/lgpd-em-programas-de-compliance-vantagem-competitiva-e-aderencia-as-praticas-esg-10062021> Acesso em: 11.06.21

TEFFÉ, Chiara Spadaccini de. Proteção de dados de crianças e adolescentes. *Revista do Advogado*, v. 39, 2019.

TEFFÉ, Chiara Spadaccini de. Proteção de dados pessoais na Rede: resenha à obra "A internet das coisas", de Eduardo Magrani. *Civilistica.com*. Rio de Janeiro, a. 7, n. 1, 2018. Disponível em: <http:// civilistica.com/protecao-de-dados-pessoais-na-rede/>. Data de acesso: 02.11.20

TEFFÉ, Chiara Spadaccini de; ALMEIDA, J. Humor e responsabilidade na Internet. In: Guilherme Martins; Nelson Rosenvald. (Org.). *Responsabilidade civil e novas tecnologias*. 1ed.Indaiatuba: FOCO, 2020, p. 125-144.

TEFFÉ, Chiara Spadaccini de; FERNANDES, Elora. Contratação em redes sociais e proteção de dados de crianças e adolescentes. In: ROQUE, André Vasconcelos; OLIVA, Milena Donato. *Direito na era digital:* aspectos negociais, processuais e registrais. Salvador: Juspodivm, 2022. p.97-122.

TEFFÉ, Chiara Spadaccini de; FERNANDES, Elora. Tratamento de dados sensíveis por tecnologias de reconhecimento facial: proteção e limites. In: Gustavo Tepedino, Rodrigo da Guia Silva. (Org.). *O Direito Civil na Era da Inteligência Artificial.* 1ed.São Paulo: Editora do Tribunais, 2020, v. 1, p. 283-310.

TEFFÉ, Chiara Spadaccini de; MAGRANI, E.; STEIBEL, F. Juguetes conectados y tutela de la privacidad de niños y adolescentes: explorando beneficios y desafíos. In: Lionel Ricardo Brossi Garavaglia; Tomás Dodds Rojas; Ezequiel Passeron (Org.). *Inteligencia artificial y bienestar de las juventudes en América Latina*. Santiago: LOM ediciones, 2019, v. 1, p. 197-202.

TEFFÉ, Chiara Spadaccini de; MEDON, Filipe. responsabilidade civil e regulação de novas tecnologias: questões acerca da utilização de inteligência artificial na tomada de decisões empresariais. *Revista estudos institucionais*, v. 6, p. 301-333, 2020.

TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. Redes sociais virtuais: privacidade e responsabilidade civil: análise a partir do Marco Civil da Internet. *Pensar*, Fortaleza, v. 22, n. 1, p. 108-146, jan./abr. 2017.

TEFFÉ, Chiara Spadaccini de; SOUZA, Carlos Affonso. Infância conectada: direitos e educação digital. In: Comitê Gestor da Internet no Brasil. (Org.). *Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil:* TIC kids online Brasil 2017. 1ed.São Paulo: Comitê Gestor da Internet no Brasil, 2018, v. 1, p. 31-40.

TEFFÉ, Chiara Spadaccini de; VIOLA, M. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. *Civilistica.com*, v. 9, p. 1-38, 2020.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. *Proposta para a criação da Autoridade Brasileira de Proteção aos Dados Pessoais.* Rio de Janeiro: ITS Rio, 2018.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11. In: BIONI, Bruno; DONEDA, Danilo; SARLET, Ingo Wolfgang; SCHERTEL, Laura; JUNIOR, Otavio Luiz Rodrigues

(Coord.). *Tratado de Proteção de Dados Pessoais*. 1ª ed. Rio de Janeiro: Editora Forense, 2021.

TEIXEIRA, Ana Carolina Brochado; RETTORE, Anna Cristina de Carvalho. O princípio do melhor interesse no ambiente digital. In: LATERÇA, Priscilla Silva; FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (Coords.). *Privacidade e Proteção de Dados de Crianças e Adolescentes*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021. Edição do Kindle.

TEIXEIRA, Ana Carolina Brochado; RETTORE, Anna Cristina de Carvalho. A autoridade parental e o tratamento de dados pessoais de crianças e adolescentes. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Revista dos Tribunais, 2019.

TELFORD, Taylor. Apple Card algorithm sparks gender bias allegations against Goldman Sachs. *Washington Post*, 11.11.2019. Disponível em: <https://www.washingtonpost.com/business/2019/11/11/apple-card-algorithm-sparks-gender-bias-allegations-against-goldman-sachs/>. Acesso em: 26.11.2020.

TEPEDINO, Gustavo; OLIVA, Milena Donato. Tratamento de dados de crianças e adolescentes na LGPD e o sistema de incapacidades do Código Civil. In: LATERÇA, Priscilla Silva; FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (Coords.). *Privacidade e Proteção de Dados de Crianças e Adolescentes*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021. Edição do Kindle.

TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (Org.). *O Direito Civil na era da inteligência artificial*. 1. ed. São Paulo: Thomson Reuters Brasil, 2020. v. 1. 800p.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. O consentimento na circulação de dados pessoais. *Revista Brasileira de Direito Civil – RBDCivil*, Belo Horizonte, v. 25, p. 83-116, jul./set. 2020.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. O consentimento na circulação de dados pessoais. *Revista Brasileira De Direito Civil*, v. 25, p. 83-116, 2020.p.109-110

THALER, Richard H.; SUNSTEIN, Cass R. *Nudge*: Improving Decisions about Health, Wealth and Happiness. New Haven: Yale University Press, 2008.

TIC KIDS ONLINE BRASIL 2019. Resumo Executivo - Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil. Novembro de 2020. p.04. Disponível em: <https://cetic.br/pt/publicacao/resumo-executivo-pesquisa-sobre-o-uso-da-internet-por-criancas-e-adolescentes-no-brasil-tic-kids-online-brasil-2019/> Acesso em: 05.06.21

TOPOL, Eric. High-performance medicine: the convergence of human and artificial intelligence. *Nature Medicine*, v. 25, p. 44-56, jan. 2019.

TORQUATO-DE-OLIVEIRA-NAVES, Bruno; GOIATA, Sarah Rêgo. Direitos Humanos, patrimônio genético e dados genéticos humanos: crítica à doutrina dos dados genéticos como interesse difuso. *Rev. Bioética y Derecho*, Barcelona, n. 40, p. 63-81, 2017. Disponível em: <http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872017000200006&lng=es&nrm=iso>. Acesso em: 03.03. 2021.

TRIBUNAL DE CONTAS DA UNIÃO. *10 passos para a boa gestão de riscos*. Brasília: TCU, Secretaria de Métodos e Suporte ao Controle Externo (Semec), 2018.

U.S. DEPARTMENT OF JUSTICE CYBERSECURITY UNIT. *Best Practices for Victim Response and Reporting of Cyber Incidents*. Version 2.0 (September 2018).

USTARAN, Eduardo. *European Data Protection Law and Practice.* Portsmouth: IAPP, 2018.

VAN DER HOF, Simone; LIEVENS, Eva. The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data under the GDPR. *Communications law*, edited by Paul Wragg, vol. 23, n. 1, 2018, p. 33-43. Disponível em: <https://ssrn.com/abstract=3107660> Acesso em: 04.08.21.

VARON, Joana. Entrevista II. *Panorama Setorial da Internet*, v. 11, n. 2, p. 12-14, 2019. Privacidade e dados pessoais. Disponível em: <https://www.cetic.br/media/docs/publicacoes/6/15122520190717-panorama_setorial_ano-xi_n_2_privacidade_e_dados_pessoais.pdf> Acesso em: 31 maio 2020

VEMOU, Konstantina; HORVATH, Anna. TechDispatch #1/2021 - Facial Emotion Recognition. Publicado em 26 de maio de 2021. Disponível em: <https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-12021-facial-emotion-recognition_en> Acesso em: 05.08.21.

VENTRE, Giovanna; CASTELLANO, Ana Carolina Heringer. O dilema do consentimento e a sobrecarga informacional. Jota, publicado em 28 de julho de 2021. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/dilema-consentimento-sobrecarga-informacional-lgpd-28072021> Acesso em: 28.07.21

VIANA, Marcio Túlio. Os dois modos de discriminar e o futuro do Direito do Trabalho. In: RENAULT, Luiz Otávio Linhares. VIANA, Márcio Tulio (coord). Discriminação: estudos. São Paulo: LTr, 2000. p. 321-328.

_____. A proteção trabalhista contra atos discriminatórios (análise da Lei 9.029/95). In: RENAULT, Luiz Otávio Linhares. VIANA, Márcio Tulio (coord). Discriminação: estudos. São Paulo: LTr, 2000. p. 354-367.

VICENT, James. California bans ‘dark patterns’ that trick users into giving away their personal data. The Verge, 16 de mar. de 2021. Disponível em: < https://www.theverge.com/2021/3/16/22333506/california-bans-dark-patterns-opt-out-selling-data>. Acesso em: 03 de jul. de 2021.

VOIGT, Paul; BUSSCHE, Axel von dem. The EU General Data Protection Regulation (GDPR). A Practical Guide. Springer, 2017.

WANG, Y.; KOSINSKI, M. Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. Disponível em: <psyarxiv.com/hv28a> Acesso: 02.11.20.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. *Harvard Law Review*. Vol. 4, No. 5 (Dec. 15, 1890), p. 193-220.

WEN, Chao Lung. Instituto de Estudos de Saúde Suplementar: Telemedicina do presente para o ecossistema de saúde conectada 5.0. Disponível em: <https://www.iess.org.br/cms/rep/Telemedicina_Chao.pdf> Acesso em: 26 fev. 21.

WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo poder público. In: Bruno Bioni, Laura Schertel Mendes, Danilo Doneda, Otavio Luiz Rodrigues Jr., Ingo Wolfgang Sarlet. (Org.). *Tratado de Proteção de dados pessoais*. 1ed.Rio de Janeiro: Forense, 2021. E-book.

WU, Tim. *The Attention Merchants: The Epic Scramble to Get Inside Our Heads.* Knopf, 2016.

YUDELL, Michael; ROBERTS, Dorothy; DESALLE, Rob; TISHKOFF, Sarah. Taking race out of human genetics. *Science*, Vol. 351, edição 6273, fev. 2016, p. 564-565. Disponível em: <https://science.sciencemag.org/content/351/6273/564> Acesso em: 29.03.21

ZANATTA, Rafael A. F. *Perfilização, Discriminação e Direitos:* do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais. Disponível em: <https://www.researchgate.net/publication/331287708> Acesso em: 09.01.21.

ZANATTA, Rafael. A tutela coletiva na proteção de dados pessoais. *Revista do Advogado*, São Paulo, a.39, n.144, nov. 2019, p.201-208.

ZANGEROLAME, Flávia; ALMEIDA, Vitor. A seletividade sexual e a intolerância à diversidade: a silenciosa discriminação cotidiana como dano injusto, migalhas, 5 de julho de 2021. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-vulnerabilidade/348038/a-seletividade-sexual-e-a-intolerancia-a-diversidade> Acesso em: 06.07.21

ZUBOFF, Shoshana. *The Age of Surveillance Capitalism*: The Fight for a Human Future at the New Frontier of Power. 1.ed. PublicAffairs: 2019.

WACHTER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review*, vol. 2019, Issue 1. p.01-130.

5 RIGHTS FOUNDATION. But how do they know it is a child? Age Assurance in the Digital World. Março de 2021. Disponível: <https://5rightsfoundation.com/in-action/but-how-do-they-know-it-is-a-child-age-assurance-in-the-digital-world.html> Acesso em: 11.06.21.