UNIVERSIDADE FEDERAL DE ALAGOAS – UFAL
FACULDADE DE DIREITO DE ALAGOAS – FDA
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO – PPGD
MESTRADO EM DIREITO

JÉSSICA ANDRADE MODESTO

O DIREITO À PRIVACIDADE NA SOCIEDADE DA INFORMAÇÃO À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: UMA ANÁLISE DA (IN)EFETIVIDADE DA LEI Nº 13.709/2018 NO BRASIL A PARTIR DO ESTUDO COMPARATIVO COM O REGULAMENTO GERAL DE PROTEÇÃO DE DADOS DA UNIÃO EUROPEIA

Maceió/AL
2021

JÉSSICA ANDRADE MODESTO

O DIREITO À PRIVACIDADE NA SOCIEDADE DA INFORMAÇÃO À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: UMA ANÁLISE DA (IN)EFETIVIDADE DA LEI Nº 13.709/2018 NO BRASIL A PARTIR DO ESTUDO COMPARATIVO COM O REGULAMENTO GERAL DE PROTEÇÃO DE DADOS DA UNIÃO EUROPEIA

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Direito da Universidade Federal de Alagoas, como requisito parcial para obtenção do grau de Mestre em Direito.

Orientador: Prof. Dr. Marcos Augusto de Albuquerque Ehrhardt Júnior

Maceió/AL

2021

Catalogação na fonte
Universidade Federal de Alagoas
Biblioteca Central
Divisão de Tratamento Técnico

Bibliotecária Responsável: Helena Cristina Pimentel do Vale - CRB4/661

M691d Modesto, Jéssica Andrade.

O direito à privacidade na sociedade da informação à luz da lei geral de proteção de dados pessoais: uma análise da (in)efetividade da lei nº 13.709/2018 no Brasil a partir do estudo comparativo com o regulamento geral de proteção de dados da União Europeia / Jéssica Andrade Modesto. – 2021.

365 f. : il.

Orientador: Marcos Augusto de Albuquerque Ehrhardt Júnior.

Dissertação (mestrado em Direito) – Universidade Federal de Alagoas. Faculdade de Direito de Alagoas. Programa de Pós-Graduação em Direito, Maceió, 2021.

Bibliografia: f. 337-365.

1. Direito. 2. Lei geral de proteção de dados pessoais. – Brasil. 3. Sociedade da informação. 4. Proteção de dados pessoais. 5. Privacidade. I. Título.

CDU: 342.721(81)

Folha de Aprovação

AUTORA: JÉSSICA ANDRADE MODESTO

O DIREITO À PRIVACIDADE NA SOCIEDADE DA INFORMAÇÃO À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: UMA ANÁLISE DA (IN)EFETIVIDADE DA LEI Nº 13.709/2018 NO BRASIL A PARTIR DO ESTUDO COMPARATIVO COM O REGULAMENTO GERAL DE PROTEÇÃO DE DADOS DA UNIÃO EUROPEIA

Dissertação submetida ao corpo docente do Programa de Pós-Graduação em Direito da Universidade Federal de Alagoas e aprovada em 29 de julho de 2021.

MARCOS AUGUSTO DE ALBUQUERQUE EHRHARDT J

Assinado de forma digital por MARCOS AUGUSTO DE ALBUQUERQUE EHRHARDT J
Dados: 2022.02.07 16:15:50 -03'00'

Prof. Dr. Marcos Augusto de Albuquerque Ehrhardt Júnior (Orientador)

M.Catalan

Prof. Dr. Marcos Jorge Catalan (Examinador Externo)

Profa. Dra. Juliana de Oliveira Jota Dantas (Examinadora Interno)

Prof. Dr. José Barros Correia Júnior (Examinador Interno)

A Deus e à Nossa Senhora das Graças, minha força e minha certeza.

AGRADECIMENTOS

A Deus, por sempre cuidar de mim e me guiar na consecução dos meus objetivos.

À Nossa Senhora das Graças, a minha santinha, pelas diversas intercessões junto ao Pai. Não importa o tamanho da adversidade, eu sei que da Senhora sempre posso me socorrer!

Aos meus pais, Joseane e José, que nunca mediram esforços para que eu atingisse meus objetivos e sempre me apoiaram e acreditaram em mim, inclusive nos momentos em que discordaram de minhas escolhas. Com os senhores eu aprendi a ter a garra e a coragem necessárias para, diariamente, advogar, desempenhar minhas atribuições como servidora da Universidade Federal de Alagoas e, ainda, enfrentar o desafio de cursar um Mestrado.

Às minhas irmãs, Érica e Mônica, por todo o amor, colaboração, incentivo, compreensão, torcida e por cada momento compartilhado. Vocês são exemplo de persistência e dedicação.

À minha madrinha Lúcia, pela preocupação e apoio de toda uma vida.

À Taliny, filha que meu coração escolheu, por fazer meus dias mais felizes.

Ao meu orientador, professor Marcos Augusto de Albuquerque Ehrhardt Júnior, por todo o empenho e dedicação nas diversas análises deste trabalho, pela acessibilidade – até mesmo em domingos –, pela compreensão, por todo o incentivo, pelas diversas oportunidades a que me apresentou e por toda a contribuição para o meu crescimento acadêmico. Concluo esse Mestrado sabendo que ainda tenho uma infinidade a aprender, mas também tendo ciência do quanto evoluí.

Agradeço aos professores José Barros Correia Júnior, Juliana de Oliveira Jota Dantas e Marcos Jorge Catalan, pela disponibilidade em participar da banca e pelas valiosas contribuições, imprescindíveis para a finalização deste trabalho. De igual forma, agradeço aos demais professores do PPGD pelos ensinamentos e reflexões significativos que me possibilitaram amadurecer o projeto e a pesquisa. Agradeço ainda aos servidores desse programa pela solicitude.

À Ianá Priscilla de Oliveira Silva, a amiga com a qual a Faculdade de Direito de Alagoas, lá na graduação, presenteou-me e que logo tratei de levar para a vida inteira. São tantas coisas que já nem sei pelo que agradecer. Perdi a conta de quantas vezes solicitei o seu auxílio e, em todas elas, você sempre esteve lá. Tenho certeza que mais esta jornada que ora se encerra teria sido muito mais árdua sem você. Muito obrigada por tudo e, principalmente, pela sua amizade.

À família do Modesto & Oliveira Advocacia e Consultoria Jurídica, por toda a compreensão e colaboração nestes dois anos em que realizar satisfatoriamente as exigências da minha tripla jornada nem sempre foi tarefa fácil.

Aos meus amigos da UFAL, que sempre me auxiliaram no que fosse preciso e nunca hesitaram em trocar de horário comigo para que eu pudesse assistir às aulas que ocorreram durante meu turno normal de trabalho, em especial ao Jonatas, ao Roselito e ao Ewerton.

À Janaína, Ana Carla, Aline Teixeira, Eduardo Medeiros, Lúcia Nascimento, Shirlen Bezerra e Betânia, por toda a amizade, carinho e apoio que tornam os meus dias mais leves. E ao Leon Nogueira, por deixar meu coração quentinho e sorridente com a sua inocência de criança.

Aos colegas da turma 14, pelos encontros e reencontros, pela partilha e pela leveza durante as atividades acadêmicas, estendidas para além dos muros da universidade.

Por fim, a todos aqueles que, ainda que aqui não nominados, participaram, direta ou indiretamente, da minha formação.

A todos vocês, o meu muito obrigado!

"A preocupação com a proteção da privacidade, de fato, nunca foi tão grande como no presente; presume-se destinada a crescer no futuro; interessa a camadas cada vez mais amplas da população."

RODOTÀ, Stefano. **A vida na sociedade de vigilância –** a privacidade hoje. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 93.

RESUMO

O direito à privacidade, em sua dimensão informacional, passou a ser especialmente tutelado no Brasil a partir da sanção da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais. O presente trabalho se propôs a investigar se a referida lei provocará mudanças no comportamento dos agentes de tratamento de dados, bem como será capaz de mitigar os riscos à privacidade na sociedade da informação, de forma a promover salvaguardas efetivas aos titulares dos dados. Para isso, foi utilizado o método dedutivo – partindo do desenvolvimento histórico, social e cultural de conceitos essenciais para o estudo –, auxiliado pelo método comparativo – a partir da análise simultânea entre LGPD e RGPD –, e foi realizada uma pesquisa teórica, qualitativa, descritiva/prescritiva – visando à utilização de doutrina nacional e estrangeira sobre a temática, identificação da natureza dos conceitos abordados, exposição do tema e apresentação de propostas/soluções baseadas na experiência europeia e nacional. Constatou-se que a LGPD consegue instituir, com êxito, um sistema de proteção de dados pessoais voltado primordialmente à prevenção de danos, mas também assegurando a reparação caso estes venham a se concretizar. Para impulsionar os agentes à conformidade, a LGPD atribui poderes à Autoridade Nacional de Proteção de Dados para fiscalizar o cumprimento de suas disposições e aplicar sanções administrativas, caso verificada alguma infração. Examinando as disposições e os impactos do RGPD na Europa obteve-se importantes subsídios para a análise da efetividade da Lei nº 13.709/2018, haja vista as semelhanças entre as normas. A experiência europeia demonstra que a eficácia social do Regulamento nos Estados-membros da União Europeia depende, consideravelmente, de uma atuação forte, rápida e independente dos órgãos de controle. Nesse sentido, também no Brasil, a efetividade da LGPD em muito estará sujeita à atuação da ANPD. Tendo em vista a dimensão territorial do Brasil, sua grande população e uma cultura ainda incipiente de privacidade que vige no país, a Autoridade Nacional poderá enfrentar muitas dificuldades para conscientizar o público, atender às reclamações dos titulares, bem como orientar, fiscalizar e sancionar os agentes de tratamento. Diante disso, será necessária que a ANPD tenha recursos financeiros e humanos suficientes para desempenhar suas atribuições de maneira célere e eficaz. Como possível caminho para amenizar tais entraves, a Autoridade Nacional poderá celebrar acordos de colaboração com outros órgãos, a exemplo da SENACON, para realizar suas ações educativas, atender às demandas dos titulares e criar de mecanismos para aferir o cumprimento das normas pelos controladores e operadores.

Palavras-chave: Privacidade. Sociedade da Informação. Dados Pessoais. Lei Geral de Proteção de Dados Pessoais. Regulamento Geral de Proteção de Dados.

ABSTRACT

The right to privacy, in its informational dimension, came to be especially protected in Brazil from Law No. 13.709 / 2018 - General Law for the Protection of Personal Data. The present work aimed to investigate whether this law will cause changes in the behavior of data processing agents, and also whether it will be able to mitigate the risks to privacy in the information society, in order to promote effective safeguards for data subjects. For this, the deductive method was used - starting from the historical, social and cultural development of essential concepts for the study -, aided by the comparative method - from the simultaneous analysis between LGPD and GDPR -, and a theoretical, qualitative and descriptive/ prescriptive research was carried out,– with the use of national and foreign doctrine, identification of the nature of the concepts, exposition of the theme and presentation of proposals/solutions based on European and national experience. It was concluded that the LGPD is able to successfully institute a personal data protection system aimed at preventing damage, but also ensuring repair in case they materialize. In order to lead agents to compliance, the LGPD empowers the National Data Protection Authority to monitor compliance with its provisions and apply administrative sanctions in the event of any violation. Examining the provisions and impacts of the GDPR in Europe, important subsidies were obtained for the analysis of the effectiveness of Law No. 13.709/2018, given the similarities between the legislations. The European experience demonstrates that the social effectiveness of the Regulation in the Member States of the European Union depends, considerably, on a strong, quick and independent action from the control institutions. In this sense, also in Brazil, the effectiveness of the LGPD will largely be subject to the action of the ANPD. In view of the territorial dimension of Brazil, its large population and a still incipient culture of privacy that prevails in the country, the National Authority may face many difficulties to raise public awareness, respond to complaints from holders, as well as guide, supervise and sanction the treatment agents. Therefore, it will be necessary for ANPD to have sufficient financial and human resources to perform its duties quickly and effectively. As a possible way to alleviate such obstacles, the National Authority may enter into collaboration agreements with other institutions, such as SENACON, to carry out its educational activities, meet the demands of holders and create mechanisms to assess compliance with the rules by controllers and operators .

Keywords: Privacy. Information Society. Personal data. General Personal Data Protection Law. General Data Protection Regulation.

LISTA DE FIGURAS E GRÁFICOS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

2020 DBIR	2020 Data Breach Investigations Report (Relatório de Investigações de Violação de Dados 2020)
ACM	Association for Computing Machinery
AL	Alagoas
ANPD	Autoridade Nacional de Proteção de Dados
APEC	Cooperação Econômica Ásia-Pacífico
CBP	United States Customers and Borders Protection (Alfândega e Proteção de Fronteiras dos Estados Unidos)
CCPA	California Consumer Privacy Act
CDC	Código de Defesa do Consumidor
CE	Comissão Europeia
CEDH	Convenção Europeia dos Direitos do Homem
CEO	Chief Executive Officer (Diretor Executivo)
CEPD	Comitê Europeu para a Proteção de Dados
CF/1988	Constituição da República Federativa do Brasil de 1988
COVID-19	Corona Virus Disease 2019
CPF	Cadastro de Pessoas Físicas
CSV	Comma-Separated-Values (Valores separados por vírgulas)
CVV	Card Verification Value (Valor de Verificação do Cartão)
DGCEA	Departamento de Controle do Espaço Aéreo
DPDC	Departamento de Proteção e Defesa do Consumidor
DST's	Doenças Sexualmente Transmissíveis
EUA	Estados Unidos da América
FAT/ML	Fairness Accountability and Transparency in Machine Learning Organization
FBI	Federal Bureau of Investigation
FDD	Fundo de Defesa de Direitos Difusos
GPS	Global Positioning System
HIV	Human Immunodeficiency Virus
ICA 100-40	Instrução sobre Aeronaves não tripuladas e o Espaço Aéreo Brasileiro
IP	*Internet* Protocol
LGPD	Lei Geral de Proteção de Dados Pessoais

MG	Minas Gerais
MIT	Instituto Tecnológico de Massachusetts
MP	Medida Provisória
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
OIT	Organização Internacional do Trabalho
OLAP	Online Analytical Processing (Processamento Analítico *Online*)
OLTP	Online Transaction Processing (Processamento de Transações em Tempo Real)
PDF	Portable Document Format
PL	Projeto de Lei
PROCON	Programa de Proteção e Defesa do Consumidor
REsp	Recurso Especial
RGPD	Regulamento Geral de Proteção de Dados
RJET	Regime Jurídico Emergencial e Transitório das Relações Jurídicas de Direito Privado
SAT	Scholastic Aptitude Test
SE	Sergipe
SENACON	Secretaria Nacional do Consumidor
SMS	Short Message Service
STJ	Superior Tribunal de Justiça
SUS	Sistema Único de Saúde
TEDH	Tribunal Europeu dos Direitos do Homem
TJUE	Tribunal de Justiça da União Europeia
UE	União Europeia
URL	Uniform Resource Locator
VPN	Virtual Private Network
ZIP	Do inglês *Zip* (Formato de condensação e de registro de ficheiros)

SUMÁRIO

1 INTRODUÇÃO

"Achamos que você pode gostar". Ao adquirir determinado produto em um *website*, o indivíduo logo vê essa frase, acompanhada pela sugestão de vários itens que, de acordo com a análise do *site*, costumam ser adquiridos por pessoas que também compraram o produto.

Em outro momento, pesquisa-se um produto qualquer num provedor de pesquisa, e logo uma infinidade de anúncios relacionados ao item passam a perseguir o indivíduo nas redes sociais e nas páginas que ele visita.

Em outro lugar, uma pessoa navega em determinada rede social e acaba abrindo um vídeo sobre uma celebridade, o qual logo depois é fechado, pois não era de seu interesse. Imediatamente em seguida, a pessoa recebe várias sugestões de vídeos e de notícias relacionadas à referida celebridade.

Ainda, certo indivíduo recebe e clica em uma *fake news* sobre a vacinação contra a Covid-19 e, mesmo sem acreditar na notícia, passa a receber várias outras notícias falsas semelhantes.

Tudo isso é possível porque, na sociedade da informação, o comportamento do indivíduo é constantemente rastreado e analisado por meio da coleta e tratamento de dados pessoais. As organizações empresárias conseguem descobrir padrões nas ações dos consumidores e, após traçar o perfil do indivíduo, inferir quais são os seus interesses.

A partir do século XX, o mundo viu uma série de avanços tecnológicos que passaram a permitir a coleta e o tratamento de uma extensa quantidade de dados pessoais. Nas últimas décadas, os equipamentos tecnológicos tornaram-se acessíveis à boa parte da população e das organizações empresárias, por menores que sejam. Nesse contexto, poucas são as relações sociais que não envolvem o tratamento de informações pessoais.

A academia, que coleta, além de nossos nome e endereço, dados referentes à nossa estrutura corporal. O consultório médico, que registra um histórico detalhado acerca de nossa saúde. A escola, que armazena nossas informações acadêmicas. O *site* em que compramos um produto desejado. As redes sociais que utilizamos para postar fotos e acompanhar a vida dos amigos. O aplicativo de mensagem, praticamente indispensável hoje em dia. Todas essas atividades envolvem o tratamento de dados pessoais, de modo que o fornecimento de tais informações é uma exigência da vida moderna. É a chamada Sociedade da Informação.

Nesse cenário, a informação é utilizada das mais variadas formas e os dados pessoais tornam-se muito valiosos, chegando a constituir o principal ativo de muitas organizações. Em um país sem legislação específica atinente à proteção de dados, a coleta, o tratamento e o

compartilhamento desses dados acabam por ser regulados pelo próprio mercado, o que, muitas vezes, acarreta abusos por parte dos agentes de tratamento, de modo que a privacidade dos indivíduos não recebe a tutela adequada.

Importa dizer que são várias as possibilidades de violação à privacidade envolvidas no tratamento de dados, desde a fase de coleta, já que não raramente os indivíduos são submetidos a uma massiva recolha de suas informações e intenso monitoramento de seu comportamento sem que com isso tenham consentido ou até mesmo tenham algum conhecimento da existência de tais práticas.

A coleta de dados sem o consentimento da pessoa a quem as informações pertencem interfere na autodeterminação informativa do indivíduo, isto é, no direito de cada indivíduo decidir quando e como dispor de suas informações.

Ainda mais grave, o processamento de dados pode revelar uma série de conhecimentos sobre o indivíduo que pode afetá-lo negativamente, submetendo-o a decisões tomadas com base em informações que não foi ele que forneceu, ou que forneceu para finalidade diversa, a exemplo de determinada rede social que consegue identificar traços de personalidade ou a orientação sexual dos usuários, e repassa a descoberta para corporações parceiras. A discriminação é apenas um dos riscos envolvidos na atividade de definição de perfis.

A privacidade do indivíduo, ainda, é ameaçada por compartilhamentos indevidos de seus dados, acessos não autorizados e falhas de segurança que podem expor as suas informações mais íntimas, como informações relacionadas à sua saúde.

De fato, a privacidade é constantemente ameaçada na sociedade da informação; assegurar esse direito é de fundamental importância, permitindo a sua coexistência com os avanços tecnológicos e a economia cada vez mais orientada por dados.

Dessa forma, os países têm criado legislações específicas para regular a matéria da proteção de dados pessoais. Na Europa, que há décadas se preocupa, discute e aplica normas relacionadas à privacidade, foi aprovado, em 2016, o Regulamento Geral de Dados Pessoais da União Europeia – RGPD, que entrou em vigor em 25 de maio de 2018. Também o Brasil, com bastante atraso, aprovou em 2018 a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), a primeira legislação pátria específica sobre a matéria, que entrou em vigor em 18 de setembro de 2020.

O presente trabalho tem o objetivo de verificar se a LGPD será capaz de tutelar adequadamente a privacidade dos brasileiros nesse contexto de intenso tratamento de dados pessoais, a partir da análise de sua (in)efetividade enquanto instrumento de garantia desse direito.

Para obter os resultados e respostas acerca da problematização apresentada neste trabalho, será utilizado o método dedutivo, partindo do desenvolvimento histórico, social e cultural do conceito de privacidade, enquanto termo guarda-chuva que abarca o direito à proteção dos dados pessoais, objeto de proteção da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), para analisar a efetividade do sistema de proteção à privacidade instituído pela referida Lei com a finalidade de delimitar o sentido e alcance do direito à privacidade, sua relação com as novas tecnologias e as formas de violação e proteção a esse direito.

De forma auxiliar, será utilizado o método comparativo para promover uma análise simultânea entre a LGPD e o Regulamento Geral de Proteção de Dados da União Europeia, visando a identificar semelhanças e diferenças entre ambas legislações e, a partir da experiência europeia, verificar os avanços e limitações que podem ser enfrentados na efetivação das diretrizes da LGPD no Brasil.

A partir do método adotado, realizar-se-á uma pesquisa teórica, qualitativa e descritiva/prescritiva.

A investigação será teórica porque apoiada na doutrina nacional e estrangeira sobre a privacidade, sociedade da informação e proteção de dados pessoais, bem como na jurisprudência nacional, buscando-se firmar as bases conceituais sobre as temáticas abordadas. Também será feita uma pesquisa qualitativa, visto que se buscará identificar a natureza dos conceitos e informações analisadas, o conteúdo e possíveis consequências das legislações analisadas, contextualizando os resultados no âmbito da sociedade da informação. E, ainda, proceder-se-á a uma abordagem descritiva/prescritiva, pois, além da exposição da temática e do diagnóstico dos eventuais problemas e dificuldades relacionadas à efetividade da LGPD, serão apresentadas algumas proposições/soluções concernentes a isto, baseadas na experiência prática europeia após a vigência do RGPD e também na própria experiência nacional.

A escolha dos métodos e procedimentos técnicos adotados no presente trabalho se justifica tendo em vista que a LGPD buscou forte inspiração no Regulamento europeu, razão por que ambas as legislações possuem uma série de disposições semelhantes. Uma vez que o RGPD está em vigor há mais de dois anos, ao passo que a lei brasileira entrou em vigor apenas ano passado, a investigação dos impactos do Regulamento Geral de Proteção de Dados Pessoais nas atividades dos agentes de tratamento e na garantia dos direitos dos europeus pode dar indícios dos acertos e falhas da legislação brasileira.

Uma vez que a Lei Geral de Proteção de Dados Pessoais se aplica às operações de tratamento que podem ser realizadas nas mais diversas áreas das relações sociais e, portanto, pode envolver variados ramos do Direito, público e privado, importa esclarecer que não se pretende esgotar as discussões que permeiam essa temática.

Diante disso, faz-se necessário precisar que a pesquisa será realizada a partir de uma perspectiva civil-constitucional, de forma que a menção a outros ramos do Direito ocorrerá apenas de modo incidental, para exemplicar algumas questões aventadas. Ainda, é de se destacar, que, embora se amoldem à perspectiva adotada e guardem relação com a proteção dos dados pessoais, algumas temáticas não serão aprofundadas no texto, por não integrarem a delimitação do objeto central do estudo, qual seja, a (in)efetividade da Lei nº 13.709/2018.

Ainda, merece ser pontuado que o sentido de efetividade adotado na pesquisa diz respeito à capacidade da LGPD de produzir, além de seus efeitos jurídicos, efeitos sociais. Nessa senda, ao longo do texto as expressões eficácia, eficaz, efetivo e afins devem ser compreendidas como sinônimas de efetividade.

Iniciando o desenvolvimento do trabalho, na segunda seção, estudar-se-á o direito à privacidade, delimitando sua origem, evolução, concepções e dimensões, pois este é um conceito dinâmico, que sofre forte influência do contexto histórico, econômico, social e cultural em que é inserido. Assim, demonstrar-se-á como a concepção de privacidade se ampliou desde o seu surgimento e como ela é diferentemente percebida nos Estados Unidos, na Europa e no Oriente. Por fim, discorrer-se-á sobre a tutela do direito à privacidade no ordenamento jurídico brasileiro, tanto nas constituições quanto em nível infraconstitucional.

Uma vez delimitado o conceito e o âmbito de proteção do direito objeto de estudo deste trabalho, a terceira seção se destinará ao desenvolvimento do direito à proteção de dados pessoais, espécie do direito à privacidade, trazendo conceitos e aspectos necessários à sua compreensão. Em seguida, tratar-se-á da natureza jurídica dos dados pessoais e da sua proteção enquanto direito fundamental, diferenciando-o da privacidade e da autodeterminação informativa. Ainda, investigar-se-á o desenvolvimento geracional das normas de proteção de dados, indicando os principais pontos de convergência das leis que regulam a matéria.

A quarta seção se voltará à demonstração dos riscos à privacidade na sociedade da informação, apresentando as principais formas de tratamento de dados pessoais e seus respectivos benefícios e riscos. Será dada particular importância à mineração de dados e aos riscos associados ao *profiling*, em especial a discriminação e as influências externas à dimensão decisional da privacidade. Ademais, estudar-se-á a segurança no tratamento de dados pessoais e a forma como a LGPD regula as violações de dados.

Por fim, na última seção, buscar-se-á identificar as perspectivas para o direito à privacidade no Brasil com a vigência da LGPD. Dessa feita, serão avaliadas as sanções administrativas aplicáveis aos agentes de tratamento, bem como a forma e as condições de sua responsabilização civil. Em seguida, far-se-á um mapeamento das semelhanças e diferenças entre o Regulamento Geral de Proteção de Dados da União Europeia e a LGPD. A partir disso, uma vez investigadas as principais inovações da Lei Geral de Proteção de Dados, será analisada a (in)efetividade da LGPD, intentando-se responder ao questionamento aqui proposto, tendo como subsídio a avaliação dos impactos do Regulamento Geral de Proteção de Dados da União Europeia na proteção de dados pessoais dos europeus.

2 DIREITO À PRIVACIDADE E SOCIEDADE DA INFORMAÇÃO

A noção de privacidade sempre sofreu grande influência do contexto histórico, econômico e social em que as pessoas estão inseridas, sendo um conceito dinâmico que não pode ser entendido separado da sociedade em que foi construído. Dessa forma, as transformações provocadas pela sociedade da informação também terão impacto na acepção e regulação da privacidade, razão pela qual importa estudar suas características.

2.1 Conceito e características da sociedade da informação

Ao longo do tempo, a sociedade vivenciou diversas transformações, algumas das quais modificaram significativamente os meios e as técnicas de produção e, por conseguinte, a própria estrutura social. Nesse diapasão, verificam-se três marcos históricos: a revolução agrícola, a revolução industrial e a revolução tecnológica[1].

A esses momentos da história, Toffler denomina de ondas de mudança, por colidirem e se sobreporem[2]. Nessa senda, o homem, que vivia em constante migração e se alimentava principalmente da caça e da pesca, começa a vivenciar, há mais de dez milênios, a primeira onda, a revolução agrícola. Essa revolução se espalhou lentamente por todo o mundo, fazendo da terra a principal fonte de riquezas, bem como possibilitando o surgimento das primeiras civilizações e do escambo dos produtos agrícolas. Há, assim, uma grande transformação no modo de vida das pessoas[3].

Essa primeira onda de mudanças ainda não havia desaparecido quando teve início, na Europa, a segunda grande onda, a Revolução Industrial[4]. No século XVIII, com a associação da máquina à força do vapor, ocorreu uma importante mudança no método de produção. Nasce, assim, o sistema fabril em grande escala, que permitiu não só um aumento significativo na produção como modificou a própria organização e divisão de trabalho[5].

A Revolução Industrial possibilitou a rápida expansão do mercado, bem como inseriu na sociedade uma divisão entre duas funções, originando o que hoje se chama de produtores e

[1] SIQUEIRA JÚNIOR, Paulo Hamilton. **Teoria do Direito.** 3. ed. São Paulo: Saraiva, 2011, p. 238-239.
[2] TOFFLER, Alvin. **La Tercera Ola.** Colombia: Plaza & Janes S.A. Editores, 1980, p. 6.
[3] TOFFLER, Alvin. **La Tercera Ola.** Colombia: Plaza & Janes S.A. Editores, 1980, p. 11.
[4] TOFFLER, Alvin. **La Tercera Ola.** Colombia: Plaza & Janes S.A. Editores, 1980,p. 11.
[5] HUBERMAN, Leo. **História da Riqueza do Homem.** Zahar Editores, 1981, p. 156 [versão digital].

consumidores[6]. Com a expansão da rede de trocas, as estradas eram um pré-requisito para o desenvolvimento social, político e econômico[7].

Após a Segunda Guerra Mundial, tem início a terceira onda de mudanças. Por volta de 1955, nos Estados Unidos, pela primeira vez o número de trabalhadores do setor de serviços superou o de trabalhadores manuais. Também nessa mesma década, houve a introdução generalizada do computador, voos comerciais a jato, a pílula anticoncepcional e muitas outras inovações de alto impacto. Foi nesse período que o a terceira onda começou a ganhar força nos Estados Unidos, o que se seguiu, com alguma diferença temporal, na maioria dos países industrializados[8].

Essa terceira onda, que tem início com a revolução tecnológica, permitirá a formação do que hoje se convencionou chamar de "sociedade da informação".

Um dos primeiros escritos acerca da sociedade da informação foi elaborado por Machlup, em 1962, no qual se demonstrou que a produção de conhecimento é uma atividade econômica e que, já àquela época, a indústria do conhecimento representava 29% do produto nacional bruto dos Estados Unidos da América. Contudo, embora traga a ideia de sociedade da informação, Machlup adota a expressão "Indústria do Conhecimento"[9].

A expressão "sociedade da informação" só veio a ser utilizada alguns anos depois, não havendo um consenso acerca de qual autor foi o primeiro a usar o termo. Nessa senda, alguns creditam tal utilização ao artigo "Sociologia" de Jiro, publicado no Japão em 1964[10]. Já outros atribuem o uso inédito da expressão a Masuda e Kohyma, que escreveu, em 1968, o livro "Introdução à Sociedade da Informação". Há, ainda, um terceiro nome na disputa, Hayashi, que publicou, em 1969, o livro *The Information Society: From Hard to Soft Society*[11].

O fato é que o termo "sociedade da informação" surgiu ainda em 1960, mas somente se consolidou a partir da década de 1980, pois até então o termo "sociedade pós-industrial"

---

[6] TOFFLER, Alvin. **La Tercera Ola.** Colombia: Plaza & Janes S.A. Editores, 1980, p. 176-177.
[7] TOFFLER, Alvin. **La Tercera Ola.** Colombia: Plaza & Janes S.A. Editores, 1980, p. 231.
[8] TOFFLER, Alvin. **La Tercera Ola.** Colombia: Plaza & Janes S.A. Editores, 1980, p. 12.
[9] CRAWFORD, Susan. The Origin and Development of a Concept: the information society. **Bull. Med. Libr. Assoc,** v. 71, n. 4, out. 1983, p. 380-381. Disponível em: https://europepmc.org/backend/ptpmcrender.fcgi?accid=PMC227258&blobtype=pdf. Acesso em: 28 nov. 2020.
[10] SÁNCHEZ-TORRES, Jenny Marcela; GONZÁLEZ-ZABALA, Mayda Patrícia; MUÑOZ, María Paloma Sánchez. La Sociedad de la Información: Génesis, Iniciativas, Concepto y su Relación con Las TIC. **UIS Ingenierías –** Revista de La Facultad de Ingenierías Fisicomecánicas, v. 11, n. 1, Bucaramanga/Colombia, jan./jun. 2012, p. 113-129. Disponível em: https://www.redalyc.org/pdf/5537/553756873001.pdf. Acesso em: 28 jun. 2020, p. 115.
[11] KARVALICS, László Z. Information Society – what is it exactly? (The meaning, history and conceptual framework of an expression). **Leonardo da Vinci,** Budapeste, jan. 2007, p. 5. Disponível em: https://www.researchgate.net/publication/237332035_Information_Society_-_what_is_it_exactly_The_meaning_history_and_conceptual_framework_of_an_expression. Acesso em: 15 set. 2020.

era muito mais utilizado para descrever a grande transformação social pela qual o mundo passava. Entretanto, percebeu-se que esta última expressão não era capaz de refletir o processo mediante o qual a informação e o conhecimento tornaram-se cada vez mais utilizados e essenciais às indústrias tradicionais[12], razão por que "sociedade da informação" foi o termo que acabou se consagrando.

Para entender a que se refere a expressão Sociedade da Informação, importa dizer que não há um conceito único. Karvalics[13], ao analisar mais de cinquenta definições, destaca algumas das mais utilizadas:

> • Um novo tipo de sociedade, em que a posse de informações (e não a riqueza material) é a força motriz por trás de sua transformação e desenvolvimento […] (e onde) a criatividade intelectual humana se desenvolve. (Yoneji Masuda)
>
> • Uma sociedade em que [...] a informação é usada como recurso econômico, a comunidade a utiliza / explora e, por trás de tudo, desenvolve-se uma indústria que produz a informação necessária... (Nick Moore)
>
> • Uma estrutura social baseada na livre criação, distribuição, acesso e uso de informação e conhecimento [...] a globalização de vários campos da vida. (Estratégia Nacional (Húngara) de Informática, 1995).[14]

Webster[15] observa que é possível distinguir analiticamente cinco definições de sociedade da informação, cada uma com diferentes enfoques, não excludentes entre si, a saber: o critério tecnológico, o econômico, o ocupacional, o espacial e o cultural.

As definições que adotam o critério tecnológico enfatizam a inovação tecnológica, tendo como ideia principal que avanços no processamento, armazenamento,

---

[12] KARVALICS, László Z. Information Society – what is it exactly? (The meaning, history and conceptual framework of an expression). **Leonardo da Vinci,** Budapeste, jan. 2007, p. 6-7. Disponível em: https://www.researchgate.net/publication/237332035_Information_Society_-_what_is_it_exactly_The_meaning_history_and_conceptual_framework_of_an_expression. Acesso em: 15 set. 2020.

[13] KARVALICS, László Z. Information Society – what is it exactly? (The meaning, history and conceptual framework of an expression). **Leonardo da Vinci,** Budapeste, jan. 2007, p. 10. Disponível em: https://www.researchgate.net/publication/237332035_Information_Society_-_what_is_it_exactly_The_meaning_history_and_conceptual_framework_of_an_expression. Acesso em: 15 set. 2020.

[14] Outras definições apresentadas pelo autor são: - Uma sociedade que se organiza em torno do conhecimento no interesse do controle social e da gestão inovação e mudança [...]. (Daniel Bell); - A sociedade da informação é uma realidade econômica e não simplesmente uma abstração mental [...]A lenta disseminação de informações termina [...] novas atividades, operações e produtos gradualmente vêm à tona. (John Naisbitt); - Um novo tipo de sociedade em que a humanidade tem a oportunidade de liderar um novo modo de vida, ter um padrão de vida mais alto, realizar um trabalho melhor e desempenhar um papel melhor na sociedade graças ao uso global das tecnologias de informação e telecomunicações. (Béla Murányi). (KARVALICS, László Z. Information Society – what is it exactly? (The meaning, history and conceptual framework of an expression). **Leonardo da Vinci,** Budapeste, jan. 2007, p. 10. Disponível em: https://www.researchgate.net/publication/237332035_Information_Society_-_what_is_it_exactly_The_meaning_history_and_conceptual_framework_of_an_expression. Acesso em: 15 set. 2020).

[15] WEBSTER, Frank. What information society? **The Information Society: an international journal**, v. 10, n. 1, 3 mai. 2013. Disponível em: http://dx.doi.org/10.1080/01972243.1994.9960154. Acesso em: 15 set. 2020.

e transmissão de informações levaram à aplicação de tecnologias da informação em praticamente todos os setores da sociedade.

Já sob o enfoque econômico, a sociedade da informação seria aquela cujos principais setores de atividade econômica são os produtores de bens e serviços de informação. Por sua vez, as definições ocupacionais se concentram nas mudanças laborais, isto é, uma sociedade da informação é aquela cuja predominância de ocupações é encontrada no trabalho informacional como o de professores, advogados e artistas em vez de mineradores, siderúrgicos, estivadores e construtores.

A concepção espacial da sociedade da informação tem como principal foco as alterações que a tecnologia provoca no tempo e no espaço, já que as inovações tecnológicas permitem a criação de redes capazes de conectar diferentes locais em tempo real. Por fim, as concepções culturais da sociedade da informação focam no aumento, nas mudanças e influências verificadas pelo fluxo de informações no cotidiano das pessoas.

Para Castells, que analisa o que ele chama de "Sociedade em Rede" nos três volumes de sua obra "A Era da Informação: economia, sociedade e cultura", uma sociedade da informação não é uma sociedade que usa tecnologia da informação, mas uma estrutura social específica associada à ascensão do paradigma informacional, apesar de por este não ser determinada[16].

Para o autor, a tecnologia não determina a sociedade nem a sociedade escreve o curso da transformação tecnológica. Na verdade, "a tecnologia é a sociedade, e a sociedade não pode ser entendida ou representada sem suas ferramentas tecnológicas". No entanto, embora não determine a evolução histórico-social, a tecnologia incorpora a capacidade de transformação das sociedades[17].

Castells prefere o termo "sociedade informacional" por acreditar que a expressão "sociedade da informação" enfatiza o papel da informação na sociedade; no entanto, o autor destaca que a informação teve um papel crucial em todas as sociedades. Assim, "sociedade informacional" indicaria o atributo de uma forma específica de organização social em que a geração, o processamento e a transmissão da informação tornam-se as fontes fundamentais de produtividade e poder devido às novas condições tecnológicas.

O autor busca estabelecer um paralelo com a distinção entre indústria e industrial, haja vista que uma sociedade industrial não é apenas uma sociedade em que há indústrias, mas

[16] CASTELLS, Manuel. **La era de la información:** Economía, sociedad y cultura. (Fin del Milenio; v. 3), 1999, p. 172, [versão digital].
[17] CASTELLS, Manuel. **A Sociedade em Rede.** (A era da informação: economia, sociedade e cultura; v. 1). São Paulo: Paz e Terra, 1999, p 43-44.

uma sociedade em que as formas sociais e tecnológicas de organização social permeiam todas as esferas de atividades[18].

Assim, segundo Castells, surge um novo paradigma ao qual se associa uma igualmente nova forma de organização social na qual a informação é uma fonte essencial de poder e produção.

Ao tratar do surgimento desse novo paradigma, o autor leciona que, durante a Segunda Guerra Mundial e no período seguinte, o homem fez as suas principais descobertas tecnológicas em eletrônica, o primeiro computador programável e o transistor, considerado o verdadeiro cerne da revolução da tecnologia da informação no século XX[19].

A partir da década de 1970, essas novas tecnologias da informação difundiram-se amplamente e passaram a convergir para um novo paradigma. Logo que se espalharam pelos diferentes países, culturas, organizações e objetivos, tais tecnologias foram apropriadas para diversos usos e aplicações, produzindo inovação tecnológica, o que acelerou e ampliou o escopo das transformações tecnológicas, bem como diversificou suas fontes[20].

Além das tecnologias relacionadas à eletrônica, computação e telecomunicações, nas últimas décadas do século XX houve uma constelação de grandes avanços tecnológicos no que toca a materiais avançados, fontes de energia, aplicações na medicina, técnicas de produção e tecnologias de transportes. Dessa feita, o mundo se tornou digital[21].

Entretanto, ao contrário do que possa parecer, as novas tecnologias da informação não são simplesmente ferramentas a serem aplicadas, mas processos a serem desenvolvidos, uma vez que os usuários podem assumir o controle da tecnologia, como no caso da *internet.* Diante disso, os processos sociais de criação (isto é, a própria cultura) interagem com as forças produtivas, possibilitando que usuários e criadores se tornem a mesma coisa. “Pela primeira vez na história, a mente humana é uma força direta de produção, não apenas um elemento decisivo no sistema produtivo.” Nesse cenário,

> computadores, sistemas de comunicação, decodificação e programação genética são todos amplificadores e extensões da mente humana. O que pensamos e como pensamos é expresso em bens, serviços, produção material e intelectual, sejam

[18] CASTELLS, Manuel. **A Sociedade em Rede.** (A era da informação: economia, sociedade e cultura; v. 1). São Paulo: Paz e Terra, 1999, p. 64-65.
[19] CASTELLS, Manuel. **A Sociedade em Rede.** (A era da informação: economia, sociedade e cultura; v. 1). São Paulo: Paz e Terra, 1999, p. 76.
[20] CASTELLS, Manuel. **A Sociedade em Rede.** (A era da informação: economia, sociedade e cultura; v. 1). São Paulo: Paz e Terra, 1999, p. 43-44.
[21] CASTELLS, Manuel. **A Sociedade em Rede.** (A era da informação: economia, sociedade e cultura; v. 1). São Paulo: Paz e Terra, 1999, p. 67-68.

> alimentos, moradia, sistemas de transporte e comunicação, mísseis, saúde, educação ou imagens[22].

A revolução tecnológica caracteriza-se não pela centralidade de informação, mas por sua aplicação para a geração de novos conhecimentos, bem como de dispositivos de processamento e comunicação da informação, num ciclo de realimentação cumulativo entre a inovação e seu uso[23].

Nesse novo paradigma, as atividades, os grupos sociais e os diferentes territórios estão conectados num sistema tecnológico[24]. Enquanto na Revolução Industrial o desenvolvimento social, político e econômico dependia das estradas, atualmente tal desenvolvimento necessita das inovações tecnológicas e de um sistema de comunicações eletrônicas, a fim de permitir que as pessoas e organizações se conectem em todo o mundo[25].

À vista disso, conforme Castells[26], a base material da sociedade da informação se confunde com os aspectos centrais do paradigma da tecnologia da informação, os quais serão apresentados a seguir.

A primeira característica desse novo paradigma é que a informação é a sua matéria-prima, de modo que "são tecnologias para agir sobre a informação, não apenas informação para agir sobre a tecnologia, como foi o caso das revoluções tecnológicas anteriores".

Ademais, a informação se torna parte integral de toda atividade humana, de forma que todos os processos da existência, individual e coletiva, são moldados pelo novo meio tecnológico. Trata-se do que o autor chama de "penetrabilidade dos efeitos das novas tecnologias".

A terceira característica do paradigma informacional é a "lógica de redes". Em qualquer sistema ou conjunto de relações, em todos os processos e organizações, é possível criar conexões entre pessoas, entidades, procedimentos, isto é, implementar uma rede adaptável à crescente complexidade de interação e aos modelos imprevisíveis do desenvolvimento que decorre do poder criativo dessa interação.

O quarto aspecto do paradigma da tecnologia da informação é a sua flexibilidade, sua capacidade de reconfiguração. Não somente os processos são reversíveis, mas as próprias

---

[22] CASTELLS, Manuel. **A Sociedade em Rede.** (A era da informação: economia, sociedade e cultura; v. 1). São Paulo: Paz e Terra, 1999, p. 69.
[23] CASTELLS, Manuel. **A Sociedade em Rede.** (A era da informação: economia, sociedade e cultura; v. 1). São Paulo: Paz e Terra, 1999, p. 69.
[24] CASTELLS, Manuel. **A Sociedade em Rede.** (A era da informação: economia, sociedade e cultura; v. 1). São Paulo: Paz e Terra, 1999, p. 70.
[25] TOFFLER, Alvin. **La Tercera Ola.** Colombia: Plaza & Janes S.A. Editores, 1980, p 231.
[26] CASTELLS, Manuel. **A Sociedade em Rede.** (A era da informação: economia, sociedade e cultura; v. 1). São Paulo: Paz e Terra, 1999, p. 108-111.

organizações podem ser modificadas, o que é essencial numa sociedade marcada pela constante mudança e fluidez organizacional. “Tornou-se possível inverter as regras sem destruir a organização, porque a base material da organização pode ser reprogramada e reaparelhada”.

Ainda, outra característica da revolução tecnológica é a “convergência de tecnologias específicas para um sistema altamente integrado”, tornando-se praticamente impossível distinguir em separado as trajetórias tecnológicas antigas. Assim, as telecomunicações, os computadores e a microeletrônica são todos integrados aos sistemas de informação, de modo que, ainda que exista alguma distinção comercial, um elemento não pode ser imaginado sem o outro; eles se tornam interdependentes.

Esse processo de convergência entre os diferentes campos tecnológicos resulta da lógica compartilhada na geração da informação. Como visto, todos os atores envolvidos podem contribuir para a produção do conhecimento.

Moore[27] defende que a sociedade da informação tem três características principais.

A primeira delas é que a informação é usada como recurso econômico, seja para aumentar a eficiência das organizações, seja para estimular a inovação e ampliar sua eficácia e posições competitivas por meio de melhorias na qualidade dos bens e serviços que produzem.

A segunda característica é que há um maior uso de informações entre o público nas suas atividades de consumo, no acesso a serviços públicos e nas tomadas de escolhas e controle sobre suas próprias vidas. As pessoas frequentemente utilizam a informação como cidadãos para exercer seus direitos e responsabilidades civis.

A terceira característica das sociedades da informação é o desenvolvimento de um setor de informação dentro da economia, o qual se preocupa com a infraestrutura tecnológica.

Como se vê, não há uma definição única do que seja a “Sociedade da Informação”, contudo, das definições e características acima apresentadas, é possível destacar alguns pontos em comum.

O que realmente caracteriza a sociedade da informação não é a utilização de recursos tecnológicos, mas a utilização da informação, em que pese a tecnologia seja cada vez mais fundamental no tratamento da informação.

A sociedade organiza-se em torno do uso da informação. Esta é utilizada quase o tempo inteiro e nos mais variados setores da sociedade: economia, prestação de serviços públicos, comunicação, relacionamentos, ciência, reprodução, lazer.

---

[27] MOORE, Nick. The Information Society**.** *In:* MOORE, Nick. **World Information Report.** UNESCO Reference Books, Bernan Assoc. Geneva, 1998, p. 271-272. [versão digital].

Além de a informação ser utilizada em todas as atividades humanas, a principal característica da sociedade em comento é que a informação é utilizada como matéria-prima e ferramenta de tomadas de decisão.

Assim, a informação é utilizada para gerar novos conhecimentos que, por sua vez, serão utilizados na economia para melhorar serviços, tornar processos e funcionários mais produtivos, personalizar ofertas, criar novos modelos de negócio e desenvolver vantagens competitivas; ou pelo setor público, para a execução de suas políticas públicas. Ainda, a informação pode ser utilizada para direcionar, de maneira personalizada, o conteúdo no intento de influenciar as escolhas de vida das pessoais, tais como decisões políticas, ou para determinar qual o tratamento médico mais adequado a um paciente.

O leque de possibilidades de utilização da informação é imenso, razão por que a informação se torna um dos mais relevantes instrumentos de poder e de produção, e os dados pessoais são muito valorizados, inclusive monetariamente. Na sociedade da informação, o fluxo de dados é gigantesco e contínuo. Estima-se que, até 2025, o volume de dados armazenados em todo o mundo chegue a 175 *zettabytes* (o que equivale a 175 trilhões de *gigabytes*)[28].

O tratamento adequado desses dados pode trazer muitos benefícios para o desenvolvimento da sociedade. A enorme quantidade de dados produzida diariamente pelos estabelecimentos de saúde, por exemplo, pode ser tratada, analisada e utilizada para que os médicos tenham mais informações sobre os avanços das doenças e os melhores tratamentos, salvando e melhorando a qualidade de vida de diversos pacientes.

Os milhares de gigabytes gerados diariamente pelas movimentações financeiras são analisados tanto para a identificação de atividades comerciais problemáticas, prevenindo fraudes, como para ajudar empresas a crescer e a fortalecer a economia[29]. Os dados também são de grande importância para as análises estatísticas que serão utilizadas pelos governos para a elaboração dos seus planos de desenvolvimento, permitindo estimar, com um bom grau de precisão, relevantes variáveis como tamanho da população, taxa de emprego e desemprego e índices de inflação[30].

---

[28] REINSEL, David; GANTZ, John; RYDNING, John. The Digitization of the World: from edge to core. **IDC White Paper,** nov. 2018. Disponível em: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf. Acesso em: 15 jun. 2020.

[29] BSA. Qual é o "x" da questão em relação a dados? **BSA.org – The Software Aliance.** Disponível em: https://data.bsa.org/wp-content/uploads/2015/10/BSADataStudy_br.pdf. Acesso em: 11 jun. 2019, p. 8.

[30] IGNÁCIO, Sérgio Aparecido. Importância da estatística para o processo de conhecimento e tomada de decisão. **Revista Paranaense de Desenvolvimento,** Curitiba, n. 118, jan./jun. 2010. Disponível em: http://www.ipardes.pr.gov.br/ojs/index.php/revistaparanaense/article/view/89/645. Acesso em: 11 jun. 2019, p. 187.

Obviamente, nem todos os dados que são produzidos são dados pessoais. Existem dados, por exemplo, que são produzidos pelo monitoramento climático por satélite ou pelo desempenho de turbinas de aviões e que não se relacionam com nenhuma pessoa natural identificável. No entanto, uma parcela bastante considerável dos dados produzidos é pessoal.

O fornecimento de tais informações é hoje uma exigência da vida moderna. A academia coleta dados referentes à estrutura corporal do indivíduo para elaborar os exercícios mais adequados ao objetivo por ele pretendido. O consultório médico registra um histórico detalhado acerca da saúde dos pacientes. A escola armazena as informações acadêmicas. O *site* em que a pessoa compra o livro desejado logo em seguida passa a lhe mostrar diversos outros títulos de que ela "pode gostar". As redes sociais são utilizadas para postar fotos e acompanhar a vida dos amigos. Os aplicativos de mensagens tornam-se praticamente indispensáveis, permitindo a comunicação entre pessoas distantes geograficamente. Todas essas atividades envolvem o tratamento de dados pessoais

Uma situação que evidenciou como esses dados são essenciais na atual sociedade foram as diversas medidas de enfrentamento à pandemia da Covid-19. Isso porque, em todo o mundo, o tratamento de dados pessoais permitiu a identificação das pessoas com quem o infectado teve contato, possibilitando a testagem dessas pessoas e o consequente diagnóstico de novos infectados, inclusive dos assintomáticos. Ademais, também foi possível inferir, a partir da manipulação de tais dados, o nível de adesão das pessoas ao distanciamento social, permitindo a adoção de medidas governamentais voltadas à efetividade dos decretos governamentais que determinaram tal distanciamento.

No Brasil, o governo do Estado do Amazonas decretou regime de quarentena para os passageiros que desembarcassem no Aeroporto Internacional Eduardo Gomes, os quais deveriam instalar em seus *smartphones* um aplicativo destinado a monitorar em tempo real a localização dessas pessoas durante o período de 14 dias[31]. Em Recife, a prefeitura municipal começou a utilizar sistemas de localização de celulares dos recifenses para coordenar ações de incentivo ao isolamento social, como o envio de carros de som, notificações por celular, além de outras ações de comunicação para bairros em o que o nível de adesão ao distanciamento social estivesse baixo[32].

---

[31] AMAZONAS. Governo do Estado. **Wilson Lima anuncia monitoramento remoto de pessoas que chegam pelo aeroporto e aquisição de testes rápidos.** 25 mar. 2020. Disponível em: http://www.amazonas.am.gov.br/2020/03/wilson-lima-anuncia-monitoramento-remoto-de-pessoas-que-chegam-pelo-aeroporto-e-aquisicao-de-testes-rapidos/. Acesso em: 6 abr. 2020.

[32] G1 PE. **Recife rastreia 700 mil celulares para monitorar isolamento social e direcionar ações contra coronavírus.** 24 mar. 2020. Disponível em: https://g1.globo.com/pe/pernambuco/noticia/2020/03/24/recife-

Além de o Estado utilizar dados pessoais para o gerenciamento de suas políticas públicas, o acesso a muitos dos seus serviços demanda o fornecimento de informações pessoais pelos administrados. Na sociedade da informação, o indivíduo necessita constantemente fornecer seus dados pessoais, já que o custo de não fazê-lo é imenso.

Nessa nova estrutura social, o indivíduo não só é inundado com uma quantidade quase imensurável de informação, como também contribui ativamente para a produção do conhecimento e até mesmo manipula dados pessoais.

Basta pensar na quantidade de conteúdo gerada por pessoas comuns nas plataformas digitais, como memes, vídeos e postagens, que representam a aprovação ou a desaprovação de parcela da população a determinados temas. Também os aplicativos, *sites*, profissionais, produtos e serviços são constantemente avaliados pelos usuários. Até mesmo as pautas de programas de grandes redes de televisão passam a ser influenciadas pelos assuntos que estão em evidência nas redes sociais.

Ainda, os indivíduos passam a capturar imagens de outras pessoas, seja por meio de câmeras privadas de vigilâncias que se tornaram bem mais acessíveis nas últimas décadas, seja por meio das câmeras dos *smartphones*, que estão presentes em todos os lugares. Essas imagens podem gerar danos à privacidade do indivíduo, como no caso de sua divulgação não autorizada, mas também têm se tornado importantes instrumentos na luta contra o abuso de poder, como se extrai das diversas denúncias de violência policial que só se tornam possível graças à utilização dessas filmagens.

Com o barateamento dos recursos tecnológicos, o indivíduo deixa de ser um mero receptor de informações, de ser apenas um consumidor, um espectador, um reprodutor de dados e padrões, e passa a ser um importante contribuinte do processo de conhecimento, sendo capaz de influenciar, mesmo que minimamente, a própria sociedade.

A *internet* tem um papel essencial na sociedade da informação. Por meio dela, processos, atividades e pessoas de todo o mundo podem se conectar a qualquer momento. Nas palavras de Castells, esse meio de comunicação permite, pela primeira vez, a comunicação de muitos com muitos, num momento escolhido e em escala global[33].

A *internet*, que em seus primórdios tinha objetivos militares, viu seu uso como sistema de comunicação e forma de organização expandir-se consideravelmente a partir da década de 1990, permitindo a formação do que Castells chama de "sociedade de rede". Assim, em todo

---

rastreia-700-mil-celulares-para-monitorar-isolamento-social-e-direcionar-acoes-contra-coronavirus.ghtml. Acesso em: 6 abr. 2020.

[33] CASTELLS, Manuel. **A galáxia da internet:** reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar Ed., 2003, p. 8.

o mundo, atividades econômicas, sociais, políticas e culturais passam a ser estruturadas pela *internet* e em torno dela. Isso significa que "ser excluído dessas redes é sofrer uma das formas mais danosas de exclusão em nossa economia e em nossa cultura"[34].

Esse uso continua a crescer globalmente, alcançando mais de 53% da população mundial[35]. No Brasil, 71% dos domicílios têm acesso à *internet*, o que representa mais de 130 milhões de usuários[36]. Entretanto, 3,6 bilhões de pessoas ainda continuam excluídas da comunicação *online*, conforme dados da União Internacional de Telecomunicações[37], o que significa que quase metade dos habitantes do mundo não tem acesso às oportunidades oferecidas pela rede.

De fato, uma imensa quantidade de atividades humanas a distância se torna possível por causa da *internet*: relacionamentos, *home office*, reuniões, *delivery*, educação, telemedicina, compras e uma série de outras atividades. Os tempos de distanciamento social por causa da pandemia evidenciaram a importância do uso da *internet* nos dias de hoje.

Para se ter uma noção do fluxo de dados, inclusive internacional, que ocorre por esse meio de comunicação, em apenas um minuto na *internet* são feitos 1 milhão de *logins* no *Facebook*, 4,5 milhões de vídeos são assistidos no Youtube, são realizadas 3,8 milhões de buscas no *Google*, 347 mil postagens são visualizadas no Instagram, mais de 40 milhões de mensagens são trocadas por meio do *WhatsApp* e do *Facebook* Messenger e quase 1 milhão de dólares são gastos *online*[38].

Na atual organização social, a informação é utilizada das mais variadas formas e os dados pessoais se tornam muito valiosos, chegando a constituir o principal ativo de muitas organizações, que os utilizam para o cumprimento de exigências consequenciais das relações contratuais, como a emissão de nota fiscal, a personalização de seus serviços e até mesmo a realização de transações negociais cujo objeto são as próprias informações armazenadas em seus bancos de dados, além de diversas outras finalidades, como será estudado mais adiante.

---

[34] CASTELLS, Manuel. **A galáxia da internet:** reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar Ed., 2003, p. 8.

[35] MHADHBI, A. Estudo da ONU revela que mundo tem abismo digital de gênero. **ONU News**, 6 nov. 2019. Disponível em: https://news.un.org/pt/story/2019/11/1693711. Acesso em: 28 jun. 2020.

[36] BRIGATTO, Gustavo. Acesso à internet cresce no Brasil, mas 28% dos domicílios não estão conectados. **Valor Econômico,** 26 maio 2020. Disponível em: https://valor.globo.com/empresas/noticia/2020/05/26/acesso-a-internet-cresce-no-brasil-mas-28percent-dos-domicilios-nao-estao-conectados.ghtml. Acesso em: 28 jun. 2020.

[37] MHADHBI, A. Estudo da ONU revela que mundo tem abismo digital de gênero. **ONU News**, 6 nov. 2019. Disponível em: https://news.un.org/pt/story/2019/11/1693711. Acesso em: 28 jun. 2020.

[38] FORBES. **O que representa um minuto na internet em 2019.** 3 abr. 2019. Disponível em: https://forbes.com.br/colunas/2019/04/o-que-representa-um-minuto-na-internet-em-2019/. Acesso em: 17 jun. 2020.

A seguir, para o adequado estudo da proteção de dados pessoais, faz-se necessário o exame da evolução conceitual de privacidade desde sua concepção originária de "direito a ser deixado só" até uma definição ampliada, que engloba o controle dos dados pessoais.

2.2 Origem e evolução do direito à privacidade

Na Antiguidade Clássica, o significado original da palavra "privado" correspondia àquilo que era "não público"[39]. Assim, o adjetivo *publicus*[40] dizia respeito àquilo que pertencia ao povo romano, enquanto *privatus* se referia a tudo que não se relacionasse ao Estado, bem como ao cidadão que não era magistrado, isto é, que não exercia um múnus público[41]. Nessa época, não se envolver com assuntos de interesse público, ausentando-se da *res pública*, era algo socialmente reprovável, haja vista ser tal distanciamento algo destinado aos destituídos. Além disso, também era algo perigoso e extremamente dispendioso[42].

Isso não implica que o indivíduo não realizava algumas atividades de conotação privada, como festividades familiares, por exemplo. Na filosofia antiga, encontram-se diversas menções que se relacionam a aspectos da privacidade, como à solidão, ao retiro e à interiorização. Contudo, não se identificava nessas sociedades "algo equivalente aos direitos individuais, visto que a liberdade era exercida basicamente na esfera pública"[43].

Na lição de Arendt, o que distinguia a esfera familiar da esfera pública era que, naquela, os homens viviam juntos por serem compelidos pelas suas necessidades de sobrevivência, ao passo que a esfera da *polis* era a esfera da liberdade, uma vez que na *polis*, ao contrário do que acontecia no seio familiar, todos eram iguais e ser livre "significava ao mesmo tempo não estar sujeito às necessidades da vida nem ao comando de outro *e* também não comandar"[44].

Dessa forma, viver uma vida inteiramente privada significava ser destituído de coisas essenciais à vida humana, como ser privado do fato de ser visto e ouvido pelos outros, bem

---

[39] POSNER, Richard A. **A Economia da Justiça.** São Paulo: WMF Martins Fontes, 2010, p. 317.
[40] Danilo Doneda esclarece que, embora a difusão do vocábulo tenha se dado na língua inglesa (*privacy*), a palavra "privacidade" tem raiz latina, do adjetivo *privatus.* 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. 102.
[41] PEIXOTO, Erick L. C; EHRHARDT JÚNIOR, Marcos. Breves Notas sobre a Ressignificação da Privacidade. *In:* **Revista Brasileira de Direito Civil,** Belo Horizonte, v. 16, jan./jun. 2018. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/230. Acesso em: 12 jun. 2019, p. 37.
[42] POSNER, Richard A. **A Economia da Justiça.** São Paulo: WMF Martins Fontes, 2010, p. 318.
[43] 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. 114.
[44] ARENDT, Hannah. **A Condição Humana.** 10. ed. Rio de Janeiro: Forense Universitária, 2007, p. 39-41.

como ser privado da possibilidade de realizar algo mais permanente que a própria vida. Nesse sentido, "o homem privado não se dá a conhecer e, portanto, é como se não existisse. O que quer ele faça permanece sem importância ou consequência para os outros"[45].

Também na Idade Média não há um anseio geral pela privacidade, entretanto, já havia a possibilidade de alguns senhores feudais isolarem-se dos demais, se assim o desejassem, o que não era a regra naquele momento histórico[46], uma vez que, no feudalismo, todos os indivíduos eram ligados por uma série de relações que se refletiam na própria organização da vida cotidiana[47].

Assim, a família urbana medieval incluía, como parte da família, além dos parentes, um grupo de trabalhadores industriais e domésticos, cuja relação era a de membros secundários da família. Os membros comiam juntos à mesa e até dormiam no mesmo salão comum. Ainda no século XVII, as criadas costumavam dormir em camas de rodas ao pé do seu senhor e senhora, os quais dormiam na cama grande[48].

O espaço não estava previsto para a solidão individual, mesmo no interior das grandes moradas. Quando as pessoas se arriscavam fora da vida doméstica, sempre o faziam em grupo. Os segredos eram necessariamente compartilhados por todos os membros da família ampla e qualquer um que intentasse isolar-se, como em um jardim fechado, era objeto de suspeita, já que alguém que se afastasse dos demais ou era para fazer o mal, ou se tornava vulnerável ao ataque dos inimigos, ou era um desencaminhado, um louco[49].

No decorrer da Idade Média, porém, mudanças culturais que ocorreram primeiramente na aristocracia foram, lentamente, infiltrando-se no resto da população.

Nas palavras de Mumford:

> A primeira alteração radical, que iria modificar a forma da cidade medieval, foi o desenvolvimento do sentido de isolamento. Isso significava, na realidade, retirada voluntária da vida comum e renúncia aos interesses comuns dos semelhantes. Recolhimento no sono; recolhimento para comer; isolamento no ritual religioso e social; recolhimento, por fim, no pensamento[50].

---

[45] ARENDT, Hannah. **A Condição Humana.** 10. ed. Rio de Janeiro: Forense Universitária, 2007, p. 68.
[46] 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. 116.
[47] RODOTÀ, Stefano. **A vida na sociedade da vigilância –** a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 26.
[48] MUMFORD, Lewis. **A Cidade na História** – suas origens, transformações e perspectivas. 4. ed. São Paulo: Martins Fontes, 2004, p. 307-312.
[49] DUBY, Georges (Org.). **História da Vida Privada.** São Paulo: Companhia das Letras, 2009, p. 528-529.
[50] MUMFORD, Lewis. **A Cidade na História** – suas origens, transformações e perspectivas. 4. ed. São Paulo: Martins Fontes, 2004, p. 311.

A partir do século XII, é possível visualizar marcas das conquistas de uma autonomia pessoal. A economia começa a se distender; o crescimento agrícola impulsiona as estradas, os mercados e as aldeias, e transporta pouco a pouco para a cidade todos os sistemas de controle; o uso da moeda adquire notável importância e se difunde por toda a parte o uso da palavra "ganhar". Cresce a vontade do indivíduo de poupar para tornar-se menos dependente da família, bem como se amplia o espaço de liberdade, principalmente para empreendimentos individuais. Os subúrbios humanos tornam-se povoados de traficantes e artesãos, alguns dos quais fazem rápida fortuna, e as grandes famílias começam a se dissociar[51].

Assim, ao longo do tempo, quando se tornou econômica e fisicamente seguro possuir certa privacidade, o vocábulo foi perdendo as conotações desfavoráveis, sendo o conceito recente de privacidade uma criação do Ocidente[52].

Rodotà associa o nascimento da privacidade, em sua noção moderna, à desagregação da sociedade feudal. A possibilidade de isolamento estende-se a todos que dispunham de meios materiais para reproduzir condições que satisfizessem esta nova necessidade de intimidade. Essa nova realidade recebe bastante influência das transformações socioeconômicas relacionadas à Revolução Industrial, como as novas técnicas de construção das habitações e a separação entre a casa e o local de trabalho[53].

Nesse cenário, a privacidade surge não como a realização de uma exigência natural de cada indivíduo, mas como a aquisição de um privilégio por parte de um grupo, a burguesia, já que a classe operária ficou excluída da privacidade em virtude de suas condições materiais. Por esta razão, os instrumentos jurídicos utilizados para tutelar a privacidade nesse momento foram modelados com base no direito à propriedade[54]. Tem origem então uma concepção de privacidade diretamente associada à proteção da propriedade, a qual muitas vezes ainda faz sentir sua influência[55].

Como se percebe, até esse momento a privacidade ainda não era tida como um direito autônomo. Em 1890, Warren, que além de advogado era membro de uma das famílias mais abastadas de Boston, incomodado com os excessos da imprensa ao noticiar fatos da sua família, e seu sócio Brandeis reuniram decisões judiciais antigas, as quais, concluíram, baseavam-se num princípio mais amplo que o direito à propriedade, que o reconhecimento da

---

[51] DUBY, Georges (Org.). **História da Vida Privada.** São Paulo: Companhia das Letras, 2009, p. 531-533.
[52] POSNER, Richard A. **A Economia da Justiça.** São Paulo: WMF Martins Fontes, 2010, p. 318.
[53] RODOTÀ, Stefano. **A vida na sociedade da vigilância –** a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 26.
[54] RODOTÀ, Stefano. **A vida na sociedade da vigilância –** a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 27.
[55] 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. 119.

quebra de confiança ou de contrato ou que os remédios contra a calúnia e a difamação. Tratava-se do que chamaram de "*right to privacy*" – ou, em português, direito à privacidade –, o qual merecia autonomia[56].

Escreveram o artigo "*The rigth to privacy*", lançando as bases do conceito tradicional de privacidade como "*the right to be let alone*", isto é, "o direito a ser deixado só" ou "o direito de ser deixado em paz":

> Invenções recentes e métodos de negócios chamam a atenção para o próximo passo que deve ser dado para a proteção da pessoa e para garantir ao indivíduo o que o juiz Cooley chama de direito de "ser deixado em paz". Fotografias instantâneas e empresas de jornais invadiram os recintos sagrados da vida privada e doméstica; e numerosos dispositivos mecânicos ameaçam fazer cumprir a previsão de que "o que é sussurrado no armário deve ser proclamado do alto da casa". Durante anos, tem-se a sensação de que a lei deve fornecer algum remédio para a circulação não autorizada de retratos de pessoas privadas; a [...] questão de saber se nossa lei reconhecerá e protegerá o direito à privacidade neste e em outros aspectos deve em breve ser levada aos tribunais para consideração[57].

Ressalte-se que o texto não é o primeiro a abordar a proteção jurídica de determinados aspectos da privacidade, mas é o primeiro a tratá-la de modo autônomo, diferente de outros direitos, em especial do direito de propriedade e do direito autoral, daí a sua importância. Os próprios autores citam a obra do juiz Cooley, *A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract*, na qual o autor faz uma classificação dos direitos do indivíduo cuja violação gera responsabilidade civil extracontratual, referindo-se, assim, ao direito à imunidade pessoal, que ele define como "um direito de completa imunidade: o direito de ser deixado em paz"[58].

---

[56] WARREN, Samuel D; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review,** v. 4, n. 5, 15 dez. 1890, p. 193-220. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em: 2 dez. 2019.

[57] "Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone" Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops'. For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of invasion of privacy by the newspapers, long keenly felt, has been but recently discussed by an able writer. The alleged facts of a somewhat notorious case brought before an inferior tribunal in New York a few months ago, directly involved the consideration of the right of circulating portraits; and the question whether our law will recognize and protect the right to privacy in this and in other respects must soon come before our courts for consideration." WARREN, Samuel D; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review,** v. 4, n. 5, 15 dez. 1890, p. 193-220. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em: 2 dez. 2019.

[58] "Personal Immunity. *The right to one's person may be said to be a right of complete immunity: to be let alone. The corresponding duty is, not to inflict an injury, and not, within such proximity as might render it successful, to attempt the infliction of an injury. In this particular the duty goes beyond what is required in most cases; for usually an unexecuted purpose or an unsuccessful attempt is not noticed."* COOLEY, Thomas M. **A**

Ao romperem com a tradição anterior de associar a tutela da privacidade à propriedade, Warren e Brandeis fundamentam a proteção daquela à inviolabilidade da personalidade:

> Essas considerações levam à conclusão de que a proteção oferecida a pensamentos, sentimentos e emoções, expressos por meio da escrita ou das artes, na medida em que consiste em impedir a publicação, é apenas um exemplo da aplicação do direito mais geral do indivíduo de ser deixado em paz [...]. O princípio que protege os escritos pessoais e todas as outras produções pessoais, não contra roubo e apropriação física, mas contra publicação de qualquer forma, não é, na realidade, o princípio da propriedade privada, mas o de uma personalidade inviolável[59].

Assim, ao tratarem da privacidade, os autores não fizeram uma correspondência perfeita entre esta e o "*right to be let alone*". Na verdade, inseriram o direito à privacidade na categoria de um direito mais geral, o direito do indivíduo a ser deixado em paz, o qual estava inserido num direito ainda mais geral: o direito de gozar a vida. Este direito fazia parte do direito fundamental à própria vida, reconhecido na Constituição dos Estados Unidos[60].

Nesse cenário, defenderam os autores que o direito à privacidade tutelaria não apenas o direito de o indivíduo isolar-se dos demais, mas também o direito de não ter seus pensamentos, sentimentos e manifestações violados e compartilhados sem a sua autorização, haja vista que essa publicação pode provocar danos, além de sofrimento, àquele que fora exposto, ainda que a informação seja verdadeira. Logo, caberia a cada indivíduo definir quais aspectos da sua vida privada seriam compartilhados[61], de forma que já nesse momento o consentimento ganha um papel de destaque no tratamento da violação à privacidade.

Dessa forma, o direito à privacidade tinha um caráter fortemente individualista, identificando-se com a proteção à vida íntima, familiar e pessoal de cada indivíduo. A sua

---

Treatiseonthe Law of Torts or the Wrongs Which Arise Independent of Contract. Chicago: Callaghan, 1879. Disponível em: https://repository.law.umich.edu/books/11/. Acesso em: 13 dez. 2019, p. 29.

[59] These considerations lead to the conclusion that the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone. [...]The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality. WARREN, Samuel D; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review,** v. 4, n. 5, 15 dez. 1890, p. 193-220. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em: 2 dez. 2019, p. 205.

[60] GLANCY, Dorothy J. The invention of the right to privacy. **Arizona Law Review**. v. 21, n. 1, 1979. Disponível em: https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1318&context=facpubs. Acesso em: 8 dez. 2019, p. 3.

[61] WARREN, Samuel D; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review,** v. 4, n. 5, 15 dez. 1890, p. 193-220. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em: 2 dez. 2019, p. 214-218.

tutela assumia uma conotação puramente negativa, uma vez que "impunha aos outros somente um dever geral de abstenção (não fazer)"[62].

Os anos que se seguiram foram marcados por certa tendência "elitista", pois as demandas que chegavam aos tribunais costumavam estar relacionadas a pessoas com determinada projeção social[63].

A partir de 1960, contudo, esse cenário começa a se alterar. Doneda aponta como principais motivos para tanto a transformação de um modelo de Estado liberal num Estado de bem-estar social, a mudança no relacionamento entre cidadão e Estado, uma demanda mais generalizada por direitos fruto dos movimentos sociais e das reivindicações da classe trabalhadora, bem como o desenvolvimento tecnológico e o consequente crescimento do fluxo de informações, cuja importância também crescia[64].

O aumento da capacidade técnica de recolher, processar e utilizar a informação permitiu que os Estados realizassem, em nome da eficiência administrativa, coletas de diversos dados dos cidadãos, muitos de cunho pessoal[65]. Instituições privadas também começam a coletar informações pessoais. Esse fato começa a provocar preocupações acerca de como o tratamento de dados poderia se apresentar como um instrumento para o autoritarismo e para a execução de uma política de discriminação baseada em opiniões políticas, religiosas, sindicais e até mesmo sobre a raça[66].

A Lei do Censo Populacional, na Alemanha, por exemplo, que visava coletar para fins estatísticos os dados da população como profissão, moradia e local de trabalho, provocou, em 1983, uma grande discussão jurídica, pois previa a possibilidade de os dados coletados serem comparados com outros registros públicos, bem como de serem transmitidos a outras repartições públicas para que fossem utilizados para fins outros, como a execução de dívidas[67].

---

[62] SCHREIBER, Anderson. **Direitos da Personalidade.** 3. ed. São Paulo: Atlas, 2014, p. 137.
[63] 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. 32-33.
[64] 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. 33.
[65] BOLESINA, Iuri. **O "Direito à Extimidade" e a sua Tutela por uma Autoridade Local de Proteção de Dados Pessoais:** as inter-relações entre identidade, ciberesapaço, privacidade e proteção de dados pessoais em face das intersecções jurídicas entre o público e o privado. 2016. Tese (Doutorado – área de concentração em Demandas Sociais e Políticas Públicas – eixo temático Diversidade e Políticas Públicas) – Programa de Pós-Graduação em Direito da Universidade de Santa Cruz do Sul – UNISC, Santa Cruz do Sul. Disponível em: https://unisc.br/images/curso-24/teses/2016/rosane_porto.pdf. Acesso em: 2 dez. 2019, p. 208.
[66] RODOTÀ, Stefano. **A vida na sociedade da vigilância –** a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 28-30.
[67] BOLESINA, Iuri. **O "Direito à Extimidade" e a sua Tutela por uma Autoridade Local de Proteção de Dados Pessoais:** as inter-relações entre identidade, ciberesapaço, privacidade e proteção de dados pessoais em face das intersecções jurídicas entre o público e o privado. 2016. Tese (Doutorado – área de concentração em

Ademais, o tratamento de dados passa a permitir a produção de perfis individuais, familiares ou de grupos, os quais, inclusive, podem ser cedidos a terceiros. Tal categorização de indivíduos pode prejudicar sobremaneira o livre desenvolvimento da personalidade, uma vez que solidifica cada pessoa no perfil que lhe foi traçado em determinada situação, dificultando o acesso a produtos e serviços que se distanciem desse perfil, além de possibilitar um perigoso processo de discriminação de minorias[68].

Nesse contexto, desenvolve-se a compreensão de que os dados pessoais são capazes de revelar até mesmo os aspectos mais íntimos do indivíduo e que o tratamento de tais dados ou a sua divulgação podem provocar tantos danos à personalidade quanto à veiculação não autorizada de uma imagem ou de um segredo.

Já não era mais possível analisar a questão da privacidade por meio de um pêndulo entre recolhimento e divulgação; entre o homem que guarda segredos e o que nada tem a esconder; entre a casa-fortaleza e a casa-vitrine[69]. O sentido e o alcance da privacidade então são modificados para se propor algo mais que a sua finalidade inicial, restrita à proteção da vida íntima, passando a abranger também o direito da pessoa humana de manter o controle sobre os seus dados pessoais[70].

Acerca disso, Rodotà, trazendo diferentes definições, demonstra essa reinvenção pela qual passou a noção de privacidade:

> Depois da definição histórica feita por Warren e Brandeis – "o direito de ser deixado em paz" –, outras definições foram desenvolvidas para espelhar diferentes clamores. Num mundo onde nossos dados estão em movimento incessante, "o direito a controlar a maneira na qual os outros utilizam as informações a nosso respeito" (A. Westin) torna-se igualmente importante. De fato, coletar dados sensíveis e perfis sociais e individuais pode levar à discriminação; logo a privacidade deve ser vista como "a proteção de escolhas de vida contra qualquer forma de controle público e estigma social" (L.M. Friedman), como a "reivindicação dos limites que protegem o direito de cada indivíduo a não ser simplificado, objetivado, e avaliado fora de contexto". (J. Rosen)[71].

Observa-se que, atualmente, tendem a prevalecer definições funcionais da privacidade, as quais, de diversas formas, relacionam-se à possibilidade de o indivíduo conhecer, controlar,

---

Demandas Sociais e Políticas Públicas – eixo temático Diversidade e Políticas Públicas) – Programa de Pós-Graduação em Direito da Universidade de Santa Cruz do Sul – UNISC, Santa Cruz do Sul. Disponível em: https://unisc.br/images/curso-24/teses/2016/rosane_porto.pdf. Acesso em: 2 dez. 2019, p. 208.

[68]RODOTÀ, Stefano. **A vida na sociedade da vigilância –** a privacidade hoje. Rio de Janeiro: Renovar, 2008p. 46.

[69] RODOTÀ, Stefano. **A vida na sociedade da vigilância –** a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 25.

[70] SCHREIBER, Anderson. **Direitos da Personalidade.** 3. ed. São Paulo: Atlas, 2014, p. 137-138.

[71] RODOTÀ, Stefano. **A vida na sociedade da vigilância –** a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 15.

endereçar e interromper o fluxo de informações que lhe dizem respeito[72]. Isto é, as atuais definições de privacidade não especificam qual o objeto da proteção jurídica, mas sim trazem instrumentos, procedimentos de tutela. Quando se define a privacidade relacionando-a ao controle do fluxo de informações pessoais, por exemplo, não se diz o que se protege, mas como se protege.

O autor ressalta que as definições de privacidade não são mutuamente exclusivas, porque marcam a progressiva inclusão de novos aspectos de liberdade nesse conceito que é constantemente ampliado, de modo que as definições mais recentes não superam as anteriores[73]. Evidente, portanto, a dinamicidade do conceito de privacidade. Essa compreensão dinâmica permite a tutela integral da pessoa, "haja vista que não se podem clausular em conceitos ou previsões normativas todos os aspectos pessoais que devem ser tutelados"[74].

Quebra-se, assim, o nexo de identificação da privacidade com a classe burguesa, uma vez que ela se transforma em uma forma de promover a paridade de tratamento entre os cidadãos e de realizar a igualdade e não mais de resguardar o privilégio[75]. Agora não mais somente as figuras de grande relevo social estão sujeitas a ter sua privacidade violada, mas uma parcela muito maior da população e em uma ampla variedade de situações[76].

A privacidade adquire uma feição coletiva. Isso porque a esfera pessoal e a esfera política se unem, uma vez que a distribuição de poder na sociedade sofre forte influência das regras de circulação das informações que atingem a todos[77]. A privacidade projeta-se para além da esfera privada, tornando-se elemento constitutivo da cidadania e de garantia da liberdade das escolhas existenciais e políticas, numa ideia de tutela global de tais escolhas contra qualquer forma de controle público e estigmatização social[78].

Nesse cenário, a tutela da privacidade não se limita à proibição de interferência alheia na vida íntima, mas impõe também deveres de caráter positivo, a exemplo do dever de

---

72 RODOTÀ, Stefano. **A vida na sociedade da vigilância –** a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 92.
73 RODOTÀ, Stefano. **A vida na sociedade da vigilância –** a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 15.
74 CASTRO, Thamis D. V. de. Notas sobre a teoria tríplice da autonomia, paternalismo e direito de não saber na legalidade constitucional. *In:* **OpenAccess**, ano. Disponível em: https://openaccess.blucher.com.br/download-pdf/404/21235. Acesso em: 12 dez. 2019, p. 147.
75 RODOTÀ, Stefano. **A vida na sociedade da vigilância –** a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 30.
76 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. 33.
77 RODOTÀ, Stefano. **A vida na sociedade da vigilância –** a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 45.
78 RODOTÀ, Stefano. **A vida na sociedade da vigilância –** a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 129.

solicitar autorização para a inclusão do nome de determinada pessoa num banco de dados ou o dever de possibilitar que o titular dos dados acesse quais informações suas serão inseridas no banco de dados, bem como que possa corrigi-las a qualquer tempo[79].

Dessa forma, atualmente a privacidade, para muito além da lógica de proteção contra o mundo externo de Warren e Brandeis, assume a função promocional de assegurar a livre construção da esfera pessoal de cada indivíduo, o que a faz ganhar cada vez mais relevância na proteção da pessoa humana.

A expressão "privado", por sua vez, passa a assumir o significado de pessoal, e não mais de secreto. Agora, ao se falar em "privado", não mais necessariamente se identificam áreas às quais serão atribuídas uma proteção especial por razões de intimidade, pois essa noção passa a "abranger o conjunto das atividades e situações de uma pessoa que tem um potencial de 'comunicação' verbal e não verbal, e que pode, portanto, se traduzir em informações"[80].

No que diz respeito ao reconhecimento da privacidade, em 1948, este direito foi previsto na Declaração Universal de Direitos do Homem[81]. Em 1950, foi a vez de a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, em seu artigo 8º, reconhecer o direito à privacidade[82]. Em 1966, o Pacto Internacional de Direitos Civis e Políticos, em seu artigo 17º, também previu tal direito[83]. Em 1969, o Pacto de São José da Costa Rica, em seu artigo 11, dispôs que "Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação"[84].

---

[79] SCHREIBER, Anderson. **Direitos da Personalidade.** 3. ed. São Paulo: Atlas, 2014, p. 139.

[80] RODOTÀ, Stefano. **A vida na sociedade da vigilância –** a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 93.

[81] XII: Ninguém será objeto de ingerências arbitrárias em sua vida privada, sua família, seu domicílio ou sua correspondência, nem de ataques a sua honra ou a sua reputação. Toda pessoa tem direito à proteção da lei contra tais ingerências e ataques. ONU. Assembleia Geral. **Declaração Universal dos Direitos Humanos.** 10 dez. 1948. Disponível em: https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf. Acesso em: 8 dez. 2019.

[82] Art. 8.º: *Direito ao respeito pela vida privada e familiar*

1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.

2. Não pode haver ingerência de autoridade pública no exercício desse direito senão quando esta ingerência estiver prevista na lei [...]. CONSELHO DA EUROPA. Corte Europeia de Direitos Humanos. **Convenção Europeia dos Direitos do Homem.** Roma, 4 nov. 1950. Disponível em: https://www.echr.coe.int/Documents/Convention_POR.pdf. Acesso em: 20 abr. 2020.

[83] Art. 17º: [...] §1. Ninguém poderá ser objeto de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra e reputação. ONU. **Pacto Internacional de Direitos Civis e Políticos,** adoptado e aberto à assinatura, ratificação e adesão pela Assembleia Geral das Nações Unidas pela Resolução nº 2200-A (XXI), de 16 de dezembro de 1966. Disponível em: http://www.cidadevirtual.pt/cpr/asilo2/2pidcp.html. Acesso em: 8 dez. 2019.

[84] OEA. Comissão Interamericana de Direitos Humanos. **Convenção Americana sobre Direitos Humanos,** assinada na Conferência Especializada Interamericana sobre Direitos Humanos, San José, Costa Rica, em 22 de

Paulatinamente, os países foram reconhecendo o direito à privacidade em seus ordenamentos jurídicos internos, por meio de suas constituições ou legislações infraconstitucionais. Hoje, há previsão constitucional desse direito em quase todos os países democráticos do mundo.

Com a ampliação do conceito de privacidade de modo a abarcar também o direito à proteção de dados pessoais, tem-se a Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, de 1981, como importante marco no reconhecimento desse direito como fundamental[85]. Seguiram-se várias outras legislações nacionais e internacionais tratando da matéria, como a Diretiva 95/46/CE do Parlamento Europeu e do Conselho e o Regulamento Geral da União Europeia. No Brasil, recentemente, entrou em vigor a Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)[86], a qual será objeto de estudo deste trabalho.

Diante de toda essa exposição acerca da evolução do conceito de privacidade, torna-se imprescindível conceituar e delimitar o alcance desse direito, o que se intentará satisfazer na próxima subseção.

2.3 Conceito de privacidade

Privacidade não é um conceito único. Varia em cada sociedade, em cada momento histórico e econômico, em cada cultura. Em razão disso, privacidade é um termo que abarca diversas definições ao longo do tempo, possuindo natureza altamente dinâmica e modificando-se progressivamente para incluir novos aspectos de proteção da personalidade.

Solove afirma que privacidade "é um conceito em desordem", vago, que ninguém pode articular o que significa. É um termo genérico que significa tantas coisas para tantas pessoas diferentes que perdeu qualquer conotação legal precisa que poderia ter tido[87].

---

novembro de 1969. Disponível em: https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm. Acesso em: 8 dez. 2019.

[85] DONEDA, Danilo. A Proteção dos Dados Pessoais como um Direito Fundamental. **Espaço Jurídico,** Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: https://dialnet.unirioja.es/descarga/articulo/4555153.pdf. Acesso em: 17 abr. 2020, p. 102.

[86] A *vacatio legis* da LGPD sofreu diversas modificações, as últimas fixaram-na do seguinte modo: Em relação às sanções administrativas, a Lei entrará em vigor em 1° de agosto de 2021. Quanto às demais disposições, apesar da previsão de *vacatio legis* de 24 meses, a LGPD entrou em vigor um pouco depois disso, em 18 de setembro, data da publicação da Lei 14.058/2020, sem o conteúdo que dilatava a vacância.

[87] SOLOVE, Daniel J. A Taxonomy of Privacy. **University of Pennsylvania Law Review,** v. 154, n. 3, jan. 2006. Disponível em: https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf. Acesso em: 2 dez. 2019, p. 477-479.

A esse respeito, a Conferência Internacional de Juristas de 1967 definiu dez diretrizes para delimitar o direito à privacidade como a proteção contra: a interferência na vida privada, familiar e doméstica; a interferência na integridade física ou mental, ou sobre a liberdade moral ou intelectual; os ataques contra a honra ou reputação; situações de *false light*; a divulgação de fatos irrelevantes ou embaraçosos, relatando a vida privada de alguém; o uso do nome, da identidade ou qualquer outra semelhança de outrem; a prática de espionagem, curiosidade, observação ou assédio sobre a vida alheia; a interferência sobre a correspondência; o tratamento inadequado de correspondência escrita ou verbal; e a divulgação de informações fornecidas ou recebidas de alguém em circunstâncias de sigilo profissional[88].

Doneda esclarece que a falta de uma definição âncora, que reflita uma consolidação do seu tratamento semântico, não é um problema somente da doutrina brasileira, a qual se utiliza de vários termos para representar a privacidade, além dessa própria expressão, tais como "vida privada", "intimidade", "segredo", "sigilo", "reserva" e "intimidade da vida privada"[89].

A privacidade assumiu diferentes concepções nos diversos ordenamentos jurídicos, cada uma delas representando as particularidades da sociedade em que estavam inseridas, o que contribuiu para a profusão de diferentes conceitos desse direito. Dessa forma, a privacidade é um termo que se presta a certa manipulação pelo ordenamento, muitas vezes sendo utilizada para suprir algumas necessidades estruturais da ordem jurídica, o que dificulta a sua redução a um sentido comum[90].

Essa dificuldade de redução, ao contrário do que possa parecer, não é algo ruim, haja vista que definições reducionistas podem acabar por abranger apenas um ou outro entre os vários aspectos da privacidade. Essa dinamicidade do conceito de privacidade é essencial para uma proteção global da pessoa, tendo em vista que diferentes dimensões da personalidade podem ser tuteladas por meio desse direito fundamental, dispensando-se um reconhecimento próprio e apartado de cada um dos direitos da privacidade para que estes sejam assegurados, como o que por muito tempo aconteceu, no Brasil, com o direito à proteção de dados pessoais. Assim, a noção de privacidade evolui juntamente com a sociedade, já conferindo proteção a novos interesses jurídicos, evitando que estes fiquem sem tutela jurídica enquanto o ordenamento não trata da matéria.

---

[88] BOFF, Salete O.; FORTES, Vinícius B; FREITAS, Cinthia O. de A. **Proteção de Dados e Privacidade:** do Direito às novas Tecnologias na Sociedade da Informação. Rio de Janeiro: Lumen Juris, 2018, p. 70-71.
[89] 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. 98-99.
[90] 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. 99-100.

Por esta razão, Doneda afirma que "a indefinição quanto ao conteúdo do direito à privacidade deve ser tomada mais como uma característica intrínseca da matéria do que como um defeito ou obstáculo"[91]. Assim, verificam-se diferentes definições de privacidade posteriores à conceituação inicial de "direito a ser deixado só".

Posner definiu privacidade como "a restrição ou ocultação de informações, sobretudo pessoais"[92]. José Afonso da Silva entende a privacidade como "o conjunto de informação acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições"[93].

Por sua vez, Westin a define como o direito do indivíduo de controlar a maneira de utilização das suas informações pessoais pelos outros. Já Friedman entende privacidade como a proteção das escolhas da vida contra qualquer forma de controle público e estigma social, ao passo que Rosen define esse direito como a reivindicação de limites que impedem que o indivíduo seja simplificado, objetivado e avaliado fora de contexto[94].

Importante e atual conceito de privacidade é o de Rodotà, que a define como "o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da esfera privada", incluindo-se aí o direito do indivíduo de "não saber", de não tomar conhecimento sobre determinada informação, ainda que tal informação lhe diga respeito, ou de excluir da própria esfera privada uma determinada categoria de informações[95].

Esses conceitos não se excluem, ao contrário, dão um maior destaque a um dos aspectos da privacidade, ou incluem, progressivamente, novos âmbitos de proteção de um conceito ampliado de privacidade.

Nesse diapasão, para Solove, atualmente a privacidade é um conceito abrangente, que engloba, entre outras coisas, a liberdade de pensamento, o controle sobre o próprio corpo, a solidão em sua casa, o controle sobre informações pessoais, a proteção da reputação de alguém e a proteção contra buscas e interrogatórios, sendo um direito fundamental, essencial para a liberdade, a democracia, o bem-estar psicológico, a individualidade e a criatividade[96].

---

[91] 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. 101.
[92] POSNER, Richard A. **A Economia da Justiça.** São Paulo: WMF Martins Fontes, 2010, p. 274.
[93] SILVA, José Afonso da. **Curso de Direito Constitucional Positivo.** 25. ed. São Paulo: Malheiros, 2005, p. 206.
94 RODOTÀ, Stefano. **A vida na sociedade da vigilância –** a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 15.
[95] RODOTÀ, Stefano. **A vida na sociedade da vigilância –** a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 109.
[96] SOLOVE, Daniel J. **Understanding privacy.** Londres: Harvard University Press, 2008, p. 13-17.

Também Silva afirma que o direito à privacidade é uma expressão genérica e ampla, a qual abarca todas as manifestações da esfera íntima, privada e da personalidade. Essa esfera de inviolabilidade abrange o modo de vida doméstico, as relações familiares e afetivas em geral, fatos, hábitos, local, nome, imagem, pensamentos, segredos, além das origens e planos futuros do indivíduo[97].

Nessa mesma esteira, Lobo afirma que "Sob a denominação privacidade cabem os direitos da personalidade que resguardam de interferências externas os fatos da intimidade e da reserva da pessoa, que não devem ser levados ao espaço público", incluindo-se aí os direitos à intimidade, à vida privada, ao sigilo, à imagem e aos dados pessoais[98].

Diante disso, a privacidade é um um termo guarda-chuva, que abrange uma série de direitos, como o direito ao sigilo, o direito à inviolabilidade de domicílio, o direito à imagem, o direito à intimidade e o direito à proteção de dados pessoais. Isso significa que o direito à privacidade é gênero do qual todos esses, além de vários outros direitos, são espécie.

Ressalte-se, por fim, que a noção de privacidade, por variar em cada cultura, pode estar ligada à ideia de liberdade em uma sociedade e à dignidade em outra, como será detalhado mais adiante.

Antes disso, porém, será feita uma breve distinção entre intimidade e vida privada, com vistas a esclarecer o conteúdo e a abrangência do direito à privacidade aqui adotado, uma vez que muitos autores defendem que os três conceitos tratam do mesmo direito.

2.3.1 Distinção entre intimidade e vida privada

Não raramente as expressões privacidade, intimidade e vida privada são tratadas como sinônimas, contudo, como visto, a primeira é gênero da qual as outras duas são espécies. O direito à intimidade e o direito à vida privada também possuem âmbitos de proteção distintos.

A Constituição brasileira de 1988, em seu artigo 5º, X, prevê que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas"[99], o que sugere que o ordenamento jurídico pátrio reconhece que intimidade e vida privada são duas manifestações distintas da privacidade.

---

[97] SILVA, José Afonso da. **Curso de Direito Constitucional Positivo.** 25. ed. São Paulo: Malheiros, 2005, p. 206.

[98] LÔBO, Paulo. Direito à Privacidade e sua Autolimitação. *In*: EHRHARDT JÚNIOR, Marcos; LOBO, Fabiola Albuquerque (Coord.). **Privacidade e sua Compreensão no Direito Brasileiro.** Belo Horizonte: Fórum, 2019, p. 17-18.

[99] BRASIL. **Constituição Federal de 1988.** Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 13 dez. 2019.

A jurisprudência brasileira, no entanto, embora reconheça a diferença entre intimidade e privacidade, muitas vezes considera esta última como sinônimo de "vida privada", como se verifica no julgamento da Ação Direta de Inconstitucionalidade nº 4.815/Distrito Federal, que julgou o caso das biografias não autorizadas:

> 7. A liberdade é constitucionalmente garantida, não se podendo anular por outra norma constitucional (inc. IV do art. 60), menos ainda por norma de hierarquia inferior (lei civil), ainda que sob o argumento de se estar a resguardar e proteger outro direito constitucionalmente assegurado, qual seja, o da inviolabilidade do **direito à intimidade, à privacidade**, à honra e à imagem.
> 8. Para a coexistência das normas constitucionais dos incs. IV, IX e X do art. 5º, há de se acolher o balanceamento de direitos, conjugando-se o direito às liberdades com a inviolabilidade **da intimidade, da privacidade**, da honra e da imagem da pessoa biografada e daqueles que pretendem elaborar as biografias. (Grifos nossos)[100].

A doutrina brasileira também não é unânime na definição de intimidade e vida privada, inclusive há aqueles que fundem ambos os direitos num mesmo conceito: "o estar só, a tranquilidade e a paz de espírito"[101]. São os chamados unitaristas, sendo Caio Mário da Silva Pereira um dos adeptos dessa linha de pensamento[102].

Diante dessa dificuldade de conceituação, cabe aqui fazer uma rápida distinção entre intimidade e vida privada. Para tanto, elaborou-se uma tabela com as definições de ambos os direitos apresentadas por constitucionais e civilistas.

Quadro 1 – Distinções doutrinárias de intimidade e vida privada

Autor	Intimidade	Vida Privada
José Afonso da Silva[103]	Protege a esfera secreta da vida do indivíduo na qual este tem o poder legal de evitar os demais, abrangendo a inviolabilidade do domicílio, o sigilo da correspondência e o segredo profissional.	É um conceito mais abrangente que o de intimidade, significando o conjunto de modo de ser e de viver, o direito de o indivíduo viver sua vida. Para o autor, a vida das pessoas compreende dois aspectos, um voltado para o exterior e outro voltado para o interior. Esta última se debruça sobre a própria pessoa, sobre os membros de sua família e sobre seus amigos. É essa vida interior que integra o conceito de vida privada. Distingue-o de privacidade, que seria mais amplo e abarcaria todas as manifestações da esfera íntima, privada e da

[100] BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 4.815/Distrito Federal**. Requerente: Associação Nacional dos Editores de Livros – ANEL. Intimados: Presidente da República e Presidente do Congresso Nacional. Relatora: Ministra Cármen Lúcia. Brasília/DF, 10 de Junho de 2015. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=10162709. Acesso em: 8 mar. 2018.
[101] VIEIRA, José Ribas et al. (Coords.). **Direitos à Intimidade e à Vida Privada.** Curitiba: Juruá, 2008, p. 125.
[102] PEREIRA, Caio Mario da Silva. **Instituições de Direito Civil.** 24. ed. v. 1. Introdução ao Direito Civil; Teoria Geral de Direito Civil. Rio de Janeiro: Forense, 2011, p. 217.
[103] SILVA, José Afonso da. **Curso de Direito Constitucional Positivo.** 37. ed. São Paulo: Malheiros, 2014, p. 208-211.

		personalidade, definida como o conjunto de informação acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle.
Gilmar Mendes e Paulo Gustavo Gonet Branco[104]	Tem como objeto as conversações e os episódios ainda mais íntimos, envolvendo relações familiares e amizades mais próximas. Faz parte do direito à privacidade (vida privada), o qual seria um conceito mais amplo.	Tem por objeto os comportamentos e acontecimentos atinentes aos relacionamentos pessoais em geral, às relações comerciais e profissionais que o indivíduo não deseja que se espalhem ao conhecimento público. Para o autor, é sinônimo de privacidade.
Luís Roberto Barroso[105]	Tem como objeto o indivíduo consigo próprio, abrigado em sua consciência.	Tem como objeto os acontecimentos que se referem às relações de família, de amizade e outras relações de afeto. Para o autor, é sinônimo de privacidade.
Ingo Sarlet, Luiz Guilherme Marinoni e Daniel Mitidiero[106]	Guarda relação com a proteção de uma esfera mais íntima da vida do indivíduo, envolvendo suas relações familiares e suas amizades. É uma esfera, um nível da vida privada.	Trata da reserva sobre comportamentos e acontecimentos atinentes aos relacionamentos pessoais em geral, além de incluir a intimidade no seu âmbito de proteção. Considera como sinônimo de privacidade.
Paulo Lobo[107]	Refere-se aos fatos, situações e acontecimentos mantidos sob domínio exclusivo da pessoa, isto é, que não são compartilhados com outras pessoas. Estariam tutelados pela intimidade "os dados e documentos cuja revelação possa trazer constrangimento e prejuízos à reputação da pessoa, quer estejam na moradia, no automóvel, nos ambientes do trabalho, na *internet*".	Diz respeito ao ambiente familiar, e sua lesão acaba por resvalar nos outros membros do grupo. Diferencia-o de direito à privacidade, o qual seria um direito amplo que abarcaria uma série de outros direitos, entre os quais o direito à intimidade e o direito à vida privada.
Caio Mário da Silva Pereira[108]	Não o distingue de vida privada.	Sinônimo de privacidade. Direito de estar só, de não se comunicar; e simultaneamente de não ser molestado por outrem ou pelo Estado.

Fonte: Elaborado pela autora.

Da análise dos conceitos acima, observa-se que, à exceção de Pereira, representante da corrente unitarista, as definições de intimidade podem ser agrupadas em duas abordagens distintas:

a) uma, que restringe o âmbito de proteção desse direito aos acontecimentos e informações relacionados ao próprio indivíduo e somente a ele, abarcando, em seu objeto,

[104] MENDES, Gilmar; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional.** 12. ed. São Paulo: Saraiva, 2017, p. 245.
[105] BARROSO, Luís Roberto. **Curso de Direito Constitucional Contemporâneo –** os conceitos fundamentais e a construção do novo modelo. 2. ed. São Paulo: Saraiva, 2010, p. 70-72.
[106] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de Direito Constitucional.** 4. ed. São Paulo: Saraiva, 2015, p. 706-708.
[107] LÔBO, Paulo. Direito à Privacidade e sua Autolimitação. *In*: EHRHARDT JÚNIOR, Marcos; LOBO, Fabiola Albuquerque (Coord.). **Privacidade e sua Compreensão no Direito Brasileiro.** Belo Horizonte: Fórum, 2019, p. 17-19.
[108] PEREIRA, Caio Mario da Silva. **Instituições de Direito Civil.** 24. ed. v. 1. Introdução ao Direito Civil; Teoria Geral de Direito Civil. Rio de Janeiro: Forense, 2011, p. 217.

expressões como segredo, domínio exclusivo da pessoa e indivíduo abrigado em sua consciência. Adotam essa perspectiva Silva, Barroso e Lobo;

b) outra, que além de abarcar em seu âmbito de proteção os mesmos elementos objeto da primeira abordagem, tal como o segredo, engloba os fatos, conversas e informações relacionadas à família do indivíduo e suas amizades. Essa abordagem é a utilizada por Mendes, Branco, Sarlet, Marinoni e Mitidiero.

No que diz respeito à vida privada, também se observam quatro diversas perspectivas relacionadas com as abordagens do direito à intimidade:

a) a primeira, para a qual a vida privada tem como objeto os acontecimentos e informações que dizem respeito às relações familiares e de amizade próximas, não incluindo em sua tutela a intimidade e não abrangendo relações pessoais em geral. Adotam essa perspectiva Silva, Barroso e Lobo;

b) outra, que inclui, em seu âmbito de proteção, os comportamentos e informações relacionados às relações pessoais em geral, excetuando-se as relações familiares e de amizade, que estariam protegidas pela intimidade. Essa é a abordagem da definição de Mendes e Branco;

c) outra, ainda, que inclui, em seu âmbito de proteção, os comportamentos e informações relacionados às relações pessoais em geral, além das relações familiares e de amizade, mesmo estas sendo protegidas pela intimidade, pois se incluiria na tutela da vida privada. Essa é a perspectiva adotada por Sarlet, Marinoni e Mitidiero;

d) por fim, tem-se a abordagem da definição de Pereira, o qual, ao definir vida privada como o direito a estar só e de não se comunicar, acaba por aproximar o seu objeto mais do direito à intimidade do que dos demais conceitos de vida privada.

Ainda no que se refere à vida privada, algumas dessas definições a consideram como sinônimo de privacidade, ao passo que outras defendem que a privacidade seria um direito ainda mais amplo, a tutelar tanto a intimidade e a vida privada quanto outros direitos e manifestações da personalidade.

Neste trabalho, compreende-se a intimidade como tudo aquilo que diz respeito, exclusivamente, à própria pessoa, não sendo compartilhado com mais ninguém.

Por sua vez, a vida privada se refere aos fatos, acontecimentos e informações que não devem ser tornados públicos, mas que também não são secretos, íntimos. Assim, este direito tutela os fatos ocorridos no âmbito das relações sociais que o indivíduo tece, como as familiares, profissionais e de amizade.

Apesar destas definições, na prática existem muitas situações em que é difícil distinguir se estão relacionadas a um ou a outro direito. Outrossim, diante da pluralidade de conceitos presentes da doutrina e na jurisprudência, sempre que houver referência à intimidade ou à vida privada, deve-se entender que o outro direito também está envolvido.

Por fim, importa destacar que, em que pese parcela doutrina considere que vida privada e privacidade são sinônimos, estes direitos não se confundem, haja vista que este último possui um alcance bem maior. Com efeito, a vida privada é apenas um dos direitos da privacidade, a qual abrange, inclusive, o direito à proteção de dados que, como visto, vai além da esfera privada do indivíduo.

Uma vez delimitados os conceitos de intimidade, vida privada e privacidade que são adotados neste trabalho, parte-se agora ao estudo dos diferentes modelos de privacidade.

2.3.2 Modelos jurídicos de privacidade

Como visto, o conceito de privacidade não é único, sendo fortemente influenciado pela cultura em que este direito está inserido. Existem três principais concepções de privacidade, as quais implicam a regulação de tal direito, a saber: a privacidade americana, a privacidade europeia e a privacidade oriental. As próximas subseções dedicam-se ao estudo desses modelos jurídicos, destacando-se seus traços distintivos.

2.3.2.1 A privacidade no direito americano

Não é novidade que os Estados Unidos possuem uma cultura fortemente marcada pela resistência à intervenção do Estado não somente na economia, mas também na vida dos cidadãos. A liberdade é um dos valores mais caros na cultura americana, de modo que os estadunidenses julgam inadmissível que o Estado cerceie seu poder de escolha ou dite regras acerca de como devem viver suas vidas.

No Brasil, por exemplo, a mudança de prenome exige requisitos que fazem com que ela somente seja possível em determinados casos, como na hipótese de um prenome vexatório. Já nos Estados Unidos, essa alteração pode ser algo bem simples, como o preenchimento de um formulário, o pagamento de uma taxa, a publicação de um anúncio no

jornal e a explicação das razões da mudança em uma audiência judicial[109]. O Estado não deve opor tantos obstáculos para que o indivíduo possa escolher o próprio nome.

Nesse sentido, seria possível apresentar uma série de exemplos de como a liberdade individual é privilegiada e assegurada nos Estados Unidos, a despeito de muitos defensores do conservadorismo em alguns campos, como o do aborto. Assim, os americanos não aceitam que o Estado diga em qual escola seu filho deve estudar, ou mesmo que ele deva estudar num estabelecimento de ensino e não em casa; o porte e a aquisição de armamentos são relativamente fáceis de se conseguir nos Estados Unidos; e a Suprema Corte decidiu a favor de um confeiteiro que, em 2012, negou-se a preparar um bolo de casamento para uma cerimônia entre pessoas do mesmo sexo em razão de suas crenças religiosas[110].

Como já visto, a noção de privacidade sofre grande influência do seu contexto histórico, econômico e social. Diante disso, a cultura americana de liberdade influencia bastante na forma como os americanos enxergam a privacidade.

Apesar de toda a importância do artigo de Warren e Brandeis, a jurisprudência dos Estados Unidos não absorveu, de imediato, seus argumentos. No mesmo ano de publicação do artigo, em Nova Iorque foi reconhecido, de maneira autônoma, o direito à privacidade, no caso *Manola v. Stevens*, no qual o demandado havia tirado uma fotografia da atriz Marion Manola vestida em um *collant* e foi proibido de publicá-la por decisão judicial[111].

No entanto, embora três outas decisões de Nova Iorque e uma de Massachusetts tenham seguido por esse caminho, o Tribunal de Michigan, no caso *Atkinson v. John E. Doherty & Co.*, e o Tribunal de Nova Iorque, em 1902, no caso *Roberson v. Rochester Folding box Co.*, romperam com esse progresso. Nesse último, a Corte de Nova Iorque afirmou inexistir direito à privacidade na utilização não autorizada de fotografia numa propaganda, sob o fundamento de que não havia precedentes, pois a lesão possuía caráter puramente mental e uma decisão favorável poderia aumentar a litigiosidade. Seria muito

---

[109] UOL NOTÍCIAS. **Norte-Americana quer ser chamada de "sexy".** 30 jan. 2014. Disponível em: https://noticias.uol.com.br/tabloide/ultimas-noticias/2014/01/30/norte-americana-quer-ser-chamada-de-sexy.htm?cmpid=copiaecola. Acesso em: 5 jan. 2020.

[110] G1 MUNDO. **Suprema Corte dos EUA decide a favor de confeiteiro que se recusou a fazer bolo para casal gay.** 4 jun. 2018. Disponível em: https://g1.globo.com/mundo/noticia/suprema-corte-dos-eua-decide-a-favor-de-confeiteiro-que-se-recusou-a-fazer-bolo-a-casal-gay.ghtml. Acesso em: Acesso em: 8 dez. 2019.

[111] PROSSER, William L. Privacy. *In:* **California Law Review,** v. 48, n. 3, ago. 1960. Disponível em: https://heinonline.org/HOL/LandingPage?handle=hein.journals/calr48&div=31&id=&page=. Acesso em: 2 dez. 2019, p. 385.

difícil traçar uma linha entre figuras privadas e públicas e o medo de uma restrição indevida à liberdade de imprensa[112].

Três anos depois, no caso *Pavesich v. New England Life Insurance Co.*, em que o demandado utilizou o nome e a imagem do demandante no anúncio de seguro, a Suprema Corte da Geórgia rejeitou o precedente *Roberson v. Rochester Folding box Co.* e, aceitando os pontos de vista de Warren e Brandeis, reconheceu a existência do direito à privacidade[113]. Os trinta anos seguintes foram marcados por uma contínua disputa entre estes dois precedentes – Roberson e Pavesich –, até que, em 1939, o *Restatement of Torts*[114], em sua Seção 867, adotou o posicionamento de que uma pessoa que interfira seriamente no interesse de outrem de não ser exposto ao público deve ser responsabilizada[115], o que fortaleceu o reconhecimento do direito à privacidade que, paulatinamente, foi sendo adotado pela maioria dos tribunais, sob os fundamentos postos por Warren e Brandeis.

Em 1960, a obra de Warren e Brandeis já sofrera muitas críticas, principalmente acerca da definição do *rigth to privacy* como *rigth to be let alone* (direito a ser deixado só) e sobre tal conceito abrigar diversos ilícitos. William Prosser, professor da *California School of Law* escreveu o artigo "*Privacy*", no qual, com base no artigo de Warren e Brandeis, analisou o desenvolvimento do direito à privacidade na doutrina e jurisprudência americanas, bem como aperfeiçoou a concepção de privacidade então existente.

Nesse artigo, Prosser afirma que pelo uso de uma única palavra fornecida por Warren e Brandeis, os tribunais criaram uma base independente de responsabilidade, que é um complexo de quatro tipos distintos e pouco relacionados de ilícitos, quais sejam: 1) Intrusão na reclusão ou solidão do autor, ou em seus assuntos particulares (*intrusion)*; 2) Publicação de fatos privados embaraçosos *(public disclosure of private facts*) sobre o indivíduo; 3) Publicidade que coloca o demandante sob uma "falsa luz" aos olhos do público, isto é, publicação que é capaz de criar um julgamento equivocado pelo público da pessoa exposta (*false light in the*

---

[112] PROSSER, William L. Privacy. *In:* **California Law Review,** v. 48, n. 3, ago. 1960. Disponível em: https://heinonline.org/HOL/LandingPage?handle=hein.journals/calr48&div=31&id=&page=. Acesso em: 2 dez. 2019, p. 385.

[113] PROSSER, William L. Privacy. *In:* **California Law Review,** v. 48, n. 3, ago. 1960. Disponível em: https://heinonline.org/HOL/LandingPage?handle=hein.journals/calr48&div=31&id=&page=. Acesso em: 2 dez. 2019, p. 386.

[114] *Restatements* são publicações das várias áreas do direito com um conjunto de discussões acadêmicas e analíticas da lei e jurisprudência americana. Têm o objetivo de informar os aplicadores do direito sobre os precedentes judiciais, uma vez que o sistema jurídico dos Estados Unidos é a *commom law.* ALI. The American Law Institute. **Restatement of the Law Second, Torts.** 2020. Disponível em: https://www.ali.org/publications/show/torts/. Acesso em: 5 jan. 2020.

[115] *Restatement of Tort,* § 867*:* "Interference with Privacy. A person who unreasonably and seriously interferes with another's interest in not having his affairs known to others or his likeness exhibited to the public is liable to the other". CUDD, Ann E; NAVIN, Mark C. (Edit.). **Core Concepts and Contemporary Issues in Privacy**. Boston: Springer, 2018 [livro digital].

public eye); e 4) Apropriação, em proveito do demandado, do nome ou imagem do demandante (*apropriation*). Para Prosser, esses quatro tipos de violação poderiam estar, pelo menos em alguns aspectos, sujeitos a regras diferentes[116].

Como se vê, o *right to privacy* possui um conteúdo bastante amplo, englobando os aspectos pessoais do direito à imagem e até mesmo aspectos do que, no Brasil, consideram-se como crimes de calúnia, injúria ou difamação. Por essa razão, Adriana Sawaris afirma que o conteúdo da *privacy* americana é tão extenso que abarca todo o direito de personalidade[117]. Também Doneda afirma que o *rigth to privacy* tem o conteúdo do direito geral de personalidade[118].

É inegável que o artigo de Warren e Brandeis teve influência da tradição jurídica europeia – como a doutrina alemã dos direitos da "personalidade" –, tanto que os autores citaram a legislação francesa de privacidade de 1868, a lei do insulto da Alemanha e caracterizaram o *rigth to privacy* como um aspecto da proteção de "personalidade". Brandeis estudou o ensino médio na Alemanha durante a década de 1870 e permaneceu um admirador apaixonado da cultura desse país. Por esta razão, Whitman afirma que os autores tentaram introduzir um direito à privacidade num estilo europeu – cuja concepção, como se verá, é diferente da noção americana[119].

No entanto, a cultura americana é bastante diversa da europeia, de modo que, sendo a noção de privacidade fortemente variável em cada contexto, não havia como os Estados Unidos entenderem o direito à privacidade da mesma forma que se entende na Europa, embora ambos façam parte do Ocidente.

Parte da resistência da lei e jurisprudência americanas às ideias de Warren e Brandeis baseou-se em dois valores em particular: o valor da imprensa livre e o valor do livre

---

[116] PROSSER, William L. Privacy. *In:* **California Law Review,** v. 48, n. 3, ago. 1960. Disponível em: https://heinonline.org/HOL/LandingPage?handle=hein.journals/calr48&div=31&id=&page=. Acesso em: 2 dez. 2019, p. 389.

[117] PIRES, Lucas de Almendra Freitas. **Direito à Privacidade no Âmbito da Sociedade da Informação:** reflexões em torno da questão nos inícios do século XXI. 2014. Dissertação (Mestrado Científico em Ciências Jurídico-Políticas) – Faculdade de Direito da Universidade de Coimbra, Portugal. Disponível em: https://eg.uc.pt/bitstream/10316/34844/1/Direito%20a%20privacidade%20no%20ambito%20da%20sociedade%20da%20informacao%20reflexoes%20em%20torno%20da%20questao%20nos%20inicios%20do%20seculo%20XXI.pdf. Acesso em: 12 jun. 2019, p. 65.

[118] 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. 125.

[119] WHITMAN, James Q. The Two Western Cultures of Privacy: dignity versus liberty. **The Yale Law Journal,** v. 113, n. 1.151. Disponível em: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1647&context=fss_papers. Acesso em: 2 dez. 2019, p. 1.204-1.206.

mercado[120]. Isso porque a *privacy* americana "é um corpo preso na órbita gravitacional dos valores da liberdade, enquanto o direito à privacidade europeu está na órbita da dignidade"[121]; contudo, quando os americanos pensam em liberdade, pensam em defesa contra o Estado, pensam em ampla liberdade para realizar transações mercantis sem interferências estatais, pensam em poder proteger sua propriedade, em especial o seu lar, de todas as formas possíveis. O inimigo é sempre o Estado[122].

Assim, até a ideia americana de liberdade é diferente do entendimento europeu do que é ser livre. Para este, a liberdade está muito mais relacionada à possibilidade de cada indivíduo poder realizar plenamente seu potencial como indivíduo, o que muitas vezes pode ser obstado pelo comportamento de outros entes privados, bem como pode exigir uma atuação positiva do Estado no sentido de proporcionar os meios necessários para que o indivíduo possa se autorrealizar.

Dessa forma, o limite fundamental do pensamento americano sempre permanece: a lei americana de privacidade costuma imaginar o lar como a principal defesa, e o Estado como o inimigo principal. Onde a lei americana percebe uma ameaça à privacidade normalmente é porque o Estado está envolvido. Em seu núcleo conceitual, o direito americano à privacidade ainda assume grande parte da forma que levou no século XVIII: é o direito à liberdade de invasões por parte do Estado, especialmente em sua própria casa[123].

Isso não quer dizer que o direito à privacidade protege a pessoa apenas em sua própria casa e somente contra o Estado. O artigo de Warren e Brandeis, a doutrina de Prosser e a jurisprudência aqui apresentada demonstram que não. Entretanto, este é o núcleo, o aspecto mais fortemente protegido pela privacidade americana, o que significa que situações nas quais muitas vezes os europeus vislumbram uma violação à privacidade não são assim entendidas nos Estados Unidos.

---

[120] WHITMAN, James Q. The Two Western Cultures of Privacy: dignity versus liberty. **The Yale Law Journal,** v. 113, n. 1.151. Disponível em: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1647&context=fss_papers. Acesso em: 2 dez. 2019, p. 1.208.

[121] Tradução livre de: "If I may use a cosmological metaphor: American privacy law is a body caught in the gravitational orbit of liberty values, while European law is caught in the orbit of dignity". WHITMAN, James Q. The Two Western Cultures of Privacy: dignity versus liberty. **The Yale Law Journal,** v. 113, n. 1.151. Disponível em: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1647&context=fss_papers. Acesso em: 2 dez. 2019, p. 1.163.

[122] WHITMAN, James Q. The Two Western Cultures of Privacy: dignity versus liberty. **The Yale Law Journal,** v. 113, n. 1.151. Disponível em: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1647&context=fss_papers. Acesso em: 2 dez. 2019, p. 1.181.

[123] WHITMAN, James Q. The Two Western Cultures of Privacy: dignity versus liberty. **The Yale Law Journal,** v. 113, n. 1.151. Disponível em: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1647&context=fss_papers. Acesso em: 2 dez. 2019, p. 1.214-1.215.

Na hipótese de a imprensa publicar uma informação bastante pessoal de alguém, sobre a qual o indivíduo não mantinha segredo, mas que tampouco desejava que fosse exposta nacionalmente, esse mesmo fato muito provavelmente não será visto como uma ofensa à privacidade nos Estados Unidos, ao passo que os europeus tenderão a enxergar a lesão.

É claro que o *right to privacy* também protege os americanos contra os abusos da imprensa, contudo, a liberdade de expressão é um valor de magnitude constitucional nos Estados Unidos e costuma pesar mais quando em conflito com o direito à privacidade. Existem também decisões que protegem a própria imagem, principalmente os casos envolvendo imagens nuas ou de conteúdo sexual de mulheres jovens que não consentiram com a realização da fotografia ou que são vítimas de agressões sexuais. Existem, igualmente, casos envolvendo invasões não governamentais da "privacidade da casa"[124], indicando que o *rigth to privacy* tutela a privacidade além do domicílio e, ainda, contra outros indivíduos e organizações privadas.

A dificuldade em definir com precisão o escopo da privacidade motivou a jurisprudência dos EUA a identificar o conjunto de interesses relevantes que integram, progressivamente, essa noção numa perspectiva constitucional. Nessa senda, embora nem a Constituição Americana de 1787 nem suas Emendas mencionem expressamente o direito à privacidade, a Suprema Corte Americana a considera implícita: a) no direito de associação, previsto na Primeira Emenda, a qual protege o indivíduo contra qualquer obrigação legal de revelar participação em um grupo ou organização; b) na garantia da Quarta Emenda contra buscas e apreensões arbitrárias do Estado em residências, documentos e objetos pessoais; c) na Quinta Emenda, que protege contra a autoincriminação e a obrigação de divulgar informações pessoais; d) no conceito de liberdade que a Suprema Corte atribuiu à Décima Quarta Emenda, que garante o direito fundamental da pessoa à autonomia na tomada de decisões de relevância especial para o desenvolvimento da personalidade individual sem nenhuma interferência estatal. Destaque-se que, a partir da década de 60, começa a emergir uma jurisprudência que, aos poucos, tende a incluir na área da privacidade protegida por esta emenda o interesse individual em evitar a divulgação de informações pessoais[125].

---

[124] WHITMAN, James Q. The Two Western Cultures of Privacy: dignity versus liberty. **The Yale Law Journal,** v. 113, n. 1.151. Disponível em: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1647&context=fss_papers. Acesso em: 2 dez. 2019, p. 1.203-1.208.

[125] SALDANA, María N. The rigth to privacy: la genesis de la proteción de la privacidad em el sistema constitucional norteamericano, el centenario legado de Warren y Brandeis. **Revista de Derecho Político** n. 85, set./dez. 2012, p. 195-240. Disponível em: http://revistas.uned.es/index.php/derechopolitico/article/view/10723. Acesso em: 12 dez. 2019, p. 201-203.

Assim, o direito à privacidade americano resulta da visão individualista do Estado e da vida, e acaba por ser pertencente a um só sujeito; "cria-se via de consequência uma verdadeira zona reservada para cada pessoa, independentemente de qualquer valoração ética"[126]. A privacidade como liberdade contempla um espaço em que as normas sociais não são aplicadas, para que cada pessoa possa agir com autonomia. Privacidade como liberdade tutela os aspectos independentes, espontâneos e exclusivamente individuais do ser e não os seus aspectos socializados. A privacidade como liberdade protege, portanto, a autonomia individual[127].

Observa-se que apesar da amplitude do *rigth to privacy*, o direito à privacidade nos Estados Unidos está muito mais preocupado com a intrusão na reclusão do indivíduo ou em seus assuntos particulares, com a publicação de fatos embaraçosos ou distorcidos sobre a pessoa, ou com a apropriação por outrem do nome ou imagem do indivíduo, do que, por exemplo, em impor limites à atuação empresarial acerca da utilização dos dados pessoais que o indivíduo, no exercício de sua autonomia privada, voluntariamente cedeu à determinada organização nos termos de um contrato que o indivíduo muitas vezes nem leu.

Isso não quer dizer que não existam leis americanas que amparem a privacidade nos Estados Unidos no que diz respeito à proteção de dados pessoais, contudo, essas leis são fragmentadas e, na maioria das vezes, surgem de maneira reativa, como a Lei de Proteção à Privacidade de Vídeo, aprovada rapidamente em 1988, depois que um jornal publicou os registros de aluguel de vídeo do juiz Bork durante suas audiências de indicação à Suprema Corte[128].

Não há uma lei federal sobre a proteção de dados; o surgimento recente de algumas legislações sobre a matéria reflete a preocupação ainda incipiente do país em proteger esse aspecto da privacidade. O *California Consumer Privacy Act* (CCPA)[129], que entrou em vigor em 1º de janeiro de 2020, foi a primeira lei abrangente dos Estados Unidos sobre privacidade,

---

[126] SAWARIS, Adriana.**A Tutela do Direito à Reserva sobre a Intimidade da Vida Privada no Regulamento nº 2016/679 da União Européia.** 2017. Dissertação (Mestrado em Ciências Jurídico-Civilistas – Direito Civil) – Faculdade de Direito da Universidade de Coimbra, Coimbra. Disponível em: https://eg.uc.pt/bitstream/10316/81104/1/Dissertac%CC%A7a%CC%83o%20Adriana%20S..pdf. Acesso em: 8 dez. 2019, p. 64.

[127] POST, Robert C. Three Concepts of Privacy. *In:* **The Georgetown Law Journal,** v. 89, n. 2089, 2000-2001, p. 2.087-2.098. Disponível em: https://digitalcommons.law.yale.edu/fss_papers/185/. Acesso em: 2 dez. 2019, p. 2.095-2.096.

[128] SULLIVAN, Bob. Privacy Lost: EU, U.S. laws differ greatly. **NBC NEWS: Technology & Science – Privacy Lost,** 19 out. 2006. Disponível em: http://www.nbcnews.com/id/15221111/ns/technology_and_science-privacy_lost/t/la-difference-stark-eu-us-privacy-laws/. Acesso em: 2 dez. 2019, p. 3.

[129] CALIFORNIA. **The California Privacy Rights Act of 2020.** Disponível em: https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf. Acesso em: 5 jan. 2020.

trazendo uma série de regulações a respeito da coleta e tratamento de dados pessoais, permitindo que os consumidores da Califórnia tenham acesso, pela primeira vez, a quais dados estão sendo coletados pelos varejistas e que não autorizem a comercialização de seus dados a terceiros.

Nada disso, porém, significa que o americano não se importe com a sua privacidade ou que a proteja menos que os europeus. Trata-se, apenas, de formas diferentes de conceber a privacidade, o que implicará, por conseguinte, modos distintos de assegurá-la.

2.3.2.2 A privacidade no direito europeu

Na Europa, após a Segunda Guerra Mundial e principalmente a partir da tutela da privacidade em instrumentos internacionais, a maioria dos países europeus passou a prever o direito à privacidade em suas constituições, além de também tutelar tal direito em nível infraconstitucional.

Assim, por exemplo, o ordenamento jurídico de Portugal reconhece o direito à privacidade desde 1966, por meio do seu Código Civil, artigo 80º, nº 1, o qual reserva a intimidade da vida privada. Posteriormente, a Constituição portuguesa de 1976, em seu artigo 26º, nº 1, dispôs que "A todos são reconhecidos os direitos [...] ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à protecção legal contra quaisquer formas de discriminação". Na Espanha, a Constituição de 1978, em seu artigo 18º, nº 1, também assegura proteção à intimidade e à vida privada. Já na França, a privacidade é protegida por meio dos artigos 22º e 23º da Lei 70.643/1970[130].

Como visto, com a crescente preocupação dos europeus com o fluxo das informações pessoais a partir da década de 60, a noção de privacidade se amplia e passa a abarcar a proteção de dados pessoais.

Já na década de 70 surgem as primeiras leis específicas e decisões judiciais sobre proteção de dados pessoais, as quais compartilham o entendimento de que esses dados constituem uma projeção da personalidade do indivíduo e, por conseguinte, demandam uma tutela jurídica. A primeira legislação nesse sentido foi a Lei de Proteção de Dados do Estado de Hesse, de 1970, na Alemanha Ocidental. Logo depois, a Suécia, em 11 de maio de 1973,

---

[130] PIRES, Lucas de Almendra Freitas. **Direito à Privacidade no Âmbito da Sociedade da Informação:** reflexões em torno da questão nos inícios do século XXI. 2014. Dissertação (Mestrado Científico em Ciências Jurídico-Políticas) – Faculdade de Direito da Universidade de Coimbra, Portugal. Disponível em: https://eg.uc.pt/bitstream/10316/34844/1/Direito%20a%20privacidade%20no%20ambito%20da%20sociedade%20da%20informacao%20reflexoes%20em%20torno%20da%20questao%20nos%20inicios%20do%20seculo%20XXI.pdf. Acesso em: 12 jun. 2019, p. 52-53.

sancionou o *Datalegen*, a primeira lei nacional a tratar da matéria. Tem-se, ainda, o Estatuto de Proteção de Dados do Estado Alemão de Rheinland-Pfalz, de 1974, e a Lei Federal de Proteção de Dados da Alemanha, de 1977[131].

Em seguida, foram aprovados importantes instrumentos internacionais e transnacionais que contribuíram para relacionar a noção de privacidade com a proteção de dados pessoais, como a Convenção 108 do Conselho da Europa, de 1981, as diretrizes da OCDE para a proteção da privacidade de dados pessoais e a Diretiva Europeia 95/46/CE, relativa à proteção de dados pessoais, de 1995[132].

Em 2016, foi aprovado o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados[133], o chamado Regulamento Geral de Proteção de Dados (RGPD). Este estabelece uma série de regras de defesa dos direitos e das liberdades fundamentais das pessoas singulares no que concerne a esse aspecto da privacidade e dispõe que os Estados-Membros deverão manter ou aprovar disposições nacionais para especificar a aplicação das regras do Regulamento, de modo a assegurar em toda a União a aplicação coerente e homogênea da legislação.

Como se observa, desde a década de 60, a ideia de privacidade no continente europeu vai paulatinamente se expandindo para abarcar a proteção de dados pessoais, adquirindo feição coletiva e função promocional. Torna-se instrumento essencial na garantia do livre desenvolvimento da personalidade, da igualdade e da cidadania. Assim, a privacidade na Europa não está ligada à liberdade, como nos Estados Unidos, mas à dignidade da pessoa humana.

Isso porque, como esclarece Whitman, os valores de "dignidade" e "honra" são bastante importantes para os europeus, de modo que, na Europa, o direito sempre está preocupado em proteger as pessoas da vergonha, da humilhação e da perda da dignidade. O ordenamento jurídico desse continente é voltado ao respeito interpessoal, sendo a privacidade parte dessa proteção jurídica[134].

---

[131] MENDES, Laura Schertel. **Privacidade, Proteção de Dados e Defesa do Consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 29-30.

[132] MENDES, Laura Schertel. **Privacidade, Proteção de Dados e Defesa do Consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 30.

[133] UNIAO EUROPEIA. **Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho,** de 27 de abril de 2016, relativo a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e a livre circulação desses dados e que revoga Diretiva 95/46/CE (Regulamento Geral de Proteção de Dados). Disponível em: https://www.uc.pt/protecao-de-dados/rgpd. Acesso em: 5 jan. 2020.

[134] WHITMAN, James Q. The Two Western Cultures of Privacy: dignity versus liberty. **The Yale Law Journal,** v. 113, n. 1.151. Disponível em: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1647&context=fss_papers. Acesso em: 2 dez. 2019, p. 1.164.

Da mesma forma que nos Estados Unidos a cultura americana de liberdade influencia no conceito de privacidade, a cultura europeia de dignidade se refletirá na noção daquele direito. Acerca dessa cultura, é comum associá-la aos traumas advindos dos horrores do fascismo e do nazismo que marcam o pós-guerra, contudo, a valorização da dignidade pelo direito europeu inicia-se muito antes disso, já desde o século XVII. Entretanto, até o século XX, apenas pessoas de alto *status* social poderiam esperar que fossem respeitadas no dia a dia e que tivessem sua "honra pessoal" protegida nos tribunais[135]; posteriormente, essa proteção se expandiu a todos os europeus.

Em 1867, o autor francês Alexandre Dumas e Adah Menke, seu caso de amor, deixaram-se fotografar em situações bem íntimas. O fotógrafo, contudo, resolveu vender as fotos, razão pela qual Dumas o processou, mesmo admitindo em audiência que havia vendido os direitos autorais ao fotógrafo. O caso chegou ao Tribunal de Apelações de Paris, que entendeu que ainda que uma pessoa tivesse tacitamente consentido com a publicação de fotos embaraçosas, ela deve manter o direito de retirar o seu consentimento. Entendeu também que a vida privada deve ser isolada no interesse dos indivíduos e, muitas vezes, dos bons costumes também, de modo que o direito à vida privada e à dignidade, nesse caso, superava o direito à propriedade do fotógrafo. O Tribunal decidiu que qualquer venda feita por uma pessoa que momentaneamente "esqueceu sua dignidade" deveria permanecer efetivamente anulável, uma vez que a privacidade de alguém, como outros aspectos de sua honra, não é uma mercadoria de mercado que pode ser vendida definitivamente[136].

Assim, os europeus sempre viram o Estado como um instrumento de defesa contra irregularidades de agentes particulares. Essa visão de que o Estado deve, ativamente, proteger as pessoas será impressa também no direito à privacidade deste continente. Para os europeus, o poder estatal deve assegurar-lhes o controle de sua própria imagem e de seus dados pessoais, coibindo sua apropriação e divulgação indevida.

Nessa senda, Post ensina que a privacidade como dignidade localiza a privacidade nos aspectos inter-relacionais da vida social, de modo que sua violação causa sofrimento porque atinge os espaços de socialização essenciais à construção da própria identidade. Para o autor, a invasão da privacidade é uma ofensa intrínseca contra a dignidade individual, pois causa dano independentemente das consequências da conduta danosa. Por esta razão, "se a

---

[135] WHITMAN, James Q. The Two Western Cultures of Privacy: dignity versus liberty. **The Yale Law Journal,** v. 113, n. 1.151. Disponível em: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1647&context=fss_papers. Acesso em: 2 dez. 2019, p. 1.165.

[136] WHITMAN, James Q. The Two Western Cultures of Privacy: dignity versus liberty. **The Yale Law Journal,** v. 113, n. 1.151. Disponível em: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1647&context=fss_papers. Acesso em: 2 dez. 2019, p. 1.175-1.176.

privacidade é entendida como uma forma de dignidade, não pode haver outra medida de privacidade a não ser as normas sociais que realmente existem em nossa civilização"[137].

Nessa visão de privacidade, uma violação desse direito deixa uma pessoa vulnerável ao julgamento público, de modo que, sem privacidade, o indivíduo não é livre para desenvolver sua personalidade, já que, por estar sempre sendo visto pelos demais, buscaria moldar seu comportamento, em qualquer situação, no intento de construir não o seu eu interior, mas a imagem pública que deseja.

A privacidade englobaria, então, o direito de o indivíduo manter desconhecidos do restante da sociedade certos aspectos de sua vida para, assim, construir diferentes "personalidades", uma vez que a pessoa demonstra, para cada círculo social em que se insere, os atributos e informações sobre si que considere apropriado e desejável[138]. A impossibilidade de o indivíduo gerenciar livremente suas informações pessoais pode ter profundas consequências sociais, como a discriminação no ambiente de trabalho por conta de sua opção religiosa, por exemplo. Nesse contexto, violar a privacidade de alguém significa afrontar a sua dignidade humana.

Assim, as leis europeias visam proteger o nome, a honra, a reputação e o fluxo de informações do indivíduo da vergonha e humilhação públicas e da perda de sua dignidade[139]. É por esta razão que a tutela jurídica da privacidade no continente europeu se preocupa com os abusos praticados pelos particulares e pelo livre mercado: a dignidade humana não pode ser reduzida a mera mercadoria.

O direito à privacidade na Europa, por exemplo, protege os *e-mails* dos trabalhadores, impõe limites à utilização de câmeras de vigilâncias pelos empregadores e tutela até mesmo ligações pessoais realizadas pelos telefones corporativos, protegendo a "esfera pessoal" dos trabalhadores. Assim, a pessoa não perde sua esfera privada por estar utilizando a propriedade de outrem. Uma decisão da França considerou uma violação à dignidade o fato de um

---

[137] POST, Robert C. Three Concepts of Privacy. *In:* **The Georgetown Law Journal,** v. 89, n. 2.089, 2000-2001, p. 2.087-2.098. Disponível em: https://digitalcommons.law.yale.edu/fss_papers/185/. Acesso em: 2 dez. 2019, p. 2.092- 2.094.

[138] LEVIN, Avner; ABRIL, Patricia Sánchez. Two Notions of Privacy Online. *In:* **Vanderbilt J. of Ent. and Tech. Law,** v. 11, n. 4. Disponível em: POST, Robert C. Three Concepts of Privacy. *In:* **The Georgetown Law Journal,** v. 89, n. 2.089, 2000-2001, p. 2.087-2.098. Disponível em: https://digitalcommons.law.yale.edu/fss_papers/185/. Acesso em: 13 dez. 2019, p. 1013.

[139] WHITMAN, James Q. The Two Western Cultures of Privacy: dignity versus liberty. **The Yale Law Journal,** v. 113, n. 1.151. Disponível em: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1647&context=fss_papers. Acesso em: 2 dez. 2019, p. 1.161.

empregador numa loja de varejo exigir que os funcionários mostrassem a nota fiscal da mercadoria que estavam levando para casa[140].

Tendo em vista que a dignidade humana é a qualidade intrínseca e distintiva de cada ser humano que implica um complexo de direitos e deveres que protege a pessoa contra todo ato de cunho degradante e desumano, para os europeus a privacidade não pode ser sobreposta pelo direito à propriedade porque qualquer ofensa à privacidade é também uma ofensa à dignidade.

2.3.2.3 A privacidade no direitos dos países do Oriente

Enquanto o Ocidente possui uma cultura mais individualista, os orientais tendem a ser coletivistas. Isso não significa que, no Ocidente, as pessoas não integram grupos, contudo, elas se veem como independentes, mesmo da família, o que lhes permite priorizar metas e objetivos pessoais com pouca ou nenhuma referência a terceiros. Já no Oriente, as pessoas se percebem como interdependentes dos grupos a que pertencem, de modo que as suas relações sociais são mais importantes que seus atributos únicos, razão pela qual os orientais priorizam as necessidades coletivas em vez de seus próprios anseios[141].

Cumpre dizer, ainda, que a referida cultura coletivista é bem mais forte na Ásia que no Oriente Médio, porque, enquanto neste essa interdependência entre indivíduo e grupo está muito mais relacionada à família que à sociedade em geral, os asiáticos são definidos principalmente com base em todas as suas relações sociais e não somente em relação à família. Desse modo, os países do Oriente Médio possuem uma cultura que se aproxima de um ponto médio entre o individualismo e o coletivismo[142].

O Oriente possui uma forte tradição de associação de grupo e de comportamentos de apoio e proteção de indivíduos dentro do grupo, mas isso não quer dizer que não há privacidade entre os orientais; o que difere do Ocidente é a concepção e a forma de exercer esse direito.

---

[140] WHITMAN, James Q. The Two Western Cultures of Privacy: dignity versus liberty. **The Yale Law Journal,** v. 113, n. 1.151. Disponível em: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1647&context=fss_papers. Acesso em: 2 dez. 2019, p. 1.194.

[141] MARKUS, Hazel R; KITAYAMA, Shinobu. Cultural variation in the Self-Concept. *In:* STRAUSS, J; GOETHALS, G. R. (Ed.). **The Self:** interdisciplinary approaches. Springer, Nova York, 1991. Disponível em: https://link.springer.com/chapter/10.1007/978-1-4684-8264-5_2. Acesso em: 27 set. 2020, p. 19-22.

[142] ZABIHZADEH, Abbas et al. Cultura differences in conceptual representation of “Privacy”: a comparison between Iran and the United States. **The Journal of Social Psychology,** v. 159, n. 4, 10 ago. 2018. Disponível em: https://www.tandfonline.com/doi/full/10.1080/00224545.2018.1493676. Acesso em: 27 set. 2020, p. 11.

No Japão, por exemplo, diante da cultura de convivência familiar e do tamanho pequeno das habitações, é muito difícil manter-se um diálogo sem que outras pessoas o escutem, de forma que a dimensão espacial da privacidade nem sempre pode ser exercitada. Entretanto, também faz parte da cultura dos japoneses agir como se nada tivessem ouvido, isto é, não se toca no assunto com os interlocutores da conversa e, ainda mais importante, nenhuma informação ouvida é repassada[143].

Enquanto no Ocidente a nudez é considerada uma das coisas mais íntimas de um indivíduo, no Japão existe o costume de as pessoas se banharem em fontes termais, lavando tanto o corpo quanto a alma. Além da reflexão pessoal, esses banhos servem como um momento de socialização, no qual os familiares, os amigos e os vizinhos se reúnem e entram nus na água[144].

Já nos países de maioria islâmica, a religião influencia fortemente na noção de privacidade. Conforme o Alcorão, ninguém pode intervir na privacidade de outrem sem permissão, razão pela qual surgem normas comportamentais destinadas a preservar este direito, tais como não olhar para a casa de alguém, utilizar roupas adequadas e a mulher deve limitar a exposição visual de si mesma na presença de convidados do sexo masculino[145].

Além disso, é grande o uso de elementos físicos como cortinas e persianas para permitir a liberdade de roupas, liberdade nas atividades e controle das informações sobre a casa. Nos países de maioria islâmica, a noção de privacidade abrange uma importante preocupação em manter a relação familiar, as atividades domésticas e os membros femininos longe da vista de quem não pertença à família[146].

Nesse cenário, apesar de algumas diferenças entre os países, em especial entre os asiáticos e os do Oriente Médio, tem-se que, enquanto os ocidentais, mais orientados ao individualismo, exibem altos níveis de preocupação com a privacidade pessoal, os orientais são mais propensos a renunciar à privacidade pessoal para o bem de todos. Assim, aceitam mais facilmente práticas organizacionais invasivas à privacidade, mas que beneficiam a

---

[143] MIZUTANI, Masahiko; DORSEY, James; MOOR, James H. The internet and Japanese conception of privacy. **Ethics and Information Technology,** 2004. Disponível: https://link.springer.com/article/10.1023/B:ETIN.0000047479.12986.42. Acesso em: 27 set. 2020, p. 124.

[144] CROSSELEY-BAXTER, Lily. As águas termais do Japão onde todo mundo fica nu. **BBC News Brasil,** 25 jul. 2020. Disponível em: https://www.bbc.com/portuguese/vert-tra-52930115. Acesso em: 27 set. 2020.

[145] RAHIM, Zaiton Abdul. The influence of culture and religion on visual privacy. **Procedia – Social and Behavioral Sciences,** v. 170, 27 jan. 2015. Disponível em: https://www.sciencedirect.com/science/article/pii/S1877042815000701. Acesso em: 27 set. 2020, p. 537-544.

[146] RAHIM, Zaiton Abdul. The influence of culture and religion on visual privacy. **Procedia – Social and Behavioral Sciences,** v. 170, 27 jan. 2015. Disponível em: https://www.sciencedirect.com/science/article/pii/S1877042815000701. Acesso em: 27 set. 2020, p. 537-544.

organização ou decisões governamentais intrusivas à esfera pessoal, que favorecerão a sociedade[147].

Mesmo os países orientais democráticos e que valorizam os direitos individuais, como Taiwan, têm o legado cultural de priorizar o coletivo sobre o individual e, por conseguinte, de aceitar e obedecer a medidas rigorosas tomadas pelo Governo, caso vislumbrem que elas servirão ao bem comum, ao passo que os ocidentais até aceitam abrir mão de suas liberdades individuais em nome do interesse público, mas não com a mesma tolerância, estando mais propensos ao questionamento e à desobediência que os coletivistas.

Também na luta contra a Covid-19, a Coreia do Sul procedeu a uma intensa coleta de dados pessoais dos infectados pelo coronavírus pelos mais diversos meios, como entrevista do paciente, verificação das transações dos cartões de crédito, dados de localização dos *smatphones* e imagens de câmeras de vigilância, para recriar a rota do infectado um dia antes de os sintomas aparecerem[148].

Em seguida, o governo enviava alertas por meio de mensagens de celular para os sul-coreanos, nos quais constava uma série de informações, como onde o infectado teria contraído o vírus, de que modo, por onde teria passado, seu sexo e sua idade. O objetivo era que a população tivesse dados suficientes para avaliar a possibilidade de ter entrado em contato com o infectado, mas os dados informados eram tão vastos que os indivíduos podiam ser facilmente identificados, apesar de nenhum nome ou endereço ser divulgado, o que levou a população a ter tanto ou até mais medo do estigma social, das críticas e de outros danos do que da própria doença[149].

O governo da Coreia do Sul foi bastante criticado, em 2015, após o surto de Mers – uma epidemia asiática de outro coronavírus –, por não ter divulgado informações que, na visão dos críticos, teriam ajudado a conter a disseminação da doença, tais como dados sobre a localização dos pacientes. Diante disso, o país promoveu mudanças significativas em sua legislação acerca do gerenciamento e compartilhamento público de informações sobre

---

[147] LUO, Robert; WARKENTIN, Merrill; JOHNSTON, Allen C. The impact of national culture on workplace privacy expectations in the context of information security assurance. **DBLP,** jan. 2009. Disponível em: https://www.researchgate.net/publication/220893655_The_Impact_of_National_Culture_on_Workplace_Privacy_Expectations_in_the_Context_of_Information_Security_Assurance. Acesso em: 27 set. 2020, p. 4.

[148] BBC NEWS. Coronavirus privacy: are South Korea's alerts too revealing? 5 mar. 2020. Disponível em: https://www.bbc.com/news/world-asia-51733145. Acesso em: 6 abr. 2020.

[149] BBC NEWS. Coronavirus privacy: are South Korea's alerts too revealing? 5 mar. 2020. Disponível em: https://www.bbc.com/news/world-asia-51733145. Acesso em: 6 abr. 2020.

pacientes de doenças infecciosas, permitindo toda essa divulgação de informações que se observou no enfrentamento da Covid-19[150].

Verifica-se que a preocupação dos sul-coreanos não era com a vigilância estatal, com a coleta e tratamento massivo de seus dados. Se não houvesse o risco de identificação e posterior julgamento pelos seus pares, os infectados não demonstrariam muito incômodo com o seu monitoramento por razões sanitárias.

Assim, nos regimes democráticos, observa-se uma variação no sopesamento entre privacidade e interesse público, estando os indivíduos orientais mais propensos a concordar com medidas mais radicais, inclusive no que diz respeito a monitoramento e rastreio. Tendem a considerar tais medidas adequadas, necessárias e proporcionais ante o interesse coletivo[151].

Isso implica que a noção de privacidade, no Oriente, tenha bem menos preocupação com a intervenção do Estado na esfera privada do que ocorre no Ocidente, contrastando principalmente com a *privacy* americana. De fato, a privacidade oriental liga-se muito mais a um componente coletivo que a um individual; a preocupação se dirige mais a manter privado, longe dos olhos e do conhecimento de quem não pertença ao grupo, o que ali acontece do que em manter na esfera íntima, em segredo, algo que ocorre com o indivíduo.

Na China, a privacidade não está expressa na Constituição; apesar de haver disposição constitucional que protege a dignidade pessoal, os tribunais chineses não têm independência e autoridade suficientes para desenvolver doutrinas de privacidade a partir de tal cláusula[152]. Os direitos humanos são concebidos como derivados do próprio Estado, o que significa que os interesses do Estado ficam acima dos do indivíduo, bem como que a proteção de tais direitos não é garantida, de modo que as pessoas não têm meios para pleitear quaisquer soluções para as violações de sua privacidade realizadas pelo governo chinês[153].

---

[150] MODESTO, Jéssica Andrade; EHRHARDT JÚNIOR, Marcos. Danos colaterais em tempos de pandemia: preocupações quanto ao uso dos dados pessoais no combate à Covid-19. **Redes – Revista Eletrônica Direito e Sociedade,** Canoas, v. 8, n. 2. Ago. 2020. Disponível em: https://revistas.unilasalle.edu.br/index.php/redes/article/view/6770/pdf. Acesso em: 27 set. 2020, p. 149.

[151] PALHARES, Gabriela Capobianco et al. A privacidade em tempos de pandemia e a escada de monitoramento e rastreio. **Estudos Avançados,** v. 34, n. 99, São Paulo, jul. 2020. Disponível em: https://www.scielo.br/pdf/ea/v34n99/1806-9592-ea-34-99-175.pdf. Acesso em: 27 set. 2020, p. 182-186.

[152] KUI, Shen. The stumbling balance between public health and privacy amid the pandemic in China. **The Chinese Journal of Comparative Law,** 1 fev. 2021. Disponível em: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7929056/. Acesso em: 10 fev. 2021, p. 5.

[153] PERNOT-LEPLAY, Emmanuel. China's approach on data privacy law: a third way between the U.S. and the E.U.? **Penn State Journal of Law & International Affairs,** v. 8, n. 1, mai. 2020. Disponível em: https://www.researchgate.net/profile/Emmanuel-Pernot-Leplay/publication/337103856_China%27s_Approach_on_Data_Privacy_Law_A_Third_Way_Between_the_US_and_the_EU/links/5ecc32a292851c11a88a90d0/Chinas-Approach-on-Data-Privacy-Law-A-Third-Way-Between-the-US-and-the-EU.pdf. Acesso em: 27 set. 2020, 108-109.

Enquanto a privacidade, em especial a proteção dos dados pessoais, é fortalecida nas relações dos indivíduos com as entidades privadas, o Estado continua a aumentar o seu acesso às informações dos chineses pelos mais diversos meios, incluindo o reconhecimento facial[154]. Nessa senda, em 2016, a China aprovou a Lei de Cibersegurança, a qual, ao tempo que eleva a cibersegurança em nível nacional, permite ao governo registrar e controlar informações disseminadas na *internet* que forem consideradas ilegais e impõe regras para garantir que o usuário seja identificado[155].

Durante o combate à pandemia do coronavírus, cidades chinesas instalaram câmeras em frente às casas das pessoas em quarentena, permitindo o monitoramento destas 24 horas por dia, de modo a economizar gastos com funcionários. De forma ainda mais intrusiva, alguns chineses disseram que tiveram câmeras instaladas dentro de suas casas:

> Zhou contou que não gostou da ideia. Ele questionou o funcionário sobre o que o dispositivo iria gravar e este mostrou a ele a gravação no celular. "Eu estava parado na minha sala e a câmera me gravou claramente", disse Zhou, que ficou furioso.
> Ele perguntou por que a câmera não seria instalada do lado de fora, e o policial respondeu que ela poderia ser vandalizada. No fim, o dispositivo foi instalado, mesmo sob protesto.
> Naquela mesma tarde, Zhou disse que ligou para a prefeitura e para o centro local de controle de epidemias para reclamar da situação. Dois dias depois, dois funcionários do governo local apareceram em sua casa, pedindo que ele entendesse e cooperasse com os esforços para controlar a pandemia[156].

Verifica-se que, apesar de os chineses aceitarem elevados níveis de intromissão do Estado em sua esfera privada em nome do coletivo, a medida relatada ultrapassou os limites da tolerância, provocando forte sensação de violação à privacidade. Juridicamente, no entanto, esses indivíduos nada puderam fazer.

O sentimento de interferência alheia à privacidade no momento em que a vigilância estatal alcançou a casa dos chineses demonstra que, mesmo nos países marcados por uma

---

[154] PERNOT-LEPLAY, Emmanuel. China's approach on data privacy law: a third way between the U.S. and the E.U.? **Penn State Journal of Law & International Affairs,** v. 8, n. 1, mai. 2020. Disponível em: https://www.researchgate.net/profile/Emmanuel-Pernot-Leplay/publication/337103856_China%27s_Approach_on_Data_Privacy_Law_A_Third_Way_Between_the_US_and_the_EU/links/5ecc32a292851c11a88a90d0/Chinas-Approach-on-Data-Privacy-Law-A-Third-Way-Between-the-US-and-the-EU.pdf. Acesso em: 27 set. 2020, p. 107.

[155] MOREIRA, Bernardo João do Rego Monteiro; DURAN, Felipe Pessoa. Sobre a questão da ciber-soberania na China. *In:* OPPERMANN, Daniel (Ed.). **Internet Governance in the Global South –** history, theory, and contemporary debates. 11 nov. 2020. Disponível em: https://nupri.prp.usp.br/blog/sobre-a-questao-da-ciber-soberania-na-china/#:~:text=Em%20novembro%20de%202016%2C%20a,disseminadas%20na%20internet%20que%20fossem. Acesso em: 27 set. 2020.

[156] GAN, Nectar. Na China, há câmeras na porta da casa das pessoas – às vezes, do lado de dentro. **CNN Brasil – Internacional,** 29 abr. 2020. Disponível em: https://www.cnnbrasil.com.br/internacional/2020/04/29/na-china-ha-cameras-na-porta-da-casa-das-pessoas-as-vezes-do-lado-de-dentro. Acesso em: 27 set. 2020.

maior ingerência estatal, existe alguma ideia de privacidade, até mesmo na relação dos indivíduos com o Estado.

Nesse diapasão, a noção de estar sozinho, de segredo, de restringir o acesso de terceiros a determinados locais, objetos e informações e de manter algum controle da esfera pessoal também está presente entre os orientais, sendo estes elementos básicos e comuns da ideia de privacidade[157]/[158].

Juridicamente, enquanto no Ocidente as legislações protetivas desse direito foram se desenvolvendo ao longo dos anos e acompanharam os avanços tecnológicos, no Oriente só mais recentemente se desenvolveram estruturas jurídicas voltadas à proteção da privacidade. De igual modo, a jurisprudência acerca da matéria não é tão vasta no referido continente[159].

Assim, por exemplo, o direito à privacidade somente foi inserido na Constituição do Nepal em 1990. Na Índia, apenas em 2009 o Supremo Tribunal de Mumbai derrubou as leis antissodomia da era colonial com base na proteção da privacidade[160]. Na Indonésia, como a Constituição não menciona explicitamente esse direito, somente em 2010 o Tribunal Constitucional do país reconheceu que o direito à dignidade e a estar seguro abarcava o direito à privacidade e, com este fundamento, decidiu restringir a vigilância das comunicações, entendendo ser necessária uma lei que a regulasse, não sendo possível permitir a escuta telefônica por meio de regulamentos do Executivo[161].

Nas últimas décadas a tutela da privacidade tem crescido nos países do Oriente, seja como resposta a casos individuais, seja por necessidade econômica, ou, ainda, pela consagração desse direito nas constituições ou mediante a adesão a tratados internacionais[162]. Nesse cenário, a privacidade informacional teve considerável avanço.

---

[157] ZABIHZADEH, Abbas et al. Cultura differences in conceptual representation of “Privacy”: a comparison between Iran and the United States. **The Journal of Social Psychology,** v. 159, n. 4, 10 ago. 2018. Disponível em: https://www.tandfonline.com/doi/full/10.1080/00224545.2018.1493676. Acesso em: 27 set. 2020, p. 10.

[158] MIZUTANI, Masahiko; DORSEY, James; MOOR, James H. The internet and Japanese conception of privacy. **Ethics and Information Technology,** 2004. Disponível: https://link.springer.com/article/10.1023/B:ETIN.0000047479.12986.42. Acesso em: 27 set. 2020, p. 122.

[159] PRIVACY INTERNATIONAL. **A New Dawn**: privacy in Asia. 9 dez. 2012. Disponível em: https://privacyinternational.org/sites/default/files/2017-12/A%20New%20Dawn_Privacy%20in%20Asia.pdf. Acesso em: 27 set. 2020, p. 10.

[160] PRIVACY INTERNATIONAL. **A New Dawn**: privacy in Asia. 09 dez. 2012. Disponível em: https://privacyinternational.org/sites/default/files/2017-12/A%20New%20Dawn_Privacy%20in%20Asia.pdf. Acesso em: 27 set. 2020, p. 10.

[161] PRIVACY INTERNATIONAL. **The Right to Privacy in the Indonesia.** Set. 2016. Disponível em: https://uprdoc.ohchr.org/uprweb/downloadfile.aspx?filename=3914&file=EnglishTranslation. Acesso em: 27 set. 2020, p. 2.

[162] PRIVACY INTERNATIONAL. **A New Dawn**: privacy in Asia. 09 dez. 2012. Disponível em: https://privacyinternational.org/sites/default/files/2017-12/A%20New%20Dawn_Privacy%20in%20Asia.pdf. Acesso em: 27 set. 2020, p. 11.

Em 1988, o Japão adotou a primeira lei sobre as informações pessoais, voltada ao setor público. A Coreia do Sul, em 1995, adotou a Lei de Proteção de Dados de Agências Públicas. Em 1997, a Tailândia aprovou a Lei de Informação Oficial, que forneceu alguma proteção dos dados pessoais em relação a agências governamentais. Direcionada ao setor privado, em 1995, o governo de Hong Kong promulgou uma Portaria de Dados Pessoais, que cobria os setores público e privado. Nesse mesmo ano, Taiwan promulgou uma lei de proteção de dados pessoais processados por computador, direcionada ao setor público e a oito áreas do setor privado[163].

Mais recentemente, a Coreia do Sul dispõe de uma lei de privacidade de dados mais rigorosa e aplicável ao setor privado desde 2011. Em 2016, o Qatar aprovou uma proteção da privacidade de dados pessoais, também aplicável ao setor privado. O centro financeiro internacional localizado na Ilha Al Maryah, nos Emirados Árabes Unidos (Emirados Árabes Unidos), aprovou, em 2015, um Regulamento de Proteção de Dados que, apesar de ser aplicável somente à ilha, tem um grande impacto regional, dado o número de empresas estabelecidas na região[164].

Por fim, nas últimas décadas, máxime com a popularização da *internet*, os orientais têm desenvolvido uma maior consciência das questões de privacidade, enquanto liberdade individual, principalmente no tocante a suas informações pessoais, o que também impulsiona os avanços legislativos sobre a matéria[165].

2.3.2.4 Principais distinções entre os modelos regulatórios americano, europeu e oriental de tutela da privacidade

Como visto, a noção de privacidade é diferente em cada cultura. Assim, há um modelo de tutela da privacidade europeu e outro americano, os quais apresentam algumas diferenças, mas ambos são influenciados pela cultura individualista do Ocidente. Há, ainda, o modelo de privacidade oriental, notadamente marcado pela tradição coletivista. A seguir, serão apontadas as principais diferenças entre esses três modelos de privacidade.

---

[163] GREENLEAF, Graham. **Privacy Laws –** trade and human rights perspectives. Reino Unido: OXFORD University Press, 2014, p. 86.

[164] WARREN, Scott. Security and Privacy: a view from Asia and the Middle East. **Security & Privacy II Bytes** – Global updates from our Data Privacy & Cybersecurity team. 24 jan. 2018. Disponível em: https://www.securityprivacybytes.com/2018/01/security-and-privacy-a-view-from-asia-and-the-middle-east/#page=1. Acesso em: 27 set. 2020.

[165] PRIVACY INTERNATIONAL. **A New Dawn**: privacy in Asia. 09 dez. 2012. Disponível em: https://privacyinternational.org/sites/default/files/2017-12/A%20New%20Dawn_Privacy%20in%20Asia.pdf. Acesso em: 27 set. 2020 p. 5-6.

Inicialmente, tem-se que a privacidade na Europa está ligada à dignidade da pessoa humana. Isso não quer dizer que os Estados Unidos não se preocupem com violações à dignidade humana. O que acontece, contudo, é que os americanos não fazem essa relação direta entre privacidade e dignidade. Ao contrário, nos Estados Unidos a privacidade liga-se à liberdade, entendida esta, principalmente, como a não interferência do Estado em sua propriedade. Não é difícil imaginar como as citadas proteções à privacidade dos trabalhadores europeus chegam a beirar o absurdo para o americano, que vê o seu local de trabalho como uma extensão da sua casa. Não é admissível permitir ao Estado impor limites às formas como o americano protege a sua propriedade.

Já a privacidade, no Oriente, liga-se muito mais a um componente coletivo que a um individual, isto é, a preocupação se dirige mais a manter privadas as informações do grupo do que as do indivíduo. Além disso, e principalmente, a privacidade oriental se preocupa muito pouco com a intervenção do Estado na esfera privada, contrastando especialmente com a *privacy* americana.

No que diz respeito à proteção das informações pessoais, a Europa demanda uma preocupação muito maior em regulamentar juridicamente o tratamento desses dados, enquanto os Estados Unidos, em que pese a existência de algumas legislações sobre a matéria, aposta muito mais na autorregulamentação dos setores privados. Enquanto os Estados europeus possuem uma ação positiva de proteção dos dados pessoais, os Estados Unidos ainda guardam muito de sua visão abstencionista.

O Regulamento Geral de Proteção de Dados da União Europeia prevê que os Estados-membros deverão criar uma ou mais autoridades públicas independentes, as chamadas Autoridades de Controle, que fiscalizarão a aplicação do regulamento, razão pela qual constituem "elemento essencial da proteção das pessoas singulares no que respeita ao tratamento dos seus dados pessoais"[166].

Os Estados-membros da União Europeia se comprometem não somente a fazer alterações legislativas para oferecer o nível de proteção aos dados pessoais previsto no RGPD, mas também a criar uma Autoridade que assegure a eficácia da lei, seja fiscalizando a aplicação do Regulamento, seja promovendo a sensibilização e a compreensão do público relativamente aos riscos, às regras, às garantias e aos direitos associados ao tratamento, bem

[166] UNIAO EUROPEIA. **Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho,** de 27 de abril de 2016, relativo a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e a livre circulação desses dados e que revoga Diretiva 95/46/CE (Regulamento Geral de Proteção de Dados). Disponível em: https://www.uc.pt/protecao-de-dados/rgpd. Acesso em: 5 jan. 2020.

como orientando os responsáveis pelo tratamento e os subcontratantes para as suas obrigações nos termos do Regulamento, conduzindo investigações sobre a aplicação da Lei.

Isso não significa, como visto, que os Estados Unidos não conferem, juridicamente, proteção aos dados pessoais; entretanto, essas leis não são abrangentes e muitas não se aplicam ao setor privado, tendo sido o *California Consumer Privacy Act* (CCPA)[167], que entrou em vigor em 2020, a primeira legislação ampla do país a tratar da matéria.

Na Europa, as informações pessoais não podem ser coletadas sem a permissão dos titulares dos dados, os quais têm o direito de revisá-los, corrigir imprecisões, impedir o compartilhamento sem sua permissão expressa e pedir o apagamento de tais informações. Já nos Estados Unidos, não há uma lei federal sobre a proteção de dados. O surgimento recente de algumas legislações sobre a matéria reflete a preocupação ainda incipiente do país em proteger esse aspecto da privacidade, impulsionada pela ressignificação desse direito em boa parte do mundo, uma vez que legislações como o RGPD, na Europa, e a LGPD, no Brasil, podem dificultar as transações comerciais entre as organizações americanas e os países que adotam legislações rígidas e específicas sobre a proteção de dados.

Isso aconteceu no final dos anos 90, quando o comércio eletrônico entre a Europa e os Estados Unidos quase parou depois que a Diretiva de Proteção de Dados da União Europeia proibiu a transferência de dados para países sem leis abrangentes de proteção à privacidade. Pelos padrões da União Europeia, os Estados Unidos estavam aquém dos requisitos, contudo, depois de dois anos de negociações, fez-se um acordo pelo qual os Estados Unidos se comprometeram a controlar a privacidade dos dados da União Europeia que fluíam para aquele país[168].

Os debates e escândalos relacionados às violações dos dados pessoais têm proporcionado mudanças entre os americanos, que começam a demonstrar uma crescente preocupação com a privacidade de suas informações, de modo que a proteção dos dados pessoais tem se tornado um valor para algumas empresas dos Estados Unidos, a exemplo da *Apple*, que logo em sua página principal anota:

> A privacidade é um direito humano fundamental. Na *Apple*, esse também é um dos nossos principais valores. Sabemos que seus aparelhos são importantes em vários setores da sua vida, e só você deve decidir o que e com quem compartilha essas experiências. Criamos nossos produtos para proteger sua privacidade e para que

[167] CALIFORNIA. **The California Privacy Rights Act of 2020.** Disponível em: https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf. Acesso em: 5 jan. 2020.

[168] SULLIVAN, Bob. Privacy Lost: EU, U.S. laws differ greatly. **NBC NEWS: Technology & Science – Privacy Lost,** 19 out. 2006. Disponível em: http://www.nbcnews.com/id/15221111/ns/technology_and_science-privacy_lost/t/la-difference-stark-eu-us-privacy-laws/. Acesso em: 2 dez. 2019, p. 2.

> você sempre tenha controle sobre suas informações. Nem sempre é uma tarefa fácil. Mas é nesse tipo de inovação que nós acreditamos[169].

Entretanto, os Estados Unidos ainda têm um longo caminho a percorrer para proteger os dados pessoais dos americanos, principalmente tendo-se em vista que as mudanças já verificadas refletem muito mais necessidades mercadológicas de um mundo globalizado do que um novo modo de ver a privacidade.

No tocante ao Oriente, as legislações em matéria de privacidade e proteção de dados pessoais tiveram um desenvolvimento tardio e muitas vezes reativo. Surgiram mais como resposta a uma situação concreta ou a uma necessidade econômica do que pela preocupação dos legisladores com a privacidade dos indivíduos.

As primeiras leis de proteção de informações pessoais aplicáveis tanto ao setor público quanto ao privado surgiram apenas na década de 1990. Antes de 2010, apenas seis países asiáticos tinham leis abrangentes em matéria de privacidade de dados. Entre 2010 e 2020, mais 13 jurisdições promulgaram novas leis de privacidade de dados e sete alteraram suas leis já existentes. Há, ainda, outros países que estão trabalhando para aprovar leis de proteção de informações pessoais, tais como a Índia e o Vietnã[170]. Alguns países do Oriente Médio também têm desenvolvido normas sobre o tema, a exemplo do Qatar.

Esse crescimento de legislação sobre a matéria se deu principalmente por necessidade econômica, já que países como China, Taiwan, Japão e Coreia do Sul possuem várias corporações globais que utilizam a tecnologia e o tratamento de dados pessoais, fundamentais para o sucesso econômico de tais nações. Outras regiões como Cingapura, Hong Kong, Tóquio e Sidney são importantes centros de negócios, abarcando bancos globais. Índia, Filipinas e Malásia são líderes em suporte empresarial global. Percebeu-se que para continuar a competir no mercado global, fazia-se necessário o desenvolvimento de legislação de proteção de dados pessoais[171].

Desde que o Regulamento Geral de Proteção de Dados da União Europeia entrou em vigor, muitos países estão buscando fortalecer suas legislações para obter da Comissão Europeia uma decisão de que oferecem um nível de proteção adequado aos dados pessoais, a exemplo da Coreia do Sul, das Filipinas e de Taiwan, já que isto facilitará bastante o fluxo de

---

[169] APPLE. **Política de Privacidade**. 2020. Disponível em: https://www.apple.com/br/privacy/. Acesso em: 5 jan. 2020.

[170] RICH, Cynthia J. Transformation of the privacy landscape in Asia. **Morrison Foerster,** 4 jan. 2021. Disponível em: https://www.mofo.com/resources/insights/210104-transformation-privacy-landscape-asia.html. Acesso em: 27 set. 2020.

[171] DELOITTE. **Unity in Diversity –** the Asia Pacific privacy guide. Jul. 2019. Disponível em: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-unity-diversity-privacy-guide.pdf. Acesso em: 27 set. 2020 p. 7.

dados pessoais com a União. Atualmente, a Nova Zelândia e Japão são os únicos países na região da Ásia-Pacífico com uma decisão de adequação[172].

Também nas últimas décadas, sobremodo com a popularização da *internet*, os orientais têm ampliado sua noção de privacidade, enquanto liberdade individual, em especial no que diz respeito a seus dados pessoais.

Resta evidente que o direito à privacidade na Europa e nos Estados Unidos possui conteúdo e abrangência distintos. Enquanto nos Estados Unidos o direito à privacidade está relacionado à liberdade e possui uma feição muito mais individualista, demandando uma atuação negativa do Estado, a Europa desenvolve o aspecto social da privacidade, atrelando-a à dignidade e exigindo uma atuação estatal positiva, com vistas a evitar a discriminação que os indivíduos podem sofrer em decorrência do tratamento de seus dados pessoais.

Ambas as noções são marcadas pela cultura individualista, mesmo a privacidade europeia, com seu aspecto social, já que busca proteger o indivíduo em suas relações sociais, e não priorizar o interesse de um grupo sobre o pessoal.

Já a privacidade no Oriente se distingue bastante de tais noções. Primeiro, como já visto, não demanda uma atuação negativa do Estado. Ao contrário, em nome do coletivo, ingerências estatais, até as mais intrusivas, são toleradas. Em segundo lugar, no que toca às relações sociais, intromissões à privacidade também tendem a ser aceitas, caso sirvam ao grupo, como a família ou a organização de trabalho, não se exigindo atuação do Estado para proteger o indivíduo em seu meio social.

O ponto de maior contato deste modelo de privacidade com os outros dois está na proteção dos dados pessoais. Como a privacidade da associação é bastante valorizada no Oriente, existe uma cultura de não divulgar as informações ouvidas, intencionalmente ou não, no grupo, principalmente familiar, independentemente de legislação.

A popularização das tecnologias e da *internet* e as exigências do mercado global fizeram surgir a necessidade de tutelar as informações dos indivíduos, de modo que alguns países orientais desenvolverem leis abrangentes sobre o tema e têm buscado implementar mecanismos aptos a oferecer uma proteção adequada aos dados, a exemplo da instituição de autoridades de controle, como a Comissão de Proteção de Informações Pessoais do Japão, o que revela que alguns países do Oriente, assim como a Europa, caminham para uma atuação positiva do Estado na proteção da privacidade de seus indivíduos.

---

[172] DELOITTE. **Unity in Diversity –** the Asia Pacific privacy guide. Jul. 2019. Disponível em: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-unity-diversity-privacy-guide.pdf. Acesso em: 27 set. 2020, p. 7.

Antes do estudo da concepção e da regulação da privacidade no direito brasileiro, faz-se necessário analisar as dimensões desse direito, pois a classificação tridimensional da privacidade auxilia na identificação dos objetos incluídos em seu âmbito de proteção e dos problemas que se relacionam com cada uma dessas facetas, proporcionando um melhor entendimento desse direito.

2.4 Dimensões do direito à privacidade

Tendo em vista a abrangência da proteção conferida pela privacidade, esta assume, em cada situação, um ou mais de seus aspectos. Isso significa que a privacidade possui diferentes dimensões e que determinado evento danoso pode atingir uma ou mais dessas perspectivas.

Dworkin ensina que a privacidade às vezes é territorial, isto é, quando às pessoas é legítimo fazer o que desejarem em um espaço demarcado, como a própria casa. Às vezes, é uma questão de confidencialidade, quando se permite que as pessoas mantenham suas informações na esfera privada, como suas convicções políticas, por exemplo. Ainda, a privacidade pode significar, em determinados momentos, soberania quanto a decisões pessoais, como a decisão dos pais acerca de em qual escola matricularão seus filhos[173].

Já Bert-Jaap Koops e outros defendem que existem oito tipos de privacidade, a saber: privacidade corporal, privacidade espacial, privacidade comunicacional, privacidade proprietária, privacidade intelectual, privacidade decisional, privacidade associativa e privacidade comportamental[174].

Para os autores, a privacidade corporal protege o corpo do indivíduo contra procedimentos invasivos não autorizados ou contra a restrição da liberdade de movimento corporal. Por sua vez, a privacidade espacial restringe o acesso de outras pessoas ao espaço privado de cada um. A privacidade comunicacional limita o acesso a comunicações ou controla o uso de informações repassadas a terceiros. A privacidade proprietária relaciona-se ao interesse de uma pessoa em usar a propriedade como um meio de proteger atividades, fatos, coisas ou informações do ponto de vista dos outros, como quando se usa uma bolsa para ocultar itens ou informações que a pessoa prefere manter em sigilo enquanto está em espaços

---

[173] DWORKIN, Ronald.**Domínio da Vida –** aborto, eutanásia e liberdades individuais. São Paulo: Martins Fontes, 2003 [livro digital].

[174] KOOPS, Bert-Jaap et al. A Typology of Privacy. **U. Pa. J. Int'l L.** v. 38, a. 2, p. 485-575. Disponível em: https://scholarship.law.upenn.edu/jil/vol38/iss2/4/. Acesso em: 2 dez. 2019, p. 567-568.

públicos. A privacidade intelectual protege o interesse de uma pessoa em manter somente para si seus pensamentos, opiniões e crenças[175].

Já a privacidade decisional relaciona-se às decisões íntimas do indivíduo, principalmente de natureza sexual e sobre outros assuntos sensíveis, de modo que se relaciona intimamente com a vida familiar do indivíduo. A privacidade associativa tutela a liberdade do indivíduo para escolher com quem interagir – amigos, associações, grupos e comunidades. A privacidade comportamental relaciona-se aos interesses de privacidade que uma pessoa tem enquanto conduz atividades publicamente visíveis. Por fim, os autores mencionam a privacidade informacional, que tutela o interesse do indivíduo em impedir a coleta de informações sobre si, bem como em controlar as informações sobre si a que os outros legitimamente têm acesso; contudo, entendem que a privacidade informacional não seria uma dimensão específica da privacidade, mas sim um conceito de sobreposição que toca em cada um dos tipos principais[176].

Na verdade, as dimensões da privacidade se comunicam não somente no que se refere à privacidade informacional; essas dimensões coexistem, havendo situações em que será bastante difícil identificar a qual delas determinado assunto diz respeito, bem como há situações em que identificam mais de uma dimensão da privacidade[177]. Dessa forma, um mesmo evento danoso pode violar vários direitos da privacidade, como a exposição de informações médicas de um indivíduo, que pode violar o direito à proteção de dados pessoais e o direito à intimidade, e em diferentes dimensões, como a informacional e a decisional.

No que diz respeito à classificação das dimensões da privacidade, a doutrina não é uníssona, existindo classificações que abarcam mais dimensões, como a de Bert-Jaap Koops, enquanto outras trazem uma classificação menos extensa. Neste trabalho, adota-se a classificação tridimensional da privacidade[178]: privacidade espacial, privacidade decisional e privacidade informacional, por se entender que as classificações mais detalhadas podem ser agrupadas nessas três dimensões.

---

[175] KOOPS, Bert-Jaap et al. A Typology of Privacy. **U. Pa. J. Int'l L.** v. 38, a. 2, p. 485-575. Disponível em: https://scholarship.law.upenn.edu/jil/vol38/iss2/4/. Acesso em: 2 dez. 2019, p. 567.

[176] KOOPS, Bert-Jaap et al. A Typology of Privacy. **U. Pa. J. Int'l L.** v. 38, a. 2, p. 485-575. Disponível em: https://scholarship.law.upenn.edu/jil/vol38/iss2/4/. Acesso em: 2 dez. 2019, p. 568.

[177] PEIXOTO, Erick L. C; EHRHARDT JÚNIOR, Marcos. Os Desafios da Compreensão do Direito à Privacidade no Sistema Jurídico Brasileiro em face das Novas Tecnologias. *In*: EHRHARDT JÚNIOR, Marcos; LOBO, Fabiola Albuquerque (Coord.). **Privacidade e sua Compreensão no Direito Brasileiro.** Belo Horizonte: Fórum, 2019, p. 41.

[178] Sobre isso, ver PEIXOTO, Erick L. C; EHRHARDT JÚNIOR, Marcos. Os Desafios da Compreensão do Direito à Privacidade no Sistema Jurídico Brasileiro em face das Novas Tecnologias. *In*: EHRHARDT JÚNIOR, Marcos; LOBO, Fabiola Albuquerque (Coord.). **Privacidade e sua Compreensão no Direito Brasileiro.** Belo Horizonte: Fórum, 2019, p. 33-54.

Importa dizer, ainda, que essas dimensões não são excludentes, mas complementares, de modo que, numa mesma situação, é possível verificar uma violação ou interferência externa em mais de uma dimensão da privacidade. Nessa senda, a teoria da tridimensionalidade também é útil por permitir uma análise mais detalhada das ameaças a este direito na sociedade da informação e, por conseguinte, além de fornecer maiores critérios para aferição da lesão e sua posterior reparação, possibilitar a implantação de medidas de mitigação de riscos, prevenindo os danos.

2.4.1 Dimensão Espacial

Trata-se da dimensão original da privacidade, com respeito à privacidade existente em um determinado espaço físico, como a casa da pessoa[179].

No ordenamento jurídico pátrio, a maior expressão dessa dimensão da privacidade encontra-se na previsão do artigo 5º, XI, da Constituição brasileira de 1988, a qual dispõe que a "casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial"[180]. Aqui, cabe dizer que a proteção dispensada à casa por esta norma é diferente da conferida pelo direito de propriedade, haja vista que visa proteger não o imóvel, mas o ambiente privado do lar e as relações ali desenvolvidas distantes dos olhos do público[181].

A privacidade espacial não se limita à casa do indivíduo, estende-se também a quartos de hotéis, escritórios e a qualquer lugar físico no qual a pessoa possa manter um espaço privado. O adolescente encontra essa dimensão da privacidade em seu quarto e o motorista é protegido em seu carro da ação das câmeras de vigilância. Essa dimensão da privacidade tutela também os objetos pessoais do indivíduo, como a bolsa que não pode ser aberta sem sua autorização, autorização judicial ou na presença de outra hipótese legal.

---

[179] PEIXOTO, Erick L. C; EHRHARDT JÚNIOR, Marcos. Os Desafios da Compreensão do Direito à Privacidade no Sistema Jurídico Brasileiro em face das Novas Tecnologias. *In*: EHRHARDT JÚNIOR, Marcos; LOBO, Fabiola Albuquerque (Coord.). **Privacidade e sua Compreensão no Direito Brasileiro.** Belo Horizonte: Fórum, 2019, p. 44.

[180] BRASIL. **Constituição Federal de 1988.** Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 13 dez. 2019.

[181] PEIXOTO, Erick L. C; EHRHARDT JÚNIOR, Marcos. Os Desafios da Compreensão do Direito à Privacidade no Sistema Jurídico Brasileiro em face das Novas Tecnologias. *In*: EHRHARDT JÚNIOR, Marcos; LOBO, Fabiola Albuquerque (Coord.). **Privacidade e sua Compreensão no Direito Brasileiro.** Belo Horizonte: Fórum, 2019, p. 44.

Esse aspecto da privacidade que, em seus primórdios, era facilmente protegido, torna-se cada vez mais ameaçado com o desenvolvimento das tecnologias.

Equipamentos fotográficos conseguem capturar imagens a longa distância de ambientes privados, como aconteceu em 2012 com o casal real Kate Midleton e o príncipe William, que foram fotografados curtindo suas férias no terraço de um palácio na região da Provença, num local afastado, sem vizinhança e a quilômetros do povoado de Gignac, que tem menos de cem habitantes. As fotos, em que a duquesa de *Cambridge* aparece fazendo *topless* na piscina, foram publicadas pela revista *Closer*[182].

Atualmente, os drones representam uma grave ameaça à privacidade. Estes equipamentos, cujo uso é crescente, podem ser utilizados para a realização de fotos e vídeos aéreos. Ao sobrevoar áreas residenciais, são capazes de fazer imagens do ambiente privado de pessoas que muitas vezes demandam grandes esforços para proteger a sua privacidade, como a construção de altos muros, por exemplo.

Para atenuar esse risco, a Portaria do Departamento de Controle do Espaço Aéreo nº 224/DGCEA, de 20 de novembro de 2018, que aprovou a Instrução sobre Aeronaves não tripuladas e o Acesso ao Espaço Aéreo Brasileiro – ICA 100-40, estabeleceu que os drones não devem sobrevoar áreas povoadas e aglomeração de pessoas, exceto aquelas anuentes, bem como não devem voar a menos de trinta metros de altura de pessoas não anuentes e de edificações, estruturas, patrimônios, animais, a menos que autorizados pelos proprietários[183].

Essa dimensão da privacidade é importante não somente por manter os aspectos mais privados do indivíduo longe da exposição e julgamento da sociedade, mas principalmente por permitir que cada pessoa possa desenvolver livremente sua personalidade, uma vez que, estando num espaço protegido do julgamento alheio, o indivíduo não tem seus pensamentos e comportamentos tolhidos pelas normas sociais.

2.4.2 Dimensão Decisional

Essa dimensão da privacidade tutela o modo de vida do indivíduo, seus gostos, seus projetos pessoais, suas características, suas escolhas e, sobretudo, as decisões mais

---

[182] O GLOBO. **Casal processa publicação e critica invasão grotesca de sua privacidade**. 19 set. 2012. Disponível em: [182]https://oglobo.globo.com/mundo/revista-francesa-publica-fotos-de-kate-middleton-de-topless-6090825. Acesso em: 8 dez. 2019.

[183] BRASIL.Ministério da Defesa. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. **Portaria DECEA nº 224/DGCEA,** de 20 de novembro de 2018. Aprova a edição da ICA 100-40, Instrução sobre "Aeronaves não tripuladas e o Acesso ao Espaço Aéreo Brasileiro. Disponível em: https://publicacoes.decea.gov.br/?i=publicacao&id=4944. Acesso em: 12 dez. 2019.

fundamentais sobre sua vida[184]. Protege, portanto, o direito de cada pessoa decidir o seu destino e a forma como quer viver sem sofrer interferências externas em tais decisões.

Essa perspectiva de privacidade começou a se estruturar a partir da jurisprudência americana que fundamenta as liberdades reprodutivas no direito à privacidade[185]. No caso *Griswold v. Connecticut*, de 1965, por exemplo, a Suprema Corte americana entendeu que o *rigth to privacy* impede os estados de tornarem ilegal o uso da contracepção por casais[186]. Já no caso *Roe v. Wade*, de 1973, a Suprema Corte americana decidiu que uma pessoa pode optar por fazer um aborto até que o feto se torne viável, com base no direito à privacidade, contido na previsão de devido processo da Décima Quarta Emenda[187].

Em que pesem esses precedentes judiciais, no julgamento do caso *Bowers v. Hardwick*, de 1986, a Suprema Corte entendeu que o direito à privacidade não impedia que um Estado criminalizasse a conduta sexual privada envolvendo pessoas do mesmo sexo[188]. Posteriormente, em 2003, essa decisão foi anulada pelo caso *Lawrence v. Texas*, no qual se decidiu que uma lei do Texas que criminalizava as relações homossexuais consensuais entre adultos violava o direito à privacidade, previsto na Décima Quarta Emenda[189].

Nítido que essa perspectiva da privacidade abrange também uma privacidade corporal. No Brasil, contudo, costuma-se inserir a discussão sobre tais liberdades no âmbito de proteção de outros direitos, como o do livre planejamento familiar, da autonomia privada e da dignidade da pessoa humana.

A dimensão decisional da privacidade liga-se ao direito à autodeterminação, entendido como o direito de cada pessoa controlar a sua vida e o seu destino, atuando como principal agente causal da sua própria vida e se opondo à determinação dos outros. Pressupõe uma

---

[184] PEIXOTO, Erick L. C; EHRHARDT JÚNIOR, Marcos. Os Desafios da Compreensão do Direito à Privacidade no Sistema Jurídico Brasileiro em face das Novas Tecnologias. *In*: EHRHARDT JÚNIOR, Marcos; LOBO, Fabiola Albuquerque (Coord.). **Privacidade e sua Compreensão no Direito Brasileiro.** Belo Horizonte: Fórum, 2019, p. 41-42.

[185] PEIXOTO, Erick L. C; EHRHARDT JÚNIOR, Marcos. Os Desafios da Compreensão do Direito à Privacidade no Sistema Jurídico Brasileiro em face das Novas Tecnologias. *In*: EHRHARDT JÚNIOR, Marcos; LOBO, Fabiola Albuquerque (Coord.). **Privacidade e sua Compreensão no Direito Brasileiro.** Belo Horizonte: Fórum, 2019, p. 42.

[186] SUPREMA CORTE AMERICANA. **Case Griswold v. Connecticut.** v. 381, 1965. Disponível em: https://supreme.justia.com/cases/federal/us/381/479/. Acesso em: 13 dez. 2019.

[187] SUPREMA CORTE AMERICANA. **Case Roe v. Wade.** v. 410, 1973. Disponível em: https://supreme.justia.com/cases/federal/us/410/113/. Acesso em: 13 dez. 2019.

[188] SUPREMA CORTE AMERICANA. **Case Bowers v. Hardwick.** v. 478, 1986. Disponível em: https://supreme.justia.com/cases/federal/us/478/186/. Acesso em: 13 dez. 2019.

[189] SUPREMA CORTE AMERICANA. **Case Lawrence v. Texas.** v. 539, 2003. Disponível em: https://supreme.justia.com/cases/federal/us/539/558//. Acesso em: 13 dez. 2019.

construção pessoal que exclui qualquer fator que possa determinar o comportamento ou a ação de cada sujeito[190].

Esse espaço de autodeterminação tem como fim a própria realização existencial da pessoa, uma vez que ninguém melhor que o próprio indivíduo para estabelecer quais atos proporcionarão sua realização e seu pleno desenvolvimento[191]. A privacidade decisional estabelece, assim, um espaço no qual o indivíduo pode agir dentro de sua esfera de liberdade, longe da interferência alheia e da intimidação dos olhares dos outros. A pessoa, desde que observe a licitude de seus atos, não deve explicação sobre suas decisões, seu comportamento ou o seu jeito de vida a ninguém; "muito pelo contrário, deve-se esperar moderação, reserva e indiferença dos outros em relação a tudo aquilo que não lhes disser respeito"[192].

Essa dimensão da privacidade busca assegurar que o indivíduo possa tomar as decisões referentes à sua vida sem sofrer discriminação social por isso e sem que o Estado imponha obstáculos a tais escolhas. Essa perspectiva da privacidade abrange o direito de cada pessoa professar a sua fé, de se associar a determinada organização política ou sindical, de ouvir as músicas de que mais goste, de assistir aos filmes que queira, de desenvolver relacionamentos amorosos da forma que entender mais conveniente, enfim, o direito do indivíduo de realizar livremente suas escolhas.

Ressalte-se que a interferência alheia nesse espaço decisório pode ser positiva, por meio da aprovação, uma vez que até mesmo os elogios podem significar uma interferência no modo de agir do indivíduo, já que muitas pessoas buscam a aprovação social. Essa dimensão da privacidade protege as pessoas de serem mal interpretadas ou julgadas fora de contexto[193].

Assim, o conceito original de privacidade dilatou-se e passou a abranger novas perspectivas. Nesse diapasão, a dimensão decisional da privacidade assegura a liberdade das escolhas existenciais contra qualquer forma de controle público e social.

---

[190] SIMÕES, Cristina. **O direito a autodeterminação das pessoas com deficiência**.Porto: Associação do Porto de Paralisia Cerebral; Faculdade de Direito da Universidade do Porto, 2016. Disponível em: https://www.appc.pt/_pdf/eBook_FDUP_Dir_PessoasDeficiencia.pdf. Acesso em: 13 dez. 2019, p. 8.

[191] BERALDO, Ana de M. S. Ponderações constitucionais sobre a autonomia psicofísica. *In*: **Civilistica.com**, a. 3, n. 1, 2014. Disponível em: http://civilistica.com/ponderacoes-constitucionais-sobre-a-autonomia-psicofisica/. Acesso em: 13 dez. 2019, p. 6-7.

[192] PEIXOTO, Erick L. C; EHRHARDT JÚNIOR, Marcos. Os Desafios da Compreensão do Direito à Privacidade no Sistema Jurídico Brasileiro em face das Novas Tecnologias. *In*: EHRHARDT JÚNIOR, Marcos; LOBO, Fabiola Albuquerque (Coord.). **Privacidade e sua Compreensão no Direito Brasileiro.** Belo Horizonte: Fórum, 2019, p. 42.

[193] PEIXOTO, Erick L. C; EHRHARDT JÚNIOR, Marcos. Os Desafios da Compreensão do Direito à Privacidade no Sistema Jurídico Brasileiro em face das Novas Tecnologias. *In*: EHRHARDT JÚNIOR, Marcos; LOBO, Fabiola Albuquerque (Coord.). **Privacidade e sua Compreensão no Direito Brasileiro.** Belo Horizonte: Fórum, 2019, p. 42-43.

Na sociedade da informação, na qual se verifica uma intensa coleta de informações pessoais, muitas das decisões tomadas na esfera de liberdade, protegidas por esta dimensão da privacidade, acabam se transformando em dados pessoais, inclusive as de foro mais íntimo e que tornam o indivíduo mais vulnerável a discriminações, como a opção religiosa, dados estes que são protegidos pela dimensão informacional da privacidade.

2.4.3 Dimensão Informacional

A dimensão informacional da privacidade, a mais recente perspectiva desse direito, é a que mais se relaciona com este trabalho, porque protege as informações pessoais do indivíduo da coleta, o tratamento e a disseminação não autorizados.

Floridi define a privacidade informacional como a liberdade de interferência ou intrusão epistêmica alcançada quando existe uma restrição a fatos desconhecidos sobre determinada pessoa[194]. Tavani ensina que estes fatos seriam informações pessoais, como as atividades diárias, o estilo de vida, o histórico médico e o desempenho acadêmico, armazenadas em bancos de dados ou transmitidas entre as partes, usando dispositivos de *e-mail*, telefonia e comunicação sem fio[195].

A privacidade informacional seria, então, o direito de o indivíduo controlar as suas informações pessoais, podendo conceder ou restringir o acesso de outras pessoas a tais informações[196].

Essa dimensão da privacidade relaciona-se à autodeterminação informativa, a qual será estudada adiante, e confere ao indivíduo o poder de controlar o fluxo de informações relativas a uma pessoa, tanto na "saída" quanto na "entrada", uma vez que tutela inclusive o direito do indivíduo de não saber, de não tomar conhecimento sobre determinada informação, de excluir da própria esfera privada uma determinada categoria de informações[197].

Protege, então, as informações pessoais no que se refere à possibilidade de o indivíduo controlar o que os outros sabem sobre si, com quem aqueles que coletaram os dados podem compartilhar tais informações, para quais finalidades os dados coletados podem ser utilizados,

---

[194] FLORIDI, Luciano. Information Ethics: on the philosophical foundation of computer ethics. **Ethics and Information Technology,** mar. 1999. Disponível em: https://link.springer.com/article/10.1023/A:1010018611096. Acesso em: 2 dez. 2019, p. 52.

[195] TAVANI, Herman T. Informational Privacy: concepts, theories, and Controversies.. *In:* HIMMA, Kenneth E; TAVANI, Herman T. (Edt.). **The Handbook of Information and Computer Ethics.** Wiley, 2008, p. 139.

[196] TAVANI, Herman T. Informational Privacy: concepts, theories, and Controversies.. *In:* HIMMA, Kenneth E; TAVANI, Herman T. (Edt.). **The Handbook of Information and Computer Ethics.** Wiley, 2008, p. 141-142.

[197] RODOTÀ, Stefano. **A vida na sociedade da vigilância –** a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 109.

de que maneira devem ser armazenadas as informações pessoais, com qual nível de segurança, por quanto tempo devem ser armazenadas, quem pode acessar tais dados.

Essa dimensão da privacidade é bastante ameaçada na atual sociedade da informação. Com o avanço da tecnologia, a coleta e o tratamento de dados pessoais são cada vez mais frequentes. A utilização desses dados traz inúmeros benefícios não só às grandes organizações que lucram a partir dessas informações e para quem os dados pessoais se tornaram valiosos ativos, mas também para a sociedade, haja vista que tais dados são a principal matéria-prima de muitos serviços de utilidade pública. O tratamento desses dados não pode gerar danos à privacidade dos indivíduos; privacidade e avanços tecnológicos devem coexistir.

Solove, ao desenvolver a taxonomia da privacidade, afirma que existem quatro grupos básicos de ações prejudiciais à privacidade, quais sejam: a) coleta de informações; b) processamento de informações; c) disseminação da informação; d) invasão[198].

Nessa senda, várias entidades coletam informações: o Estado, organizações empresárias, outras pessoas. Nem toda coleta de informações é prejudicial, mas certos tipos de coleta podem ser, como a realizada por meio de escutas não autorizadas. Após a coleta, ocorre o processamento dos dados, isto é, o armazenamento, a combinação, a manipulação e o uso dos dados. Algumas atividades desse grupo podem ser danosas à privacidade, como a utilização da informação com finalidade diversa daquela para a qual foi coletada e o armazenamento dos dados sem a segurança adequada, o que pode gerar vazamentos[199].

Por sua vez, o terceiro grupo de ações envolve aquelas relacionadas à disseminação da informação, como a exposição de uma imagem de nudez de alguém, a divulgação de um segredo e a transferência não autorizada de dados pessoais. Esse é o grupo de atividades no qual a informação mais se afasta do controle do indivíduo. Por último, no quarto grupo estão as atividades invasivas nos assuntos particulares dos indivíduos, como a intrusão na tranquilidade ou solidão de alguém e a interferência decisional, que ocorre quando o conhecimento ou a possibilidade de conhecimento de determinada informação pessoal pelos outros acaba por interferir nas decisões do indivíduo[200]. Aqui, vê-se um ponto de contato entre a dimensão informacional e a dimensão decisional da privacidade.

---

[198] SOLOVE, Daniel J. A Taxonomy of Privacy. **University of Pennsylvania Law Review,** v. 154, n. 3, jan. 2006. Disponível em: https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf. Acesso em: 2 dez. 2019, p. 488.

[199] SOLOVE, Daniel J. A Taxonomy of Privacy. **University of Pennsylvania Law Review,** v. 154, n. 3, jan. 2006. Disponível em: https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf. Acesso em: 2 dez. 2019, p. 488

[200] SOLOVE, Daniel J. A Taxonomy of Privacy. **University of Pennsylvania Law Review,** v. 154, n. 3, jan. 2006. Disponível em: https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf. Acesso em: 2 dez. 2019, p. 488-489.

Sobre as violações da privacidade informacional, Floridi afirma que esta requer uma reinterpretação da privacidade que leve em consideração a natureza essencialmente informativa dos seres humanos e de suas operações como agentes sociais informacionais. Essa reinterpretação deve considerar cada pessoa como constituída por suas informações, de modo que uma violação da privacidade informacional é uma forma de agressão à própria identidade pessoal do indivíduo[201].

Baião e Gonçalves afirmam que na sociedade da informação o novo conceito integral de pessoa se manifesta pela sua identidade social e individual, pelo seu corpo físico e eletrônico, este último formado pelo conjunto dos nossos dados[202].

A dimensão informacional da privacidade protege as informações pessoais visando a proteger a pessoa a quem tais informações dizem respeito, principalmente quando se tem em mente que os dados pessoais podem representar os aspectos mais íntimos do indivíduo e o seu tratamento inadequado pode gerar discriminação e outras graves violações à dignidade humana. É fundamental tutelar as informações pessoais para evitar que sua exposição não autorizada ou o seu tratamento para fins outros que não aqueles para os quais os dados foram coletados acabem por gerar interferências alheias na vida do indivíduo, prejudicando o livre desenvolvimento de sua personalidade.

No Brasil, a privacidade informacional passou a ser especialmente protegida por meio da Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Esta lei entrou em vigor em setembro de 2020.

Uma vez entendidos os diferentes modelos jurídicos de privacidade, bem como as suas dimensões, adiante será analisada a concepção e a tutela desse direito no ordenamento jurídico pátrio.

2.5 O direito à privacidade no ordenamento jurídico brasileiro

---

[201] FLORIDI, Luciano. The Ontological Interpretation of Informational Privacy. **Ethics and Information Technology,** dez. 2005. Disponível em: https://link.springer.com/article/10.1007/s10676-006-0001-7. Acesso em: 2 dez. 2019, p. 10.

[202] BAIÃO, Kelly S; GONÇALVES, Kalline C. A garantia da privacidade na sociedade tecnológica: um imperativo à concretização do princípio da dignidade da pessoa humana. **Civilistica.com**, a. 3, n. 2, 2014. Disponível em: http://civilistica.com/a-garantia-da-privacidade-na-sociedade-tecnologica-um-imperativo-a-concretizacao-do-principio-da-dignidade-da-pessoa-humana/. Acesso em: 12 dez. 2019, p. 2.

Até o ano de 1824, a privacidade no Brasil tinha uma tutela bastante tímida, que se dava por meio da aplicação das Ordenações do Reino, as quais, no que diz respeito a esse direito, resumiam-se ao sigilo das correspondências. Também no período compreendido entre a independência do Brasil e a Constituição Federal de 1988, as constituições brasileiras continuaram a oferecer uma tutela bastante tênue da privacidade, resumida ao sigilo das comunicações e à inviolabilidade do domicílio.

Já a atual Carta Magna assim dispõe em seu artigo 5º:

> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal[203];

Como se vê, a Constituição Federal de 1988 já dispensa uma maior proteção à privacidade, apesar de não utilizar tal expressão, tipificando várias espécies desse direito. Importante dizer, ainda, que a CF/1988 não positivou todos os direitos fundamentais, o que não implica que não existem direitos fundamentais além dos expressos na Carta Magna, haja vista que, de seu texto, depreendem-se outros direitos, os chamados direitos fundamentais implícitos. Dessa feita, verifica-se, em nosso ordenamento jurídico, uma cláusula geral de tutela da pessoa humana que permite "estender a tutela a situações não previstas"[204].

Essa tutela decorre do valor fundante e unificador do sistema jurídico pátrio, a dignidade da pessoa humana. Isso significa que a Constituição federal vigente reconhece não somente o direito fundamental à privacidade, enquanto gênero, mas as várias espécies de direito abarcadas pelo direito à privacidade, sejam os expressamente previstos no texto constitucional, como o direito à intimidade e à imagem, sejam aqueles implícitos, como o direito ao esquecimento e o direito à proteção de dados pessoais.

Ainda, foi aprovada no Senado Federal, em 2 de julho de 2019, a Proposta de Emenda à Constituição nº 17/2019, que visa incluir a proteção de dados pessoais entre os direitos

---

[203] BRASIL. **Constituição Federal de 1988.** Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 13 dez. 2019.

[204] EHRHARDT JÚNIOR, Marcos A. A; TORRES, Marcio R. Direitos Fundamentais e as Relações Privadas. Superando a (pseudo) tensão entre aplicabilidade direta e eficácia indireta para além do patrimônio. **Revista Jurídica**, v. 4, n. 53, 2018, p. 343. Disponível em: http://revista.unicuritiba.edu.br/index.php/RevJur/article/view/3222/371371738. Acesso em: 1 abr. 2019, p. 343.

fundamentais do cidadão elencados no artigo 5º da CF/1988. O texto tramita na Câmara dos Deputados[205].

No entanto, a Constituição já confere proteção à privacidade informacional por meio do inciso LXXII, do mesmo artigo 5º, o qual estabelece que será concedido *habeas data* para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público, bem como para possibilitar a retificação de tais dados.

No plano infraconstitucional, o Código Civil brasileiro, em seu artigo 20, protege a imagem do indivíduo contra a sua exposição ou utilização não autorizada, bem como estabelece, em seu artigo 21, que a vida privada da pessoa natural é inviolável[206], inviolabilidade esta oponível ao Estado, à sociedade e à própria pessoa[207].

Existem diversos outros diplomas legais que visam proteger a privacidade.

Nesse sentido, a Lei nº 9.296/1996 dispõe que a interceptação telefônica somente poderá ocorrer mediante autorização judicial e nas hipóteses previstas na referida lei[208]. A Lei Complementar nº 105/2001 dispõe sobre o sigilo das operações de instituições financeiras e define as hipóteses legais de compartilhamento dessas informações[209].

---

[205] Art. 1° Inclua-se no art. 5º, da Constituição Federal, o seguinte inciso XII-A: Art. 5° [...]. XII-A – é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais. [...]". BRASIL. **Proposta de Emenda à Constituição nº 17, de 2017.** Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria.Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1567535523044&disposition=inline. Acesso em: 15 abr. 2020.

[206] Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais.
Parágrafo único. Em se tratando de morto ou de ausente, são partes legítimas para requerer essa proteção o cônjuge, os ascendentes ou os descendentes.
Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma. BRASIL. **Lei nº 10.406,** de 10 de janeiro de 2002**.** Institui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 13 dez. 2019.

[207] LÔBO, Paulo. Direito à Privacidade e sua Autolimitação. *In*: EHRHARDT JÚNIOR, Marcos; LOBO, Fabiola Albuquerque (Coord.). **Privacidade e sua Compreensão no Direito Brasileiro.** Belo Horizonte: Fórum, 2019, p. 18.

[208] Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.
Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.
BRASIL. **Lei nº 9.296,** de 24 de julho de 1996**.** Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 13 dez. 2019.

[209] Art. 1º (...)
§ 3º Não constitui violação do dever de sigilo:

Também o Código Tributário Nacional, em seu artigo 198, estabelece que, fora das hipóteses legais, "é vedada a divulgação, por parte da Fazenda Pública ou de seus servidores, de informação obtida em razão do ofício sobre a situação econômica ou financeira do sujeito passivo ou de terceiros e sobre a natureza e o estado de seus negócios ou atividades"[210].

O Código de Defesa do Consumidor, em seu artigo 43, prevê que o consumidor terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes, além de que deverá ser comunicado por escrito acerca da abertura de cadastro por ele não solicitada[211].

A Lei 12.737/2012, a chamada Lei Carolina Dieckmann, altera o Código Penal para tipificar como crime a invasão de dispositivo informático alheio, conectado ou não à rede de

---

I – a troca de informações entre instituições financeiras, para fins cadastrais, inclusive por intermédio de centrais de risco, observadas as normas baixadas pelo Conselho Monetário Nacional e pelo Banco Central do Brasil;
II – o fornecimento de informações constantes de cadastro de eminentes de cheques sem provisão de fundos e de devedores inadimplentes, a entidades de proteção ao crédito, observadas as normas baixadas pelo Conselho Monetário Nacional e pelo Banco Central do Brasil;
III – o fornecimento das informações de que trata o § 2º do art. 11 da Lei nº 9.311, de 24 de outubro de 1996;
IV – a comunicação, às autoridades competentes, da prática de ilícitos penais ou administrativos, abrangendo o fornecimento de informações sobre operações que envolvam recursos provenientes de qualquer prática criminosa;
V – a revelação de informações sigilosas com o consentimento expresso dos interessados;
VI – a prestação de informações nos termos e condições estabelecidos nos artigos 2º, 3º, 4º, 5º, 6º, 7º e 9 desta Lei Complementar.
VII – o fornecimento de dados financeiros e de pagamentos, relativos a operações de crédito e obrigações de pagamento adimplidas ou em andamento de pessoas naturais e jurídicas, a gestores de bancos de dados, para formação de histórico de crédito, nos termos de lei específica.
§ 4º A quebra de sigilo poderá ser decretada, quando necessária para apuração de ocorrência de qualquer ilícito, em qualquer fase do inquérito ou do processo judicial, e especialmente nos seguintes crimes:
I – de terrorismo;
II – de tráfico ilícito de substâncias entorpecentes ou drogas afins;
III – de contrabando ou tráfico de armas, munições ou material destinado a sua produção;
IV – de extorsão mediante seqüestro;
V – contra o sistema financeiro nacional;
VI – contra a Administração Pública;
VII – contra a ordem tributária e a previdência social;
VIII – lavagem de dinheiro ou ocultação de bens, direitos e valores;
IX – praticado por organização criminosa.
BRASIL. **Lei Complementar nº 105 ,** de 10 de janeiro de 2001**.** Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm. Acesso em: 13 dez. 2019.

[210] BRASIL. **Lei nº 5.172,** de 25 de outubro de 1966**.** Dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l5172.htm. Acesso em: 13 dez. 2019.

[211] Art. 43.O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
§ 1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
§ 2º A abertura de cadastro físico, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
BRASIL. **Lei nº 8.078,** de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 13 dez. 2019.

computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo, ou instalar vulnerabilidades para obter vantagem ilícita[212].

A Lei nº 12.414/2011 (Lei do Cadastro Positivo) disciplina a formação e consulta a bancos de dados com informações de adimplemento de pessoas naturais ou jurídicas para formação de histórico de crédito[213].

A Lei nº 12.965/2014 (Marco Civil da *Internet*) traz algumas disposições que tutelam a privacidade do indivíduo, principalmente em sua dimensão informacional[214].

Esses são alguns exemplos de como o ordenamento jurídico pátrio tutela a privacidade no plano infraconstitucional.

O presente trabalho tem como objeto o estudo da Lei 13.709/2019 (Lei Geral de Proteção de Dados Pessoais), a primeira lei brasileira que trata especificamente da proteção de

---

[212] **"Invasão de dispositivo informático"** – Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.
BRASIL. **Lei nº 12.737**, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-lei n° 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providencias. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 13 dez. 2019.

[213] Art. 3º Os bancos de dados poderão conter informações de adimplemento do cadastrado, para formação do histórico de crédito, nas condições estabelecidas nesta Lei.
§ 1º 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.
§ 2º Para os fins do disposto no § 1º, consideram-se informações:
I – objetivas: aquelas descritivas dos fatos e que não envolvam juízo de valor;
II – claras: aquelas que possibilitem o imediato entendimento do cadastrado independentemente de remissão a anexos, fórmulas, siglas, símbolos, termos técnicos ou nomenclatura específica;
III – verdadeiras: aquelas exatas, completas e sujeitas à comprovação nos termos desta Lei; e
IV – de fácil compreensão: aquelas em sentido comum que assegurem ao cadastrado o pleno conhecimento do conteúdo, do sentido e do alcance dos dados sobre ele anotados.
§ 3º Ficam proibidas as anotações de:
I – informações excessivas, assim consideradas aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor; e
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.
BRASIL. **Lei nº 12.414**, de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 13 dez. 2019.

[214] Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial.
BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 13 dez. 2019.

dados pessoais, a qual, em 65 artigos inspirados no Regulamento Geral de Proteção de Dados da União Europeia, visa proteger a privacidade e o livre desenvolvimento da personalidade por meio da tutela das informações pessoais, disciplinando a sua coleta e tratamento por entes privados e estatais.

Como se observa, a proteção da privacidade no Brasil se aproxima mais da noção de privacidade do direito europeu, ligando a tutela desse direito à dignidade da pessoa humana. Assim, o direito brasileiro dispensa vasta proteção à privacidade tanto no plano constitucional quanto no infraconstitucional, estabelecendo limitações à atuação dos entes privados e estatais, com vistas a assegurar a privacidade.

O inimigo não é só o Estado, a imprensa ou a exposição pública de informações íntimas do indivíduo. A privacidade não está somente no lar. As pessoas não podem abrir mão completamente de sua privacidade em troca de um emprego ou dinheiro. As organizações empresárias não são livres para coletar e compartilhar os dados pessoais do brasileiro sem a sua autorização. A tutela da privacidade, no Brasil, tal qual na Europa, também possui um caráter mais social e exige uma atuação positiva do Estado. A privacidade não é diretamente ligada à liberdade, por conseguinte, não se assegura ampla proteção aos particulares contra a interferência estatal em sua vida e negócios, de modo que os atores privados não são irrestritamente livres para realizar suas transações negociais. Ao contrário, a privacidade é vista como pressuposto essencial para o respeito da dignidade da pessoa humana.

Sarlet ensina que a garantia da isonomia de todos os seres humanos constitui pressuposto essencial para o respeito da dignidade da pessoa humana, não sendo lícita a submissão dos indivíduos a tratamento discriminatório. A garantia da identidade pessoal do indivíduo constitui uma das principais expressões da dignidade da pessoa humana, concretizando-se, entre outros aspectos, na liberdade de consciência, de pensamento, de culto, na proteção da intimidade, da honra, da esfera privada, de tudo que esteja associado ao livre desenvolvimento de sua personalidade, bem como ao direito de autodeterminação sobre os assuntos que dizem respeito à sua esfera particular e, ainda, à garantia de um espaço privativo no qual o indivíduo se encontra resguardado contra ingerências na sua esfera pessoal. Por conseguinte, onde a privacidade for objeto de ingerências indevidas, não haverá espaço para a dignidade da pessoa humana[215].

[215] SARLET, Ingo Wolfgang. **A Eficácia dos Direitos Fundamentais –** uma teoria geral dos direitos fundamentais na perspectiva constitucional. 10. ed. rev. atual. e ampl. Porto Alegre: Livraria do Advogado, 2009, p. 104.

O *right to privacy* possui um conteúdo bastante amplo, englobando os aspectos pessoais do direito à imagem e até mesmo aspectos do que, no Brasil, considera-se como crimes de calúnia, injúria ou difamação.

Apesar disso, a tutela da privacidade no Brasil e na Europa possui suas diferenças. Assim, enquanto na Europa entende-se que viola a privacidade do trabalhador o monitoramento constante e imotivado das comunicações do trabalhador, ainda que enviadas por *e-mail* corporativo ou por perfil, também corporativo, em programa de troca de mensagens instantâneas e utilizando-se de ferramentas tecnológicas de propriedade do empregador, no horário e local de trabalho[216], a jurisprudência brasileira entende que os direitos do empregado à privacidade e ao sigilo de correspondência aplicam-se somente à comunicação estritamente pessoal, ainda que virtual, de modo que apenas o *e-mail* pessoal ou particular do empregado desfruta da proteção constitucional, o que não ocorre com o *e-mail* corporativo, o qual se entende ostentar natureza jurídica equivalente à de uma ferramenta de trabalho proporcionada pelo empregador ao empregado para a consecução do serviço[217]. Ao menos nesse ponto, a jurisprudência brasileira acabou se aproximando mais da concepção americana de privacidade que da europeia.

Desse modo, verifica-se que o Brasil possui um modelo próprio de regulação de privacidade, o qual sofre influência tanto do modelo europeu quanto do modelo americano de privacidade.

Nessa esteira, assim como na Europa, o país entende este direito como primordial ao livre desenvolvimento da personalidade e à dignidade humana, bem como compreende que não é suficiente que o Estado apenas se abstenha de intervir no direito à privacidade, faz-se necessário que o assegure, daí a relevância da heterorregulação e a razão pela qual possui várias normas de proteção à privacidade.

A esse respeito, a recente entrada em vigor da Lei Geral de Proteção de Dados Pessoais aproximou ainda mais o Brasil do modelo europeu de tutela desse direito, com a instituição de um sistema que, de forma exitosa, dedica-se a evitar danos e não somente a repará-los. Ademais, trata-se de uma legislação genérica, aplicada aos diversos setores privados e públicos, e que cria um órgão de fiscalização do cumprimento da lei.

---

[216] CORTE EUROPEIA DE DIREITOS HUMANOS. **Case of Barbulescu v. Romania.** Strasbourg, 5 set. 2017. Disponível em: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22barbulescu%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-177082%22]}. Acesso em: 8 dez. 2019.

[217] BRASIL. Tribunal Superior do Trabalho. **RR 61300-23.2000.5.10.0013,** 1ª Turma, Relator: Ministro João Oreste Dalazen, DEJT 10/06/2005. Disponível em: https://jurisprudencia.tst.jus.br/#19f32e7a289f9dc436bceeadc762069e. Acesso em: 12 dez. 2019.

Por estas mesmas razões, o modelo regulatório brasileiro se afasta do americano, que exige, principalmente, uma conduta negativa do Estado e que tutela a privacidade por meio de legislações esparsas voltadas a setores específicos e da autorregulação, na qual os atores privados estabelecem condutas e se fiscalizam mutuamente.

No entanto, observa-se que a concepção da privacidade no Brasil ainda está em evolução. Nessa senda, por muito tempo vigorou uma noção de que o âmbito de proteção deste direito cingia-se a situações íntimas ou privadas, predominando, pois, a feição individual da privacidade, no que se assemelhava à *privacy* americana.

No quadro apresentado no item 2.3.1, por exemplo, verificou-se que muitos doutrinadores consideram que privacidade é sinônimo de vida privada, entendo que somente abarcaria os fatos e acontecimentos que são compartilhados com um número limitado de pessoas, com quem o indivíduo tece relações sociais, e que não são ou não devem ser divulgados ao público.

Contudo, nos últimos anos, máxime com os debates em torno da aprovação da Lei Geral de Proteção de Dados Pessoais, nota-se que a concepção de privacidade tem sido ampliada também no Brasil para abarcar o controle do indivíduo sobre as próprias informações. Esse processo de ampliação do âmbito de proteção da privacidade, entretanto, não é tão rápido, de modo que a doutrina e a jurisprudência ainda levarão certo tempo para consolidarem essa nova acepção.

Dessa feita, o modelo jurídico de privacidade brasileiro é híbrido, cuja concepção desse direito sofre forte influência da compreensão americana, mas a forma de regular a matéria é muito semelhante ao modelo regulatório da Europa. Entretanto, a vigência da LGPD tem provocado mudanças no modo de se enxergar a privacidade, por conseguinte, a tendência é que este hibridismo se desfaça e dê lugar a uma correspondência, ainda que imperfeita, com o modelo europeu de acepção e tutela da privacidade.

3 O DESENVOLVIMENTO DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS

Como visto no capítulo anterior, a privacidade é um direito dinâmico cujo âmbito de proteção acompanha a evolução da sociedade a fim de tutelar novos aspectos da pessoa humana. Dessa forma, o direito à privacidade abarca vários outros direitos, entre os quais está o objeto de estudo deste trabalho: o direito à proteção de dados pessoais.

Para o estudo da efetividade da Lei Geral de Proteção de Dados Pessoais, faz-se necessário entender não só os principais conceitos relacionados ao direito à proteção de dados pessoais, mas o próprio caminho percorrido por esse direito. Neste capítulo será investigado o contexto em que surgiram as primeiras normas sobre a matéria, a evolução experimentada por essas legislações, o reconhecimento do direito à proteção dos dados pessoais como fundamental e as suas principais bases normativas. É a isso que esta seção se propõe.

3.1 Conceitos e aspectos relevantes

Antes de proceder ao estudo do direito à proteção de dados pessoais, é importante apreender os principais conceitos utilizados pelas legislações sobre a matéria, em especial pela LGPD, bem como as questões relevantes que os circundam, uma vez que isso ajudará a compreensão do próprio direito e de sua aplicação em todo o ciclo de vida da informação. Assim, serão analisados os seguintes conceitos: dados pessoais, dados sensíveis, tratamento de dados e dados anonimizados.

3.1.1 Dados Pessoais e sua Titularidade

Tradicionalmente, a doutrina costuma distinguir os termos “dado” e “informação”. Doneda explica que há certa confusão no uso das expressões em razão de o conteúdo de ambas se sobrepor em várias circunstâncias, o que faz com que muitas vezes a doutrina e a lei tratem-nos indistintamente. Contudo, em que pese os dois termos servirem a representar um fato, um aspecto de determinada realidade, possuem peculiaridades que os diferenciam[218].

[218] 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.

Catala, ao formular a sua teoria jurídica da informação, define a informação como toda mensagem que possa ser comunicada a outras pessoas por qualquer meio[219].

Nessa esteira, o "dado" seria um ato ou sinal que requer interpretação para que possa fazer sentido[220]; possui, portanto, uma conotação mais primitiva e fragmentada, sendo entendido como uma informação em potencial, uma espécie de pré-informação, anterior à transmissão, interpretação e compreensão, ao passo que a "informação" pressupõe a depuração do conteúdo do dado[221], isto é, a informação é o conteúdo de um dado, o qual foi transmitido a outrem e por ele compreendido. Por tal razão, "a informação é um bem criado e não fornecido"[222].

Em outras palavras, o dado é uma informação em estado bruto, tornando-se útil e, portanto, valioso a partir do momento em que é tratado e dele se extrai um conhecimento, ou seja, quando se transforma em informação. Desse modo, esta é criada pela intelecção, pelo processo cognitivo que leva à compreensão do dado. Por conseguinte, o uso de um dado somente terá valor se puder ser transformado.

Aqui, importa dizer que, enquanto o dado pessoal possui um valor dignidade, pois, como será visto adiante, é atributo da personalidade, a informação que o uso, que o tratamento desse dado revela possui notável valor econômico para as organizações que a utilizam. Isso posto, enquanto o dado pessoal, como elemento da personalidade, possui um valor intrínseco, o valor monetário da informação pessoal é atribuído pelo tratamento a que este dado é ou será submetido.

A informação pode apresentar-se em várias formas, como a gráfica, a fotográfica e a acústica[223]. Catala identifica quatro tipos de informações: a) informações sobre pessoas e seus patrimônios; b) informações que envolvem a opinião subjetiva de terceiros sobre alguém; c) as obras da mente; d) demais informações que servem para medir os fenômenos, descrever

---

[219] CATALA, Pierre. Ebauche d'une théorie juridique de l'information**. Informatica e Diritto,** n. 1, v. 15, 1983. Disponível em: http://www.ittig.cnr.it/EditoriaServizi/AttivitaEditoriale/InformaticaEDiritto/1983_01_015-031_Catala.pdf. Acesso em: 15 mar. 2020, p. 19.

[220] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 55.

[221] 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.

[222] CATALA, Pierre. Ebauche d'une théorie juridique de l'information**. Informatica e Diritto,** n. 1, v. 15, 1983. Disponível em: http://www.ittig.cnr.it/EditoriaServizi/AttivitaEditoriale/InformaticaEDiritto/1983_01_015-031_Catala.pdf. Acesso em: 15 mar. 2020, p. 19.

[223] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 55.

coisas, relacionar eventos, enfim, dizer qualquer outra coisa que esteja fora das categorias anteriores[224].

Se a informação possuir um vínculo objetivo com uma pessoa, revelando aspectos sobre ela, isto é, referindo-se às características ou ações que a ela podem ser atribuídas em conformidade com a lei – tal qual o nome civil ou o domicílio – ou em razão de seus atos, como os dados referentes ao seu consumo, às suas manifestações, suas opiniões, entre outros atos, tal informação será considerada uma informação pessoal[225].

Para que a informação seja pessoal, os dados que a compõem precisam ser objetivos, isto é, não podem refletir a opinião subjetiva de terceiros[226]. As obras intelectuais de uma pessoa não são consideradas informação pessoal, embora o fato de sua autoria o seja, em virtude de tal obra não dizer respeito a uma característica objetiva da pessoa, mas sim ter sido por ela produzida[227]. Assim, relaciona-se à pessoa apenas de forma anexa.

O estabelecimento do vínculo objetivo da informação com uma pessoa é fundamental para afastar da categoria de informação pessoal outras informações que, apesar de se relacionarem de algum modo com determinado indivíduo, não possuem como objeto a própria pessoa[228]. Nesse sentido, informação pessoal é toda informação extraída a partir de dados cujo objeto é um sujeito de direito[229]. Tal distinção serve para esclarecer que o direito à proteção de dados pessoais tutela qualquer dado e não somente a informação pessoal.

Cumpre mencionar que, em que pese a distinção apresentada, muitas vezes as expressões "dado pessoal" e "informação pessoal" são utilizadas neste trabalho como sinônimas, por se entender que o uso de ambos os termos em nada prejudica a intelecção do que aqui é discutido.

Nessa senda, no que concerne ao conceito de dados pessoais, definição esta essencial ao desenvolvimento desse trabalho, importa dizer que as legislações sobre proteção de dados

---

[224] CATALA, Pierre. Ebauche d'une théorie juridique de l'information**. Informatica e Diritto,** n. 1, v. 15, 1983. Disponível em: http://www.ittig.cnr.it/EditoriaServizi/AttivitaEditoriale/InformaticaEDiritto/1983_01_015-031_Catala.pdf. Acesso em: 15 mar. 2020, p. 20-22.

[225] 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. 139.

[226] CATALA, Pierre. Ebauche d'une théorie juridique de l'information**. Informatica e Diritto,** n. 1, v. 15, 1983. Disponível em: http://www.ittig.cnr.it/EditoriaServizi/AttivitaEditoriale/InformaticaEDiritto/1983_01_015-031_Catala.pdf. Acesso em: 15 mar. 2020, p. 20.

[227] 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. 139.**

[228] 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. 139.

[229] CATALA, Pierre. Ebauche d'une théorie juridique de l'information**. Informatica e Diritto,** n. 1, v. 15, 1983. Disponível em: http://www.ittig.cnr.it/EditoriaServizi/AttivitaEditoriale/InformaticaEDiritto/1983_01_015-031_Catala.pdf. Acesso em: 15 mar. 2020, p. 20.

pessoais podem adotar uma concepção ampla ou restrita de dado pessoal, o que, por conseguinte, impacta diretamente sobre quais dados são protegidos por cada legislação.

Numa definição restrita, são considerados dados pessoais apenas as informações que se relacionam a uma pessoa identificada, específica. O vínculo entre o dado e a pessoa a quem esse dado está associado é estabelecido de forma direta, imediata[230].

Já a acepção ampla abrange também os dados que potencialmente permitam a identificação do titular da informação, ou seja, um dado será considerado pessoal se a partir dele existir a possibilidade de se individualizar a pessoa a quem ele se refere, ainda que indiretamente[231]. Nesse sentido, o conceito de dado pessoal pode ser entendido como os fatos, comunicações e ações que se referem a um indivíduo identificado ou identificável[232].

No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD), assim como o Regulamento Geral de Proteção de Dados da União Europeia (RGPD), adotou a concepção mais extensa de dado pessoal, definindo-o como a informação relacionada à pessoa natural identificada ou identificável[233].

O RGPD, por sua vez, em seu artigo 4º, diz que é identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular.

Pelos exemplos trazidos pelo RGPD, é mais perceptível que informações que só permitam a identificação do titular pela via indireta podem ser consideradas como dados pessoais, como no caso do IP de computador, pelo qual se pode chegar à identificação de alguém, ainda que seja necessária autorização judicial para isso.

Dessa forma, dado pessoal pode ser entendido como a expressão de uma característica, de um fato, de um atributo, de uma ação ou de qualquer outro elemento constitutivo de uma informação pessoal, isto é, qualquer elemento constitutivo de um conhecimento inerente a

---

[230] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais -** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 68.

[231] MACHADO, Diego; DONEDA, Danilo. Proteção de Dados Pessoais e Criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. **Revista dos Tribunais**, v. 998, Caderno Especial, p. 99-128, São Paulo: RT, dez. 2018. Disponível em: https://www.researchgate.net/publication/330401277_Protecao_de_dados_pessoais_e_criptografia_tecnologias_criptograficas_entre_anonimizacao_e_pseudonimizacao_de_dados. Acesso em: 17 abr. 2020, p. 106.

[232] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 55-56.

[233] Artigo 5º, I, da Lei 13.709/2018. BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 abr. 2020.

uma pessoa singular identificada ou identificável, independentemente da forma como o dado se apresente, incluindo som e imagem.

Quanto à titularidade, a LGPD, em seu artigo 5º, inciso V, define o titular como a "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento". De igual forma, o RGPD, em seu artigo 4º, define que é titular dos dados pessoais a pessoa singular identificada ou identificável a quem se relaciona a informação.

Uma vez que os dados pessoais têm como objeto a própria pessoa, outro não poderia ser o titular de tais dados senão o indivíduo a quem os dados se referem.

3.1.2 Dados pessoais sensíveis e as dificuldades de sua delimitação

A utilização dos dados pessoais demonstrou, na prática, que o tratamento de determinados tipos de dados pessoais pode provocar efeitos muito mais danosos que o tratamento das demais informações pessoais, como as informações sobre raça, a orientação sexual, o histórico médico ou os dados genéticos de um indivíduo[234].

Tais dados, se conhecidos e submetidos a tratamento, podem ser utilizados com finalidades discriminatórias ou lesivas, isto é, seu uso representa riscos potenciais muito maiores do que outros tipos de informação[235]. Por essa razão, esses dados pessoais merecem ser especialmente protegidos contra os riscos de sua circulação, estabelecendo-se regras mais rigorosas para sua coleta, tratamento e armazenamento[236].

Diante disso, criou-se uma categoria para esse tipo de dados pessoais, à qual se aplicam disciplinas específicas. Os dados pessoais cuja circulação apresenta elevado potencial lesivo aos seus titulares são classificados como "dados sensíveis".

A esse respeito, a Lei Geral de Proteção de Dados Pessoais, em seu artigo 5º, II, dispõe que são sensíveis os dados pessoais 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.

---

[234] 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. 143.
[235] 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. 143.
[236] RODOTÀ, Stefano. **A vida na sociedade de vigilância – a privacidade hoje.** Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 96.

Por sua vez, o RGPD estabelece que merecem proteção específica os dados pessoais que sejam, por sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais[237].

No que diz respeito à delimitação dos dados sensíveis, surgem alguns questionamentos relevantes, máxime na atualidade, em que uma vasta quantidade de dados é tratada e analisada por algoritmos.

Nesse diapasão, indaga-se se um dado pessoal é sensível em si, isto é, apenas por se relacionar à origem étnica ou convicção religiosa de um indivíduo ou pela função que exerce. Ainda, deve-se buscar compreender se um dado deve ser considerado sensível pelo simples fato de se encaixar no rol do artigo 5º, II, da LGPD, independentemente do contexto em que está inserido e da finalidade para que será utilizado. Outrossim, impõe-se averiguar se na situação hipotética em que o dado pessoal, isoladamente, não disser respeito ao referido rol, mas, ao ser combinado com outros dados, for capaz de revelar informações sensíveis sobre seu titular, esse dado deverá ou não ser considerado sensível e, portanto, receber o tratamento diferenciado previsto na LGPD.

No escândalo da Cambrigde Analytica que foi tão noticiado em razão de supostamente ter influenciado as eleições americanas, os usuários do *Facebook* respondiam ao teste de personalidade *This is Your Digital Life*, que consistia em perguntas sobre os usuários serem ou não extrovertidos, vingativos, se concluíam os projetos que começavam, se estavam constantemente preocupados, se gostavam de arte, entre outras questões acerca dos gostos e hábitos pessoais. Posteriormente, os resultados obtidos eram combinados com os dados extraídos dos perfis e amizades do *Facebook*[238], que incluíam detalhes sobre a identidade das pessoas, como o nome, a profissão e o local de moradia, além da rede de contatos.

Segundo informações divulgadas na mídia, esse teste foi respondido por mais de 270 mil pessoas. Como os dados dos amigos dos participantes também foram coletados, mais de 50 milhões de usuários foram afetados. Esses dados, então, foram vendidos à Cambridge Analytica e utilizados para criar e catalogar perfis das pessoas, de modo a se direcionar, de

---

[237] Considerando 51 do RGPD. UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016**. Relativo à proteção de dados pessoais 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 Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679#d1e1554-1-1. Acesso em: 28 jun. 2020.

[238] O GLOBO. **Psicólogo que criou aplicativo da Cambridge Analytica acreditava que sistema era legal.** 21 mar. 2018. Disponível em: https://oglobo.globo.com/mundo/psicologo-que-criou-aplicativo-da-cambridge-analytica-acreditava-que-sistema-era-legal-22510640. Acesso em: 15 abr. 2020.

forma mais personalizada, materiais pró-Trump e mensagens contrárias à adversária dele[239]. Assim, os dados coletados, se considerados individualmente, não eram classificados como sensíveis, entretanto, foi possível fazer inferências sensíveis dos usuários do *Facebook* pelo contexto em que tais dados estavam inseridos[240].

Nesse mesma esteira, um estudo que analisou as interações dos usuários do *Facebook* por meio de curtidas em fotos, atualizações de *status* de amigos, páginas de produtos, esportes, músicos, livros e restaurantes concluiu que é possível inferir diversas informações sensíveis que os usuários acreditam ser privadas – como orientação sexual, etnia, opiniões religiosas e políticas e traços de personalidade – por meio de tais interações[241].

Outro estudo, realizado por pesquisadores da Universidade de *Stanford*, demonstrou que os metadados[242] do telefone de cada pessoa podem ser extremamente reveladores, permitindo uma série de inferências sensíveis a respeito das associações familiares, políticas, profissionais, religiosas e sexuais[243].

Nesse estudo, os participantes instalavam um aplicativo chamado *MetaPhone*, que enviava para os pesquisadores informações sobre o histórico de chamadas do usuários: números de telefone para quem os participantes ligaram, dia e horário das chamadas, quantas vezes ligaram para determinado número e quais as durações das chamadas. Em seguida, os pesquisadores combinaram os números de telefone destinatários da chamada com os diretórios públicos do *Yelp* e do *Google Places* para identificá-los. A partir disso, os pesquisadores conseguiram realizar uma série de inferências sensíveis acerca dos participantes.

Assim, por exemplo, se uma pessoa conversa durante muito tempo com uma instituição religiosa, é bem provável que ela professe determinada fé. Em outro exemplo, um participante conversou por muito tempo com o cardiologista, comunicou-se brevemente com

---

[239] BBC BRASIL. **Entenda o escândalo de uso político de dados que derrubou valor do *Facebook* e o colocou na mira de autoridades.** 20 mar. 2018. Disponível em: https://www.bbc.com/portuguese/internacional-43461751. Acesso em: 17 mar. 2020.

[240] Sobre o caso da Cambrigde Analytica, a Netflix lançou o documentário original "Privacidade Hackeada", que se encontra disponível na referida plataforma: https://www.netflix.com/br/title/80117542.

[241] KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. Private traits and atributes are precictable from digital records of human behavior. **PNAS,** Califórnia, vol. 110, n. 15, 9 abr. 2013. Disponível em: https://www.pnas.org/content/pnas/110/15/5802.full.pdf. Acesso em: 17 mar. 2020.

[242] Metadados são dados sobre os dados. MENEZES NETO, Elias J; MORAIS, José Luis B; BEZERRA, Tiago José S. L. O projeto de Lei de Proteção de Dados Pessoais (PL 5276/2016) no mundo do Big Data: o fenômeno da Dataveillance em relação à utilização de metadados e seu impacto nos direitos humanos. **Revista Brasileira de Políticas Públicas,** v. 7, n. 3, 2017. Disponível em: https://www.publicacoesacademicas.uniceub.br/RBPP/article/view/4840. Acesso em: 17 mar. 2020, p. 191.

[243] MAYER, Jonathan; MUTCHLER, Patrick. **MetaPhone:** The Sensivity of Telephone Metadata. 12 mar. 2014. Disponível em: http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/. Acesso em: 17 mar. 2020. No mencionado estudo, os dados seriam o conteúdo das ligações, os metadados seriam as informações sobre a chamada, como data e duração da ligação.

um laboratório médico, recebeu ligações de uma farmácia e fez breves telefonemas para um serviço relacionado a um dispositivo médico usado para monitorar a arritmia cardíaca. Os pesquisadores puderam confirmar que esse paciente realmente possuía um problema de saúde[244].

Os casos acima expostos demonstram que dados que, considerados isoladamente, não são classificados como sensíveis, ao serem analisados em conjunto desempenham tal função.

Entretanto, a Lei Geral de Proteção de Dados traz uma definição de dados sensíveis que não leva em consideração a função que o dado exerce no contexto em que está inserido. Ao contrário, traz um rol de dados que, historicamente e pela sua natureza, são informações que podem gerar discriminação.

Essa técnica legislativa falha tanto por deixar de fora outros dados que podem gerar discriminação, como os relacionados à situação socioeconômica, como por desconsiderar que a partir de dados pessoais não sensíveis podem-se fazer inferências sensíveis, máxime na sociedade da informação, na qual os algoritmos e a inteligência artificial ampliam sobremaneira a capacidade de análise de dados.

Como ensina Doneda, uma das críticas que a elaboração dessa categoria de dados sofre é a de que seria impossível definir antecipadamente os efeitos do tratamento de informação, independentemente de sua natureza. Assim, o dado em si não é perigoso ou discriminatório, mas sim o uso que dele se faz[245].

A esse respeito, Mendes afirma que dados aparentemente insignificantes podem se tornar sensíveis, a depender do tratamento a que são submetidos. “Trata-se, na realidade, de um tratamento sensível dos dados, que é capaz de transformar dados inofensivos em informações potencialmente discriminatórias”. Aduz, ainda, que não existem dados insignificantes no contexto do processamento eletrônico[246].

Conforme Ribeiro:

> Entende-se que a apreciação da natureza do dado sensível depende do tratamento automático que lhe é dado, por exemplo: um enfermeiro que presta apoio domiciliário a um idoso com a doença de Alzheimer incluindo a compra do medicamento com o seu cartão de débito e que o banco utiliza para construir o seu perfil de compras está a tratar dados sensíveis. A conexão entre o comprador e o

[244] MAYER, Jonathan; MUTCHLER, Patrick. **MetaPhone:** The Sensivity of Telephone Metadata. 12 mar. 2014. Disponível em: http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/. Acesso em: 17 mar. 2020.
[245] 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. 143-144.
[246] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 76.

> produto não parece evidente, dado que há uma aquisição por conta de outrem. O dado que originalmente não é sensível, que depois de recolhido e tratado tem um determinado valor econômico, pode transformar-se em dado sensível dependendo da natureza da comunicação, isto é, o enfermeiro que mais tarde se dirige ao banco para celebrar um contrato de mútuo para aquisição de habitação poderá ser confrontado com a recusa da celebração de um contrato de seguro associado ao mútuo devido à doença que foi incluída no seu perfil[247].

Tendo em vista os efeitos nefastos que o tratamento e a utilização inadequada de informações sensíveis podem trazer aos titulares dos dados, faz-se necessário que a classificação de um dado como sensível ou não seja dinâmica e contextual, considerando o uso que se fará dos dados e quais inferências se podem obter a partir deles.

Dessa forma, visando tutelar, ainda que parcialmente, esse tipo de situação, a Lei Geral de Proteção de Dados Pessoais, em seu artigo 11, § 1º, prevê que as disposições relativas ao tratamento de dados pessoais sensíveis, ressalvado o disposto em legislação específica, aplicam-se a qualquer tratamento de dados que, embora isoladamente não sejam sensíveis, acabem por revelar informações pessoais que o sejam.

Quanto à disciplina dos dados pessoais sensíveis, embora haja diferenças em cada ordenamento jurídico, costuma-se, de um modo geral, ou proibir o tratamento de tais dados, indicando as exceções em que o tratamento pode ocorrer, ou se permitir o tratamento desses dados, mas em hipóteses muito mais restritas que a dos demais dados pessoais e sob regras mais rígidas[248].

---

[247] RIBEIRO, Florbela da Graça Jorge da Silva. **O Tratamento de Dados Pessoais de Clientes para Marketing.** 2017. Dissertação (Mestrado em Direito – Especialidade em Ciências Jurídico-Políticas) – Departamento de Direito da Universidade Autônoma de Lisboa, Lisboa. Disponível em: https://www.academia.edu/33292289/
O_TRATAMENTO_DE_DADOS_PESSOAIS_DE_CLIENTES_PARA_MARKETING. Acesso em: 15 abr. 2020, p. 62.

[248] Nesse sentido, a Lei Francesa de Proteção de Dados Pessoais dispõe, em seu artigo 6º, I, que é proibido processar dados pessoais sensíveis, mas logo em seguida prevê exceções a tal proibição, conforme transcrição a seguir: Artigo 6. I.- É proibido processar dados pessoais que revelem alegada origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas ou a associação sindical de uma pessoa singular ou processar dados genéticos, dados biométricos com o objetivo de identificar exclusivamente uma pessoa natural, dados relacionados à saúde ou dados relacionados à vida sexual ou orientação sexual de uma pessoa singular. II.- As exceções à proibição mencionada em I são fixadas nas condições previstas no artigo 9, parágrafo 2, do Regulamento (UE) 2016/679, de 27 de abril de 2016 e por esta lei; III.- Da mesma forma, as operações de processamento, automatizadas ou não, justificadas pelo interesse público e autorizadas de acordo com os procedimentos previstos no II do artigo 31 e no artigo 32, não estão sujeitas à proibição prevista no I. (tradução nossa). FRANÇA. Le Service Public de La Diffusion Du Droit. **Loi nº 78/17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertes.** Version consolidée au 25 ma 2020. Disponível em: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460. Acesso em: 17 maio 2020.
Por sua vez, a Lei Federal de Proteção de Dados da Alemanha não proíbe, *a priori*, o tratamento de dados sensíveis; estabelece que o tratamento de categorias especiais de dados pessoais só deve ser permitido quando estritamente necessário ao desempenho das tarefas do responsável pelo tratamento.
No entanto, dispõe que, ocorrendo esse tratamento, deverão ser implementadas medidas adequadas a proteger os interesses do titular dos dados, tais como: a) requisitos específicos para a segurança dos dados ou monitoramento de proteção de dados; b) prazos especiais dentro dos quais os dados devem ser revisados quanto à relevância e à

O RGPD estabelece, como regra geral, a proibição de tratamento de dados pessoais sensíveis, entretanto, prevê algumas exceções a essa vedação, entre as quais se destacam: a) o fornecimento de consentimento explícito pelo titular dos dados e desde que o direito da União ou de um Estado-Membro não tenha previsto que a proibição não pode ser anulada pelo titular; b) o tratamento ser necessário para o cumprimento de obrigações legais, para o exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados, ou para proteger interesses vitais; c) o tratamento ser necessário por motivos de interesse público importante e desde que sejam previstas medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados.

A Lei Geral de Proteção de Dados Pessoais traz uma seção específica acerca das particularidades no tratamento desses dados, tornando mais restritas as hipóteses em que é lícito o referido tratamento e exigindo que, quando a base legal para o tratamento for o consentimento do titular, este seja fornecido de forma específica, destacada e para finalidades especificadas[249].

Ademais, a lei brasileira veda a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com o objetivo de obter vantagem econômica, salvo se referentes à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que seja em benefício do titular. Quanto aos demais dados sensíveis, a LGPD prevê que a sua comunicação ou o uso compartilhado entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação pela Autoridade Nacional de Proteção de Dados.

---

eliminação; c) restrições, dentro do próprio agente controlador, quanto ao acesso aos dados sensíveis; d) tratamento separado desses dados; e) pseudonimização e criptografia; f) códigos de conduta específicos para garantir o tratamento legal em caso de transferência ou processamento para outros fins. (ALEMANHA. Bundesministerium der Justiz und für Verbraucherschutz. **Federal Data Protection Act de 30 de junho de 2017 (Federal Law Gazette I, p. 2097),** com a última redação que lhe foi dada pelo artigo 12 da Lei de 20 de novembro de 2019 (Federal Law Gazette I, p. 1626). Disponível em: https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html. Acesso em: 15 mar. 2020).

[249] Art. 11. 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; II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: 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; 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 nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; 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 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 desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Apesar do potencial risco dos dados sensíveis, seria inviável a proibição total do tratamento desses dados, haja vista que muitas vezes se faz necessária a manipulação dessas informações, como para o desenvolvimento da atividade médica ou a execução de uma pesquisa científica que precise obter dados relacionados à saúde ou à opinião política dos indivíduos, entre tantas outras finalidades bastante úteis à sociedade.

3.1.3 Tratamento de dados pessoais e agentes de tratamento

Como visto, um dado pessoal não é, por si mesmo, valioso, porquanto o seu valor é determinado pelo uso que se pode fazer dele. Para tanto, o dado deve passar por um processo no qual será manipulado para determinados fins. Nesse sentido, o dado pessoal passa por uma série de procedimentos que vão desde a sua coleta, até a sua transferência, passando pelo seu armazenamento e processamento. Essas operações são formas de tratar o dado.

Mendes ensina que a expressão "tratamento de dados pessoais" é utilizada "para designar as operações técnicas que podem ser efetuadas sobre os dados pessoais, de modo informatizado ou não, com a finalidade de se refinar a informação, tornando-a mais valiosa ou útil". Portanto, o tratamento de dados possui um viés dinâmico[250].

A Lei Geral de Proteção de Dados Pessoais exemplifica quais seriam esses procedimentos, ao definir, em seu artigo 5º, tratamento como toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Definição bastante semelhante é a trazida pelo Regulamento Geral de Proteção de Dados da União Europeia, diferenciando-se apenas por destacar que as operações podem ser efetuadas por meios automatizados ou não[251].

O tratamento dos dados pessoais deve respeitar os direitos dos titulares, a boa-fé e os princípios doutrinariamente já consolidados no que diz respeito à proteção dos dados pessoais, os quais serão estudados mais adiante. Dispõe o RGPD que "o tratamento dos dados

---

[250] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 58.

[251] Artigo 4º **Definições.** Para efeitos do presente regulamento, entende-se por: [...] 2) "Tratamento", uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

pessoais deverá ser concebido para servir às pessoas"[252] e não o contrário. Para que o tratamento de dados pessoais seja considerado lícito, deve ser realizado com base no consentimento do titular ou em outro fundamento legítimo[253].

A LGPD prevê que o tratamento de dados pessoais somente poderá ser realizado: a) mediante o fornecimento de consentimento pelo titular; b) para o cumprimento de obrigação legal ou regulatória pelo controlador; c) pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas; d) para a realização de estudos por órgão de pesquisa; e) quando necessário para a execução de contrato; f) para o exercício regular de direitos em processo judicial, administrativo ou arbitral; g) para a proteção da vida ou da incolumidade física do titular ou de terceiro; h) para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; i) quando necessário para atender aos interesses legítimos do controlador ou de terceiro; j) para a proteção do crédito.

O RGPD também prevê hipóteses semelhantes para a licitude do tratamento dos dados pessoais[254].

Como se observa, o consentimento possui bastante relevância no tratamento de dados, embora não seja a única hipótese que autoriza o processamento de dados, bem como não haja hierarquia entre tais hipóteses. Essa é uma característica não apenas da lei brasileira, mas das legislações de proteção de dados pessoais de um modo geral. A questão do consentimento será retomada adiante.

---

[252] Considerando 4, RGPD. UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016**. Relativo à proteção de dados pessoais 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 Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679#d1e1554-1-1. Acesso em: 28 jun. 2020.

[253] Considerando 40, RGPD. UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016**. Relativo à proteção de dados pessoais 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 Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679#d1e1554-1-1. Acesso em: 28 jun. 2020.

[254] Artigo *6º* **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; b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados; c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

Dispõe a LGPD que o tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar[255]. Não basta que o tratamento de dados pessoais seja realizado com base em fundamento previsto em lei; faz-se necessário que o agente de tratamento adote medidas adequadas a garantir a proteção dos dados pessoais contra riscos como o do vazamento das informações, o da reidentificação, o acesso não autorizado, bem como que adote práticas que visem à minoração de riscos em eventual violação de dados, como o armazenamento de dados criptografados ou pseudoanonimizados.

Tanto a LGPD quanto o Regulamento adotam a ideia da *privacy by design*, segundo a qual a proteção de dados deve ser observada desde a concepção do produto ou serviço até a sua execução, os quais devem ser "embarcados com tecnologias que facilitem o controle e a proteção das informações pessoais"[256].

Isso significa que a concepção deve antecipar e prevenir os riscos à privacidade. Além disso, a privacidade deve ser protegida por padrão (*privacy by default*), isto é, o indivíduo não deve ter de tomar nenhuma atitude para proteger sua privacidade, já que esse cuidado deve ser intrínseco ao sistema. Ainda, o agente de tratamento deverá tomar medidas de segurança adequadas a proteger a privacidade dos indivíduos durante todo o ciclo de vida dos dados[257].

Por essa razão, o RGPD estabelece que, antes do tratamento de dados pessoais de grande escala ou que impliquem um elevado risco para os direitos e liberdades dos titulares dos dados, o responsável pelo tratamento deverá proceder a uma avaliação do impacto sobre a proteção de dados, a fim de avaliar a probabilidade ou a gravidade particular do elevado risco, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento e as fontes do risco, incluindo as medidas, garantias e procedimentos previstos para atenuar esse risco e assegurar a proteção dos dados pessoais[258].

---

[255] Artigo 44, LGPD. BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 abr. 2020.

[256] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 176.

[257] SOUZA, Carlos Affonso Pereira de. Segurança e Sigilo dos Dados Pessoais: primeiras impressões à luz da Lei 13.709/2018. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coords.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** São Paulo: Thomson Reuters Brasil, 2019, p. 429.

[258] Considerando 90, RGPD. UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016**. Relativo à proteção de dados pessoais 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 Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679#d1e1554-1-1. Acesso em: 28 jun. 2020.

Ainda, prevê que a autoridade de controle deverá ser consultada antes de as atividades de tratamento terem início, sempre que a avaliação de impacto indicar que o tratamento implica um elevado risco para os direitos e liberdades das pessoas singulares e o responsável pelo tratamento considerar que o risco não poderá ser atenuado por meio de medidas razoáveis, atendendo à tecnologia disponível e aos custos de aplicação[259].

A LGPD tem norma parecida, dispondo, em seu artigo 38, que a autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente às suas operações de tratamento de dados.

Contudo, o relatório de impacto previsto na legislação brasileira não é, ao contrário do que estabelece o RGPD, uma obrigação que todo agente que realizar tratamento de uma grande quantidade de dados ou de informações de elevado risco potencial deva cumprir antes de iniciar as manipulações dos dados, havendo tão só a obrigação de elaborar o referido relatório, se requisitado pela Autoridade Nacional de Proteção de Dados. Apesar disso, é altamente recomendável que as organizações elaborem o relatório de maneira prévia, haja vista que o documento pode ser uma importante ferramenta para a implementação de medidas de proteção aos dados pessoais e à privacidade desde a concepção do produto ou serviço.

Os métodos de tratamento utilizados podem ser automatizados ou manuais. Além disso, podem ser operações necessárias às finalidades para a qual os dados foram coletados ou podem ser, ainda, operações que visam à proteção da privacidade dos titulares dos dados. Há tratamentos de dados que visam não a torná-los mais úteis, mas sim mais protegidos. Trata-se de procedimentos que eliminam ou modificam os atributos que podem identificar o titular dos dados pessoais, a exemplo da encriptação, da pseudonimização e da anonimização.

A criptografia pode ser definida como uma técnica por meio da qual os dados são codificados e apenas aquele que tiver acesso à chave criptográfica pode decifrar aquela informação. No caso da criptografia ponta a ponta, somente o emissor e o destinatário têm acesso a essa chave e, em consequência, apenas eles podem ter acesso às informações enviadas e recebidas[260].

---

[259] Considerando 94, RGPD. UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016**. Relativo à proteção de dados pessoais 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 Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679#d1e1554-1-1. Acesso em: 28 jun. 2020.

[260] MACHADO, Diego; DONEDA, Danilo. Proteção de Dados Pessoais e Criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. **Revista dos Tribunais**, v. 998, Caderno Especial, p. 99-128, São Paulo: RT, dez. 2018. Disponível em: https://www.researchgate.net/publication/330401277_Protecao_de_dados_pessoais_e_criptografia_tecnologias_criptograficas_entre_anonimizacao_e_pseudonimizacao_de_dados. Acesso em: 17 abr. 2020, p. 114.

Já a pseudonimização é um instrumento utilizado para dificultar a identificação das pessoas quando do tratamento de dados pessoais[261]. Essa técnica se efetiva pela criação de pseudônimos, isto é, pela substituição de um atributo de um registro por outro[262]. Para que ocorra a pseudonimização, as informações do indivíduo não podem estar conectadas ao titular específico, a não ser que se recorra à utilização de informações suplementares, as quais devem ser mantidas separadas dos dados principais[263]. Entretanto, como há possibilidade de a identificação do titular vir a ocorrer, os dados pseudoanonimizados submetem-se ao regime de proteção conferido aos dados pessoais.

O uso da criptografia e da pseudoanonimização é bastante incentivado, já que podem auxiliar na proteção à privacidade. Já a anonimização é um processo que retira a identificabilidade do dado e, por essa razão, afasta a incidência das legislações sobre a proteção de dados pessoais, conforme se verá.

No que toca ao término do tratamento de dados pessoais, segundo a Lei Geral de Proteção de Dados Pessoais este ocorrerá quando: a) sua finalidade for alcançada; b) os dados deixarem de ser necessários ou pertinentes ao alcance da finalidade específica almejada; c) encerrar o período de tratamento; d) o titular revogar o consentimento; e) houver determinação da autoridade nacional, decorrente de violação da lei. Uma vez encerrado o tratamento, os dados pessoais deverão ser eliminados, sendo autorizada a conservação para as finalidades específicas previstas na LGPD.

No que diz respeito aos agentes envolvidos no tratamento de dados pessoais, a Lei Geral de Proteção de Dados os classifica em: a) controlador, entendido como a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; b) operador, que é definido pela lei como a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

---

[261] RIBEIRO, Florbela da Graça Jorge da Silva. **O Tratamento de Dados Pessoais de Clientes para Marketing.** 2017. Dissertação (Mestrado em Direito – Especialidade em Ciências Jurídico-Políticas) – Departamento de Direito da Universidade Autônoma de Lisboa, Lisboa. Disponível em: https://www.academia.edu/33292289/
O_TRATAMENTO_DE_DADOS_PESSOAIS_DE_CLIENTES_PARA_MARKETING. Acesso em: 15 abr. 2020, p. 59-60.

[262] GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29º. **Parecer 5/2014 sobre as técnicas de anonimização.** 10 abr. 2014. Disponível em: https://www.gpdp.gov.mo/uploadfile/2016/0831/20160831042518381.pdf. Acesso em: 17 mar. 2020, p. 22.

[263] MACHADO, Diego; DONEDA, Danilo. Proteção de Dados Pessoais e Criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. **Revista dos Tribunais**, v. 998, Caderno Especial, p. 99-128, São Paulo: RT, dez. 2018. Disponível em: https://www.researchgate.net/publication/330401277_
Protecao_de_dados_pessoais_e_criptografia_tecnologias_criptograficas_entre_anonimizacao_e_pseudonimizacao_de_dados. Acesso em: 17 ar. 2020, p. 112-113.

O Regulamento da União Europeia também faz uma classificação semelhante, contudo, além de designações diferentes, as definições dos agentes de tratamento são mais amplas, de modo a ser menos suscetível, na prática, de gerar dúvidas acerca da caracterização ou não de determinado ente como um dos referidos agentes[264].

Essa classificação repercutirá na responsabilização civil, uma vez que tanto a Lei Geral de Proteção de Dados Pessoais quanto o RGPD responsabilizam os respectivos agentes de tratamento de formas distintas, como será visto adiante.

3.1.4 Dados anonimizados

A maior parte das legislações sobre proteção de dados exige o consentimento do titular para que os dados sejam objeto de tratamento[265]. Aquele que pretende armazenar, tratar os dados pessoais e compartilhá-los deverá obter consentimento expresso dos titulares das informações. Na atualidade, em que a produção e o fluxo de dados são imensos, atender a essa obrigação nem sempre será tarefa fácil.

A anonimização consiste na remoção ou na ofuscação de toda a informação pessoal de uma base de dados, com o objetivo de impedir a identificação dos indivíduos. Aplicam-se técnicas que pretendem tornar impraticável a reidentificação do titular, inclusive pelo próprio técnico que realizou a operação[266]. Considera-se anônimo aquele dado que seja "incapaz de revelar a identidade de uma pessoa"[267].

A anonimização desponta como uma importante alternativa àqueles que precisarem coletar e tratar dados pessoais. Isso porque a Lei Geral de Proteção de Dados, em seu artigo 12, estabelece que os dados anonimizados não serão considerados dados pessoais para os fins da lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido,

---

[264] Artigo 4º Definições. [...]. 7) "Responsável pelo tratamento", a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro; 8) "Subcontratante", uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes.

[265] Nesse sentido, artigo 7º, I, da Lei Geral de Proteção de Dados Pessoais. BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 abr. 2020.

[266] PINHO, Frederico A. S. O. **Anonimização de bases de dados empresariais de acordo com a nova Regulamentação Europeia de Proteção de Dados.** 2017. Dissertação (Mestrado em Segurança Informática), Departamento de Ciência de Computadores, Faculdade de Ciências, Universidade do Porto. Disponível em: https://cracs.fc.up.pt/sites/default/files/MSI_Dissertacao_FINAL.pdf. Acesso em: 17 mar. 2020, p. 29.

[267] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 70.

utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. Assim como a LGPD, a maioria das leis específicas sobre a proteção de dados pessoais dispõe que o seu âmbito de aplicação não abrange os dados anônimos.

A anonimização é um relevante mecanismo de proteção da privacidade dos indivíduos, além de que as pessoas podem se mostrar mais dispostas a revelar seus dados se elas acreditarem que estes serão anonimizados[268].

Assim, por décadas acreditou-se que a privacidade poderia ser protegida a partir do emprego de técnicas simples de anonimização, ao tempo que a utilidade dos dados seria preservada, de modo que hoje a anonimização é onipresente[269].

Nesse contexto, "a crença na idoneidade da anonimização [...] se espraia por diversos ordenamentos jurídicos, de sorte a tornar-se parte integrante de leis de proteção da privacidade e de dados pessoais mundo afora"[270]. Apesar disso, a anonimização não é livre de riscos. Dessa feita, enquanto alguns pesquisadores veem a anonimização como a chave para permitir o uso justo de dados pessoais, outros atentam para as suas falhas.

Os críticos da anonimização afirmam que uma base de dados anonimizados sempre poderá ser combinada com outras bases e essa agregação poderá levar à reidentificação dos dados. É o que se chama de entropia da informação[271].

A esse respeito, Bruno Bioni comenta que, com o crescimento da cultura do *open data*, nossas vidas têm sido cada vez mais datificadas e nossas informações, dispersas e publicamente acessíveis na rede. Além disso, a crescente interação das pessoas com o mundo *online* cria uma biografia digital de suas vidas, que é compartilhada com inúmeros indivíduos que fazem parte desses "relacionamentos *online*"[272].

Narayanan e Shmatikov afirmam que há um amplo espectro de características humanas que permitem reidentificação, como preferências de consumo, transações

---

[268] HARGITAI, Viktor; SHKLOVSKI, Irina; WASOWSKI, Andrzej. Going Beyond Obscurity: organizational approaches to Data Anonymization. **Proceedings of the ACM on Human-Computer Interaction,** vol. 2, n. XSCW, nov. 2018. Disponível em: https://dl.acm.org/citation.cfm?id=3274335. Acesso em: 17 abr. 2020, p. 68.

[269] OHM, Paul. Broken Promises of Privacy: responding to the surprising failure of anonymization. **UCLA Law Review,** n. 1.701, 2010. Disponível em: https://www.uclalawreview.org/pdf/57-6-3.pdf. Acesso em: 17 abr. 2020, p. 1.706.

[270] MACHADO, Diego. **Tutela jurídica da privacidade, anonimização de dados e anonimato na internet**. 2018. Disponível em: https://www.researchgate.net/publication/328784970_Tutela_juridica_da_privacidade_anonimizacao_de_dados_e_anonimato_na_internet. Acesso em: 17 abr. 2020, p. 276.

[271] OHM, Paul. Broken Promises of Privacy: responding to the surprising failure of anonymization. **UCLA Law Review,** n. 1701, 2010. Disponível em: https://www.uclalawreview.org/pdf/57-6-3.pdf. Acesso em: 17 abr. 2020, p. 1.749.

[272] BIONI, Bruno R. Xeque-Mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. **Privacidade e Vigilância,** USP, 2015. Disponível em: https://www.academia.edu/28752561/Xeque-Mate_o_trip%C3%A9_de_prote%C3%A7%C3%A3o_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil. Acesso em: 17 abr. 2020, p. 29.

comerciais, navegação na *web* e históricos de pesquisa, os livros que uma pessoa leu ou até mesmo as roupas em seu guarda-roupa: "embora nenhum elemento seja um (quase) identificador, qualquer subconjunto suficientemente grande identifica exclusivamente o indivíduo"[273].

Ohm alerta para o problema que ele denomina de *"accretion problem"*: uma vez que um adversário[274] tenha vinculado dois bancos de dados anonimizados, ele pode utilizar essas novas informações para abrir outros bancos de dados anônimos. Por conseguinte, eventos de reidentificação que exponham apenas informações não sensíveis também devem ser objeto de preocupação, haja vista que tais informações aumentam a capacidade de vinculação dos dados, o que expõe as pessoas a um potencial dano futuro[275].

Para ilustrar como os dados anonimizados são suscetíveis de reidentificação, apresentam-se alguns casos a seguir.

No ano de 2006, a *Netflix* lançou o *NetflixPrize*, por meio do qual oferecia um prêmio no valor de $ 1.000.000,00 (um milhão de dólares), desafiando os concorrentes a aprimorarem seu algoritmo de recomendação de filmes (*Cinematch*). Para a realização da competição, foram disponibilizadas avaliações de usuários dos serviços da empresa, coletados entre os anos de 1999 e 2005, os quais haviam sido submetidos à anonimização, segundo sua política de privacidade em vigor à época do tratamento dos dados[276].

Então, pesquisadores da Universidade do Texas cruzaram as informações disponibilizadas pela *Netflix* com os dados de outra plataforma de avaliação de filmes. Como resultado, o estudo pôde identificar 96% dos consumidores da *Netflix* cujos registros foram lançados no conjunto dos dados, de forma exclusiva. Para 64% desses usuários, o conhecimento de apenas duas das avaliações e data foi suficiente para a desanonimização total[277].

---

[273] NARAYANAN, Arvind; SHMATIKOV. Privacy and Security: myths and fallacies of "Personally Identifiable Information". **Comunicationofthe ACM,** vol. 53, n. 6, jun. 2010. Disponível em: https://pdfs.semanticscholar.org/44f3/2957fd4cdd2633b6d0cb744b3461f1b73124.pdf. Acesso em: 15 mar. 2020, p. 26.

[274] Essa é a expressão correntemente utilizada na literatura científica para designar aquele que busca a reidentificação.

[275] OHM, Paul. Broken Promises of Privacy: responding to the surprising failure of anonymization. **UCLA Law Review,** n. 1.701, 2010. Disponível em: https://www.uclalawreview.org/pdf/57-6-3.pdf. Acesso em: 17 abr. 2020, p. 1.746.

[276] NARAYANAN, Arvind; SHMATIKOV. Privacy and Security: myths and fallacies of "Personally Identifiable Information". **Comunicationofthe ACM,** vol. 53, n. 6, jun. 2010. Disponível em: https://pdfs.semanticscholar.org/44f3/2957fd4cdd2633b6d0cb744b3461f1b73124.pdf. Acesso em: 15 mar. 2020, p. 1.

[277] MACHADO, Diego. Tutela jurídica da privacidade, anonimização de dados e anonimato na internet. 2018. Disponível em: https://www.researchgate.net/publication/328784970_Tutela_juridica_da_privacidade_anonimizacao_de_dados_e_anonimato_na_internet. Acesso em: 17 abr. 2020, p. 277.

Outro estudo, realizado pelo Instituto Tecnológico de Massachusetts (MIT), visando verificar a efetividade da anonimização das informações contidas em metadados, demonstrou que as informações de quatro compras realizadas por meio de cartão de crédito são suficientes para reidentificar os indivíduos em 90% dos casos[278].

Já o estudo realizado por Sweeney, durante a década de 1990, cruzou informações anonimizadas de saúde da população estadunidense com uma lista de dados referentes a eleitores cadastrados para votar. A autora utilizou informações que estavam sendo comercializadas pela indústria de saúde, dados esses que não continham nomes, endereços ou número de Seguro Saúde dos indivíduos, mas continham informações sobre diagnósticos, DSTs, uso de drogas, além de data de nascimento, sexo e código postal[279].

O cruzamento de poucas características – código postal, data de nascimento e sexo – permitiu reidentificar os indivíduos, titulares dos dados pessoais de saúde, de forma simples e muito precisa, resultando na possibilidade de identificação dos titulares de dados pessoais anonimizados em 87% dos casos. A reidentificação foi possível em 50% dos casos apenas pela utilização de lugar, sexo e data de nascimento (sem código postal)[280].

Yakowitz, embora não negue o risco da reidentificação, afirma que a utilidade social dos dados é muito desvalorizada pelos estudiosos da privacidade, bem como que estes riscos são insignificantes, não havendo ocorrências conhecidas de reidentificação indevida de um conjunto de dados de pesquisa. Para a autora, os riscos relacionados aos dados anonimizados são menores que outros riscos relacionados à informação, como o vazamento de dados e a pirataria, riscos estes que, por conveniência, são tolerados[281].

Yakowitz aduz que quase todos os debates recentes sobre políticas públicas beneficiaram-se da disseminação em massa de dados anônimos, contudo, caso se presuma que a anonimização dos dados é impossível, o futuro dos dados abertos e toda a sua utilidade

---

[278] MONTJOYE, Yves-Alexandre; RADAELLI, Laura; SINGH, Vivek; PENTLAND, Alex. Unique in the shopping mall: On the reidentifiability of credit card metadata. **Science,** v. 347, n. 6221, jan. 2015. Disponível em: https://www.researchgate.net/publication/271591449_Unique_in_the_shopping_mall_On_the_reidentifiability_of_credit_card_metadata. Acesso em: 15 abr. 2020.

[279] FORD FOUNDATION. Advice to my younger self: Latanya Sweeney. **Ford Foundation,** 12 mar. 2019. Disponível em: https://www.fordfoundation.org/ideas/equals-change-blog/posts/advice-to-my-younger-self-latanya-sweeney/. Acesso em: 17 mar. 2020.

[280] SWEENEY, Latanya. Simple Demographics Often Identify People Uniquely. **Carnegie Mellon University,** Pitsburgh, 2000. Disponível em: https://dataprivacylab.org/projects/identifiability/paper1.pdf. Acesso em: 17 abr. 2020, p. 2.

[281] BAMBAUER, Jane R. Tragedy of the Data Commons. **Harvard Journal of Law and Technology,** vol. 25, 19 mar. 2011.Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1789749. Acesso em: 15 mar. 2020, p. 4.

social serão postos em questão, o que fará com que os indivíduos não queiram fornecer seus dados[282].

O Parecer 5/2014, do Grupo de Trabalho de Proteção de Dados do Artigo 29[283], assevera que nenhuma técnica analisada no documento satisfaz completamente os critérios de anonimização eficaz, entretanto, os resultados das técnicas podem ser robustecidos por meio de um planejamento meticuloso na definição de qual técnica será utilizada, tendo em vista as peculiaridades da situação específica, bem como por meio da combinação de técnicas[284]. Conclui que "as técnicas de anonimização podem fornecer garantias de privacidade e podem ser utilizadas para gerar processos eficazes de anonimização, mas apenas se a sua aplicação for adequadamente construída"[285].

As legislações e os debates jurídicos sobre proteção de dados não têm ficado alheios aos riscos da reidentificação dos dados anonimizados, assim como também não são desprezados todos os benefícios que os dados anônimos proporcionam à sociedade. Tanto a LGPD quanto o RGPD buscaram equilibrar essa questão a partir do critério da razoabilidade dos meios que podem ser utilizados para a reversão do processo de anonimização.

Dessa feita, "a função da anonimização deixa de ser determinada pela lógica do tudo ou nada",[286] de forma que não é a aplicação de uma técnica de anonimização que, por si só, dispensará a aplicação das normas de proteção de dados. Havendo potencial identificabilidade do titular dos dados diante dos meios existentes de serem razoavelmente utilizados para tanto, o ente responsável deverá cumprir os princípios e regras do direito de proteção dos dados pessoais[287].

---

[282] BAMBAUER, Jane R. Tragedy of the Data Commons. **Harvard Journal of Law and Technology,** vol. 25, 19 mar. 2011.Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1789749. Acesso em: 15 mar. 2020, p. 9.

[283] O Grupo de Trabalho do Artigo 29 da Diretiva 95/46/CE era um órgão consultivo europeu independente em matéria de proteção de dados e privacidade, cuja criação estava prevista no artigo 29 da mencionada Diretiva. O Grupo do Artigo 29 deixou de existir em 25 de maio de 2018 e foi substituído pelo Conselho Europeu de Proteção de Dados (EDPB), estabelecido pelo RGPD. Os documentos do Grupo de Trabalho do Artigo 29 podem ser encontrados em: https://ec.europa.eu/newsroom/article29/news-overview.cfm.

[284] GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29º. **Parecer 5/2014 sobre as técnicas de anonimização.** 10 abr. 2014. Disponível em: https://www.gpdp.gov.mo/uploadfile/2016/0831/20160831042518381.pdf. Acesso em: 17 mar. 2020, p. 26.

[285] GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29º. **Parecer 5/2014 sobre as técnicas de anonimização.** 10 abr. 2014. Disponível em: https://www.gpdp.gov.mo/uploadfile/2016/0831/20160831042518381.pdf. Acesso em: 17 mar. 2020, p. 3-4.

[286] MACHADO, Diego. **Tutela jurídica da privacidade, anonimização de dados e anonimato na internet**. 2018. Disponível em: https://www.researchgate.net/publication/328784970_Tutela_juridica_da_privacidade_anonimizacao_de_dados_e_anonimato_na_internet. Acesso em: 17 abr. 2020, p. 282.

[287] MACHADO, Diego. **Tutela jurídica da privacidade, anonimização de dados e anonimato na internet**. 2018. Disponível em: https://www.researchgate.net/publication/328784970_Tutela_juridica_da_privacidade_anonimizacao_de_dados_e_anonimato_na_internet. Acesso em: 17 abr. 2020, p. 282.

Nesse sentido, a Lei Geral de Proteção de Dados Pessoais reconhece que as técnicas de anonimização são, em algum grau, falíveis, de modo que sempre existirá a possibilidade de que um dado seja atrelado a um indivíduo específico. No entanto, uma vez que esse fato poderia expandir imensuravelmente o espectro de incidência do conceito amplo de dados pessoais, há a necessidade de se estabelecer um filtro a fim de que nem toda e qualquer possibilidade seja suficiente para que se considere o dado identificável e, portanto, pessoal[288].

Uma lei cujo conceito de dado pessoal se expandisse de tal forma tornar-se-ia "a lei de tudo", mas tornaria na prática muito difícil o seu cumprimento. Se não houvesse esse filtro, isso significaria que não existiriam dados anônimos, o que, como já visto, implicaria grandes obstáculos aos avanços tecnológicos e às vantagens que estes podem proporcionar ao desenvolvimento da sociedade.

A Lei 13.709/2018 estabelece que a determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios. Definição semelhante é adotada no Considerando 26 do Regulamento Geral de Proteção de Dados Pessoais[289].

O contexto e as circunstâncias de um caso concreto influenciam diretamente a identificabilidade. As ferramentas e as capacidades da tecnologia evoluem, razão por que não seria viável nem útil especificar, num rol taxativo, todas as hipóteses em que a identificação deixa de ser possível[290]. Não há uma unidade de medida para avaliar previamente o tempo ou o esforço necessário para a reidentificação após o tratamento dos dados[291].

Em face disso, a LGPD, em seu artigo 12, § 3º, estabeleceu que a autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar

---

[288] BIONI, Bruno R. Xeque-Mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. **Privacidade e Vigilância,** USP, 2015. Disponível em: https://www.academia.edu/28752561/Xeque-Mate_o_trip%C3%A9_de_prote%C3%A7%C3%A3o_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil. Acesso em: 17 abr. 2020, p. 32.

[289] (26) [...] Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica [...].

[290] GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29º. **Parecer 5/2014 sobre as técnicas de anonimização.** 10 abr. 2014. Disponível em: https://www.gpdp.gov.mo/uploadfile/2016/0831/20160831042518381.pdf. Acesso em: 17 mar. 2020, p. 9.

[291] GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29º. **Parecer 5/2014 sobre as técnicas de anonimização.** 10 abr. 2014. Disponível em: https://www.gpdp.gov.mo/uploadfile/2016/0831/20160831042518381.pdf. Acesso em: 17 mar. 2020, p. 30.

verificações acerca de sua segurança. Assim, na LGPD, quem dirá o que é ou não razoável será a Autoridade Nacional.

Uma vez que as evoluções tecnológicas podem tornar uma técnica de anonimização falha, permitindo que a identificabilidade aconteça sem maiores esforços, um dado anonimizado pode voltar a ser um dado pessoal. Por essa razão, a Autoridade Nacional, ao dispor sobre os padrões e técnicas utilizados em processos de anonimização, bem como ao realizar verificações acerca de sua segurança, deverá levar em conta que a caracterização de um dado como anonimizado deve ser contextual.

Assim, caberá à Autoridade Nacional estabelecer procedimentos capazes de identificar novos riscos de reidentificação, bem como reavaliar, regularmente, a razoabilidade de utilização dos meios para os riscos já identificados. Essas medidas são necessárias para que, ao se verificar que o risco de reidentificação não é mais tolerável, os dados sejam imediatamente considerados pessoais e a LGPD lhes seja aplicável, permitindo que a privacidade das pessoas continue segura mesmo com a evolução das tecnologias.

O Grupo de Trabalho de Proteção de Dados do Artigo 29 da Diretiva 95/46/CE, em seu Parecer 5/2014, sugere que, além dos meios, deve-se avaliar a probabilidade e a gravidade da identificação. Este Parecer apresenta uma importante reflexão acerca da obrigação do terceiro que fará o tratamento de dados anonimizados: ele deve considerar os fatores contextuais e circunstanciais, incluindo as características específicas das técnicas de anonimização de dados pessoais aplicadas pelo responsável pelo tratamento de dados inicial, ao decidir como utilizar e, em especial, combinar tais dados anonimizados para fins próprios, de modo que sempre que tais fatores e características implicarem um risco inaceitável de identificação dos titulares dos dados, o tratamento deverá sujeitar-se à legislação de proteção de dados[292].

Por fim, cabe aqui uma crítica. Tendo em vista os riscos inerentes à anonimização, excluir os dados anonimizados de qualquer proteção conferida pela Lei Geral de Proteção de Dados Pessoais não se mostra a técnica legislativa mais adequada.

É claro que a exigência, sempre, do consentimento para a utilização dos dados anonimizados seria um entrave muito grande às inovações tecnológicas. Contudo, exigir dos responsáveis pelo tratamento de dados anônimos certas práticas conferiria mais proteção aos

[292] GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29º. **Parecer 05/2014 sobre as técnicas de anonimização.** 10 abr. 2014. Disponível em: https://www.gpdp.gov.mo/uploadfile/2016/0831/20160831042518381.pdf. Acesso em: 17 mar. 2020, p. 11.

direitos fundamentais tutelados pela LGPD, de forma a garantir mais efetividade da legislação sem obstaculizar os avanços tecnológicos.

Nesse sentido, a LGPD poderia ter previsto, no setor privado, a publicidade do compartilhamento e uso que se faz dos dados anônimos, para que as pessoas e a Autoridade Nacional pudessem ter ciência e controle do que acontece com os dados depois de anonimizados. Ademais, poderia ter exigido das organizações que manipulam dados anonimizados uma série de medidas para prevenir a reidentificação ou minimizar seus efeitos, responsabilizando os terceiros que lidassem com esses dados em caso de identificabilidade.

Entretanto, como a LGPD preferiu excluir os dados anonimizados de sua abrangência material, caberá à Autoridade Nacional, dentro de suas competências, adotar medidas que protejam os brasileiros dos riscos da reidentificação.

Uma vez entendidas as principais questões conceituais relacionadas ao direito à proteção de dados pessoais, passa-se, agora, ao estudo do desenvolvimento de tal direito ao longo das últimas décadas e do reconhecimento de sua fundamentalidade.

3.2 O direito à proteção de dados pessoais

Na sociedade da informação, como será mais bem detalhado adiante, o fornecimento de dados pessoais se torna, praticamente, uma exigência da vida moderna. Isso porque, como nas últimas décadas os equipamentos tecnológicos tornaram-se acessíveis à boa parte da população e das organizações empresárias, por menores que sejam, a maioria das relações negociais envolve o tratamento de informações pessoais, as quais são utilizadas das mais variadas formas, que vão desde o cumprimento de obrigações legais, como a emissão de uma nota fiscal, até a monetização de tais dados.

Assim, para ter acesso a uma grande quantidade de produtos e serviços, o indivíduo precisa fornecer seus dados, os quais se tornam bastante valiosos. De igual forma, para ter acesso a uma série de serviços estatais, esse fornecimento também é necessário.

Ocorre, ainda, que muitas vezes o indivíduo não tem completo conhecimento do tratamento que envolve seus dados: não sabe exatamente quais dados estão sendo coletados, para que serão utilizados e, muito menos, se serão compartilhados com os chamados “parceiros” das organizações. Dessa forma, muitas entidades tratam os dados pessoais, que chegam a se tornar o principal ativo de boa parte delas, como se fossem sua propriedade.

Nesse cenário, é importante apreender a natureza jurídica dos dados pessoais. Verificar se eles seriam uma “coisa”, um bem passível de comercialização e apropriação, de

modo que aquele que adquire a sua propriedade poderá usá-lo independentemente da vontade da pessoa à qual esse dado está vinculado, ou se, pelo contrário, seriam uma extensão da personalidade.

Ademais, indaga-se se existe no sistema jurídico brasileiro, um direito fundamental à proteção de dados pessoais, bem como se esse direito conferiria alguma forma de controle aos titulares das informações. Além disso, busca-se averiguar a forma como as legislações sobre a proteção de dados pessoais têm disciplinado a tutela dessas informações ao longo das últimas décadas.

Esses pontos serão objeto de análise nessa seção.

3.2.1 Natureza jurídica dos dados pessoais

No que diz respeito à natureza jurídica dos dados pessoais, há duas teses: uma realista, segundo a qual os dados seriam bens, e uma personalista, que defende que os dados pessoais são elementos da personalidade de cada indivíduo.

Conforme Rochfeld, entre aqueles que defendem a tese realista existem quatro posições. A primeira entende que cada indivíduo é proprietário de seus dados, podendo reivindicar seu uso, sua destinação e seu valor junto a um operador. Contudo, esta acepção falha ao transferir a responsabilidade de gestão e proteção de dados para o indivíduo, máxime quando se tem em conta que uma imensa quantidade de pessoas não tem conhecimento para gerenciar e proteger seus dados. Ademais, partindo-se dessa ideia, enquanto as grandes organizações aufeririam grande vantagem econômica com o uso desses dados, o benefício individual seria ínfimo, já que cada usuário teria direito a uma pequena receita apenas, na ordem de algumas dezenas de centavos[293]. Isso porque cada dado, individualmente, não tem valor econômico, uma vez que o dado tão somente adquire valor quando é refinado, analisado pelas organizações e em conjunto com os demais dados coletados e armazenados pelos empresários.

A segunda posição defende que os dados são *res nullius*, não pertencendo a ninguém até que sejam capturados. Desse modo, as organizações empresárias, ao capturarem os dados pessoais, destes se apropriariam e poderiam monetizá-los e utilizá-los como melhor lhes

[293] ROCHFELD, Judith. Como qualificar os dados pessoais? Uma perspectiva teórica e normativa da União Europeia em face dos gigantes da Internet. **Revista de Direito, Estado e Telecomunicações,** Brasília, v. 10, n. 1, p. 67, maio 2018. Disponível em: https://periodicos.unb.br/index.php/RDET/article/view/21500/19816. Acesso em: 16 abr. 2020.

aprouvesse[294]. Tal concepção não oferece proteção alguma à pessoa a quem os dados se relacionam.

A terceira posição compreende que os dados pessoais são uma "criação" da pessoa a quem eles se referem, de modo que esta, assim como qualquer autor quanto à propriedade intelectual, deve ser consultada e remunerada pelo uso de seus dados[295].

Por fim, a quarta posição defende que os dados pessoais são um bem de propriedade comum. Nessa percepção, os dados teriam um destino coletivo e seu uso seria o mais aberto possível, o que favoreceria a inovação e impediria a concentração dos dados nas mãos das grandes corporações. Essa concepção poderia ser utilizada como justificativa para, em nome do interesse coletivo, permitir o uso dos dados pessoais sem o consentimento do indivíduo[296].

As posições realistas supraexpostas desconsideram, ou ao menos deixam de dar a devida atenção, ao fato de que os dados pessoais podem revelar os aspectos mais íntimos da pessoa, mormente quando se trata de dados que podem levar à discriminação, como informações a respeito da origem racial ou étnica, convicção religiosa, opinião política, saúde ou vida sexual.

Quando se protegem os dados pessoais da coleta, tratamento, uso e circulação inadequados, não se está conferindo proteção aos dados por si mesmos, mas à pessoa a quem esses dados se relacionam, haja vista que o uso e a circulação inadequados não causarão danos aos dados pessoais em si, senão aos titulares desses dados.

A tese realista acerca dos dados pessoais, além de não atribuir a devida importância a tais dados enquanto componentes da identidade e da personalidade de cada pessoa, não lhes oferece proteção adequada, ignorando todos os riscos e potenciais danos e violações que envolvem a manipulação e o uso dos dados pessoais. Já a concepção personalista compreende o dado pessoal como elemento da própria personalidade do indivíduo.

---

[294] ROCHFELD, Judith. Como qualificar os dados pessoais? Uma perspectiva teórica e normativa da União Europeia em face dos gigantes da Internet. **Revista de Direito, Estado e Telecomunicações,** Brasília, v. 10, n. 1, p. 67, maio 2018. Disponível em: https://periodicos.unb.br/index.php/RDET/article/view/21500/19816. Acesso em: 16 abr. 2020.

[295] ROCHFELD, Judith. Como qualificar os dados pessoais? Uma perspectiva teórica e normativa da União Europeia em face dos gigantes da Internet. **Revista de Direito, Estado e Telecomunicações,** Brasília, v. 10, n. 1, p. 68, maio 2018. Disponível em: https://periodicos.unb.br/index.php/RDET/article/view/21500/19816. Acesso em: 16 abr. 2020.

[296] ROCHFELD, Judith. Como qualificar os dados pessoais? Uma perspectiva teórica e normativa da União Europeia em face dos gigantes da Internet. **Revista de Direito, Estado e Telecomunicações,** Brasília, v. 10, n. 1, p. 69, maio 2018. Disponível em: https://periodicos.unb.br/index.php/RDET/article/view/21500/19816. Acesso em: 16 abr. 2020.

Miranda define os direitos da personalidade como todos aqueles "necessários à realização da personalidade e à sua inserção nas relações jurídicas"[297], podendo-se entender a personalidade como o conjunto de características e atributos da pessoa humana, a qual é objeto de proteção do ordenamento jurídico[298].

Os direitos da personalidade são aqueles que, tomando o homem como objeto de direitos sobre si mesmo e suas projeções na sociedade, permitem-lhe manter e desenvolver suas potencialidades, tanto individuais quanto sociais, para que alcancem suas respectivas metas[299].

A esse respeito, Mendes afirma que a informação pessoal possui um vínculo objetivo com a pessoa, revelando aspectos que lhe dizem respeito e, justamente por isso, diferenciam-se das demais informações[300]. Dessa forma, uma vez que o objeto dos dados pessoais é a própria pessoa, "a informação [pessoal] é um atributo da personalidade"[301].

Não é difícil perceber como os dados pessoais são uma exteriorização daqueles elementos que compõem a personalidade do indivíduo, tais quais a sua imagem, suas opiniões políticas, sua condição de saúde, seus gostos e desejos de consumo.

Por exemplo, no momento em que o indivíduo busca atendimento em um estabelecimento de saúde, tendo ali seus dados coletados e registrados, os quais indicam seu nome, endereço, seus sintomas e o diagnóstico de uma eventual enfermidade, esses dados exteriorizam aspectos da própria pessoa. De igual forma, quando alguém adquire produtos num *site* de compras, os dados sobre a transação representam os gostos, as necessidades e os desejos da pessoa naquele momento. As postagens dos usuários são o exemplo mais significativo de como projetamos a nós mesmos por meio dos dados pessoais.

Na "sociedade da Informação, a representação da pessoa em informações é a própria pessoa que se conhece *a priori*, eis que é primeiramente representada por informações"[302], de modo que, ainda que o dado possa dissociar-se do indivíduo e circular pela *internet*, sendo um

---

[297] MIRANDA, Francisco Cavalcanti Pontes de. **Tratado de Direito Privado.** Tomo VII – Parte Especial – Direito de Personalidade. Direito de família: direito matrimonial. São Paulo: Bookseller, 2003. [Livro Digital], p. 38.

[298] TEPEDINO, Gustavo. A tutela da personalidade no ordenamento civil constitucional brasileiro. *In*: TEPEDINO, Gustavo. **Temas de Direito Civil.** 2. ed. Rio de Janeiro:Renovar, 2001, p. 27.

[299] BITTAR, Carlos Alberto. **Reparação Civil por Danos Morais**. 4. ed. São Paulo: Saraiva, 2015, p. 236.

[300] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 56.

[301] CATALA, Pierre. Ebauche d'une théorie juridique de l'information**. Informatica e Diritto,** n. 01, v. 15, 1983. Disponível em: http://www.ittig.cnr.it/EditoriaServizi/AttivitaEditoriale/InformaticaEDiritto/1983_01_015-031_Catala.pdf. Acesso em: 15 mar. 2020, p. 20.

[302] PEZZELLA, Maria Cristina Cereser; GHISI, Silvano. A manipulação de dados pessoais nas relações de consumo e o sistema "*crediscore*". **Civilista.com,** ano 4, n. 1, 2015. Disponível em: http://civilistica.com/a-manipulacao-de-dados-pessoais/. Acesso em: 17 abr. 2020, p. 19.

dado pessoal e, portanto, permanecendo com a qualidade de identificação de um indivíduo, deve ser entendido como uma extensão da personalidade[303]. É por isso que Rodotà afirma que o direito à proteção de dados relaciona-se com a proteção da personalidade e não da propriedade[304].

Atualmente a sociedade movimenta-se a partir dos "signos identificadores" do indivíduo, os quais constituem verdadeiros "dossiês digitais", que devem externar informações corretas para que a identidade do titular dos dados seja fidedignamente projetada. Dessa forma, um dado, para ser pessoal, deve ser caracterizado "como uma projeção, extensão ou dimensão do seu titular", o que justifica "dogmaticamente a inserção dos dados pessoais na categoria dos direitos da personalidade", assegurando direitos ao indivíduo que permitam uma projeção precisa desse novo tipo de identidade, como o direito de retificação, por exemplo[305].

Proteger esses dados é fundamental para garantir o livre desenvolvimento da personalidade das pessoas a quem tais dados se referem. Se os dados dos indivíduos pudessem ser compartilhados e utilizados sem nenhuma limitação por aqueles que o coletam, as pessoas não se sentiriam seguras para agir livremente, distantes da pressão social.

Assim, é provável que os produtos adquiridos no *e-commerce*, os *sites* visitados, as buscas realizadas na *internet*, os aplicativos utilizados, enfim, os dados que produzidos diariamente, que identificam e exteriorizam quem se é, fossem diferentes, haja vista que sempre se estaria preocupado com o julgamento social que se sofreria a partir dessas informações. A tutela desses dados pessoais oferece certa segurança às pessoas para que estas possam agir com liberdade, ainda que para isso precisem fornecer seus dados, já que estes estarão protegidos da exposição indevida.

Nesse cenário, tutelam-se os dados pessoais para proteger a pessoa que é seu titular, máxime quando se tem em mente que tais dados podem representar os aspectos mais íntimos do indivíduo. Entende-se que a natureza jurídica dos dados pessoais é de atributo da própria personalidade do indivíduo, de modo que a concepção personalista desses dados é a mais adequada, além de permitir que a dignidade da pessoa humana seja tutelada de maneira mais efetiva, o que não se verifica quanto às teorias realistas.

---

[303] PASSOS, Bruno Ricardo dos Santos. **O Direito à Privacidade e a Proteção aos Dados Pessoais na Sociedade da Informação:** uma abordagem acerca de um novo direito fundamental. 2017. Dissertação (Mestrado em Direito Público) – Programa de Pós-Graduação em Direito da Universidade Federal da Bahia, Salvador. Disponível em: https://repositorio.ufba.br/ri/handle/ri/22478. Acesso em: 17 mar. 2020.

[304] RODOTÀ, Stefano. **A vida na sociedade de vigilância – a privacidade hoje.** Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 97.

[305] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 65.

Importa ressaltar que existe certa preocupação de que essa visão personalista dos dados pessoais impeça o desenvolvimento da economia digital, haja vista que os direitos da personalidade são indisponíveis. Entretanto, é possível que o indivíduo conceda a terceiros o direito de usar seus dados pessoais, como acontece com os direitos de imagem, o que deve acontecer por meio do consentimento informado, afirmando-se a autodeterminação informativa do titular dos dados e respeitando-se seus direitos fundamentais.

Verificada a natureza jurídica dos dados pessoais, investiga-se agora como essas informações são protegidas em nível constitucional, haja vista que, uma vez que o direito à proteção de dados se destina à tutela da própria pessoa, importante se faz reconhecer a fundamentalidade de tal direito, buscando-se evitar sua disciplina somente no nível infraconstitucional, o que o colocaria em posição hierárquica inferior em relação às demais liberdades fundamentais.

3.2.2 A proteção de dados pessoais como direito fundamental: enquadramento constitucional

A Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, de 1981, é considerada um importante marco no reconhecimento do direito à proteção de dados como fundamental por ser uma das primeiras que, em seu preâmbulo[306], entende a proteção de dados como um pressuposto do Estado democrático e, por isso, relaciona-se com a proteção dos direitos humanos e das liberdades fundamentais[307].

O objetivo da Convenção é garantir, no território de cada Parte, para cada indivíduo, qualquer que seja sua nacionalidade ou residência, que o processamento automático de dados pessoais não viole seus direitos e liberdades fundamentais, bem como conciliar o respeito à privacidade e o livre fluxo de informações.

---

[306] "Os Estados-membros do Conselho da Europa, signatários da presente Convenção: Considerando que a finalidade do Conselho da Europa é conseguir uma união mais estreita entre os seus membros, nomeadamente no respeito pela supremacia do direito, bem como dos direitos do homem e das liberdades fundamentais; Considerando desejável alargar a proteção dos direitos e das liberdades fundamentais de todas as pessoas, nomeadamente o direito ao respeito pela vida privada, tendo em consideração o fluxo crescente, através das fronteiras, de dados de carácter pessoal susceptíveis de tratamento automatizado; [...]".
CONSELHO DA EUROPA PARA A PROTEÇÃO DAS PESSOAS SINGULARES. **Convenção nº 108, de 1981.** Tratamento Automatizado de Dados Pessoais. Disponível em: https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm. Acesso em: 25 abr. 2020.

[307] DONEDA, Danilo. A Proteção dos Dados Pessoais como um Direito Fundamental. **Espaço Jurídico,** Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: https://dialnet.unirioja.es/descarga/articulo/4555153.pdf. Acesso em: 17 abr. 2020, p. 102.

A referida Convenção foi ratificada por todos os Estados-Membros da União Europeia. Além disso, a Convenção 108 prevê a possibilidade de que Estados que não sejam membros do Conselho da Europa possam ela aderir, o que permitiu a países como Argentina, Cabo Verde, México, e Uruguai ratificarem-na mais recentemente[308]. O Brasil ainda não a ratificou.

Apesar disso, o Brasil firmou, em 15 de novembro de 2003, na XIII Cúpula Ibero-Americana de Chefes de Estado e de Governo, a Declaração de Santa Cruz de La Sierra, na qual se lê:

> 45. Da mesma forma, somos conscientes de que a proteção de dados pessoais é um direito fundamental das pessoas e destacamos a importância das iniciativas regulatórias ibero-americanas para proteger a privacidade dos cidadãos, contidas na Declaração de Antigua, pela qual se cria a Rede Ibero-Americana de Proteção de Dados, aberta a todos os países de nossa Comunidade[309].

Um pouco antes, em junho desse ano, o Brasil já havia firmado a Declaração de Antigua[310], pela qual reconheceu, juntamente com os demais participantes[311] do II Encontro Ibero-Americano de Proteção de Dados, que a proteção de dados pessoais é um verdadeiro direito fundamental das pessoas, "especialmente a fim de respeitar sua privacidade e sua capacidade de controle e disposição sobre eles".

Por essa razão, a referida Declaração criou a Rede Ibero-Americana de Proteção de Dados. O documento reconhece que o direito à proteção de dados pessoais fortalece o Estado de direito e ajuda a fortalecer a democracia nos países ibero-americanos, bem como seu prestígio e credibilidade num mundo globalizado.

Verifica-se, assim, que também no Brasil a proteção de dados pessoais é vista como um direito fundamental. No entanto, existe na doutrina uma discussão acerca da autonomia desse direito.

A primeira corrente entende que o direito à proteção de dados pessoais encontra guarida no direito à privacidade. Dessa forma, estaria tutelado por diversos documentos

---

[308] CONSELHO DA EUROPA. **Carta de Assinaturas e Ratificações do Tratado 108.** Convenção para a proteção de indivíduos no que diz respeito ao processamento automático de dados pessoais. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=GGLmmfdZ. Acesso em: 17 abr. 2020.

[309] BOLÍVIA. **Declaración de Santa Cruz de la Sierra.** XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno. 14 y 15 de noviembre 2003. Disponível em: https://www.segib.org/wp-content/uploads/DeclaraciondeSantaCruz.pdf. Acesso em: 15 abr. 2020.

[310] GUATEMALA. **Declaración de La Antigua.** II Encuentro Iberoamericano de Protección de Datos. 2003. Disponível em: https://www.redipd.org/sites/default/files/inline-files/declaracion_2003_II_encuentro_es.pdf. Acesso em: 17 abr. 2020.

[311] Argentina, Brasil, Chile, Colômbia, Costa Rica, Equador, El Salvador, Espanha, Guatemala, México, Nicarágua, Paraguai, Peru, Portugal e Uruguai.

internacionais, a exemplo da Declaração Universal dos Direitos do Homem e do Pacto Internacional sobre os Direitos Civis e Políticos, bem como pelas disposições constitucionais que protegem a privacidade.

Nessa senda, Mendes aduz que, no Brasil, o conceito de privacidade evoluiu, passando a abarcar a proteção de dados pessoais. Dessa feita, reconhece-se o direito fundamental à proteção de dados pessoais como uma dimensão da inviolabilidade dos direitos previstos pelo artigo 5º, X, da Constituição brasileira, quais sejam: intimidade e vida privada[312].

Também Mulholland entende que, muito embora a Constituição brasileira não preveja, expressamente, o direito à proteção de dados pessoais como uma categoria de direitos fundamentais, o lócus constitucional desse direito é a tutela da privacidade, que tem seu conceito ampliado em razão de a evolução das formas de divulgação e apreensão de dados pessoais ter expandido as formas potenciais de violação da esfera privada, máxime pelo acesso não autorizado de terceiros a esses dados[313].

Nessa mesma esteira, Schreiber observa que, diante do constante intercâmbio de informações, o direito à privacidade não pode se restringir à proteção da vida íntima, devendo abarcar também o direito do indivíduo de manter o controle sobre seus dados pessoais[314].

A jurisprudência do Tribunal de Justiça da União Europeia (TJUE) também não faz distinção entre esses dois direitos, entendendo que a "vida privada" inclui a proteção de dados pessoais, atribuindo, portanto, ampla interpretação àquele termo[315].

De igual forma, o Tribunal Europeu dos Direitos do Homem (TEDH) vem reconhecendo que, de acordo com uma interpretação dinâmica do direito ao respeito à vida privada e familiar, previsto no artigo 8º da Convenção Europeia dos Direitos do Homem (CEDH)[316], nesse direito se encontra o direito fundamental à proteção de dados pessoais[317].

---

[312] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 170-171.

[313] MULHOLLAND, Caitlin Sampaio. 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 Direitos e Garantias Fundamentais**, Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018. Disponível em: http://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603. Acesso em: 17 abr. 2020, p. 171-172.

[314] SCHREIBER, Anderson. **Direitos da Personalidade.** 3. ed. São Paulo: Atlas, 2014, p. 137.

[315] KOKOTT, Juliane; SOBOTTA, Christoph. The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR **International Data Privacy Law,** Oxford Academic**.** v. 3, n. 4, 15 set. 2013. Disponível em: https://academic.oup.com/idpl/article/3/4/222/727206. Acesso em: 17 abr. 2020.

[316] ARTIGO 8º Direito ao respeito pela vida privada e familiar. 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem - estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros. CONSELHO DA EUROPA. Corte Europeia de Direitos Humanos. **Convenção Europeia dos Direitos do Homem.** 4 nov. 1950. Disponível em: https://www.echr.coe.int/Documents/Convention_POR.pdf. Acesso em: 20 abr. 2020.

A segunda corrente defende a autonomia do direito à proteção de dados pessoais. Para essa posição, em suma, o direito à proteção de dados pessoais possuiria, no que se refere à tutela da informação, um escopo mais amplo que o direito à privacidade, pois tutelaria qualquer informação relacionada a uma pessoa, ainda que não esteja incluída no âmbito da vida privada[318].

Para Rodotà[319], a Carta de Direitos Fundamentais da União Europeia acertadamente distinguiu o direito à proteção de dados pessoais do direito à vida privada e familiar ao prever, em seu artigo 7º, que "Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações". Em seguida, estabelece que:

> Artigo 8º
> Proteção de dados pessoais
> 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
> 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação.
> 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente[320].

Rodotà defende que o direito à vida privada e familiar consiste em impedir a interferência alheia nesses âmbitos da vida de um indivíduo e, por conseguinte, reflete um componente mais individualista, sendo um tipo de proteção estático, negativo. Já o direito à proteção de dados pessoais estabelece regras sobre os mecanismos de processamento de dados e a legitimidade para que uma autoridade tome medidas em sua defesa. Este seria um tipo de proteção dinâmico, que segue o dado em todos os seus movimentos[321].

O autor defende que a autonomia da proteção de dados é o último ponto de uma longa evolução pela qual passou esse direito e que o separou da privacidade. Assim, entende que,

---

[317] MARTÍNEZ, Andrés García. **La Tutela Multinivel del Derecho a la Protección de Datos Personales del Contribuyente: TEDH-TJUE. AFDUAM,** n. 22, 2018. Disponível em: https://repositorio.uam.es/bitstream/handle/10486/690020/AFDUAM_22_19.pdf?sequence=1&isAllowed=y. Acesso em: 22 abr. 2020, p. 508-509.

[318] KOKOTT, Juliane; SOBOTTA, Christoph. The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR **International Data Privacy Law,** Oxford Academic**.** v. 3, n. 4, 15 set. 2013. Disponível em: https://academic.oup.com/idpl/article/3/4/222/727206. Acesso em: 17 abr. 2020.

[319] RODOTÀ, Stefano. **A vida na sociedade de vigilância – a privacidade hoje.** Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 16-17.

[320] UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia.** 07 jun. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR. Acesso em: 15 mar. 2020.

[321] RODOTÀ, Stefano. **A vida na sociedade de vigilância** – A privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 17.

para permitir uma proteção forte aos indivíduos, o direito à proteção de dados não deve ser considerado subordinado a nenhum outro, porque ele próprio "é um direito fundamental"[322].

Por sua vez, Doneda afirma que, no direito brasileiro, o reconhecimento da autonomia do direito à proteção de dados deriva da consideração dos riscos que o tratamento de dados, máxime o automatizado, "traz à proteção da personalidade à luz das garantias constitucionais de igualdade substancial, liberdade e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada"[323].

Para o autor, a Constituição brasileira tutelaria esse direito a partir da proteção à vida privada e à intimidade (art. 5º, X), da garantia ao sigilo das comunicações telefônicas, telegráficas ou de dados (art. 5º, XII), assim como por meio da ação de *habeas data*. Nessa senda, o direito à proteção de dados, apesar de autônomo, encontraria proteção constitucional, no Brasil, por estar diretamente relacionado àqueles dois direitos, bem como em razão de o tratamento inadequado de dados representar um risco a outros direitos fundamentais e à própria dignidade humana[324].

Em que pesem tais argumentos, neste trabalho comunga-se do entendimento, já exposto no capítulo anterior, de que o direito à privacidade é gênero dos quais são espécies vários direitos da mesma família, como o direito ao sigilo, o direito à intimidade e o direito à proteção dos dados pessoais.

Dessa forma, entende-se que, na sociedade da informação, a privacidade não mais se limita ao direito de ser deixado só, alcançando novos contornos, alicerçados no direito de cada indivíduo decidir quando e como dispor de suas informações.

Assim, o conceito de privacidade não se restringe a situações "íntimas", abrangendo também certos aspectos da vida e do comportamento em público. Por conseguinte, a corrente que defende a autonomia do direito à proteção de dados pessoais, por entender que este protege qualquer tipo de informação pessoal, inclusive as que não sejam de natureza privada, não se coaduna com a concepção atual de privacidade. É nesse contexto que, também no Brasil, o direito à proteção de dados é reconhecido como um direito fundamental.

Por fim, importa dizer que, em 2 de julho de 2019, foi aprovada no Senado Federal a Proposta de Emenda à Constituição nº 17/2019, que visa incluir a proteção de dados pessoais

---

[322] RODOTÀ, Stefano. **A vida na sociedade de vigilância** – A privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 18.

[323] DONEDA, Danilo. A Proteção dos Dados Pessoais como um Direito Fundamental. **Espaço Jurídico,** Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: https://dialnet.unirioja.es/descarga/articulo/4555153.pdf. Acesso em: 17 abr. 2020, p. 103.

[324] DONEDA, Danilo. A Proteção dos Dados Pessoais como um Direito Fundamental. **Espaço Jurídico,** Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: https://dialnet.unirioja.es/descarga/articulo/4555153.pdf. Acesso em: 17 abr. 2020.

entre os direitos fundamentais do cidadão elencados no artigo 5º da CF/1988. O texto agora tramita na Câmara dos Deputados[325].

Independentemente do enquadramento constitucional, a doutrina é unânime em afirmar que, diante dos riscos que o tratamento de dados representa ao livre desenvolvimento da personalidade, à dignidade da pessoa humana e a outros direitos fundamentais, o direito à proteção de dados pessoais deve ser entendido também como um direito fundamental.

Esse direito tem como principal base a autodeterminação informativa. Para se compreender o direito à proteção de dados pessoais, faz-se necessário entender o que é o direito à autodeterminação informativa, o que ele protege e como se efetiva.

3.2.3 Direito à autodeterminação informativa e consentimento

Como visto, a autodeterminação informativa foi reconhecida pela primeira vez em 1983, no julgamento acerca da inconstitucionalidade parcial da Lei do Censo (*Volkszählung)* pelo Tribunal Constitucional alemão[326].

A referida lei dispunha sobre a coleta de vários dados pessoais, inclusive dados sensíveis. Assim, questionavam-se os indivíduos acerca de seus nomes, endereço, conexão telefônica, data de nascimento, estado civil, religião, profissão, local de trabalho, dimensões da habitação, além de várias outras informações. Ademais, estabelecia que os cidadãos eram obrigados a fornecer seus dados, sob pena de multa. Ainda, previa que as informações do censo poderiam ser comparadas com os registros populacionais e usadas para corrigi-los, bem como possibilitava o compartilhamento das informações com órgãos públicos federais, desde que não identificados com o nome de cada titular.

Diante disso, foram ajuizadas reclamações constitucionais sob o argumento de que a Lei do censo violava o livre desenvolvimento da personalidade. Na decisão, o Tribunal Constitucional Federal alemão entendeu que, embora a lei fosse constitucional, alguns de seus dispositivos eram incompatíveis com a Lei Fundamental, razão por que eram inválidos

---

[325] Art. 1º Inclua-se no art. 5º da Constituição Federal o seguinte inciso XII-A: Art. 5° [...]. XII-A – é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais. [...]" . BRASIL. **Proposta de Emenda à Constituição nº 17, de 2017.** Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1567535523044&disposition=inline. Acesso em: 15 abr. 2020.

[326] TSCHENTSCHER, A; BROICHHAGEN, Seven. **Urteil des Ersten Senats vom 15 Dezember 1983 auf die mündliche Verhandlung vom 18 und 19 oktober in den Verfahren über die Verfassungsbeschwerden.** 1983. Disponível em: http://www.servat.unibe.ch/dfr/bv065001.html. Acesso em: 18 mar. 2020.

aqueles que previam a comparação dos dados informados com os registros populacionais e o compartilhamento das informações com outros órgãos.

Nesse diapasão, o Tribunal afirmou que, nas condições do processamento moderno de dados, a proteção dos indivíduos contra a coleta, armazenamento, uso e transferência ilimitados de seus dados pessoais é conferida pelos artigos da Lei Fundamental de Bonn que tutelam o livre desenvolvimento da personalidade e a dignidade humana, isso porque a manipulação irrestrita de dados permitiria a formação de um retrato completo do indivíduo, sem o seu conhecimento e, muito menos, participação.

A decisão também considerou que o uso para fins estatísticos e administrativos dos dados coletados no censo implicava uma diversidade de finalidades que impossibilitaria ao indivíduo tomar conhecimento da utilização efetiva de seus dados. Ademais, essas duas finalidades seriam inconciliáveis, uma vez que "o rigor estatístico não poderia coexistir com a necessidade dos órgãos administrativos de identificar os titulares destes dados". Nesse diapasão, o Tribunal reconheceu que a coleta e o tratamento de dados pessoais devem observar o princípio da finalidade[327].

A decisão entendeu não ser correta a ideia de que o tratamento de determinados dados pessoais não acarretaria prejuízos à privacidade, haja vista que na sociedade da informação não existem dados irrelevantes, pois um dado que é aparentemente sem importância, pode ser tratado e adquirir um novo valor. Mais do que a natureza do dado, dever-se-ia levar em consideração a sua necessidade e utilização diante da finalidade para a qual foi coletado.

Ainda, o Tribunal afirmou que, mesmo diante do atual desenvolvimento tecnológico, a autodeterminação individual pressupõe que o indivíduo seja livre para tomar decisões sobre suas informações, incluindo a possibilidade de agir de acordo com a forma com que realmente quer se comportar. Nessa senda, o direito à autodeterminação informacional não seria compatível com uma ordem social na qual os cidadãos não poderão mais saber o quê, quando e em que ocasião os outros conhecem informações a seu respeito.

Desse modo, se as pessoas não tiverem certeza sobre quais informações a elas relacionadas são conhecidas em determinadas áreas do ambiente social, elas podem ter sua liberdade de planejar ou tomar decisões significativamente restritas, já que qualquer pessoa que não tenha certeza se o comportamento desviante é anotado a qualquer momento e permanentemente armazenado, usado ou transmitido como informação, tentará não ser percebida por esse comportamento.

---

[327] 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. 167.

Por exemplo, quem espera que o fato de participar de uma reunião ou de alguma iniciativa de cidadania seja oficialmente registrado e que isso possa gerar riscos no exercício de seus direitos fundamentais, poderá abrir mão de tal participação. Isso prejudicaria não apenas as chances de desenvolvimento do indivíduo, mas também o bem comum, porque a autodeterminação é uma condição funcional elementar de uma comunidade democrática livre, baseada na capacidade de agir e na capacidade de ação de seus cidadãos.

Por essa razão, ficou consignado na decisão que todos os órgãos que coletam dados pessoais para executar suas tarefas deverão limitar-se ao mínimo necessário para atingir a meta estabelecida, bem como que, para assegurar o uso adequado dos dados pessoais, são essenciais garantias aos indivíduos como a informação acerca do tratamento de suas informações e a possibilidade de exclusão desses dados, quando o armazenamento não estiver legalmente respaldado.

Assim, na referida decisão, o Tribunal entendeu que o direito fundamental ao livre desenvolvimento demanda que se garanta ao indivíduo o direito de determinar a si mesmo, permitindo-lhe decidir sobre a divulgação e o uso de seus dados pessoais, ao que se chamou de "direito à autodeterminação informativa", direito este que só poderia sofrer restrições no interesse geral superior.

Essa decisão é considerada o marco em que surge a autodeterminação informativa, embora a ideia de um direito a controlar os dados pessoais já estivesse presente desde a década de 1970 na doutrina norte-americana, a exemplo de Alan Westin[328], que a essa época já entendia a privacidade como "o direito a controlar a maneira na qual os outros utilizam as informações a nosso respeito"[329].

Como consequência da decisão, em 1985 foi promulgada uma nova lei com o objetivo de sanar os pontos contestados, de modo que, no censo realizado em 1987, os dados para fins estatísticos eram separados das informações individuais, o cidadão era informado sobre as finalidades da coleta e a obrigação de fornecer os dados e a transferência de informações entre autoridades regionais foi vetada[330].

Além disso, o direito à autodeterminação informativa passou a exercer grande influência na tutela de informações pessoais em países do sistema jurídico romano-germânico,

---

[328] 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. 168.
[329] RODOTÀ, Stefano. **A vida na sociedade da vigilância –** a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 15.
[330] 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.168.

sendo, inclusive, um dos fundamentos da proteção de dados no Brasil, conforme previsto na Lei Geral de Proteção de Dados Pessoais[331].

Tamanha influência, bem como sua estreita ligação com o direito à privacidade e com o direito à proteção de dados pessoais, fez com que esses três conceitos muitas vezes sejam tratados como sinônimos. Entretanto, trata-se de direitos diferentes.

Como visto, a privacidade é um conceito dinâmico, que em sua atual concepção, é vista, além da sua concepção clássica de "direito a ser deixado em paz", também como "o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da esfera privada"[332].

Nessa esteira, como visto, o direito à privacidade é um termo guarda-chuva que abrange vários direitos da mesma família, tutelando diferentes aspectos da personalidade. A privacidade possui diferentes dimensões, como a espacial, a decisional e a informacional.

Essa última confere ao indivíduo o poder de controlar suas informações pessoais, decidindo acerca da concessão ou restrição do acesso de outras pessoas a tais informações. Já a dimensão decisional da privacidade tutela o modo de vida do indivíduo, seus gostos, seus projetos pessoais, suas características, suas escolhas e decisões.

Nesse contexto, o direito à autodeterminação informativa é uma espécie do direito à privacidade que se relaciona com suas dimensões informacional e decisional.

Já no que diz respeito ao direito à proteção de dados pessoais, Puccinelli afirma que este corresponde à soma de princípios, direitos e garantias estabelecidos em favor das pessoas que podem ser prejudicadas pelo tratamento dos dados pessoais, tendo como prioridade assegurar o equilíbrio de poderes e a participação democrática nos processos da informação e da comunicação por meio da disciplina dos sistemas de coleta, armazenamento e transmissão de dados[333].

Dessa feita, enquanto o direito à autodeterminação informativa corresponde ao poder do titular de decidir e consentir sobre o tratamento de dados pessoais, o direito à proteção de

---

[331] 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. 168-169.

[332] RODOTÀ, Stefano. **A vida na sociedade da vigilância –** a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 109.

[333] PUCCINELLI, Oscar Raúl. Evolución histórica y análisis de las diversas espécies, subespécies, tipos y subtipos de habeas data en América Latina: um intento clasificador con fines didácticos. Pontifícia Universidad Javeriana. Bogotá, Colômbia: **Vniversitas,** n. 107, 2004. Disponível em: https://www.redalyc.org/pdf/825/82510714.pdf..Acesso em: 20 abr. 2020, p. 475.

dados pessoais tutela o conjunto de bens e interesses que podem ser afetados pelo tratamento de tais dados[334].

Em tal conjuntura, o direito à proteção de dados pessoais, espécie do direito à privacidade, possui uma dimensão de liberdade e uma dimensão de igualdade, isto é, ao tempo que assegura à pessoa o controle sobre o fluxo de suas informações, tendo como base a autodeterminação informativa, também a protege da utilização de seus dados para fins discriminatórios, fundamentando-se no direito à igualdade.

O direito à proteção de dados pessoais possui uma dimensão individual, por permitir a construção da esfera privada do indivíduo longe de ingerências externas não autorizadas, e uma dimensão coletiva, haja vista que, ao equilibrar a distribuição de poder na sociedade, que é fortemente influenciada pela circulação de informações, o direito à proteção de dados pessoais também garante ao indivíduo a liberdade das escolhas existenciais e políticas contra qualquer forma de controle público e estigmatização social, tornando-se elemento constitutivo da cidadania, essencial à realização da democracia.

Embora o direito à proteção de dados pessoais esteja alicerçado na autodeterminação informativa, a ela não se restringe, porquanto visa proteger a pessoa contra qualquer prejuízo que possa ser causado pelo tratamento de dados pessoais.

Para tanto, pode garantir aos indivíduos direitos outros como o da revisão de decisões tomadas unicamente pelo tratamento automatizado de dados pessoais, vedar a utilização discriminatória de tais informações e até mesmo suprimir parcialmente o exercício do direito à autodeterminação em determinadas hipóteses, a exemplo da proibição do compartilhamento de dados pessoais sensíveis com objetivo de obter vantagem econômica, ainda que haja o consentimento do titular.

No que diz respeito à tutela da autodeterminação informativa, esse direito demanda a possibilidade de corrigir ou apagar dados inexatos ou tratados ilicitamente, uma vez que essas informações são a projeção da personalidade do individuo e, portanto, a pessoa deve ter o direito de determinar a qualidade dessa representação. Ademais, a realização do direito à autodeterminação informativa requer a existência de dois instrumentos essenciais: a informação e o consentimento.

A informação deve ser clara, facilitada e suficiente para que o titular dos dados possa decidir, devendo-se garantir que o indivíduo tome conhecimento das questões que envolvem o

---

[334] PUCCINELLI, Oscar Raúl. Evolución histórica y análisis de las diversas espécies, subespécies, tipos y subtipos de habeas data en América Latina: un intento clasificador con fines didácticos. Pontifícia Universidad Javeriana. Bogotá, Colômbia: **Vniversitas,** n. 107, 2004. Disponível em: https://www.redalyc.org/pdf/825/82510714.pdf..Acesso em: 20 abr. 2020, p. 475.

tratamento de seus dados pessoais, o que inclui, entre outras informações, quais são os dados objetos da coleta e do armazenamento no banco de dados, quais as finalidades de sua utilização, se haverá e para quem haverá transferência dos dados, bem como a possibilidade e as formas para a revogação do consentimento, quando esta for a base legal do tratamento.

Já o consentimento deve ser livre, informado e facilmente revogável quando o usuário assim decidir.

Assim, o titular dos dados pessoais deve receber, de modo claro, todas as informações necessárias e adequadas para a tomada de decisão no que concerne ao fornecimento do consentimento. Também, deve-se possibilitar que o indivíduo livremente consinta em fornecer seus dados para determinada finalidade, bem como no compartilhamento de suas informações com outros entes.

Nessa senda, deve-se evitar a lógica do "tudo ou nada", isto é, ou o titular consente com o tratamento de seus dados pessoais ou não pode ter acesso a determinado serviço, uma vez que isso representaria um demasiado custo social ao titular, a ser suportado em nome da sua autodeterminação informativa, levando o indivíduo a fornecer seu consentimento apenas porque é pré-requisito para a utilização de um serviço de que necessita. Não há, nessas hipóteses, liberdade de escolha, uma vez que o indivíduo é pressionado a fornecer seus dados.

Por exemplo, perquire-se se pode ser considerado livre o consentimento fornecido na hipótese de um serviço que se diz ser ofertado gratuitamente, mas que exige o fornecimento de dados pessoais para que seja utilizado, isto é, um serviço a que o indivíduo somente poderá ter acesso se consentir com a coleta e até com o compartilhamento de seus dados pessoais.

Acerca disso, o Grupo de Trabalho do Artigo 29, ao tecer suas orientações relativas ao consentimento na acepção do Regulamento Geral de Proteção de Dados da União Europeia, entende que o consentimento nessa situação não é livre e, portanto, não é válido:

> O elemento "livre" implica uma verdadeira escolha e controlo para os titulares dos dados. Regra geral, o RGPD prevê que se o titular dos dados não puder exercer uma verdadeira escolha, se sentir coagido a dar o consentimento ou sofrer consequências negativas caso não consinta, então o consentimento não é válido. Se o consentimento estiver agregado a uma parte não negociável das condições gerais do contrato, presume-se que não foi dado livremente. Assim sendo, não se considera que o consentimento foi dado de livre vontade se o titular dos dados não o puder recusar nem o puder retirar sem ficar prejudicado. A noção de desequilíbrio entre o responsável pelo tratamento e o titular dos dados também é tida em consideração no RGPD.
> [...] Em termos gerais, qualquer elemento que constitua pressão ou influência desadequada sobre o titular dos dados (que se pode manifestar de formas muito diversas) e que o impeça de exercer livremente a sua vontade tornará o consentimento inválido.
> [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[335].

Uma vez que a lei brasileira de proteção de dados pessoais sofreu forte influência do RGPD e, assim como o Regulamento, exige a liberdade do consentimento, é possível que a Autoridade Nacional de Proteção de Dados Pessoais adote semelhante interpretação.

Situação diversa seria visualizada em um cenário em que, além de oferecer a versão "gratuita" do serviço – cuja contrapartida são os dados pessoais dos usuários –, também seja ofertada uma versão *premium*, mediante a qual o usuário paga um determinado valor pela utilização do serviço. Pois, nessa situação, permite-se que o usuário realmente escolha entre pagar pela utilização do serviço ou fornecer suas informações pessoais para que sejam monetizadas pela organização empresária, inclusive com a possibilidade de cessão onerosa de tais dados. Verifica-se, por conseguinte, que o consentimento do titular pode ser qualificado como livre, nesse caso.

No Brasil, a Lei Geral de Proteção de Dados Pessoais ainda exige que o consentimento seja inequívoco, de modo que o silêncio não poderá ser considerado como manifestação da vontade. Assim, essa manifestação somente poderá ser extraída de atos positivos que revelem, de modo claro, a real vontade do titular[336].

A LGPD prevê, também, que o consentimento: a) deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular; b) se fornecido por escrito, deverá constar de cláusula destacada das demais cláusulas contratuais; c) deverá referir-se a finalidades determinadas, de modo que as autorizações genéricas para o tratamento de dados pessoais serão nulas.

No que diz respeito ao tratamento de dados pessoais sensíveis, tendo em vista que são mais suscetíveis de ser utilizados para fins discriminatórios, algumas legislações sobre proteção de dados proíbem o tratamento de tais dados, retirando do indivíduo a possibilidade de com ele consentir ou não.

---

[335] GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29º. **Parecer 05/2014 sobre as técnicas de anonimização.** 10 abr. 2014. Disponível em: https://www.gpdp.gov.mo/uploadfile/2016/0831/20160831042518381.pdf. Acesso em: 17 mar. 2020.

[336] TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coords.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** São Paulo: Thomson Reuters Brasil, 2019, p. 303.

Nesse sentido, a LGPD dispõe que a Autoridade Nacional poderá regulamentar e até mesmo vedar a comunicação ou o uso compartilhado dessas informações entre controladores, com o objetivo de obter vantagem econômica. No tocante aos dados pessoais sensíveis referentes à saúde, a Lei nº 13.709/2018 já proíbe a comunicação ou o uso compartilhado desses dados com o objetivo de obter vantagem econômica.

Há legislações que, em vez de proibir o tratamento de dados pessoais sensíveis, optam por estabelecer critérios mais rígidos para a validade do consentimento. A Lei Geral de Proteção de Dados Pessoais estabelece que, em se tratando de informações sensíveis, o consentimento deverá ser fornecido para finalidades específicas, de forma também específica e destacada.

Para a efetiva realização do direito à autodeterminação informativa, mesmo quando não for razoável exigir o consentimento do indivíduo – tendo-se em vista que o consentimento pode ser revogado a qualquer momento –, a pessoa deve ser informada acerca de quais são os procedimentos a que seus dados serão submetidos, com qual finalidade, bem como com quem serão compartilhados.

Como exemplo, cite-se o empregador que precisa manipular informações de seu empregado para cumprir obrigações legais. Em tal hipótese, não é razoável que esses dados só possam ser tratados após o consentimento do empregado, já que há um interesse legítimo do empregador em realizar tal tratamento. Entretanto, o empregado deve ser informado do destino de seus dados e para qual finalidade serão utilizados, não sendo possível ao empregador utilizá-los para finalidade diversa. A transparência quanto ao tratamento dos dados pessoais é fundamental para permitir que o indivíduo mantenha o controle sobre suas próprias informações.

Estando compreendido o objeto de tutela do direito à proteção de dados pessoais e o seu principal alicerce, isto é, a autodeterminação informativa, torna-se possível o exame do desenvolvimento experimentado pelas legislações sobre a matéria nas últimas décadas, visto que a evolução tecnológica, como não poderia deixar de ser, repercute na disciplina do direito à proteção de dados pessoais.

3.2.4 O desenvolvimento geracional das normas de proteção de dados pessoais

A tutela dos dados pessoais não foi a mesma em todos os momentos históricos. À medida que a sociedade sofre transformações, principalmente de cunho tecnológico, verificam-se alterações nas legislações que tratam da matéria. A esse respeito, Mayer-

Schönberger[337] propõe uma classificação das leis sobre proteção de dados pessoais em gerações.

O Estado Social exigia cada vez mais a coleta e o processamento de dados dos cidadãos para o funcionamento de sua burocracia e planejamento sofisticado. Projetos de leis que visavam uma enorme concentração de dados nas mãos do poder público começavam a surgir em alguns países. O Parlamento da Suécia, por exemplo, em 1960, propôs fundir todas as informações fiscais, dos registros civis e os dados do censo. Na mesma época, o governo alemão criou um Comitê para conectar os bancos de dados municipais, estaduais e federal. Essa ideia de centralização chegou até mesmo aos Estados Unidos, o qual, em 1965, propôs a criação do *National Data Center*, que consistiria num único centro de dados nacional contendo as mais diversas informações sobre os estadunidenses, que iriam desde a data de nascimento até o registro de espólio[338].

Nesse contexto, como reação ao processamento eletrônico de dados pela Administração Pública e organizações privadas, a partir da década de 1970 surgem as primeiras legislações intentando regular a concentração da coleta e gestão de dados pessoais por grandes centros de tratamento de dados[339].

Fazem parte dessa primeira geração de leis de proteção de dados pessoais: a Lei do Estado de Hesse, de 1970, na Alemanha Ocidental, que foi a primeira lei do mundo a disciplinar o assunto; o *Data Legen 289*, primeira lei nacional a tratar da matéria, sancionada na Suécia, em 11 de maio de 1973; o Estatuto de Proteção de Dados do Estado alemão de Rheinland-Pfalz, de 1974; e a Lei Federal de Proteção de Dados da Alemanha, de 1977[340].

Dessa forma, a maioria das normas de proteção de dados de primeira geração não se concentra na proteção da privacidade individual, mas na função do processamento de dados na sociedade. Tais leis partiam do ponto de vista de que o uso indiscriminado da tecnologia para o processamento de dados pessoais poderia criar perigos ainda incertos naquele momento, razão pela qual a utilização da tecnologia deve ser regulamentada para combater

---

[337] MAYER-SCHÖNBERGER, Viktor. Generational Development Data Protection in Europe**.** *In:* AGRE, Philipe E.; ROTENBERG, Marc. **Technology and Privacy:** The New Ladscape. Londres, Inglaterra: MIT Press, 2001. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=H2KB2DK4w78C&oi=fnd&pg=PA219&dq=Generational+development+of+data+protection+in+Europe&ots=1X0evcYsOo&sig=tsO6DFUyVQdFjfI2JkJLetz8WmM#v=onepage&q=Generational%20development%20of%20data%20protection%20in%20Europe&f=false. Acesso em: 20 abr. 2020, p. 219-241.

[338] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 38-39.

[339] 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. 175-176.

[340] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 38.

tais perigos e, ao mesmo tempo, permitir que o uso do processamento de dados cumpra seus objetivos sociais[341].

De modo geral, as leis da primeira geração da proteção de dados pessoais explicitamente abordam o perigo do processamento de dados pra o equilíbrio de poder no governo, haja vista que o Poder Executivo, que é quem faz a coleta dos dados dos indivíduos, tem em suas mãos um instrumento de planejamento e controle de enorme poder, enquanto o Legislativo, a quem caberia promulgar leis com base nesses dados de planejamento, careceria de acesso a essas informações. Assim, parte das primeiras leis sobre proteção de dados estabeleceu direitos de acesso dos legisladores aos dados armazenados pelo Poder Executivo[342].

As leis dessa geração focavam na atividade de processamento dos dados, estabelecendo regras concretas e específicas voltadas aos agentes diretamente responsáveis pelo processamento. Por conseguinte, a estrutura e a gramática dessas leis eram condicionadas pela informática. Tratava-se dos bancos de dados e não da privacidade[343].

No entanto, o núcleo das leis dessa geração estava na regulação dos bancos de dados. Nesse sentido, estabeleceram-se procedimentos complicados de registro e licenciamento desses bancos, isto é, o funcionamento dos bancos de dados era condicionado à autorização prévia dos órgãos competentes, os quais também realizariam, *a posteriori*, o controle desses centros de armazenamento de dados[344]. Essas legislações previam, ainda, o direito de o

---

[341] MAYER-SCHÖNBERGER, Viktor. Generational Development Data Protection in Europe**.** *In:* AGRE, Philipe E.; ROTENBERG, Marc. **Technology and Privacy:** The New Ladscape. Londres, Inglaterra: MIT Press, 2001. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=H2KB2DK4w78C&oi=fnd&pg=PA219&dq=Generational+development+of+data+protection+in+Europe&ots=1X0evcYsOo&sig=tsO6DFUyVQdFjfI2JkJLetz8WmM#v=onepage&q=Generational%20development%20of%20data%20protection%20in%20Europe&f=false. Acesso em: 20 abr. 2020, p. 223.

[342] MAYER-SCHÖNBERGER, Viktor. Generational Development Data Protection in Europe**.** *In:* AGRE, Philipe E.; ROTENBERG, Marc. **Technology and Privacy:** The New Ladscape. Londres, Inglaterra: MIT Press, 2001. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=H2KB2DK4w78C&oi=fnd&pg=PA219&dq=Generational+development+of+data+protection+in+Europe&ots=1X0evcYsOo&sig=tsO6DFUyVQdFjfI2JkJLetz8WmM#v=onepage&q=Generational%20development%20of%20data%20protection%20in%20Europe&f=false. Acesso em: 20 abr. 2020, p. 224.

[343] 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. 176.

[344] MAYER-SCHÖNBERGER, Viktor. Generational Development Data Protection in Europe**.** *In:* AGRE, Philipe E.; ROTENBERG, Marc. **Technology and Privacy:** The New Ladscape. Londres, Inglaterra: MIT Press, 2001. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=H2KB2DK4w78C&oi=fnd&pg=PA219&dq=Generational+development+of+data+protection+in+Europe&ots=1X0evcYsOo&sig=tsO6DFUyVQdFjfI2JkJLetz8WmM#v=onepage&q=Generational%20development%20of%20data%20protection%20in%20Europe&f=false. Acesso em: 20 abr. 2020, p. 224.

indivíduo acessar e corrigir seus dados pessoais, mas não o direito de decidir acerca do tratamento dessas informações[345].

Esse mecanismo de tutela de dados pessoais baseado no regime de autorizações logo se mostrou inviável, uma vez que a quantidade de banco de dados crescia veloz e significativamente como consequência das transformações e do barateamento da tecnologia que permitiram que diversas entidades privadas passassem a coletar e tratar dados pessoais de maneira autônoma e descentralizada. Buscando acompanhar todas essas transformações, surgem as legislações da segunda geração de leis de proteção de dados pessoais.

Nas leis dessa geração, verifica-se uma mudança estrutural: de disposições baseadas na informática para previsões concentradas no direito de privacidade do indivíduo, trazendo-se de volta à discussão questões como o direito a ser deixado em paz e o direito de delimitar o próprio espaço íntimo. Nessa senda, passa-se a vincular, explicitamente, a tutela dos dados pessoais ao direito à privacidade, e a proteção de tais dados passa a ser vista como uma liberdade negativa do indivíduo. O mecanismo de autorização para o funcionamento de bancos de dados se torna facilitado ou mesmo substituído pela notificação de sua criação[346].

Agora, o perigo se encontrava não mais na centralização de bancos de dados nacionais, mas no processamento de dados dispersos por milhares de computadores. Os indivíduos sofriam com a utilização por terceiros de suas informações, desprovidos de instrumentos de defesa contra tal uso de seus dados[347].

As leis dessa geração buscaram permitir que os indivíduos lutassem pela preservação de sua privacidade a partir de direitos fortes e até mesmo constitucionalmente protegidos, além de ampliar os poderes das autoridades administrativas encarregadas da proteção de dados[348].

---

[345] MAYER-SCHÖNBERGER, Viktor. Generational Development Data Protection in Europe**.** *In:* AGRE, Philipe E.; ROTENBERG, Marc. **Technology and Privacy:** The New Ladscape. Londres, Inglaterra: MIT Press, 2001. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=H2KB2DK4w78C&oi=fnd&pg=PA219&dq=Generational+development+of+data+protection+in+Europe&ots=1X0evcYsOo&sig=tsO6DFUyVQdFjfI2JkJLetz8WmM#v=onepage&q=Generational%20development%20of%20data%20protection%20in%20Europe&f=false. Acesso em: 20 abr. 2020, p. 226.

[346] MAYER-SCHÖNBERGER, Viktor. Generational Development Data Protection in Europe**.** *In:* AGRE, Philipe E.; ROTENBERG, Marc. **Technology and Privacy:** The New Ladscape. Londres, Inglaterra: MIT Press, 2001. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=H2KB2DK4w78C&oi=fnd&pg=PA219&dq=Generational+development+of+data+protection+in+Europe&ots=1X0evcYsOo&sig=tsO6DFUyVQdFjfI2JkJLetz8WmM#v=onepage&q=Generational%20development%20of%20data%20protection%20in%20Europe&f=false. Acesso em: 20 abr. 2020, p. 220.

[347] 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. 177.

[348] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p.40.

Assim, os direitos individuais foram reforçados e ampliados, e as instituições administrativas de controle passaram não só a investigar violações à proteção de dados, mas tornaram-se instrumentos de provimento dessa proteção. Algumas dessas instituições foram transformadas ou criadas com funções muito próximas às de um órgão jurisdicional para solucionar controvérsias envolvendo proteção de dados[349].

A primeira legislação dessa geração foi a lei francesa de proteção de dados pessoais[350]. As constituições da Espanha e Portugal também são classificadas como de segunda geração ao inserirem a privacidade informacional em seus textos. As leis da Dinamarca e da Áustria são, ainda, outros exemplos da segunda geração de normas de proteção de dados pessoais[351].

Apesar de todas as inovações trazidas pelas leis dessa geração, os direitos dos indivíduos no que diz respeito à tutela de seus dados ainda eram insuficientes, já que a proteção de dados pessoais era vista, até então, como uma liberdade negativa. Dessa forma, os direitos dos indivíduos previstos nessas legislações, consistiam, de modo geral, na liberdade de fornecer ou não seus dados pessoais.

Entretanto, como assinalado por Mayer-Schönberger, os Estados precisam processar dados pessoais para poderem realizar seus fins sociais, de modo que o cidadão, para ter acesso aos serviços oferecidos pelo Estado, não tem escolha a não ser fornecer seus dados. Diante disso, em que pese a proteção de dados pessoais como liberdade individual possa proteger a privacidade do indivíduo, possibilitando-lhe não fornecer as informações que lhe são solicitadas, a proteção de dados seria exercida a muito custo pelo indivíduo, que seria tolhido dos serviços estatais, bem como daqueles oferecidos pelos entes privados, como bancos e agências de viagens[352].

A tutela das informações pessoais somente por esse prisma seria inefetiva, haja vista que a coleta de dados é indispensável ao acesso do indivíduo a uma série de serviços

---

[349] MAYER-SCHÖNBERGER, Viktor. Generational Development Data Protection in Europe**.** *In:* AGRE, Philipe E.; ROTENBERG, Marc. **Technology and Privacy:** The New Ladscape. Londres, Inglaterra: MIT Press, 2001. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=H2KB2DK4w78C&oi=fnd&pg=PA219&dq=Generational+development+of+data+protection+in+Europe&ots=1X0evcYsOo&sig=tsO6DFUyVQdFjfI2JkJLetz8WmM#v=onepage&q=Generational%20development%20of%20data%20protection%20in%20Europe&f=false. Acesso em: 20 abr. 2020, p. 228.

[350] FRANÇA. Le Service Public de La Diffusion Du Droit. **Loi nº 78/17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertes.** Version consolidée au 25 ma 2020. Disponível em: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460. Acesso em: 17 maio. 2020.

[351] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 40.

[352] MAYER-SCHÖNBERGER, Viktor. Generational Development Data Protection in Europe**.** *In:* AGRE, Philipe E.; ROTENBERG, Marc. **Technology and Privacy:** The New Ladscape. Londres, Inglaterra: MIT Press, 2001. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=H2KB2DK4w78C&oi=fnd&pg=PA219&dq=Generational+development+of+data+protection+in+Europe&ots=1X0evcYsOo&sig=tsO6DFUyVQdFjfI2JkJLetz8WmM#v=onepage&q=Generational%20development%20of%20data%20protection%20in%20Europe&f=false. Acesso em: 20 abr. 2020, p. 228-229.

essenciais, sejam estatais ou particulares, como educação, fornecimento de energia, serviços telefônicos, entre tantos outros, sendo praticamente impossível viver no atual contexto histórico-social sem fornecer qualquer informação pessoal.

A partir da década de 1980, os avanços tecnológicos ampliaram a capacidade e a velocidade da transmissão de dados. Já não era mais possível localizar, fisicamente, os bancos de dados, uma vez que estes passaram a ser armazenados em rede, o que também permitia a transferência dos dados em segundos[353].

Nesse cenário, visando garantir a efetividade da proteção dos dados pessoais, as leis da terceira geração levam em consideração o contexto no qual se solicita ao indivíduo que forneça seus dados. Reconhecem que a tutela dos dados pessoais não pode ser dissociada da participação do indivíduo na sociedade e estabelecem meios de proteção para as situações em que a liberdade de decisão sobre o fornecimento de informações pessoais não é verdadeiramente livre, mas cerceada por eventuais condicionantes, garantindo-se o efetivo exercício da autodeterminação informativa[354].

A autodeterminação informativa surge como uma extensão das liberdades já reconhecidas pelas leis de segunda geração e provoca uma série de alterações estruturais nas legislações de proteção de dados[355]. Nessa senda, as emendas às leis de proteção de dados na Áustria e na Alemanha, em 1986 e 1990, respectivamente, a previsão constitucional da proteção de dados pessoais da Holanda e a Lei de Registro de Pessoas da Finlândia, de 1987, são exemplos das normas que compõem essa fase do desenvolvimento da proteção de dados pessoais[356].

A principal diferença entre as leis dessa geração e as da segunda geração é a mudança de paradigma na forma como é vista a participação do indivíduo no processamento de seus dados: abandona-se a lógica da decisão entre o "tudo ou nada" e envolve-se a participação do

---

[353] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 42.

[354] 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. 178.

[355] 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. 178.

[356] MAYER-SCHÖNBERGER, Viktor. Generational Development Data Protection in Europe**.** *In:* AGRE, Philipe E.; ROTENBERG, Marc. **Technology and Privacy:** The New Ladscape. Londres, Inglaterra: MIT Press, 2001. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=H2KB2DK4w78C&oi=fnd&pg=PA219&dq=Generational+development+of+data+protection+in+Europe&ots=1X0evcYsOo&sig=tsO6DFUyVQdFjfI2JkJLetz8WmM#v=onepage&q=Generational%20development%20of%20data%20protection%20in%20Europe&f=false. Acesso em: 20 abr. 2020, p. 231-232.

titular dos dados em todo o processo, de maneira contínua, o que vai desde a coleta até a transmissão, passando pelo armazenamento dos dados[357].

Dessa forma, o tratamento de dados passa a ser visto como um processo que vai muito além da concessão ou não da autorização da pessoa para que seus dados sejam utilizados, buscando-se fazer com que o titular participe consciente e ativamente de todo o processo de tratamento e utilização de sua informação por terceiros. Por tal razão, as leis dessa fase incluíam algumas garantias do indivíduo, como o dever de informação[358].

No entanto, na prática, tais leis também se mostraram inefetivas. Apesar de todos os esforços legislativos, a proteção de dados permanecia um privilégio das minorias, isto porque a maioria das pessoas não estava disposta a arcar com o alto custo monetário e social exigido para se exercer, rigorosamente, o direito à autodeterminação informativa, pois se temia o risco financeiro de se judicializar a questão[359].

Além disso, a maioria dos indivíduos, de maneira frequente e muitas vezes inconsciente, fechava contratos em que consentiam o tratamento de seus dados, de modo que, em casos de violação à privacidade, esse consentimento era tido como válido e a pessoa não conseguia pleitear reparação pela violação[360].

Os legisladores, então, perceberam a posição de negociação mais fraca do indivíduo diante das organizações que coletam dados pessoais, o que dificultava o exercício do direito à autodeterminação informativa. Buscaram então corrigir esse desequilíbrio por meio de duas distintas abordagens, as quais são identificadas nas normas e emendas da quarta geração de leis sobre a proteção de dados pessoais.

A primeira abordagem busca igualar as posições de negociação, fortalecendo a posição do indivíduo em relação às instituições que realizam o tratamento de seus dados, tornando mais efetivo o seu autocontrole sobre as informações pessoais. Como exemplo do uso dessa

---

[357] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 42.

[358] 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. 178.

[359] MAYER-SCHÖNBERGER, Viktor. Generational Development Data Protection in Europe**.** *In:* AGRE, Philipe E.; ROTENBERG, Marc. **Technology and Privacy:** The New Ladscape. Londres, Inglaterra: MIT Press, 2001. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=H2KB2DK4w78C&oi=fnd&pg=PA219&dq=Generational+development+of+data+protection+in+Europe&ots=1X0evcYsOo&sig=tsO6DFUyVQdFjfI2JkJLetz8WmM#v=onepage&q=Generational%20development%20of%20data%20protection%20in%20Europe&f=false. Acesso em: 20 abr. 2020, p. 232.

[360] MAYER-SCHÖNBERGER, Viktor. Generational Development Data Protection in Europe**.** *In:* AGRE, Philipe E.; ROTENBERG, Marc. **Technology and Privacy:** The New Ladscape. Londres, Inglaterra: MIT Press, 2001. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=H2KB2DK4w78C&oi=fnd&pg=PA219&dq=Generational+development+of+data+protection+in+Europe&ots=1X0evcYsOo&sig=tsO6DFUyVQdFjfI2JkJLetz8WmM#v=onepage&q=Generational%20development%20of%20data%20protection%20in%20Europe&f=false. Acesso em: 20 abr. 2020, p. 232.

técnica tem-se a emenda que introduziu, na Lei Federal de Proteção de dados da Alemanha, a compensação independentemente de comprovação de culpa nas reclamações individuais relacionadas à proteção de dados pessoais[361].

A segunda abordagem retira parte da liberdade individual conferida pelas normas de proteção até então existentes para sujeitar determinadas situações à proteção legal obrigatória. Essa técnica parte do pressuposto de que algumas áreas de privacidade das informações devem ser fortemente protegidas, não podendo ser negociadas ou submetidas exclusivamente a uma decisão individual. Nessa esteira proíbe-se, total ou parcialmente, o tratamento de dados pessoais sensíveis, os quais possuem um maior potencial de gerar discriminação[362], bem como se restringem à negociação dos direitos básicos de proteção de dados, como os direitos de acesso, correção e exclusão[363].

Nessa quarta fase de desenvolvimento das leis de proteção de dados pessoais, as normas gerais são complementadas por regulamentos setoriais específicos com vistas a ampliar a proteção do indivíduo nos mais diversos contextos em que ocorre o tratamento de seus dados e, dessa forma, contemplar as diversas especificidades setoriais existentes. A maioria dos países europeus conta com uma regulação geral sobre a matéria, a qual é suplementada por diversas normas específicas para determinados setores, como o de saúde e o de consumo[364].

Verifica-se nessa geração, ainda, uma disseminação do modelo das autoridades independentes para a atuação da lei, responsáveis por disciplinar vários aspectos da aplicação legislativa e pelo recebimento de reclamações e fiscalização acerca da proteção de dados pessoais[365].

A Diretiva da União Europeia, de 1995, e o Regulamento Geral de Proteção de Dados da União Europeia, de 2016, refletem todo o desenvolvimento geracional apresentado por Mayer-Schönberger pelo qual passou a proteção de dados pessoais, já que colocam a participação do indivíduo como uma parte essencial do tratamento de dados, estabelecem uma

---

[361] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 43.
[362] Essa categoria de dados pessoais será estudada mais adiante.
[363] MAYER-SCHÖNBERGER, Viktor. Generational Development Data Protection in Europe**.** *In:* AGRE, Philipe E.; ROTENBERG, Marc. **Technology and Privacy:** The New Ladscape. Londres, Inglaterra: MIT Press, 2001. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=H2KB2DK4w78C&oi=fnd&pg=PA219&dq=Generational+development+of+data+protection+in+Europe&ots=1X0evcYsOo&sig=tsO6DFUyVQdFjfI2JkJLetz8WmM#v=onepage&q=Generational%20development%20of%20data%20protection%20in%20Europe&f=false. Acesso em: 20 abr. 2020, p. 233.
[364] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 44.
[365] 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. 179.

disciplina bem mais rígida para o tratamento de dados pessoais sensíveis, exigem a criação de códigos de conduta que levem em consideração os diferentes setores que realizam o processamento de dados[366] e preveem a criação pelos Estados-Membros de autoridades de controle independentes, responsáveis pela fiscalização da aplicação de tais normas[367].

No Brasil, a Lei Geral de Proteção de Dados Pessoais apresenta uma estrutura semelhante às demais normas de quarta geração. Isso porque também reconhece que um direito efetivo à proteção de dados pessoais exige uma participação ativa dos titulares dos dados, embora admita que, em muitas situações, o indivíduo não poderá livremente exercer a sua autodeterminação informativa.

Diante disso, estabelece regras mais rígidas para o tratamento de dados sensíveis, restringindo as hipóteses legais em que tal tratamento é permitido, bem como exigindo que, quando o tratamento for consentido, deverá sê-lo, de forma específica e destacada, para finalidades específicas. Ainda, por meio de seus princípios, prevê que só devem ser coletados os dados estritamente necessários à finalidade do tratamento e, mesmo quando consentido, o processamento de dados pessoais não pode ser irrestrito, porém adstrito à finalidade para a qual os dados foram coletados.

A LGPD também prevê a criação da Autoridade Nacional de Proteção de Dados Pessoais (ANPD), a qual, além de zelar pela proteção de dados nos termos da referida legislação, apreciará petições de titular contra agentes de tratamento depois de comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação, conforme artigo 55-J, V, da Lei 13.709/2018.

A análise do desenvolvimento pelo qual passou as normas referentes à proteção de dados pessoais demonstra que a disciplina da matéria nem sempre foi a mesma e que o direito

---

[366] Artigo 40º Códigos de conduta. 1. Os Estados-Membros, as autoridades de controlo, o Comité e a Comissão promovem a elaboração de códigos de conduta destinados a contribuir para a correta aplicação do presente regulamento, tendo em conta as características dos diferentes setores de tratamento e as necessidades específicas das micro, pequenas e médias empresas. UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016**. Relativo à proteção de dados pessoais 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 Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679#d1e1554-1-1. Acesso em: 28 jun. 2020.

[367] Artigo 51º Autoridade de controlo. 1. Os Estados-Membros estabelecem que cabe a uma ou mais autoridades públicas independentes a responsabilidade pela fiscalização da aplicação do presente regulamento, a fim de defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e facilitar a livre circulação desses dados na União ("autoridade de controlo"). UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016**. Relativo à proteção de dados pessoais 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 Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679#d1e1554-1-1. Acesso em: 28 jun. 2020.

busca acompanhar os avanços tecnológicos, a fim de garantir efetividade aos direitos dos titulares dos dados.

A aplicação das legislações de primeira, segunda e terceira gerações, referentes à proteção de dados pessoais, revelou que a tutela ali prevista era insuficiente, muitas vezes representando mais um discurso político do que realmente um direito do indivíduo.

A partir da quarta geração, as normas passaram a prever instrumentos que não só fortaleceram os direitos dos titulares dos dados, mas também permitiram o exercício de tais direitos mesmo em situações negociais que envolvem grande desequilíbrio entre as partes, tutelando-se, assim, de maneira mais efetiva a personalidade do indivíduo.

Feitas essas considerações, importa averiguar se o direito à proteção de dados pessoais experimentou este desenvolvimento, isto é, se há certa semelhança quanto à disciplina normativa sobre a matéria nos diferentes ordenamentos jurídicos, de modo que, ainda que em determinados países as leis específicas sobre o tema tenham surgido mais tardiamente ou que a tutela das informações pessoais se dê de forma difusa e esparsa, haveria um núcleo comum de proteção dispensada aos dados pessoais por boa parte dos países.

Assim, na seção seguinte, buscar-se-á investigar se há certa convergência no que tange à tutela dos dados pessoais pelos variados sistemas jurídicos.

3.3 A convergência regulatória das normas de proteção de dados pessoais

Foi Bennett quem desenvolveu a tese da convergência regulatória da proteção de dados pessoais. Para o autor, a partir da década de 1970 surgiram fortes pressões políticas para que os Estados passassem a adotar legislações com princípios e direitos semelhantes, os quais concederiam ao indivíduo um maior controle sobre suas informações pessoais[368]. Nesse sentido, a convergência regulatória vai além da similaridade, pois sugere um processo dinâmico pelo qual os países começam em diferentes pontos de partida e, com o tempo, convergem para soluções semelhantes[369].

---

[368] BENNET, Colin. "Convergence revisited: Toward a global policy for the protection of personal data *In:* AGRE, Philipe E.; ROTENBERG, Marc. **Technology and Privacy:** The New Ladscape. Londres, Inglaterra: MIT Press, 2001. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=H2KB2DK4w78C&oi=fnd&pg= PA219&dq=Generational+development+of+data+protection+in+Europe&ots=1X0evcYsOo&sig=tsO6DFUyVQdFjfI2JkJLetz8WmM#v=onepage&q=Generational%20development%20of%20data%20protection%20in%20Europe&f=false. Acesso em: 20 abr. 2020, p. 99.

[369] BENNET, Colin. "Convergence revisited: Toward a global policy for the protection of personal data *In:* AGRE, Philipe E.; ROTENBERG, Marc. **Technology and Privacy:** The New Ladscape. Londres, Inglaterra: MIT Press, 2001. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=H2KB2DK4w78C&oi=fnd&pg= PA219&dq=Generational+development+of+data+protection+in+

Desse modo, partindo-se de uma posição em que os Estados não tinham nenhuma ou pouca legislação sobre a matéria e, por isso, havia diversos tipos de estratégia para o tema, emergiu, durante a década de 1970, um consenso em volta de princípios[370].

O principal aspecto convergente é o que Schwartz chama de paradigma de controle de privacidade, o qual concebe a privacidade como um direito pessoal de controlar o uso de seus dados[371]. A garantia de controle do indivíduo sobre as próprias informações é uma característica comum presente nas diversas legislações, as quais reconhecem a autodeterminação informativa e, por meio do consentimento do titular, possibilitam ao indivíduo, pelo menos em tese, determinar o nível de proteção de seus dados pessoais[372].

A maior parte das legislações estabeleceu princípios, mecanismos legais e direitos subjetivos, como os direitos de informação, acesso, retificação e cancelamento, que visam atribuir e tornar efetiva a liberdade do indivíduo de controlar a coleta, o armazenamento, o processamento e a disseminação de suas informações[373].

Como visto, na década de 1970 havia uma forte preocupação dos países europeus diante das novas tecnologias que permitiam massiva coleta de dados pessoais, motivo pelo qual tais países buscavam uma solução comum para a questão. A primeira lei nacional sobre proteção de dados pessoais foi a sueca, de 1973, tendo outros países do continente passado a regular a matéria logo em seguida.

Ainda nesse período, a Assembleia Consultiva do Conselho Europeu solicitou que o Comitê de Ministros elaborasse recomendações que relacionassem o tratamento de dados pessoais com o direito à privacidade, previsto no artigo 8º da Convenção Europeia para a Salvaguarda dos Direitos do Homem e das Liberdades Fundamentais[374].

Por essa razão, em 1973 foi publicada a *Resolution 22 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector (1973),* na qual o Comitê de Ministros reconheceu que eram necessárias medidas legislativas para evitar abusos no tratamento de informações pessoais pelo setor privado, bem como que, na pendência da

---

Europe&ots=1X0evcYsOo&sig=tsO6DFUyVQdFjfI2JkJLetz8WmM#v=onepage&q=Generational%20development%20of%20data%20protection%20in%20Europe&f=false. Acesso em: 20 abr. 2020, p. 102.

370 MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 45.

371 SCHWARTZ, Paul M. **Internet Privacy and the State.** 5 nov. 2000. Disponível em: https://paulschwartz.net/wp-content/uploads/2019/01/SCHWARTZ-CK1A-1.pdf. Acesso em: 15 abr. 2020, p. 45.

372 MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 46.

373 MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 45-46.

374 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. 192.

possível elaboração de um acordo internacional, mostrava-se urgente a adoção de medidas que evitassem divergências adicionais entre as leis dos Estados-Membros a respeito da matéria. Nessa senda, o Comitê recomendou aos Estados-Membros que adotassem princípios mínimos de proteção estabelecidos no anexo da Resolução[375].

As leis de proteção de dados pessoais aprovadas nessa década apresentam certa conformidade com os princípios previstos na Resolução, o que demonstra que a disciplina da matéria segue um caminho de padronização desde a primeira geração de normas que tutelam tais dados.

Um pouco antes, também em 1973, o Departamento de Saúde, Educação e Bem-Estar Social dos Estados Unidos elaborou o relatório sobre Registros, Computadores e Direitos do Cidadão, o qual trouxe a ideia de que as organizações deveriam aderir a princípios fundamentais para o tratamento de dados, definidos como *Fair Information Practice Principles (FIPPs)*, isto é, padrões de práticas necessários para garantir que as entidades que coletam e usam informações pessoais forneçam adequada proteção de privacidade a esses dados[376]. Segundo o documento, tais padrões se assentavam em cinco princípios, os quais serão vistos adiante.

Assim, internacionalmente, formou-se a consciência da necessidade de uma uniformização legislativa supranacional, tendo em vista que, como a coleta e o tratamento de dados podem ocorrer fora do Estado, uma regulação cingida ao direito interno não se mostrava suficientemente eficaz[377]. Em 1978, a Organização para a Cooperação e Desenvolvimento Econômico[378] instituiu um grupo de especialistas com o objetivo de elaborar um modelo normativo para o tráfego internacional de dados, tendo como ponto de partida os referidos FIPPs[379].

A OCDE emitiu em 1980 as *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* que intentavam estabelecer padrões normativos mínimos de proteção aos dados pessoais por meio de oito princípios: a) limitação da coleta de dados pessoais; b)

---

375 CONSELHO DA EUROPA. Committee of Ministers. **Resolution (73) 22, On The Protection of the Privacy of Individuals Vis-a-Vis Electronic Data Banks in the Private Sector**. 26 set. 1973. Disponível em: https://rm.coe.int/1680502830. Acesso em: 17 mar. 2020.

376 WARE, W. H. **Records, Computers and the Rights of Citizens.** Ago. 1973. Disponível em: https://www.rand.org/content/dam/rand/pubs/papers/2008/P5077.pdf. Acesso em: 20 abr. 2020.

377 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. 192.

378 A Organização para Cooperação e Desenvolvimento Econômico (OCDE) é uma organização internacional que visa estabelecer padrões internacionais a serem adotados pelos países membros na busca de soluções para uma série de desafios sociais, econômicos e ambientais.

379 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. 192-193.

qualidade dos dados; c) especificação da finalidade; d) limitação de uso; e) garantias de segurança; f) abertura; g) participação individual; h) responsabilidade[380].

Entretanto, a preocupação principal do documento não era com a proteção da pessoa, dos dados pessoais em si, mas com o tráfego de dados, a fim de garantir o livre fluxo de informações entre seus países membros[381]. Visava criar um "ambiente regulatório uniforme" entre tais países[382]. Nesse sentido, recomendava que:

> PARTE QUATRO. IMPLEMENTAÇÃO NACIONAL.
>
> 19. Ao implementar internamente os princípios estabelecidos nas Partes Dois e Três, os países Membros devem estabelecer procedimentos ou instituições legais, administrativas ou outras para a proteção da privacidade e das liberdades individuais em relação aos dados pessoais. Os países membros devem procurar, em particular:
> a) adotar legislação nacional apropriada;
> b) incentivar e apoiar a auto-regulação, seja na forma de códigos de conduta ou de outra forma;
> c) providenciar meios razoáveis para os indivíduos exercerem seus direitos;
> d) prever sanções e recursos adequados em caso de falha no cumprimento de medidas que implementem os princípios estabelecidos nas Partes Dois e Três; e
> e) garantir que não haja discriminação injusta contra os titulares dos dados[383].

Essas diretrizes foram revisadas em 2013 e, em que pese não sejam diretamente aplicáveis, bem como os países integrantes não sejam obrigados a segui-las em seu direito interno, tornaram-se referência na proteção de dados pessoais, sendo os princípios nela elencados ainda hoje observados pelas novas legislações sobre a matéria, inclusive pelo RGPD e pela LGPD.

O esforço comum dos Estados-Membros em adotar as diretrizes da OCDE para não obstaculizar o fluxo de informações foi reafirmado por meio da *Declaration on transborder data flows*, de 1985[384]. Não há dúvidas que as diretrizes da OCDE tiveram influência mundial na convergência da proteção dos dados pessoais.

Os países ou blocos econômicos que não incorporassem os padrões desse documento poderiam ficar de fora do mapa global de livre fluxo de dados. Assim, a emergência de leis

---

[380] OCDE. **OECD Guidelines o the Protection of Privacy and Transborder Flows of Personal Data.** 2013. Disponível em: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Acesso em: 20 abr. 2020.

[381] 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. 193.

[382] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 119.

[383] OCDE. **OECD Guidelines o the Protection of Privacy and Transborder Flows of Personal Data.** 2013. Disponível em: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Acesso em: 20 abr. 2020.

[384] OCDE**. Declaration on Transborder Data Flows.** Disponível em: https://legalinstruments.oecd.org/public/doc/108/108.en.pdf.. Acesso em: 20 abr. 2020.

nacionais e regionais sobre a proteção de dados pessoais trazia, em sua maioria, regras duras no que diz respeito à transferência internacional de dados, estabelecendo que, em princípio, tal transferência só poderia acontecer se o país destinatário tivesse um nível equivalente de proteção às informações pessoais[385].

Em 1981, o Conselho da Europa aprovou a Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais, mais conhecida como Convenção de Estrasburgo ou Convenção 108, a qual trazia alguns dos princípios elencados nas diretrizes da OCDE e pela qual os signatários comprometiam-se a adotar as medidas necessárias em sua legislação nacional para aplicar os princípios básicos de proteção de dados estabelecidos na Convenção[386].

Importa dizer que a Convenção, em seu artigo 23, previu que Estados que não fossem membros do Conselho da Europa poderiam a ela aderir, o que permitiu a países como Argentina, Cabo Verde, Marrocos, México, Senegal, Tunísia e Uruguai ratificarem, mais recentemente, a referida Convenção[387].

Logo após a Convenção 108, muitos países europeus editaram suas primeiras legislações sobre a proteção de dados pessoais, seguindo as orientações normativas da Convenção. Aqueles países que já possuíam leis sobre a matéria adequaram a disciplina aos padrões estabelecidos no documento.

Em 1995, o Parlamento Europeu e o Conselho da União Europeia aprovaram a Diretiva 95/46/CE, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, a qual possui um conteúdo normativo bem detalhado, dispondo, além dos princípios a serem observados no tratamento de dados, sobre hipóteses de tratamento, consentimento, direitos dos titulares, deveres dos responsáveis pelo tratamento, normas diferenciadas para tratamentos sensíveis, regras de

---

[385] BIONI, Bruno R.; MENDES, Laura S. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral brasileira de Proteção de Dados: mapeando convergências na direção de um nível de equivalência. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coords.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** São Paulo: Thomson Reuters Brasil, 2019, p. 801.

[386] CONSELHO DA EUROPA. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.** Strasbourg, 28 jan. 1981. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37. Acesso em: 20 abr. 2020.

[387] CONSELHO DA EUROPA. **Chart of signatures and ratifications of Treaty 108.** Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**.** Strasbourg, 28 jan. 1981. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=GGLmmfdZ. Acesso em: 20 abr. 2020.

responsabilidade, código de conduta e autoridade de controle. Além disso, a Diretiva impõe que os Estados-Membros incorporem o conteúdo do documento em seu direito interno[388].

Em 1997, os 18 países já tinham incorporado as normas da Diretiva em suas legislações nacionais, o que efetivamente padronizou a proteção de dados pessoais na União Europeia, compreendendo tanto o setor público quanto o privado[389]. Esse movimento acabou por influenciar países como Canadá e Austrália a regularem a proteção de dados também no setor privado[390].

Ademais, a Diretiva exigia que a transferência de dados pessoais de bancos de dados europeus, públicos ou privados, só fosse feita para um Estado não integrante da União Europeia se este oferecesse um nível adequado de proteção, sendo possível à Comissão Europeia constatar que o país assegurava nível de proteção adequado em virtude da sua legislação interna ou dos seus compromissos internacionais com vistas à proteção do direito à vida privada e das liberdades e direitos fundamentais das pessoas.

Após décadas de consolidação desses padrões internacionais, atestada por um alto nível de convergência entre leis de proteção de dados pessoais ao redor do mundo, surgiu um movimento com vistas a facilitar ainda mais o livre fluxo de dados: a certificação de organizações que, voluntariamente, aderissem a determinados padrões normativos de proteção de dados traçados por organismos internacionais como a Cooperação Econômica Ásia-Pacífico – APEC e a OCDE, padrões estes que levam em consideração todo o caminho percorrido pelo direito à proteção de dados pessoais até então[391].

Em 2010, a Comissão Europeia avaliou que a Diretiva 95/46/CE estabeleceu um marco na história da proteção de dados pessoais na União Europeia ao consagrar duas das ambições mais antigas e igualmente importantes do processo de integração europeu: o direito fundamental à proteção de dados e o fluxo livre de dados pessoais. Quinze anos depois, esse objetivo duplo continuava válido e os princípios consagrados no documento permaneciam

---

[388] CONSELHO DA EUROPA. **Diretiva 95/46/CE do Parlamento Europeu do Conselho, de 24 de outubro de 1995, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT. Acesso em: 20 abr. 2020.

[389] 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. 196.

[390] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 48.

[391] BIONI, Bruno R.; MENDES, Laura S. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral brasileira de Proteção de Dados: mapeando convergências na direção de um nível de equivalência. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coords.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** São Paulo: Thomson Reuters Brasil, 2019, p. 801-802.

sólidos, contudo, as mudanças tecnológicas e a globalização trouxeram novos desafios para a proteção de dados pessoais[392].

Para atender aos novos desafios, em 2016 o Parlamento Europeu e o Conselho da União Europeia aprovaram o Regulamento Geral de Proteção de Dados, objetivando criar um regime jurídico ainda mais uniforme e equivalente sobre a matéria em toda a União Europeia. Além de ser bem mais abrangente, enquanto a Diretiva 95/46/CE ainda permitia um espaço grande de variação jurídica por cada um dos Estados-Membros, o RGPD é diretamente aplicável a todos os países-membros da Comunidade, não havendo necessidade de internalização de suas normas por esses países[393].

Esse Regulamento "é o ponto de chegada de uma longa jornada europeia no campo da proteção de dados pessoais"[394]. Inspirado nele, o Brasil aprovou, em 2018, sua primeira Lei Geral de Proteção de Dados Pessoais, a qual, apesar de ser bem mais enxuta que o RGPD, possui disposições bastante convergentes com o Regulamento, como os princípios, os direitos dos titulares, o modelo *ex-ante* de proteção de dados, as hipóteses legais para tratamento dos dados e a ideia de *privacy by design*[395].

Evidente que existem diferenças entre as duas legislações, mas a convergência entre os dois sistemas de proteção é grande, o que permitirá ao Brasil utilizar a experiência europeia para desenvolver, na prática, a proteção aos dados pessoais, uma vez que, enquanto os europeus lidam com a matéria há décadas, o país ainda tem um longo caminho a percorrer.

Dessa feita, tendo em vista que, no mundo globalizado, a ausência de uma proteção de dados pessoais equivalente entre os diversos países reduziria consideravelmente a eficácia de qualquer legislação nacional, os instrumentos internacionais que buscaram traçar um padrão mínimo de proteção a ser adotado pelos países que desejavam manter a transferência internacional de dados, em especial as diretrizes da OCDE, tiveram importância fundamental

---

[392] UNIÃO EUROPEIA. **Communication from the Comission to the European Parlament, the Council, the Economic and Social Committee and the Committee of the Regions:** a comprehensive approach on personal data protection in the European Union. Disponível em: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52010DC0609. Acesso em: 20 abr. 2020.

[393] UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016**. Relativo à proteção de dados pessoais 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 Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679#d1e1554-1-1. Acesso em: 28 jun. 2020.

[394] BIONI, Bruno R.; MENDES, Laura S. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral brasileira de Proteção de Dados: mapeando convergências na direção de um nível de equivalência. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coords.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** São Paulo: Thomson Reuters Brasil, 2019, p. 803.

[395] BIONI, Bruno R.; MENDES, Laura S. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral brasileira de Proteção de Dados: mapeando convergências na direção de um nível de equivalência. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coords.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** São Paulo: Thomson Reuters Brasil, 2019, p. 799-820.

no processo de convergência regulatória que se verifica nas legislações sobre a matéria em todo o mundo.

Também a Convenção de Estrasburgo e a Diretiva 95/46/CE tiveram um papel fundamental na uniformização da proteção de dados nos países europeus, bem como na adoção de princípios essenciais no que se refere à disciplina em países não membros da União Europeia. Além disso, a Diretiva, ao impor restrições à transferência de dados a países que não tenham nível de proteção adequada, incentivou que países de outros continentes buscassem proteger minimamente os dados de seus cidadãos, ainda que não tivessem uma legislação específica sobre a matéria.

Quem mais se distancia dessa tendência convergente são os Estados Unidos, que possuem uma regulação abrangente para o setor público, mas, no que diz respeito ao setor privado, contam apenas com leis setoriais e esparsas. Dessa forma, são o único país industrial avançado que ainda não aprovou uma lei de proteção de dados que abranja também as atividades do setor privado[396]. Entretanto, observa-se que até mesmo esse país, que possui uma cultura diferente de proteção à privacidade e onde a disciplina de proteção de dados pessoais é marcadamente reativa, observa os princípios de práticas justas de informação, pelo menos no setor estatal.

Isso posto, todo esse movimento de convergência internacional marcado pela busca por soluções comum fez com que as normas de proteção de dados pessoais encontrassem semelhanças em todo o mundo. Os *FIPPs*, que com o tempo vão sendo adaptados às mudanças tecnológicos, continuam a servir de base para leis e regulamentos, na Europa, no Brasil, e em todo o mundo, além de formar a base para os códigos de conduta da indústria e de acordos internacionais sobre práticas aceitas de proteção e transferência de dados.

A próxima subseção destina-se ao exame dos princípios que norteiam o direito à proteção de dados pessoais.

3.3.1 Princípios da proteção de dados pessoais

Como visto, ao longo do processo de convergência internacional das soluções legislativas referentes à proteção de dados pessoais formou-se um consenso em torno de um quadro básico de princípios.

---

[396] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 48.

Estes princípios são preceitos que devem nortear toda a tutela das informações pessoais, desde a construção das normas relativas à matéria até a sua interpretação, dando coerência e unidade ao sistema de proteção de dados. Por conseguinte, deverão orientar e limitar a atividade de tratamento de dados, bem como atribuem ao titular poder de controle sobre suas informações.

Alguns desses princípios estiveram presentes desde as duas primeiras gerações de leis sobre a matéria e foram desenvolvidos pelas leis das gerações seguintes. Diante disso, há certo padrão nos variados ordenamentos jurídicos no que atine aos "*Fair Information Practice Principles"*, isto é, a esse grupo comum de princípios.

O já mencionado relatório sobre Registros, Computadores e Direitos do Cidadão elenca cinco princípios fundamentais que devem ser observados em todo tratamento de dados:

> 1. Não deve haver sistemas de manutenção de registros de dados pessoais cuja existência é secreta.
> 2. Deve haver um meio de uma pessoa descobrir quais informações suas estão em um registro e como são utilizadas.
> 3. Deve haver um meio de uma pessoa impedir que informações a seu respeito obtidas para uma finalidade sejam usadas ou disponibilizadas para outros fins sem o seu consentimento.
> 4. Deve haver um meio de uma pessoa corrigir ou alterar um registro de suas informações pessoais
> 5. Qualquer organização que crie, mantenha, use ou divulgue registros de dados pessoais deve garantir a confiabilidade dos dados para a finalidade pretendida e deve tomar precauções para evitar o uso indevido desses dados[397].

Logo depois, a *Resolution (73) 22 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector (1973)*, do Comitê de Ministros do Conselho da Europa, recomendou aos Estados-Membros que adotassem os seguintes princípios mínimos de proteção em suas legislações:

> Os princípios a seguir se aplicam às informações pessoais armazenadas em bancos de dados eletrônicos no setor privado.
> [...]
> 1. As informações armazenadas devem ser precisas e atualizadas.
> Em geral, informações relacionadas à vida privada íntima de pessoas ou informações que possam levar a discriminação injusta não devem ser registradas ou, se registradas, não devem ser divulgadas.
> 2. As informações devem ser apropriadas e relevantes com relação ao objetivo para o qual foram armazenadas.
> 3. As informações não devem ser obtidas por meios fraudulentos ou injustos.
> 4. Devem ser estabelecidas regras para especificar os períodos após os quais certas categorias de informações não devem mais ser mantidas ou usadas.

[397] WARE, W. H. **Records, Computers and the Rights of Citizens.** Ago. 1973. Disponível em: https://www.rand.org/content/dam/rand/pubs/papers/2008/P5077.pdf. Acesso em: 20 abr. 2020.

> 5. Sem a devida autorização, as informações não devem ser usadas para outros fins que não aqueles para os quais foram armazenadas, nem comunicadas a terceiros.
> 6. Como regra geral, a pessoa em questão deve ter o direito de conhecer as informações armazenadas sobre ela, a finalidade para a qual foram registradas e os detalhes de cada liberação dessas informações.
> 7. Todo cuidado deve ser tomado para corrigir informações imprecisas e apagar informações obsoletas ou obtidas de maneira ilegal.
> 8. Devem ser tomadas precauções contra qualquer abuso ou uso indevido de informações.
> Os bancos de dados eletrônicos devem estar equipados com sistemas de segurança que impeçam o acesso aos dados mantidos por pessoas não autorizadas a obter essas informações e que permitam a detecção de desvio de informações, intencional ou não.
> 9. O acesso às informações armazenadas deve ser restrito a pessoas que tenham um motivo válido para conhecê-las.
> A equipe operacional dos bancos de dados eletrônicos deve estar vinculada a regras de conduta destinadas a impedir o uso indevido de dados e, em particular, a regras de sigilo profissional.
> 10. Os dados estatísticos devem ser divulgados apenas de forma agregada e de forma que seja impossível vincular as informações a uma pessoa em particular[398].

As diversas legislações nacionais e os documentos internacionais que se seguiram passaram a adotar tais princípios, os quais ganharam força principalmente por meio das diretrizes da OCDE[399] e da Convenção de Estrasburgo[400].

---

[398] CONSELHO DA EUROPA. Committee of Ministers. **Resolution (73) 22, On The Protection of the Privacy of Individuals Vis-a-Vis Electronic Data Banks in the Private Sector**. 26 set. 1973. Disponível em: https://rm.coe.int/1680502830. Acesso em: 17 mar. 2020.

[399] As diretrizes da OCDE intentavam que os países incorporassem em seu direito interno os seguintes princípios: 7. Deverá haver limites para a coleta de dados pessoais e esses dados devem ser obtidos por meios legais e justos e, quando apropriado, com o conhecimento ou consentimento do titular dos dados. (Princípio da limitação da coleta); 8. Os dados pessoais devem ser relevantes para os fins para os quais devem ser utilizados e, na medida do necessário para esses fins, devem ser precisos, completos e atualizados. (Princípio da qualidade dos dados); 9. Os propósitos para os quais os dados pessoais são coletados devem ser especificados o mais tardar no momento da coleta de dados e o uso subseqüente limitado ao cumprimento desses propósitos ou de outros que não sejam incompatíveis com esses propósitos e os especificados em cada ocasião de mudança de propósito. (Princípio de especificação de finalidade); 10. Os dados pessoais não devem ser divulgados, disponibilizados ou utilizados para outros fins que não aqueles especificados em conformidade com o parágrafo 9, exceto: a) com o consentimento do titular dos dados; ou b) pela autoridade da lei. (Princípio da limitação de uso); 11. Os dados pessoais devem ser protegidos por garantias razoáveis de segurança contra riscos como perda ou acesso não autorizado, destruição, uso, modificação ou divulgação de dados. (Princípio de garantias de segurança); 12. Deve haver uma política geral de abertura sobre desenvolvimentos, práticas e políticas com relação aos dados pessoais. Devem estar prontamente disponíveis meios para estabelecer a existência e a natureza dos dados pessoais e os principais objetivos de seu uso, bem como a identidade e a residência habitual do controlador de dados. (Princípio da Abertura); 13. Um indivíduo deve ter o direito de: a) obter de um controlador de dados, ou não, a confirmação sobre se o controlador de dados possui ou não dados relacionados a ele; b) ter lhe comunicado os dados a ele dentro de um prazo razoável; a um custo, se houver, que não seja excessivo; de uma maneira razoável; e de uma forma que seja prontamente inteligível para ele; c) obter os fundamentos se um pedido feito sob as alíneas (a) e (b) for negado e poder contestar a negativa; e d) contestar dados a ele relacionados e, se a contestação for aceita, ter os dados apagados, retificados, complementados ou alterados. (Princípio da participação individual); 14. Um controlador de dados deve ser responsável pelo cumprimento de medidas que efetivem os princípios mencionados acima. (Princípio da responsabilidade).
OCDE. **OECD Guidelines o the Protection of Privacy and Transborder Flows of Personal Data.** 2013. Disponível em: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Acesso em: 20 abr. 2020.

[400] Capítulo II - Princípios básicos de proteção de dados. [...]. Artigo 5 - Qualidade dos dados. Os dados pessoais em processamento automático devem ser: a) obtidos e processados de forma justa e legal; b) armazenados para

Observa-se que há bastante semelhança entre os princípios previstos nos documentos acima, os quais influenciaram legislações nacionais, tratados, convenções internacionais e até mesmo acordos entre organizações privadas. Desse modo, mesmo com diferenças de técnicas legislativas entre os variados ordenamentos jurídicos, os *FIPPs* formam o núcleo da proteção dos dados pessoais[401].

A seguir, analisa-se o conteúdo de tais princípios.

1. Princípio da finalidade: todo dado pessoal deve ser coletado para uma finalidade específica conhecida pelo titular da informação e deve passar pelos procedimentos necessários ao alcance de tal fim. Doneda considera que esse princípio é de grande relevância prática por restringir a transferência de dados a terceiros, bem como por servir de critério para valorar a razoabilidade da utilização de determinados dados para certa finalidade, fora da qual haveria abusividade[402]. Nessa senda, esse princípio é essencial para determinar a legitimidade do tratamento de dados, o tempo de conservação desses dados, além da admissibilidade de sua conexão com outros bancos de dados[403].

2. Princípio da publicidade (ou da transparência): esse princípio exige que a existência de todo banco de dados pessoais deve ser de conhecimento público, reafirmando o preceito democrático e baseando-se na ideia de que a transparência é uma das principais formas de combate aos abusos. Essa publicidade deve ocorrer mediante a publicação do nome, sede e conteúdo do banco de dados em registros públicos ou em meios de grande circulação. Alguns países exigem autorização estatal prévia ou notificação ao órgão supervisor para o funcionamento do banco de dados[404].

---

fins específicos e legítimos e não utilizados de maneira incompatível com esses fins; c) adequados, relevantes e não excessivos em relação aos fins para os quais são armazenados; d) precisos e, quando necessário, atualizados; e) preservados de forma que permita a identificação dos titulares dos dados por um período não superior ao necessário para a finalidade para a qual esses dados são armazenados. Artigo 6 - Categorias especiais de dados Os dados pessoais que revelam origem racial, opiniões políticas ou crenças religiosas ou outras, bem como dados pessoais relativos à saúde ou vida sexual, não podem ser processados automaticamente, a menos que a lei interna forneça salvaguardas adequadas. O mesmo se aplica aos dados pessoais relacionados a condenações penais.
Artigo 7 - Segurança de dados. Devem ser tomadas medidas de segurança adequadas para a proteção de dados pessoais armazenados em arquivos de dados automatizados contra destruição ou perda acidental ou não autorizada, bem como contra acesso, alteração ou disseminação não autorizada. Artigo 8 - Garantias adicionais para o titular dos dados [...].

[401] 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. 182.

[402] 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. 182.

[403] RODOTÀ, Stefano. **A vida na sociedade de vigilância – a privacidade hoje.** Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 104.

[404] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 71.

3. Princípio da qualidade dos dados: os dados pessoais armazenados em um banco de dados devem ser fiéis à realidade, de modo que devem ser coletados com cuidado e correção, além de atualizados periodicamente de acordo com a necessidade. Constatando-se incorreções, impertinências ou obsolescência, as informações deverão ser corrigidas, suprimidas ou até mesmo sofrer acréscimos[405].

4. Princípio do livre acesso: o titular dos dados deve ter acesso ao banco de dados no qual suas informações estão armazenadas, podendo obter cópias desses registros com vistas a permitir que o indivíduo tenha controle sobre seus dados[406].

5. Princípio da segurança física e lógica: os dados pessoais devem ser protegidos contra extravios destruições, modificações, transmissões e acessos não autorizados[407].

A Lei Geral de Proteção de Dados Pessoais, seguindo esse padrão, dispôs em seu artigo 6º que as atividades de tratamento de dados pessoais deverão observar, além da boa-fé, dez princípios, quais sejam:

a) finalidade, pelo qual o tratamento somente poderá ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

b) adequação, pelo qual o tratamento de dados deve ser compatível com as finalidades informadas ao titular;

c) necessidade (ou minimização), o qual limita o tratamento de dados ao mínimo necessário para a realização da finalidade, de modo que os dados devem ser pertinentes, proporcionais e não excessivos em relação à finalidade;

d) livre acesso, que garante aos titulares a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

e) qualidade dos dados, garantindo aos titulares a exatidão, a clareza, a relevância e a atualização de seus dados, de acordo com a necessidade e a finalidade do tratamento;

f) transparência, pelo qual devem ser fornecidas ao titular informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

---

[405] 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. 182.
[406] 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. 182.
[407] 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. 182.

g) segurança, o qual exige a adoção 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;

h) prevenção, o qual impõe a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

i) não discriminação, segundo o qual o tratamento de dados não pode ocorrer visando fins discriminatórios ilícitos ou abusivos;

j) responsabilização e prestação de contas, pelo qual o agente deve demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Para uma tutela adequada da proteção de dados pessoais, estes princípios, devem coexistir, haja vista que muitos deles se complementam, de modo que a efetividade de um depende também da aplicação do outro. Exemplificativamente, o princípio da prevenção exige que o agente de tratamento aja proativamente para evitar danos, mas é pelo princípio da responsabilização e prestação de contas que os titulares e a autoridade nacional poderão aferir se o controlador ou o operador de fato aplicou aquele princípio. Da mesma forma, verificar a adoção dos princípios da finalidade, da adequação e da necessidade exige uma atuação transparente por parte do agente de tratamento.

A presença desses princípios, para além do artigo 6º, sé identificada ao longo de toda a LGPD, sobremodo nos artigos pertinentes às obrigações dos agentes de tratamentos e dos direitos dos titulares, favorecendo a concretização de tais princípios, bem como a unidade e a coerência do sistema de proteção de dados pessoais previsto na Lei nº 13.709/2018.

O Regulamento Geral da União Europeia também prevê princípios[408] com conteúdos bastante semelhantes ao da lei brasileira: a) licitude, lealdade e transparência; b) limitação das

[408] Artigo 5º Princípios relativos ao tratamento de dados pessoais. 1. Os dados pessoais são: a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados (“licitude, lealdade e transparência”); b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89º, nº 1 (“limitação das finalidades”); c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados (“minimização dos dados”); d) Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora (“exatidão”); e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89º, nº 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados (“limitação da conservação”); f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu

finalidades; c) minimização dos dados; d) exatidão; e) limitação da conservação; f) integridade e confidencialidade; g) responsabilidade, os quais concebe como princípios essenciais da proteção de dados, ante a sua importância e padronização internacional.

Em seus considerandos, o Regulamento, ainda, traz outros princípios aplicáveis ao processamento de informações pessoais, tais como o do tratamento equitativo (considerando 60), o da proporcionalidade (considerando 4), o do *no bis in idem* (considerando 149), o do direito de acesso público aos documentos oficiais (considerando 154).

Dessa forma, os princípios não precisam estar positivados para serem aplicáveis. Isso permite, por exemplo, que o princípio do tratamento equitativo exija do agente de tratamento esforços no sentido de evitar a discriminação mesmo não estando na parte obrigatória do RGPD.

Assim, quando os países foram reconhecendo que a massiva coleta de informações ameaçava direitos fundamentais dos indivíduos, surgiram iniciativas internacionais para se criar um núcleo de proteção aos dados pessoais, haja vista que muito pouco adiantaria que estas informações fossem protegidas apenas pelo ordenamento jurídico interno se tais dados facilmente podem ser coletados, tratados ou compartilhados por organizações de um país terceiro que não oferece a mesma proteção.

Ademais, vez que as legislações costumam criar restrições à transferência internacional de dados para Estados e organismos que não salvaguardam o titular dos dados, fazia-se necessário estabelecer alguma uniformização no tratamento de dados, de modo a se facilitar o fluxo de informações entre os países e viabilizar as atividades econômicas que dele dependem.

Diante disso, formou-se uma importante convergência na tutela dos dados pessoais por meio dos princípios apresentados, o que, principalmente, garante efetividade ao direito à proteção dos dados pessoais num mundo globalizado.

Estes princípios de proteção de dados pessoais são essenciais para impor limites à atuação dos agentes de tratamento, públicos e privados, nortear a interpretação das disposições legais atinentes à matéria, guiar a licitude dos processamentos de dados mesmo em situações de lacuna legislativa, bem como atribuir deveres às organizações e direitos aos titulares dos dados, já tendo a LGPD preceituado algumas obrigações e garantias que decorrem diretamente destes princípios, conforme se estudará adiante.

---

tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas (“integridade e confidencialidade”); 2. O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo (“responsabilidade”).

3.3.2 Direitos do titular dos dados pessoais

Como efeito do movimento de convergência internacional da tutela dos dados pessoais, também se verifica um padrão referente aos direitos dos titulares desses dados nos diferentes ordenamentos jurídicos. Muitos desses direitos decorrem da observância dos *FIPPs* pelas legislações.

Mendes[409] assim resume os direitos dos titulares encontrados na maior parte das leis sobre proteção de dados pessoais: a) direito geral de informação; b) direito de acesso; c) direito de notificação; d) direito de retificação, cancelamento e bloqueio dos dados; e) direito de não ficar sujeito a uma decisão individual automatizada.

O direito geral de informação é o direito dos indivíduos de tomarem conhecimento a respeito dos bancos de dados existentes, de quem é o responsável pelo tratamento de dados, qual o objetivo do tratamento, bem como quais os destinatários dos dados em caso de transferência. Além disso, a pessoa deve ser informada de quais são os seus direitos e as formas de exercê-los em cada fase do tratamento de dados pessoais.

Já o direito de acesso corresponde ao direito do indivíduo de obter, sempre que requisitar, informação sobre os seus dados pessoais que estão armazenados no banco de dados, "incluindo informações acerca da sua origem; sobre os organismos receptores das informações transmitidas ou a sua categoria; e sobre o objetivo do armazenamento", bem como sobre qual banco de dados está armazenando as suas informações, quando se tratar de uma rede de bancos de dados, cabendo a qualquer banco da rede encaminhar a solicitação do titular ao organismo responsável pelo tratamento.

O direito de notificação consiste no direito do indivíduo de ser informado sempre que seus dados forem coletados sem o seu conhecimento a respeito do armazenamento, da identidade do responsável pelo banco de dados e do objetivo do tratamento. O indivíduo deverá ser notificado, ainda, quando houver transferência de seus dados, constando da notificação os organismos receptores.

Os direitos de retificação, cancelamento e bloqueio dos dados, como o próprio nome sugere, correspondem à garantia de o indivíduo corrigir seus dados pessoais em caso de equívoco, apagá-los quando estiverem obsoletos ou tiverem sido indevidamente armazenados, bem como de bloquear o uso de tais dados quando não for permitido por lei ou não for possível, faticamente, proceder ao cancelamento dos dados. Os dados também poderão ser

---

[409] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 65-68.

bloqueados na hipótese de controvérsia sobre a veracidade dessas informações. Todos os organismos que receberam transferência de dados devem ser notificados para tomar as mesmas providências solicitadas pelo titular.

Mendes trata ainda do direito do indivíduo de não ficar sujeito a uma decisão individual automatizada, pelo qual o cidadão tem o direito de não ficar submetido a decisões que repercutem em sua posição jurídica, tomadas exclusivamente com base no tratamento automatizado de dados.

Nesse particular, cumpre dizer que, em que pese a maior parte dos países europeus aplique esse direito em virtude de já ter sido uma previsão da Diretiva Europeia 95/46/CE, reafirmada no Regulamento Geral de Proteção de Dados, no Brasil, a LGPD, em sua redação original, dispunha que o titular dos dados tinha direito a solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, revisão esta a ser realizada por pessoa natural. Essa disposição, contudo, sofreu alteração. O artigo 20º da LGPD ostenta atualmente a seguinte redação:

> Art. 20º 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. (Redação dada pela Lei nº 13.853, de 2019).
> § 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.

Ou seja, retirou-se a obrigatoriedade de as decisões tomadas por meio de tratamento automatizado serem revisadas por pessoa natural. Por outro lado, buscando-se dar alguma efetividade ao direito do indivíduo de não ficar submetido a uma decisão automatizada, a LGPD atribui ao controlador a obrigação de fornecer, sempre que solicitado, informações claras a respeito do procedimento que levou à decisão, sob pena de a autoridade nacional realizar auditoria para verificação de aspectos discriminatórios no referido tratamento.

Além desse direito, a Lei Geral de Proteção de Dados Pessoais, em seus artigos 17 a 22, prevê uma série de outros direitos dos titulares, a saber: a) confirmação da existência de tratamento de seus dados pessoais; b) acesso aos dados; c) correção de dados incompletos, inexatos ou desatualizados; c) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei; d) portabilidade dos

dados a outro fornecedor de serviço ou produto; e) eliminação dos dados pessoais tratados com o consentimento do titular; f) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; g) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; h) revogação do consentimento; i) direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional; j) direito de opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto na lei; k) direito à cópia eletrônica integral de seus dados pessoais em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento, nas hipóteses em que o tratamento tiver origem no consentimento do titular ou em contrato.

Em caso de impossibilidade de adoção imediata da providência, o controlador enviará ao titular resposta em que indicará as razões de fato ou de direito que impedem a adoção imediata da providência.

Além disso, 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 for comprovadamente impossível ou implique esforço desproporcional.

A respeito do direito de acesso, a LGPD buscou fazer que este direito possa realmente ser utilizado pelos titulares dos dados, livre de maiores obstáculos que o transformassem em uma mera previsão formal sem efetividade. Nessa senda, dispôs que o procedimento de acesso deve ser facilitado, gratuito e alcançar, além da forma e duração do tratamento, a integralidade dos dados pessoais.

Na mesma esteira, o Regulamento Geral de Proteção de Dados prevê praticamente os mesmos direitos que a lei brasileira, verificando-se convergência entre as duas leis também nesse ponto.

No entanto, o RGPD faz um detalhamento bem maior de cada um desses, o que facilitará e uniformizará a aplicação de tais direitos pelos países-membros, além de demonstrar todo o desenvolvimento que a proteção de dados experimentou na Europa, por ser uma legislação que contou com décadas de amadurecimento da matéria.

Como exemplo tem-se o direito de oposição. Ao contrário da lei brasileira que apenas faz uma previsão genérica, o Regulamento expressamente permite que o titular se oponha ao

tratamento de dados para fins de comercialização direta de seus dados pessoais, o que abrange, inclusive, a definição de perfis, caso esteja relacionada com tal comercialização[410].

No que diz respeito às decisões individuais automatizadas, o Regulamento garante ao indivíduo o direito de obter "intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão"[411], ao contrário da LGPD que, após ter seu texto alterado, deixou de assegurar o direito do indivíduo de ver revisadas por uma pessoa natural as decisões automatizadas a que está submetido.

Por fim, o RGPD prevê em seu artigo 17, expressamente, o direito ao esquecimento[412], ao passo que a Lei Geral de Proteção de Dados Pessoais é silente a esse respeito. Esse direito, que pode ser compreendido sinteticamente como o direito de o indivíduo se opor à recordação pública e opressiva de determinados fatos, os quais enfatizam, perante terceiros, aspectos de sua personalidade que já não refletem a realidade[413], sempre gerou muitos debates na doutrina brasileira; estes poderão ser reavivados com a vigência da LGPD, mesmo com a recente decisão do Supremo Tribunal Federal que afirmou que esse direito é incompatível com a

---

[410] Artigo 21º Direito de oposição [...]. 2. Quando os dados pessoais forem tratados para efeitos de comercialização direta, o titular dos dados tem o direito de se opor a qualquer momento ao tratamento dos dados pessoais que lhe digam respeito para os efeitos da referida comercialização, o que abrange a definição de perfis na medida em que esteja relacionada com a comercialização direta. 3. Caso o titular dos dados se oponha ao tratamento para efeitos de comercialização direta, os dados pessoais deixam de ser tratados para esse fim.

[411] Artigo 22º Decisões individuais automatizadas, incluindo definição de perfis. 1. O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar. 2. O nº 1 não se aplica se a decisão: a) For necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento; b) For autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou c) For baseada no consentimento explícito do titular dos dados. 3. Nos casos a que se referem o nº 2, alíneas a) e c), o responsável pelo tratamento aplica medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão. 4. As decisões a que se refere o nº 2 não se baseiam nas categorias especiais de dados pessoais a que se refere o artigo 9º, nº 1, a não ser que o nº 2, alínea a) ou g), do mesmo artigo sejam aplicáveis e sejam aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular.

[412] Artigo 17. Direito ao apagamento dos dados ("direito a ser esquecido"). 1. O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos: a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento; b) O titular retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6, n. 1, alínea (a), ou do artigo 9, n. 2, alínea (a) e se não existir outro fundamento jurídico para o referido tratamento; c) O titular opõe-se ao tratamento nos termos do artigo 21, n. 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21, n. 2; d) Os dados pessoais foram tratados ilicitamente; e) Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito; f) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8, n. 1.

[413] SCHREIBER, Anderson. Direito ao Esquecimento e Proteção de Dados Pessoais na Lei 13.709/2018: distinções e potenciais convergências. *In:* FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro.** São Paulo: Thomson Reuters Brasil, 2019, p. 375.

Constituição, já que a decisão não incluiu o direito à desindexação, o qual, para o Tribunal, difere do direito ao esquecimento[414].

Neste trabalho, adota-se a classificação de Voss e Castets-Renard, os quais afirmam que o direito ao esquecimento abrange cinco categorias: 1. direito de reabilitação, que seria o direito ao esquecimento do passado judicial; 2. direito de apagamento, isto é, a possibilidade de apagar dados, de acordo com a previsão das legislações de proteção de dados; 3. direito à desindexação, que é a exclusão dos resultados de buscas dos provedores de pesquisa de *hyperlinks* que direcionam os usuários a páginas da *internet* que apresentem conteúdos irrelevantes ou desatualizados sobre o indivíduo; 4. direito à obscuridade, pelo qual as informações não seriam apagadas ou desindexadas, mas seriam aplicadas técnicas que dificultassem os dados de ser encontrados na rede, de modo que ficariam obscuros; 5. direito ao esquecimento dos dados recolhidos na sociedade da informação, pelo qual as informações compartilhadas teriam uma data de expiração[415].

Tendo em vista tal classificação e a partir de uma interpretação sistemática da lei, em especial de acordo com o princípio da necessidade, percebe-se que a lei brasileira também reconhece o direito ao esquecimento, no âmbito da proteção de dados. Em seu artigo 16 dispõe que os dados pessoais serão eliminados após o término de seu tratamento. Já em seu artigo 18, IV e IV, estabelece que o titular tem direito à eliminação dos dados pessoais desnecessários, excessivos ou tratados em desconformidade com a lei ou sem o seu consentimento.

A LGPD, apesar de fazê-lo difusamente, traz disposições bastante semelhantes ao previsto no artigo 17 do RGPD, de forma que poderá ser usada como base legal infraconstitucional para reconhecer o direito ao esquecimento como pretensão válida no ordenamento jurídico brasileiro, ao menos de três das suas subcategorias: direito ao apagamento, direito à desindexação e direito ao esquecimento dos dados recolhidos na sociedade da informação.

Os direitos expressamente previstos na Lei Geral de Proteção de Dados Pessoais não são os únicos instrumentos que podem ser utilizados para tutelar os dados pessoais, haja vista que, no caso concreto, outros remédios mostram-se igualmente legítimos e até mais

---

[414] BELMUDES, Guilherme. Impactos do julgamento do STF sobre o direito ao esquecimento. **Jota – Opinião e Análise,** 18 fev. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/impactos-do-julgamento-do-stf-sobre-o-direito-ao-esquecimento-18022021. Acesso em: 23 fev. 2021.

[415] VOSS, W. Gregory; CASTETS-RENARD, Céline Casters. Proposal for na international taxonomy on the various forms of the "Right to be Forgotten": a study on the convergence of norms. **Colo Tech L. J.,** v. 14, n. 2, p. 298, 23 maio 2016. Disponível em: https://ctlj.colorado.edu/wp-content/uploads/2016/06/v.3-final-Voss-and-Renard-5.24.16.pdf. Acesso em: 19 mar. 2020.

adequados à proteção dos interesses do titular[416]. Isso porque uma disciplina rígida e taxativa da tutela dos dados pessoais obstaculizaria que o sistema de proteção acompanhasse a rapidez das mudanças tecnológicas, enfraquecendo-o[417].

A Lei Geral de Proteção de Dados Pessoais traz duas previsões de suma importância para garantir a efetividade dos direitos dos titulares dos dados: a) o exercício regular desses direitos pelo titular não pode ser utilizado em seu prejuízo (art. 21) nem para negar a concessão de um crédito; b) a defesa desses direitos e dos demais interesses dos titulares dos dados poderá ser exercida individual ou coletivamente (art. 22), fortalecendo a efetividade dos direitos dos titulares por meio da atuação dos legitimados, como o Ministério Público, para sua defesa a título coletivo.

Como se vê, os direitos dos titulares elencados na LGPD são basicamente os mesmos verificados na maior parte das legislações sobre proteção de dados, os quais, além de intentar sanar violações ao direito à privacidade, buscam prevenir danos, isto é, garantir a própria efetividade desse direito. Dessa feita, não são interesses juridicamente tutelados por si mesmos; trata-se de remédios que instrumentalizam a tutela da privacidade, tornando-a efetiva. Não sem razão a maioria decorre dos princípios de proteção aos dados pessoais, sendo necessários à realização de tais diretrizes.

3.3.3 Autoridade de proteção de dados pessoais

Além dos princípios e direitos dos titulares em comum previstos nas diferentes legislações sobre proteção de dados, há outro ponto convergente e que tem se mostrado essencial à efetividade de tais normas: a existência de órgãos administrativos de proteção de dados pessoais. Dos mais de 120 países que aprovaram leis sobre a matéria, somente 12 não criaram uma autoridade independente[418].

As leis não são autoimplementáveis, ao contrário, sua efetividade tem sido fortemente atrelada à existência e ao modo de atuação das autoridades de proteção de dados pessoais. Os

---

[416] SOUZA, Eduardo Nunes de; SILVA, Rodrigo da Guia. Direitos do titular de dados pessoais na Lei 13.709/2018: uma abordagem sistemática. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coords.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** São Paulo: Thomson Reuters Brasil, 2019, p. 281.

[417] RODOTÀ, Stefano. **A vida na sociedade de vigilância – a privacidade hoje.** Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 89.

[418] VASCONCELOS, Beto; PAULA, Felipe de. A autoridade nacional de proteção de dados: origem, avanços e pontos críticos. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coords.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** São Paulo: Thomson Reuters Brasil, 2019, 722.

países que não criam essas autoridades, como os Estados Unidos, são criticados por aprovar leis sem fornecer o mecanismo institucional por meio do qual a conformidade com a lei e as boas práticas serão incentivadas e fiscalizadas[419]. A cultura de privacidade não pode se estabelecer se não houver uma autoridade que a patrocine[420].

As Autoridades de Proteção de Dados exercem várias funções, sendo as principais as de ouvidoria, auditoria, consultoria, educação, consultoria e políticas públicas, negociação e execução da legislação. Ressalte-se, contudo, que esse rol de atividades não é universalmente encontrado entre as competências de todas as autoridades, de modo que algumas delas podem enfatizar a aplicação da lei, outras podem se concentrar em educar o público e as organizações, e outras podem estar mais envolvidas na orientação de políticas públicas e na elaboração de códigos de conduta[421].

As funções das Autoridades de Proteção de Dados não são globalmente uniformes. Entretanto, há um traço comum em todas elas: o monitoramento e a avaliação do desenvolvimento tecnológico em tratamento de dados pessoais. Esses órgãos geralmente são dotados de especialistas capazes de fiscalizar e educar acerca da proteção e segurança dos dados, bem como podem analisar a estrutura de entes públicos e privados quanto ao tratamento dessas informações, e rastrear todos os procedimentos que o tratamento envolve, identificando deficiências e propondo soluções adequadas[422].

O Brasil seguiu a experiência internacional. A Autoridade Nacional de Proteção de Dados, criada pela Medida Provisória nº 869, de 27 de dezembro de 2018, posteriormente convertida na Lei 13.853/2019, terá um papel essencial para a construção da cultura de privacidade no país.

A ela competirão funções essenciais, não só a de garantir a aplicação da LGPD pelos agentes de tratamento, fiscalizando e aplicando sanções em caso de tratamento de dados realizado em descumprimento à legislação, mas também na promoção do conhecimento da população acerca de seus direitos e da forma de exercê-los, bem como na implementação de

---

[419] RAAB, Charles; SZEKELY, Ivan. Data Protection Authorities and Informations Technology. **Computer Law & Security Review,** v. 33, n. 4, ago. 2017. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0267364917301619. Acesso em: 20 abr. 2020, p. 421.

[420] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 49.

[421] RAAB, Charles; SZEKELY, Ivan. Data Protection Authorities and Informations Technology. **Computer Law & Security Review,** v. 33, n. 4, ago. 2017. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0267364917301619. Acesso em: 20 abr. 2020, p. 422.

[422] RAAB, Charles; SZEKELY, Ivan. Data Protection Authorities and Informations Technology. **Computer Law & Security Review,** v. 33, n. 4, ago. 2017. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0267364917301619. Acesso em: 20 abr. 2020, p. 422.

mecanismos simplificados e virtuais para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com a lei.

À ANPD caberá dispor sobre padrões técnicos mínimos de segurança dos dados, estimular a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais, bem como reconhecer e divulgar regras de boas práticas e de governança adotadas pelos agentes de tratamento, de forma a incitar a corregulação do mercado, visando a uma mudança de cultura na qual os agentes de tratamento vão além de cumprir a legislação por medo das sanções; eles formulam suas próprias regras de boas práticas.

Ainda, compete-lhe realizar auditorias, deliberar em caráter terminativo, na esfera administrativa, sobre a interpretação da LGPD, além de 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.

Caberá à ANPD, também, regulamentar diversas disposições da lei. É, portanto, evidente a importância da autoridade nacional para a implementação da legislação sobre a proteção de dados. Sem esse órgão, mais que ficar incompleto, o sistema de proteção poderá se tornar ineficiente, causar insegurança jurídica, além de deixar nas mãos do Judiciário, já tão assoberbado e sem especialistas na matéria, a tarefa de dar concretude a muitas das previsões da Lei Geral de Proteção de Dados Pessoais, o que dificultará a manutenção de padrões atinentes à aplicação da lei.

Não sem motivo, o veto da Lei 13.709/2018, que impediu a criação da Autoridade Nacional por questões técnicas, bem como o ínterim entre a aprovação da Medida Provisória que a criou e a sua conversão em lei, gerou grande preocupação entre os especialistas da área, que temiam a entrada em vigor da lei sem que a Autoridade estivesse pronta para funcionar.

Para que a Autoridade Nacional possa exercer suas funções de maneira eficiente, faz-se necessário que ela seja independente, com real autonomia, na prática, para o desempenho de suas atividades, inclusive no que diz respeito ao setor público, que também é regulado pela LGPD.

Essa independência é de extrema relevância para uma atuação efetiva e característica de quase todas as autoridades nacionais. Acerca disso, por exemplo, o Regulamento Geral de Proteção de Dados da União Europeia estabeleceu que os Estados-Membros deveriam criar uma ou mais autoridades públicas independentes, dispondo em seu artigo 52º que:

> 1. As autoridades de controlo agem com total independência no na prossecução das suas atribuições e no exercício dos poderes que lhe são atribuídos nos termos do presente regulamento.
> 2. Os membros das autoridades de controlo não estão sujeitos a influências externas, diretas ou indiretas no desempenho das suas funções e no exercício dos seus poderes nos termos do presente regulamento, e não solicitam nem recebem instruções de outrem.
> 3. Os membros da autoridade de controlo abstêm-se de qualquer ato incompatível com as suas funções e, durante o seu mandato, não podem desempenhar nenhuma atividade, remunerada ou não, que com elas seja incompatível.
> 4. Os Estados-Membros asseguram que cada autoridade de controlo disponha dos recursos humanos, técnicos e financeiros, instalações e infraestruturas necessários à prossecução eficaz das suas atribuições e ao exercício dos seus poderes, incluindo as executadas no contexto da assistência mútua, da cooperação e da participação no Comitê.
> 5. Os Estados-Membros asseguram que cada autoridade de controlo selecione e disponha do seu próprio pessoal, que ficará sob a direção exclusiva dos membros da autoridade de controlo interessada.
> 6. Os Estados-Membros asseguram que cada autoridade de controlo fique sujeita a um controlo financeiro que não afeta a sua independência e que disponha de orçamentos anuais separados e públicos, que poderão estar integrados no orçamento geral do Estado ou nacional[423].

Foi por essa razão que, inicialmente, a Lei 13.709/2018 criou a Autoridade Nacional de Proteção de Dados (ANPD) como integrante da administração pública federal indireta, submetida a regime autárquico especial e vinculada ao Ministério da Justiça. Desse modo, intentou estabelecer uma autoridade com a independência e a autonomia necessárias.

Entretanto, essa previsão foi vetada e a Lei 13.853/2019, que posteriormente a criou, o fez como órgão da administração pública federal direta, integrante da Presidência da República, prejudicando a existência de um mecanismo institucional verdadeiramente eficaz de fiscalização e aplicação da LGPD.

Isso afasta, nesse particular, o sistema brasileiro de proteção de dados dos demais países, o que poderá impedir a inserção do Brasil na OCDE, bem como o reconhecimento, pela União Europeia, de que o país oferece um nível adequado de proteção de dados pessoais, de modo que o livre fluxo de informações entre os Estados-Membros e o Brasil poderá ser obstaculizado.

Como esperança, tem-se a previsão do artigo 55-A, da § 1º, da LGPD, que dispõe que a natureza jurídica da ANPD poderá ser transformada em entidade da administração pública federal indireta, submetida a regime autárquico especial, o que poderá ocorrer em até dois

---

[423] UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016**. Relativo à proteção de dados pessoais 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 Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679#d1e1554-1-1. Acesso em: 28 jun. 2020.

anos da data da entrada em vigor da estrutura regimental da Autoridade. Aguarda-se que tal transformação aconteça, tendo em vista a essencialidade de sua independência.

Diante do que se demonstrou nesta seção, o movimento de convergência internacional aproximou a disciplina de proteção aos dados pessoais adotada pela maioria dos países do mundo, em especial no tocante aos princípios aplicáveis aos tratamentos dos dados e aos direitos dos titulares, bem como à existência de órgãos administrativos essenciais à implementação das legislações e, portanto, à sua efetividade.

Nesse diapasão, a próxima seção intenta averiguar a importância dessas legislações e, ainda, os motivos que levam os dados pessoais a adquirir tamanha relevância na atualidade, a forma como esses dados são coletados e utilizados na sociedade da informação e como o tratamento dos dados pessoais pode violar a privacidade dos indivíduos.

4 TRATAMENTO DE DADOS PESSOAIS E OS RISCOS À PRIVACIDADE NA SOCIEDADE DA INFORMAÇÃO

O capítulo anterior se dedicou a apresentar os principais conceitos e aspectos relacionados ao direito à proteção de dados pessoais, examinando-se as principais garantias e disposições normativas trazidas pelas legislações sobre a matéria, na busca de uma tutela efetiva do direito à privacidade, numa sociedade em que o indivíduo é constantemente monitorado por meio da coleta e tratamento de seus dados.

Esta seção se propõe a investigar as principais formas de tratamento de dados pessoais na atualidade, os perigos envolvidos em tal atividade e os remédios trazidos pela Lei Geral de Proteção de Dados Pessoais para salvaguardar o direito à privacidade sem frear o desenvolvimento tecnológico. Para tanto, inicialmente será feita uma rápida análise acerca do valor que os dados pessoais adquirem na economia da informação.

4.1 A economia da informação e a monetização dos dados pessoais

Informação e conhecimento sempre foram fundamentais para o crescimento da economia, assim como a evolução tecnológica sempre influenciou as formas de organização econômica e a capacidade produtiva da sociedade. Entretanto, nas últimas décadas do século XX surge, em escala global, uma nova economia[424].

O novo paradigma tecnológico possibilita que a própria informação se torne produto do processo produtivo, de modo que os produtos das novas indústrias são dispositivos de processamento de dados ou o próprio processamento de informações[425].

A economia atual aproveita-se do fenômeno do *big data*, fazendo surgir novos modelos de negócios, que coletam e tratam dados. Essa nova economia se caracteriza como um ambiente no qual ocorrem rápidas transformações e surgem novos tipos de negócios, mas a principal característica é a quantidade de informações disponíveis para processamento[426].

Nessa nova economia, a produtividade e a competividade dos agentes dependem da sua capacidade de gerar, processar e aplicar a informação de forma eficiente. A economia se

---

[424] CASTELLS, Manuel. **A Sociedade em Rede.** (A era da informação: economia, sociedade e cultura; v. 1). São Paulo: Paz e Terra, 1999, p. 119.
[425] CASTELLS, Manuel. **A Sociedade em Rede.** (A era da informação: economia, sociedade e cultura; v. 1). São Paulo: Paz e Terra, 1999, p. 119.
[426] COHEN, Max E. Alguns aspectos do uso da informação na economia da informação. **Ciência da Informação,** v. 31, n. 3, 2002. Disponível em: http://www.scielo.br/scielo.php?pid=S0100-19652002000300003&script=sci_abstract&tlng=pt. Acesso em: 2 abr. 2020, p. 26.

torna cada vez mais capaz de aplicar seu progresso e conhecimento em determinada área no próprio setor, conduzindo a uma maior produtividade e eficiência[427].

Além de tratar e utilizar as informações com eficiência, na economia da informação as organizações bem-sucedidas devem ser flexíveis o bastante para transformar seus meios com a mesma rapidez que os impactos das transformações culturais, tecnológicas e institucionais modificam seus objetivos[428].

Essa nova economia exigiu, e ainda exige, transformações sociais, culturais e até mesmo institucionais. Castells afirma que a economia não é apenas baseada na informação, é informacional, uma vez que também "os atributos culturais e institucionais de todo o sistema social devem ser incluídos na implementação e difusão do novo paradigma tecnológico"[429].

Entre os efeitos da economia da informação, em matéria de transformação na atividade empresarial e nível da indústria, podem ser citados o aumento da eficiência, o aumento de lucro, a participação de mercado e, ainda, a inovação contínua, trazendo transformações nas organizações nos setores de varejo e atacado, logística, construção e automotivo[430].

As principais atividades produtivas, o consumo, o capital, o trabalho, a matéria-prima, a administração, a informação, a tecnologia e os mercados passam a ser organizados em escala global, diretamente ou por meio de uma rede de conexões entre agentes econômicos[431].

Castells[432] leciona que o sistema econômico se interliga globalmente por meio dos seus componentes estratégicos que se tornam igualmente globalizados: os mercados financeiros, o comércio internacional, a produção transnacional e, até certo ponto, a ciência e a tecnologia. As economias de todo o mundo passam a depender do desempenho desse núcleo globalizado.

O destino das economias em geral é decidido, em grande parte, pelo desempenho do capital nos mercados globalmente interdependentes. O capital, a poupança e os investimentos estão interconectados em todo o mundo, de bancos a fundos de pensão, bolsa de valores e câmbio. Isso permite que transações de bilhões de dólares ocorram em questão de segundos

---

[427] CASTELLS, Manuel. **A Sociedade em Rede.** (A era da informação: economia, sociedade e cultura; v. 1). São Paulo: Paz e Terra, 1999, p. 119.
[428] CASTELLS, Manuel. **A Sociedade em Rede.** (A era da informação: economia, sociedade e cultura; v. 1). São Paulo: Paz e Terra, 1999, p. 233.
[429] CASTELLS, Manuel. **A Sociedade em Rede.** (A era da informação: economia, sociedade e cultura; v. 1). São Paulo: Paz e Terra, 1999, p. 141.
[430] D'SOUZA, Chris; WILLIAMS, David. The Digital Economy. **Bank of Canada Review,** 2017. Disponível em: https://www.bankofcanada.ca/wp-content/uploads/2017/05/boc-review-spring17-dsouza.pdf. Acesso em: 02 abr. 2020, p. 4-5.
[431] CASTELLS, Manuel. **A Sociedade em Rede.** (A era da informação: economia, sociedade e cultura; v. 1). São Paulo: Paz e Terra, 1999, p. 119.
[432] CASTELLS, Manuel. **A Sociedade em Rede.** (A era da informação: economia, sociedade e cultura; v. 1). São Paulo: Paz e Terra, 1999, p. 141-147.

em qualquer parte do mundo. Na economia da informação, os fluxos financeiros cresceram em volume, velocidade, complexidade e conectividade.

Nessa nova economia, os movimentos nos mercados financeiros não atendem somente às leis de oferta e procura; são o resultado de uma complexa combinação entre leis de mercado, estratégias empresariais, regulamentos de motivação política e informações outras. O leque de situações capazes de influenciar a economia aumenta consideravelmente.

Essa globalização da economia promoveu uma nova onda de concorrência entre os agentes econômicos já existentes e os que surgiram, levando a transformações tecnológicas substanciais de processos e produtos que aumentaram a produtividade de alguns setores e organizações empresárias. Esse acréscimo produtivo e competitivo, como não podia deixar de ser, também se baseia na capacidade tecnológica, no processamento de dados e na geração de informações[433].

A economia da informação orienta-se de maneira profundamente interdependente. Isso significa que nenhuma grande organização empresária é autossuficiente, ao contrário, suas atividades são conduzidas com uma série de outras organizações, não somente com subcontratadas ou auxiliares, mas com "parceiras relativamente iguais, com as quais ao mesmo tempo cooperam e competem neste admirável mundo novo econômico, onde amigos e adversários são os mesmos"[434].

Nessa esteira, não há mudanças nas regras gerais da economia; a mudança que se verifica na economia está na forma como a informação é utilizada, razão pela qual essa nova economia é designada de "economia da informação"[435]. O que mudou não foram as atividades em que a humanidade está envolvida, mas a sua capacidade tecnológica de utilizar aquilo que a torna singular, a saber, sua capacidade de processar símbolos[436].

O avanço tecnológico abre caminho para a monetização de informações, tornando essa prática um dos principais componentes dos modelos de negócios modernos da economia da informação[437]. Nesse contexto, os dados pessoais são tidos como o novo petróleo[438] e considerados como verdadeiros ativos das organizações empresariais.

---

433 CASTELLS, Manuel. **A Sociedade em Rede.** (A era da informação: economia, sociedade e cultura; v. 1). São Paulo: Paz e Terra, 1999, p. 165.

434 CASTELLS, Manuel. **A Sociedade em Rede.** (A era da informação: economia, sociedade e cultura; v. 1). São Paulo: Paz e Terra, 1999, p. 220.

435 COHEN, Max E. Alguns aspectos do uso da informação na economia da informação. **Ciência da Informação,** v. 31, n. 3, 2002. Disponível em: http://www.scielo.br/scielo.php?pid=S0100-19652002000300003&script=sci_abstract&tlng=pt. Acesso em: 2 abr. 2020, p. 8.

436 CASTELLS, Manuel. **A Sociedade em Rede.** (A era da informação: economia, sociedade e cultura; v. 1). São Paulo: Paz e Terra, 1999, p. 142.

437 ADJEI, Joseph K. Monetization of Personal Identity Information: Technological and Regulatory Framework. **IEEE Computer Society Washington,** Washington DC/EUA, 14 dez. 2015. Disponível em:

Organizações como o *Google* e o *Facebook*, por exemplo, podem utilizar esses dados em proveito próprio, monetizando-os ou utilizando-os para a construção de modelos de negócio neles baseados, alcançando consideráveis retornos financeiros. Em 2019, o *Facebook* obteve receita de US$ 15 bilhões somente no 1º trimestre[439]; já o *Google* obteve uma receita de US$ 46,08 bilhões apenas no último trimestre do referido ano[440].

Outra situação ilustrativa da importância dos dados em relação às receitas das organizações é o caso da *Caesars Entertainment Operating Co*. que, em 2015, anunciou a falência de sua unidade operacional de cassinos, tendo como principal ponto de disputa pelos credores o seu programa de fidelidade dos clientes, o *Total Rewards Loyalty Program*[441].

A *Caesars Entertainment* administrava mais de cinquenta outros cassinos em todo o mundo e se estabeleceu como uma das primeiras líderes em *marketing* e atendimento ao cliente orientados por *big data.* Por meio do *Total Rewards*, a organização coletou, durante 17 anos, dados de mais 45 milhões de clientes desde o momento em que estes faziam a reserva até o momento em que deixavam os cassinos.

O programa oferecia refeições, *upgrades* de quarto, ingressos para shows e passeios de limusine para clientes que gastassem dinheiro nos *resorts* e mesas de jogo da *Caesars*. À medida que gastavam mais, os clientes recebiam mais recompensas. Além dos gastos, o programa de fidelidade coletava informações acerca do comportamento dos usuários nas instalações. Tudo isso permitia que as ofertas pudessem ser adaptadas e que a equipe de

---

https://www.researchgate.net/profile/Joseph_Adjei3/publication/325142873_Monetization_of_personal_digital_identity_information_Technological_and_regulatory_framework/links/5be99f48a6fdcc3a8dd1b2a1/Monetization-of-personal-digital-identity-information-Technological-and-regulatory-framework.pdf. Acesso em: 2 abr. 2020, p. 1.

438 A expressão *"Data is the new oil"* foi dita pela primeira vez, em 2006, pelo matemático Clive Humby a Michael Palmer, da Associação de Anunciantes Nacionais. Entretanto, a metáfora utilizada por Clive se destinava muito mais a apontar a necessidade de que os dados fossem tratados para que tivessem valor: *"Data is the new oil [...]. It's valuable, but if unrefined it cannot really be used. It has to be changed into gas, plastic, chemicals etc to create a valuable entity that drives profitable activity; so must data be broken down, analyzed for it to have value"*. Em tradução livre: "Dados são o novo petróleo [...]. São valiosos, mas se não forem refinados, não podem ser realmente utilizados. Eles precisam ser transformados em gás, plástico, produtos químicos etc. para criar uma entidade valiosa que impulsiona atividades lucrativas; assim, os dados devem ser discriminados, analisados para que tenham valor". (PALMER, Michael. Data is the new oil. **ANA Marketing Maestros,** 3 nov. 2006. Disponível em: https://ana.blogs.com/maestros/2006/11/data_is_the_new.html. Acesso em: 28 jun. 2020). Apesar disso, ao longo do tempo a expressão vem sendo amplamente utilizada para designar o quão valiosos são os dados na nova economia.

439 HYEON OH, Se. *Facebook* obtém receita de US$ 15 bilhões no 1º trimestre de 2019. **Canaltech**, 24 abr. 2019. Disponível em: https://canaltech.com.br/resultados-financeiros/facebook-obtem-receita-de-us-15-bilhoes-no-1o-trimestre-de-2019-137867/. Acesso em: 15 abr. 2020.

440 SANTINO, Renato. *Google* recebeu mais de US$ 15 bilhões com anúncios do YouTube em 2019. **Olhar Digital**, 3 fev. 2020. Disponível em: https://olhardigital.com.br/noticia/google-recebeu-mais-de-us-15-bilhoes-com-anuncios-do-youtube-em-2019/96248. Acesso em: 15 abr. 2020.

441 MARR, Bernard. Big Data At Caesars Entertainment – A one billion dollar asset? **Forbes,** 18 maio 2015. Disponível em: https://www.forbes.com/sites/bernardmarr/2015/05/18/when-big-data-becomes-your-most-valuable-asset/#318235b61eef. Acesso em: 28 jun. 2020.

funcionários dos cassinos estivesse pronta para receber os clientes pelo nome e direcioná-los para o jogo favorito. No nível superior de recompensas, conhecido como sete estrelas, os hóspedes recebiam até quatro noites de cortesia nos hotéis *Caesars*, bem como subsídios de tarifa aérea.

A viagem de cada cliente era monitorada em tempo real, permitindo que os representantes da organização oferecessem uma refeição ou pernoite de cortesia como prêmio de consolação a um jogador infeliz. Tudo isso, é claro, se as análises apontassem que o investimento teria um retorno a longo prazo. A grande variedade de atividades oferecidas nos locais de *Caesars*, de restaurantes e jogos a shows, compras e tratamentos de *spa*, possibilitou que uma grande variedade de dados pudesse ser coletada sobre muitos aspectos da vida dos usuários. Essa visão geral mais ampla das preferências de uma pessoa permite que sejam feitas análises mais precisas sobre como garantir que cada cliente sempre retorne aos estabelecimentos.

O *Total Rewards* foi estimado em mais de US$ 1 bilhão, sendo considerado o ativo individual de maior valor da organização, superior a qualquer bem físico da unidade falida e, por conseguinte, tornando-se bastante disputado pelos credores. No entanto, a matriz da *Caesars Entertainment*, ainda solvente, transferiu para si o programa de fidelidade, o que gerou uma investigação independente, já que os credores acusaram a organização de tentar manter para si os seus melhores ativos.

Pelo caso acima relatado, é possível concluir que os dados pessoais representam atualmente uma importante fonte de receitas para os empresários. Quando ocorrem fusões e aquisições de organizações, os dados podem ser apontados como um dos principais ativos buscados, mais até do que pessoal, propriedade intelectual e espaço físico, tal qual aconteceu na aquisição do *site Lynda.com* pelo *LinkedIn.*

Nessa aquisição, o CEO do LinkedIn, afirmou que os vídeos *premium* armazenados pelo *site Lynda.com* foram um motivo imprescindível para a sua compra, estimando-se que, do valor de US$ 1,5 milhão, uma parcela significativa tenha sido direcionada à compra dos dados de vídeo[442].

O conceito de monetização possui várias dimensões, não sendo limitado ao âmbito das informações pessoais e da *internet*. Nesse contexto, a monetização de informações seria a transformação de dados que, a princípio, não possuem nenhum valor agregado, em coisas com

[442] TODD, Steve. O valor dos dados em um mundo impulsionado por informações. **CANALTECH,** 23 out. 2015. Disponível em: https://canaltech.com.br/big-data/o-valor-dos-dados-em-um-mundo-impulsionado-por-informacoes-51425/. Acesso em: 02 abr. 2020.

algum valor, de modo que as informações pessoais podem ser utilizadas como um instrumento para facilitar transações e, ainda, como o próprio objeto dessas transações[443].

A título de exemplo, numa mesma organização é possível observar essas duas facetas da utilização das informações. Determinada organização pode coletar e tratar os dados de seus clientes e, a partir dessas informações, personalizar o serviço prestado ou o produto vendido a esses mesmos clientes. As informações são utilizadas como um meio para facilitar e aprimorar as transações dessa organização.

Esse mesmo empresário pode coletar e tratar os dados de seus clientes e repassá-los a terceiros que busquem ampliar a sua base de dados para além da sua própria carteira de clientes, mediante contraprestação, de modo que as informações tornam-se o próprio objeto da transação.

Uma descrição prática do funcionamento da monetização de dados pessoais é fornecida por Rochfeld, a partir de um questionamento: "Como é possível transformar dados pessoais em valor?":

> Eis um exemplo que permite uma imersão na economia subterrânea da segmentação e da predição, a partir do processamento de dados pessoais, para direcionar a visualização de informações dirigidas por meio de interfaces escondidas dos nossos computadores. As informações sobre as preferências e as preocupações do usuário são armazenadas no disco rígido do computador através dos *cookies* de conexão ou de navegação. Eles são pequenas sequências de códigos, armazenados à medida que as visitas são feitas pelos internautas em sítios eletrônicos variados da *Internet*. Posteriormente essas informações são ativadas quando o usuário navega: os *cookies* fornecem detalhes dessas visitas aos parceiros de agências de publicidade especializadas, responsáveis pela gestão desses dados coletados. As agências celebram contratos com os sítios eletrônicos para essa finalidade. Em seguida, as agências analisam e adaptam de forma extremamente rápida (em centésimos de segundo) a publicidade destinada especialmente à pessoa visada. Assim, um comerciante ou prestador de serviço (ou, mais precisamente, a agência que administra sua conta de publicidade) torna-se capaz de fornecer (ou deveria sê-lo), em um tempo muito curto, uma lista específica de produtos e serviços relacionados com as visitas anteriores e os interesses dos internautas, de forma direcionada. Na prática, como evidenciam os números anteriormente mencionados, os dados pessoais são assim monetizados, cedidos, revendidos, transferidos e terceirizados dentro e fora da União Europeia, enquanto novos atores – *dataminers*, *databrokers*, analistas, especialistas em algoritmos, etc. – tornam-se centrais na economia global[444].

---

[443] ADJEI, Joseph K. Monetization of Personal Identity Information: Technological and Regulatory Framework. **IEEE Computer Society Washington,** Washington DC/EUA, 14 dez. 2015. Disponível em: https://www.researchgate.net/profile/Joseph_Adjei3/publication/325142873_Monetization_of_personal_digital_identity_information_Technological_and_regulatory_framework/links/5be99f48a6fdcc3a8dd1b2a1/Monetization-of-personal-digital-identity-information-Technological-and-regulatory-framework.pdf. Acesso em: 2 abr. 2020, p. 1.

[444] ROCHFELD, Judith. Como qualificar os dados pessoais? Uma perspectiva teórica e normativa da União Europeia em face dos gigantes da Internet. **Revista de Direito, Estado e Telecomunicações,** Brasília, v. 10, n. 1, maio 2018. Disponível em: https://periodicos.unb.br/index.php/RDET/article/view/21500/19816. Acesso em: 16 abr. 2020, p. 63-64.

Assim, abrem-se novas possibilidades de remuneração para as organizações, seja por meio do aprimoramento de seus próprios negócios, seja por meio da venda desses dados a terceiros. Dessa forma, existem duas abordagens para a monetização de dados, uma interna e uma externa, sendo interna a que visa transformar os dados em inteligência capaz de alavancar resultados, e a externa a que transforma os dados pessoais num produto com relevância e valor de mercado, de modo a se apresentar como uma nova fonte de receita para o negócio[445].

As organizações utilizam as informações de diversas formas e de acordo com as estratégias almejadas pelo empresário, tais como redução de custo, criação de valor, interconectividade, inovação, redução de risco e diferenciação de produto. Manipula-se "a informação para saber como agem os clientes, para controlar estoques, aumentar a produtividade etc. A informação pode ser um ativo, ou simplesmente uma ferramenta de suporte à decisão"[446].

A utilização dos dados pessoais como verdadeiros insumos na realização de novos negócios tem a grande vantagem de estas matérias-primas serem renováveis e crescentes diariamente. Monetizar os dados pessoais significa "promover o desenvolvimento econômico, construindo negócios rentáveis"[447].

Os modelos de negócios baseados em dados pessoais podem ser produzidos em grande escala e com baixo custo, além de permitir a utilização de atrativos como a oferta de serviços "gratuitos", a exemplo de aplicativos e redes sociais. Os usuários, em troca da utilização dessas ferramentas, "pagarão" com seus dados pessoais.

Na sociedade da informação, determinados serviços são usufruídos aparentemente de graça, sem o pagamento de custos e taxas, entretanto, o financiamento desse uso ocorre por meio da coleta de dados pessoais. No mundo digital, não existe nada grátis, pois os empresários estão a todo o tempo coletando informações em troca de bens e serviços.

Dessa forma, a economia da informação provoca mudanças nos modelos de negócio e nas estratégias empresariais, mas também traz ao centro do debate a questão da violação à

---

[445] YAMAGATA, Nicolas. Monetizando você e seus dados com a função de inteligência. **Intelligence Hub,** 05 nov. 2017. Disponível em: http://www.intelligencehub.com.br/monetizando-voce-e-seus-dados-com-funcao-de-inteligencia/. Acesso em: 2 abr. 2020.

[446] COHEN, Max E. Alguns aspectos do uso da informação na economia da informação. **Ciência da Informação,** v. 31, n. 3, 2002. Disponível em: http://www.scielo.br/scielo.php?pid=S0100-19652002000300003&script=sci_abstract&tlng=pt. Acesso em: 2 abr. 2020, p. 28.

[447] CARVALHO, Victor M.B. de. **O Direito Fundamental à Privacidade ante a Monetização de Dados Pessoais na Internet: apontamentos legais para uma perspectiva regulatória**. 2018. Dissertação (Mestrado em Direito) – Programa de Pós-Graduação em Direito, Universidade Federal do Rio Grande do Norte, Natal, 2018. Disponível em: http://bdtd.ibict.br/vufind/Record/UFRN_9ee764a6de69a62f84e93f1356e90adb. Acesso em: 2 abr. 2020, p. 76.

privacidade dos titulares dos dados. Nisso reside a importância das legislações de proteção de dados pessoais: regular a coleta e o tratamento dessas informações sem impedir o desenvolvimento econômico-social.

Na próxima subseção serão apresentados os riscos envolvidos nas principais formas de tratamento de dados pessoais na sociedade da informação, bem como as disposições da Lei 13.709/2018 e do RGPD que visam a mitigá-los.

4.2 Principais formas de tratamento de dados pessoais na sociedade da informação: entre benefícios e ameaças à privacidade

Feitas as necessárias considerações acerca da sociedade da informação e compreendida a relevância dos dados pessoais como principal ativo de muitas organizações empresárias, parte-se agora ao exame dos meios mais utilizados na recolha e processamento dessas informações e da influência das legislações sobre a proteção de dados em tais atividades.

4.2.1 Coleta de dados pessoais e monitoramento do indivíduo

Como visto, as organizações sempre coletaram dados pessoais. Inicialmente, colhiam somente as informações necessárias à prestação do serviço, contudo, tão logo perceberam o valor que poderia ser extraído de tais informações, as entidades passaram a empreender formas de colher cada vez mais dados pessoais, tais como censos demográficos, pesquisas e entrevistas com os indivíduos, preenchimento de formulários para viabilizar a participação dos voluntários em sorteios e concursos, registros públicos, câmeras de vídeo e registros de transações comerciais.

Com a popularização, nas últimas décadas, dos equipamentos tecnológicos, poucas são as relações sociais que não envolvem o tratamento de dados pessoais. Nesse contexto, o uso de computadores, de dispositivos móveis e da *internet* tornou-se uma fonte inestimável para as organizações que recolhem dados pessoais. Estas, por sua vez, tornam-se cada vez mais criativas para conseguir o máximo de informação possível.

Exemplificativamente, em junho de 2019, o *Facebook* lançou o *Study from Facebook*, um aplicativo que recolhe os dados dos usuários em troca de dinheiro. O aplicativo de pesquisa de mercado – que, por enquanto, só está disponível nos Estados Unidos e na Índia para os usuários de dispositivos *Android* que sejam maiores de idade – coleta a lista de todos

os aplicativos instalados no telefone, o tempo de utilização de cada um, além de informações sobre o país, o dispositivo e o tipo de rede de acesso. Segundo o *Facebook*, o aplicativo não faz coleta do ID de usuário, senhas ou outro tipo de conteúdo, como fotos e mensagens. Em troca, os usuários do aplicativo recebem uma compensação pecuniária que não foi divulgada[448].

Em janeiro do mesmo ano, o *site Techcrunch* revelou que o *Facebook*, desde 2016, oferecia uma quantia mensal aos usuários do *Facebook Research*, inclusive aos menores de idade, em troca de diversos dados, como histórico de navegação, lista de aplicativos instalados, padrões de uso de serviços *online* e conteúdo de outros aplicativos. O programa chegou a solicitar que os usuários fizessem uma captura de tela de sua página de pedidos na *Amazon*. Depois do escândalo, principalmente por envolver coletas de dados de adolescentes, o *Facebook* anunciou que encerraria a versão do aplicativo[449].

Em 2013, o *Facebook* já havia adquirido aplicativo semelhante por US$ 200 milhões, o *Onavo Protect*, o qual, apesar de não remunerar economicamente seus usuários, oferecia uma VPN "gratuita", isto é, um serviço que permitia camuflar o endereço de IP do dispositivo para manter as informações seguras. O Onavo coletava diversas informações relacionadas aos hábitos do usuário, como tempo gasto usando outros aplicativos, *sites* visitados e tipos de dados trafegados[450].

O programa reportava ao *Facebook* até mesmo quando a tela de um usuário estava ligada ou desligada, e seu uso de dados de celular e *wi-fi* em *bytes*, até mesmo quando a VPN estava desligada. Esse aplicativo permitiu que o *Facebook* identificasse a ascensão meteórica do *WhatsApp* e justificasse o pagamento de US$ 19 bilhões para comprar a *startup* de bate-papo em 2014. Posteriormente, o *WhatsApp* triplicou sua base de usuários, demonstrando o poder da previsão do *software*[451]. Após críticas acerca da privacidade, o *Facebook* decidiu encerrar o aplicativo em maio de 2019[452].

A rede Shiru Café, com 28 lojas instaladas em *campi* de universidades no Japão, na Índia e nos Estados Unidos, permite que universitários tomem cafés, chás ou sucos em sua

---

[448] RUBIO, Isabel. *Facebook* lança aplicativo para acessar dados de usuários em troca de dinheiro. **El País – Tecnologia,** 12 jun. 2019. Disponível em: https://brasil.elpais.com/brasil/2019/06/12/tecnologia/1560347825_866607.html. Acesso em: 12 jul. 2019.

[449] CONSTINE, Josh. Facebook pays tens to install VPN that spies on them. **Tech Crunch,** fev. 2019. Disponível em: https://techcrunch.com/2019/01/29/facebook-project-atlas/. Acesso em: 12 jul. 2019.

[450] ALECRIM, Emerson. *Facebook* encerra VPN Onavo após polemica de privacidade. **Tecnoblog,** mar. 2019. Disponível em: https://tecnoblog.net/279912/facebook-fim-onavo-protect-vpn/. Acesso em: 12 jul. 2019.

[451] CONSTINE, Josh. Facebook pays tens to install VPN that spies on them. **Tech Crunch,** fev. 2019. Disponível em: https://techcrunch.com/2019/01/29/facebook-project-atlas/. Acesso em: 12 jul. 2019.

[452] ONAVO. **Onavo Protect Will no Longer be Availabe**. 2019. Disponível em: https://www.onavo.com/. Acesso em: 12 jul. 2019.

loja, ilimitadamente. Em troca, os estudantes devem concordar em compartilhar seus dados pessoais com as organizações empresárias patrocinadoras da loja. Para ter direito às bebidas "gratuitas", o usuário cria uma conta na rede com um *e-mail* universitário e responde a um questionário *online*, no qual informa seu nome, a data de nascimento, o ano de formatura, a capacidade tecnológica, a experiência profissional e o tamanho da organização em que estaria interessado em trabalhar[453].

As bebidas devem ser consumidas dentro da loja, que tem *internet* grátis e telões com anúncios das patrocinadoras. Somente a unidade da Brown University chega a atrair oitocentas pessoas por dia. A ideia da rede é conectar os universitários a organizações que possam se interessar em contratá-los. No Japão, os patrocinadores do *Shiru Cafe* incluem a *Nissan*, a *Microsoft* e a *JPMorgan*[454].

Os casos citados chamam a atenção porque as pessoas cederam o uso de seus dados pessoais a terceiros em troca de dinheiro. Contudo, bem mais frequentes são as situações em que os indivíduos fornecem seus dados pessoais para poderem utilizar serviços oferecidos "gratuitamente".

São diversos serviços de grande utilidade, fornecidos principalmente na *internet*, e que podem ser usufruídos sem uma contrapartida pecuniária. No entanto, na imensa maioria das vezes, a utilização dessas aplicações exige que os usuários compartilhem seus dados com as organizações provedoras de tais serviços. Os chamados "gigantes da tecnologia", como o *Google* e o *Facebook*, são exemplos disso.

Assim, em razão das facilidades que essas organizações oferecem a sociedade, as pessoas toleram fornecer seus dados pessoais em troca desses serviços. Hoje, é impossível imaginar um mundo no qual os indivíduos não queiram utilizar o mecanismo de busca do Google, redes sociais ou até mesmo *smartphones*, que coletam dados como informações de geolocalização mesmo com a desabilitação, no dispositivo, da opção que permite a coleta desses dados[455] [456] [457].

---

[453] GALILEU. **Vai um café grátis, em troca dos seus dados pessoais?** 2019. Disponível em: https://revistagalileu.globo.com/Tecnologia/noticia/2018/09/vai-um-cafe-gratis-em-troca-dos-seus-dados-pessoais.html. Acesso em: 12 jul. 2019.

[454] GUIMARÃES, Nathália. Bistrô troca dados pessoais de clientes por café grátis. **LeiaJa,** 3 set. 2018. Disponível em: https://m.leiaja.com/tecnologia/2018/09/03/bistro-troca-dados-pessoais-de-clientes-por-cafe-gratis/. Acesso em: 12 jul. 2019.

[455] Um estudo recente conduzido por Schmid, professor de Ciência da Computação da Universidade de Vanderbilt, demonstrou que um aparelho inativo rodando o sistema operacional Android remete informações de geolocalização ao *Google* cerca de 340 vezes por dia, o que representa uma média de 14 envios por hora. (TSUKAYAMA, Hayley. Don't want Google tracking you? You have almost no choice, according to a study. **The Washington Post,** 21 ago. 2018. Disponível em:

Nesse cenário, as organizações conseguem recolher uma quantidade imensurável de informações pessoais. O *site* do *Google*, por exemplo, informa quais dados dos usuários são coletados:

> [...] Coletamos informações sobre os apps, navegadores e dispositivos que você usa para acessar os serviços do Google, o que nos ajuda a fornecer recursos como atualizações automáticas de produtos e diminuir o brilho da tela se a bateria estiver fraca.
> As informações que coletamos incluem identificadores exclusivos, tipo e configurações de navegador, tipo e configurações de dispositivo, sistema operacional, informações de rede móvel, incluindo nome e número de telefone da operadora e número da versão do aplicativo. Também coletamos informações sobre a interação de apps, navegadores e dispositivos com nossos serviços, incluindo endereço IP, relatórios de erros, atividade do sistema, além de data, hora e URL referenciador da sua solicitação. [...]
> Coletamos informações sobre sua atividade em nossos serviços e usamos tal informação para recomendar um vídeo do YouTube de que você pode gostar, por exemplo. As informações de atividades que coletamos podem incluir o seguinte:
> - termos que você pesquisa
> - vídeos que você assiste
> - visualizações e interações com conteúdo e anúncios
> - informações de voz e áudio quando você usa recursos de áudio
> - atividade de compra
> - pessoas com quem você se comunica ou compartilha conteúdo
> - atividades em sites e apps de terceiros que usam nossos serviços
> - histórico de navegação do Chrome que você sincronizou com a Conta do *Google*
>
> Se você usa nossos serviços para fazer e receber chamadas ou enviar e receber mensagens, podemos coletar informações de registro de telefonia, como o número do seu telefone, número de quem chama, número de quem recebe, números encaminhados, horário e data de chamadas e mensagens, duração das chamadas, informações de roteamento e tipos e volumes de chamadas e mensagens. [...]
> Em algumas circunstâncias, o *Google* também coleta informações sobre você de fontes de acesso público. Por exemplo, se seu nome aparecer em um jornal local, o mecanismo de pesquisa do *Google* poderá indexar esse artigo e exibi-lo para outras pessoas, se elas pesquisarem pelo seu nome. Também podemos coletar informações sobre você de parceiros confiáveis, incluindo parceiros de marketing que nos fornecem informações sobre clientes em potencial para nossos serviços comerciais e parceiros de segurança que nos fornecem informações para proteção contra abuso. Também recebemos informações de anunciantes para fornecer serviços de publicidade e pesquisa em nome deles.

---

https://www.washingtonpost.com/technology/2018/08/22/dont-want-google-tracking-you-you-have-almost-no-choice-according-new-study/?noredirect=on&utm_term=.a644e5215606. Acesso em: 12 jul. 2019).

[456] O *Google* reconheceu que o histórico de localizações dos usuários do Android é enviado aos seus servidores mesmo com a opção desabilitada, de modo que esse compartilhamento só é efetivamente encerrado quando o usuário acessa a sua conta no *Google* e altera as configurações de privacidade na guia "Web and App Activity". (NAKASHIMA, Ryan. AP Exclusive: *Google* tracks your movements, like it or not. **AP News,** 13 ago. 2018. Disponível em: https://www.apnews.com/828aefab64d4411bac257a07c1af0ecb. Acesso em: 12 jul. 2019).

[457] No suporte de ajuda do *Google* é possível encontrar a seguinte informação: "Mesmo depois que você desativar o Histórico de localização, alguns dados de local poderão continuar a ser salvos em outras configurações, como na Atividade na Web e de apps, quando você usar outros serviços, como a Pesquisa *Google* e o Maps." (GOOGLE. **Ajuda do Conta do *Google* – Gerenciar o Histórico de localização.** 2019. Disponível em: https://support.google.com/accounts/answer/3118687?hl=pt. Acesso em: 12 ago. 2019).

> Usamos várias tecnologias para coletar e armazenar informações, incluindo cookies, tags de pixel, armazenamento local como armazenamento do navegador da Web ou caches de dados de aplicativos, bancos de dados e registros do servidor[458].

Da supracitada política de privacidade do *Google*, observa-se que todo movimento do indivíduo na *internet* é coletado. Esses dados capturados serão, então, processados para que se tornem capazes de gerar receita para a organização, como acontece quando esta direciona anúncios para o usuário baseado em seu comportamento: o anunciante fornece ao *Google* informações acerca de qual publicidade deve ser mostrada a cada grupo de consumidores e paga à corporação para que esta recolha o máximo de dados dos indivíduos, analise-os e identifique em qual grupo cada consumidor se encaixa para expô-lo aos anúncios selecionados pelo anunciante para tal categoria.

Essa coleta é feita por meio de várias tecnologias. Atualmente, os *cookies* são a principal ferramenta de recolha de dados pessoais. *Cookies* são pequenos arquivos de textos inseridos automaticamente pelos *sites* visitados pelo usuário em seu computador, os quais contêm uma cadeia de números utilizados para identificar a máquina e memorizar as informações coletadas. É uma tecnologia útil, pois permite a memorização de senhas e o reconhecimento de páginas já visitadas[459].

Compreendeu-se, contudo, que esta tecnologia não só podia servir para viabilizar as ações mais básicas do indivíduo na *internet*, mas também para rastrear o seu comportamento na rede mundial de computadores. São os *cookies* a razão de anúncios de um determinado produto serem exaustivamente mostrados após o usuário fazer uma busca simples pelo nome do item num provedor de pesquisa.

Os *cookies* podem ser inseridos pelo próprio *site* que o indivíduo está visitando (*cookies* primários) ou por *sites* externos ao que está sendo acessado (*cookies* de terceiros), mas que mantêm relação comercial com a página visitada. As informações pessoais podem ser coletadas por *sites* com os quais o usuário não mantém nenhuma relação direta. Ilustrativamente, quando se acessa uma loja virtual, este *site* gera *cookies* primários; o *Facebook* também gera marcadores digitais durante a navegação, que são *cookies* de terceiros[460].

---

[458] GOOGLE. **Política de Privacidade.** Disponível em: https://policies.google.com/privacy?hl=pt-BR. Acesso em: 25 mar. 2021.

[459] TERRA, Aline de Miranda Valverde; MULHOLLAND, Caitlin. A utilização econômica de rastreadores e identificadores on-line de dados pessoais. *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 Brasil, 2019, p. 610-611.

[460] LIMINAL. **Fim dos cookies no *Google Chrome*:** o impacto no marketing. 5 fev. 2020. Disponível em: https://liminal.pt/martech-magazine/fim-cookies-chrome-impacto-no-marketing/. Acesso em: 20 out. 2020.

Essa tecnologia de captura de dados não é, por si mesma, ruim ou violadora da privacidade. Ao contrário, ela é importante para viabilizar a utilização dos *sites* pelo usuário, em especial quando se trata de comércio eletrônico, que exige alguma forma de memorizar, ainda que temporariamente, o comportamento do *site* na página, tal qual se verifica quando um consumidor coloca vários itens num carrinho de compras, adicionando um produto por vez. É preciso memorizar cada item enquanto o usuário não finaliza a compra.

Contudo, esses arquivos digitais podem coletar e armazenar, por muito tempo, dados bem mais amplos sobre a experiência do indivíduo na *internet*, munindo as organizações de uma imensa quantidade de informações sobre o usuário, o que poderá ser usado para a realização de análises preditivas e a construção de perfis comportamentais. Isso representa riscos aos direitos individuais.

Além disso, muitas vezes o usuário não tem conhecimento de que seus dados estão sendo coletados pelos *cookies*, muito menos tem noção de todas as informações que são colhidas e por quem serão acessadas.

No Brasil, até a vigência da LGPD, os agentes de tratamento inseriam diversos *cookies* sem a autorização prévia do usuário e sem maiores informações a respeito de tal coleta. Vigorava, tanto aqui quanto na Europa – anteriormente à Diretiva 2009/136/CE da União Europeia[461] –, o modelo *opt out* de obtenção da informação, isto é, o consentimento do titular era presumido até que este se manifestasse em contrário[462], o que significava que os *cookies* eram inseridos sem que o usuário assentisse; a este restava a alternativa de bloquear e excluir os marcadores digitais por meio do navegador ou do próprio *site*.

---

[461] A Diretiva 2009/136/CE alterou a Diretiva 2002/58/CE, referente à privacidade e às comunicações eletrônicas, para exigir que os agentes de tratamento solicitem o consentimento prévio do titular para a coleta e o acesso dos dados armazenados em seu computador, o que inclui os *cookies.*
Artigo 2º Alterações à Directiva 2002/58/CE (Directiva "Privacidade e Comunicações Eletrônicas")
A Directiva 2002/58/CE (Directiva "Privacidade e Comunicações Eletrônicas") é alterada do seguinte modo: [...]
No artigo 5º, o nº 3 passa a ter a seguinte redacção:
"3. Os Estados Membros asseguram que o armazenamento de informações ou a possibilidade de acesso a informações já armazenadas no equipamento terminal de um assinante ou utilizador só sejam permitidos se este tiver dado o seu consentimento prévio com base em informações claras e completas, nos termos da Directiva 95/46/CE, nomeadamente sobre os objectivos do processamento. Tal não impede o armazenamento técnico ou o acesso que tenha como única finalidade efectuar a transmissão de uma comunicação através de uma rede de comunicações eletrônicas, ou que seja estritamente necessário ao fornecedor para fornecer um serviço da sociedade da informação que tenha sido expressamente solicitado pelo assinante ou pelo utilizador."
(UNIÃO EUROPEIA. **Directiva 2009/136/CE do Parlamento Europeu e do Conselho de 25 de Novembro de 2009.** Que altera a Directiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrônicas, a Directiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrônicas e o Regulamento (CE) nº 2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor. Disponível em: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:PT:PDF. Acesso em: 28 jun. 2020).

[462] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 103-104.

Nesse cenário, muitos indivíduos não tinham ideia de que estavam tendo suas informações coletadas por essa tecnologia e, por conseguinte, de que estavam sendo monitorados. Já os usuários que possuíam algum conhecimento a esse respeito e que eram mais preocupados com a sua privacidade, buscavam meios de minimizar o rastreamento durante sua navegação, como o uso de guias anônimas, a utilização de VPNs – que são ferramentas que permitem disfarçar o endereço IP da máquina, desconectando o dispositivo dos *cookies* – e a desabilitação e exclusão dos *cookies.*

Desabilitar esses arquivos digitais, por sua vez, pode fazer com que alguns *sites* não funcionem corretamente. Excluí-los nem sempre é tarefa simples, haja vista que enquanto os *cookies* tradicionais podem ser apagados facilmente por meio do próprio navegador, há *cookies* adaptados que são mais difíceis de ser excluídos, como os *evercookies*; estes são um mecanismo que combina várias formas de armazenar uma mesma informação, o que complexifica a remoção do dado armazenado, fazendo com que o rastreamento *online* do indivíduo seja quase eterno[463].

Hoje, alguns *sites* estão substituindo *cookies* por uma tecnologia de funcionamento bem semelhante a eles, mas que permite o armazenamento local das informações do usuário de maneira mais segura e com maior capacidade de armazenamento. Trata-se do *HTML5 Web Storage*[464].

Seja qual for a tecnologia de coleta de dados pessoais utilizada pelo agente de tratamento, sua capacidade de memorizar todo o comportamento *online* do indivíduo também revela o seu risco potencial de afetar a dimensão informacional da privacidade, máxime quando este não tem conhecimento da escolha acerca do fornecimento de suas informações.

Tanto a LGPD quanto o RGPD adotam o regime *opt in* de coleta dos dados pessoais, o qual exige que, na ausência de uma hipótese legalmente prevista que justifique tal recolha independentemente da aquiescência do indivíduo, este deve consentir previamente com a captura após ter recebido informações claras e detalhadas acerca da coleta e posterior tratamento a que os dados serão submetidos, como visto no capítulo anterior. Os *cookies* e outras tecnologias de captura de informações pessoais também deverão observar essa exigência e as demais bases legais previstas nas legislações de tratamento de tais dados.

---

[463] ROHR, Altieres. 'Cookie eterno' pode rastrear internauta e é impossível de apagar. **G1 – Tecnologias e Games,** 25 out. 2010. Disponível em: http://g1.globo.com/tecnologia/noticia/2010/10/cookie-eterno-pode-rastrear-internauta-e-e-impossivel-de-apagar.html. Acesso em: 28 jun. 2020.

[464] RUIZ, Bruno. Web Storage – HTML5. **Tableless,** 28 jan. 2014. Disponível em: https://tableless.com.br/web-storage-html5/. Acesso em: 28 jun. 2020.

O Regulamento europeu expressamente se refere aos *cookies* em seu Considerando 30, esclarecendo que os indivíduos podem a estes ser associados:

> (30) As pessoas singulares podem ser associadas a identificadores por via eletrônica, fornecidos pelos respetivos aparelhos, aplicações, ferramentas e protocolos, tais como endereços IP (protocolo *internet*) ou testemunhos de conexão (cookie) ou outros identificadores, como as etiquetas de identificação por radiofrequência. Estes identificadores podem deixar vestígios que, em especial quando combinados com identificadores únicos e outras informações recebidas pelos servidores, podem ser utilizados para a definição de perfis e a identificação das pessoas singulares.

Observa-se que o supracitado Considerando ressalta o importante papel que os identificadores eletrônicos têm na formação de perfis comportamentais, os quais serão estudados mais adiante.

Com a vigência, primeiro do RGPD e, depois, da lei brasileira, os *sites* que trabalham com *cookies* e que sofrerão incidência de uma das duas legislações começaram a solicitar o consentimento prévio do usuário para a coleta dos dados pessoais. No entanto, ainda há um longo caminho a se percorrer no que se refere à aquiescência do indivíduo quanto à recolha de suas informações por esta tecnologia e outras afins.

No *Facebook*, por exemplo, que é uma das organizações que mais coletam dados do usuário, apenas há em sua pagina inicial, em letras pequenas, a seguinte informação: "Ao clicar em Cadastre-se, você concorda com nossos Termos, Política de Dados e Política de *Cookies*. Você poderá receber notificações por SMS e cancelar isso quando quiser"[465]. Dessa feita, o consentimento prévio para a coleta dos dados pessoais é fornecido por meio do cadastro, numa lógica de "tudo ou nada", isto é, ou o usuário consente com os *cookies* ou não utiliza o serviço, não havendo a opção de permitir a recolha de algumas informações selecionadas.

Ao clicar em "Política de *Cookies*", o *Facebook* apresenta uma página com um conteúdo bem extenso, mas claro e exemplificativo acerca de todos os dados coletados. A referida política revela que pode coletar informações ainda que o indivíduo não tenha uma conta na rede social:

> Onde usamos cookies?
> Podemos colocar cookies em seu computador ou dispositivo e receber informações armazenadas nos cookies quando você usa ou visita:
> Os Produtos do *Facebook*;

[465] FACEBOOK. **Log in.** Disponível em: https://www.facebook.com/. Acesso em: 29 dez. 2020.

> Os produtos fornecidos por outros membros das Empresas do *Facebook*; e
> Os sites e aplicativos fornecidos por outras empresas que usam os Produtos do *Facebook*, como empresas que incorporam tecnologias do *Facebook* em seus sites e aplicativos. O *Facebook* usa cookies e recebe informações quando você visita esses sites e aplicativos, inclusive informações do dispositivo e informações sobre sua atividade, sem nenhuma outra ação sua. Isso acontece quer você tenha ou não uma conta do *Facebook*, estando ou não conectado(a) a ela[466].

A partir desse trecho da política de *cookies* da rede social, observa-se que os *cookies* de terceiros coletam as informações pessoais do usuário sem que haja um consentimento explícito para isso. Isto é, o indivíduo acessa uma página, vê um aviso a respeito da utilização da tecnologia por aquele *site* e, acreditando que somente este agente de tratamento recolherá seus dados, aceita a utilização de *cookies*. Ocorre que esse *site* incorpora tecnologias do *Facebook*, o qual irá coletar as informações do usuário ainda que este não possua nenhuma relação com a rede social. Mesmo que o indivíduo leia a política de privacidade ou *cookies* apresentada pelo *site* visitado, descobrirá que há coleta de *cookies* de terceiros, mas não conseguirá saber quais informações e por quem tais dados são coletados.

Exemplificativamente, ao acessar o Portal de Notícias "G1", o usuário recebe o seguinte aviso genérico:

> Nós usamos cookies e outras tecnologias semelhantes para melhorar a sua experiência em nossos serviços, personalizar publicidade e recomendar conteúdo de seu interesse. Ao utilizar nossos serviços, você concorda com tal monitoramento. Informamos ainda que atualizamos nossa Política de Privacidade. Conheça nosso Portal da Privacidade e veja a nossa nova Política[467].

Ao lado da mensagem, surge a opção "PROSSEGUIR", por meio da qual o usuário assentirá, expressamente, com o armazenamento de *cookies*. Os usuários que resolverem conhecer a política de privacidade do Portal encontrarão somente a seguinte informação no que concerne à utilização de *cookies* de terceiros:

> Prestadores de serviços de tecnologia poderão utilizar seus próprios cookies nos Serviços, com a nossa autorização, para prestação de serviços à Globo. Tais cookies coletarão os seus Dados nas nossas propriedades para as finalidades previstas nesta política[468].

---

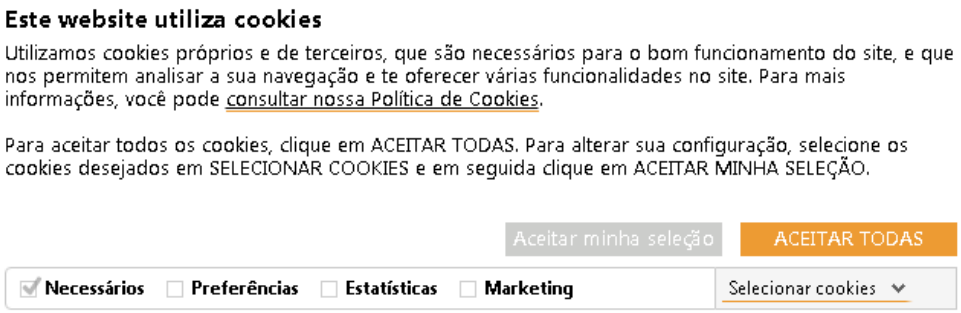
[466] FACEBOOK. **Cookies e outras tecnologias de armazenamento.** Disponível em: https://www.facebook.com/policies/cookies/. Acesso em: 29 dez. 2020.
[467] PORTAL DE NOTÍCIAS G1. **Home.** Disponível em: https://g1.globo.com/. Acesso em: 29 dez. 2020.
[468] PORTAL DE NOTÍCIAS G1. **A Globo respeita e protege sua privacidade.** Disponível em: https://privacidade.globo.com/pdf/Vers%C3%A3o%20Publica%C3%A7%C3%A3o_Pol%C3%ADtica%20de%20Privacidade_Globo.pdf. Acesso em: 29 dez. 2020.

Tal política foi atualizada em 3 de agosto de 2020, portanto, quase dois anos após a sanção da LGPD e na iminência de sua entrada em vigor. No entanto, como se observa, não há transparência acerca de quais são os terceiros que coletarão os dados do usuário, bem como sobre quais informações serão coletadas. Dessa forma, o consentimento fornecido pelo indivíduo não é totalmente informado.

Ademais, pelo menos no Brasil, a maior parte dos *sites* exige o consentimento do usuário com o armazenamento de todos os *cookies* solicitados como condição de acesso à página, não havendo, verdadeiramente, uma liberdade de escolha, nem mesmo gradual, a respeito dessa coleta de dados. Assim, se o indivíduo assentir com o armazenamento dos identificadores digitais destinados a melhorar o desempenho do *site*, mas não desejar que seus dados sejam recolhidos para fins estatísticos ou publicitários, ele não consegue consentir somente com parte dos *cookies*. De igual forma, para evitar os *cookies* de terceiros, o indivíduo precisa ir até as configurações do navegador e bloquear os *cookies* de terceiros para todos os *sites*, o que foge da racionalidade da *"privacy by default"* adotada pela LGPD.

Um bom exemplo de como conciliar a autodeterminação informativa do indivíduo com o uso de tecnologias de coleta de dados é oferecido pela Ulma Construction, que, em seu *site*, solicita o consentimento do usuário da seguinte forma:

Figura 1 – Exemplo de *site* com solicitação de consentimento do usuário



Fonte: Ulma Construction[469]

A página viabiliza ao usuário assentir com o armazenamento de apenas alguns dos *cookies* entre aqueles que o *site* pode utilizar. Essa possibilidade de consentimento gradual talvez se dê porque a Ulma é uma organização global que realiza atividades no Brasil e em outros países, principalmente europeus, de modo que deve sofrer uma maior influência da

[469] ULMA CONSTRUCTION. **Home.** Disponível em: https://www.ulmaconstruction.com.br/pt-br/ulma. Acesso em: 29 dez. 2020.

tutela mais amadurecida dos dados pessoais da Europa, além de estar adaptado a atender a diferentes legislações sobre a matéria.

Diante da crescente preocupação com a privacidade, alguns navegadores, a exemplo do Mozilla e do Safari, resolveram bloquear os *cookies* de terceiros. Também o *Google* anunciou a intenção de acabar com a utilização de tais identificadores no *Chrome* até 2022. Em substituição, pretende lançar o sistema "*Privacy Sandbox*", uma interface de programação de aplicações de preservação de privacidade que permite o agrupamento de usuários segundo seus interesses e comportamentos, mas de forma anonimizada, isto é, sem conter a identificação pessoal de cada elemento[470].

Apesar de tais medidas serem um avanço no que diz respeito à tutela da dimensão informacional da privacidade, a segmentação e a construção de perfis de grupo são capazes de afetar negativamente os direitos da personalidade do indivíduo, ainda que os dados utilizados sejam anonimizados. Os agentes de tratamento já estão desenvolvendo formas de burlar tais barreiras impostas pelos navegadores, disfarçando os *cookies* de terceiros para que recolham dados como se fossem *cookies* primários.

Nesse cenário de vasta coleta de dados pessoais, há uma verdadeira e massiva vigilância sobre as pessoas, permitindo às organizações, públicas e privadas, reunir um grande acervo de informação sobre cada pessoa, o que gera uma notável assimetria da informação entre tais agentes de tratamento e o indivíduo.

Na Coreia do Sul, visando ao enfrentamento da pandemia, o Estado procedeu a uma vasta coleta dos dados pessoais daqueles que são infectados pelo coronavírus, que vai da entrevista do paciente até a verificação das transações feitas com cartões de crédito pelo infectado, passando pela coleta de dados de localização dos *smartphones* e filmagens de câmeras de vigilância para recriar a rota do infectado um dia antes de os sintomas aparecerem.

Tal medida foi muito importante para rastrear e contatar possíveis infectados, no intento de diagnosticar a doença o mais cedo possível, mesmo nos assintomáticos, e de evitar que infectados transmitissem o vírus a outras pessoas por desconhecimento da infecção. Contudo, tamanha coleta de dados e a divulgação de algumas destas informações passaram a representar riscos à privacidade dos indivíduos.

Numa das situações ocorridas naquele país, "S" participou de uma aula, em seu trabalho, sobre assédio sexual e acabou contraindo o coronavírus em decorrência do instrutor da turma. Assim que foi diagnosticado com a doença, o governo começou a enviar mensagens

---

[470] LIMINAL. **Fim dos Cookies no *Google Chrome*:** o impacto no marketing. 5 fev. 2020. Disponível em: https://liminal.pt/martech-magazine/fim-cookies-chrome-impacto-no-marketing/. Acesso em: 20 out. 2020.

para a população informando sobre o diagnóstico. Nas mensagens constavam o sexo, a idade, o distrito de residência e o distrito de trabalho do infectado, a ocasião e de quem o infectado contraiu o vírus, os locais e horários por onde passou após a infecção e, até mesmo, a informação de que "S" e o instrutor estiveram juntos num bar até as 23h03, o que gerou boatos de que os dois teriam um romance. Apesar de nenhum nome ou endereço ser informado, não é difícil imaginar como a divulgação dessa vasta quantidade de dados, a princípio não identificados, torna-os facilmente identificáveis[471].

Outro alerta no celular informou que uma mulher de 27 anos que trabalha na Samsung, em Gumi, contraiu o coronavírus no dia 18 de fevereiro, às 23h, quando visitou sua amiga que havia participado da reunião da seita religiosa Shincheonji, a maior fonte de infecções no país. Logo depois, o prefeito de Gumi revelou o sobrenome da sul-coreana em seu *Facebook*, momento em que os moradores da cidade, em pânico, começaram a pedir que o prefeito lhes informasse o endereço da infectada. Assustada, a mulher implorou por meio da rede social que o prefeito não divulgasse suas informações pessoais, pois tal comportamento poderia trazer danos à família dela e a seus amigos[472].

Diante de tantos casos em que a identificação dos infectados foi possível, situações de linchamento virtual, além de casos que, mesmo não havendo a identificação, geraram diversos comentários vexatórios, os sul-coreanos passaram a ter tanto ou até mais medo do estigma social, das críticas e de outros danos do que da própria doença[473].

Decerto, nas situações relatadas houve um claro interesse público a legitimar a massiva coleta de dados pessoais, independentemente do consentimento do indivíduo. No entanto, mesmo que legítima, se a recolha e o posterior tratamento das informações não seguem os princípios de proteção de dados, certamente podem causar diversos prejuízos ao titular das informações.

Além dos impactos à dimensão informacional da privacidade, o intenso rastreamento do comportamento, atividades e preferências do indivíduo pode repercutir, como se discutirá mais adiante, também na dimensão decisional do referido direito.

Esse risco é potencializado quando os agentes de tratamento compartilham os dados entre si, já que as entidades passam a combinar as informações que recolheram com outras

---

[471] BBC NEWS. **Coronavirus privacy:** Are South Korea's alerts too revealing? 5 mar. 2020. Disponível em: https://www.bbc.com/news/world-asia-51733145. Acesso em: 6 abr. 2020.
[472] BBC NEWS. **Coronavirus privacy:** Are South Korea's alerts too revealing? 5 mar. 2020. Disponível em: https://www.bbc.com/news/world-asia-51733145. Acesso em: 6 abr. 2020.
[473] KIM, Nemo. 'More scary than coronavirus': South Korea's health alerts expose private lives. **The Guardian.** 6 mar. 2020. Disponível em: https://www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives. Acesso em: 6 abr. 2020.

advindas de diversas fontes, o que pode revelar uma quantidade imensurável de conhecimento sobre o indivíduo.

A esse respeito, importa ressaltar que tanto a LGPD quanto o RGPD exigem o consentimento prévio do indivíduo para que haja tal compartilhamento, inclusive entre integrantes de um mesmo grupo empresarial. Contudo, também nesse particular, muitos agentes de tratamento condicionam o uso de um serviço à aquiescência do titular com a transferência de seus dados a terceiros, tolhendo a sua liberdade do consentimento.

O *WhatsApp*, por exemplo, compartilha dados com o *Facebook* desde 2016, quando concedeu um período de trinta dias para que os usuários alterassem a configuração de sua conta de modo a evitar o compartilhamento, caso assim desejassem. Após esse intervalo, não foi mais possível impedir a transferência de dados entre as duas redes sociais. Em 2021, o *WhatsApp* fez mais mudanças em sua política de privacidade, ampliando o compartilhamento. Ao notificar os usuários, a rede social indicou os procedimentos para o apagamento da conta, caso estes discordassem da atualização[474].

De igual forma, não raramente agentes de tratamento transferem, gratuita ou onerosamente, os dados que recolhem com outras organizações, mesmo sem o consentimento ou o conhecimento da pessoa a quem essas informações se referem. Apesar das legislações de proteção de dados pessoais, a autodeterminação informativa do indivíduo sofre constantes limitações e violações na sociedade da informação.

Adiante, serão tecidas algumas considerações sobre o armazenamento dos dados pessoais coletados e o *big data*. Posteriormente, explanar-se-á acerca da extração de conhecimento de tais informações, bem como sobre os riscos envolvidos no processamento dos dados pessoais.

4.2.2 Armazenamento e processamento de dados pessoais: reflexões sobre o uso de mineração de dados e a definição de perfis

Toda a imensa quantidade de informação que é diariamente coletada somente será útil se houver formas de armazená-la e analisá-la em tempo útil para a tomada de decisão. Nesse contexto, surgem tecnologias de armazenamento e análise que permitem a extração de conhecimento dos dados pessoais num curto tempo de resposta. É o que se estudará a seguir.

---

[474] SCHREIBER, Mariana. Após reação negativa, WhatsApp adia para maio "ultimato" para usuário compartilhar dados com *Facebook*. **BBC News Brasil,** 15 jan. 2021. Disponível em: https://www.bbc.com/portuguese/brasil-55680262. Acesso em: 16 jan. 2021.

4.2.2.1 *Data warehouse*, *big data* e mineração de dados

Desde a década de 1980, as organizações, inclusive as de pequeno porte, começaram a investir em sistemas computacionais que coletam, tratam e armazenam dados com vistas a facilitar as atividades empresariais cotidianas. Esses sistemas utilizados na execução do negócio, tais como nas tarefas relacionadas à realização de uma venda ou à exclusão de um cliente, são chamados de *Online Transaction Processing* (OLTP), os quais, justamente por sua finalidade, necessitam de um tempo de resposta curto, pois seria inviável aos seus usuários a espera de vários minutos para a execução de qualquer operação no sistema[475].

A partir da década de 1990, o aumento da competitividade empresarial, a globalização e o crescimento das bases de dados fizeram com que as organizações precisassem obter informações úteis que as auxiliassem no processo de tomada de decisão. Até então, apesar de os sistemas operacionais estarem produzindo, diariamente, uma grande quantidade de dados, estes não estavam disponíveis como informações estratégicas[476].

Muitas vezes os dados estavam em bases diferentes e não integradas, o que dificultava a análise de tais informações, ou a execução dos sistemas de apoio à decisão acontecia no mesmo banco de dados utilizados para todas as demais finalidades, o que aumentava consideravelmente o tempo de resposta de qualquer processamento do sistema, inviabilizando a utilização do banco de dados para fins de análise. Em suma, cresceu a demanda por uma nova tecnologia que fosse capaz de analisar os dados de diferentes sistemas de forma rápida e eficiente. Para suprir tal necessidade, surgiu o *data warehouse*[477].

Data warehouse é um banco de dados especializado que armazena, consolida e padroniza as informações oriundas de diferentes bancos de dados operacionais e que possam ser utilizadas para análise gerencial e tomada de decisões. Essa ferramenta permite o rápido levantamento de informações concisas, confiáveis e de diferentes fontes a respeito das

---

[475] NEVES, Fabricia Vancim Frachone Neves. **Uma Análise da Aplicabilidade do Data Warehouse no Comércio Eletrônico, enfatizando o CRM analítico.** 2001.159 f. Dissertação (Mestrado em Engenharia da Produção) – Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos, 2001, p. 50-51. Disponível em: https://teses.usp.br/teses/disponiveis/18/18140/tde-10042017-160131/en.php. Acesso em: 28 nov. 2020.

[476] NEVES, Fabricia Vancim Frachone Neves. **Uma Análise da Aplicabilidade do Data Warehouse no Comércio Eletrônico, enfatizando o CRM analítico.** 2001.159 f. Dissertação (Mestrado em Engenharia da Produção) – Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos, 2001, p. 51. Disponível em: https://teses.usp.br/teses/disponiveis/18/18140/tde-10042017-160131/en.php. Acesso em: 28 nov. 2020.

[477] NEVES, Fabricia Vancim Frachone Neves. **Uma Análise da Aplicabilidade do Data Warehouse no Comércio Eletrônico, enfatizando o CRM analítico.** 2001.159 f. Dissertação (Mestrado em Engenharia da Produção) – Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos, 2001, p. 51. Disponível em: https://teses.usp.br/teses/disponiveis/18/18140/tde-10042017-160131/en.php. Acesso em: 28 nov. 2020.

operações, tendências e mudanças referentes à organização[478], integrando os dados num formato único e de fácil consulta.

Ao contrário dos dados operacionais, os dados de um *data warehouse* referem-se a um período de tempo bastante amplo: de cinco a dez anos. A não volatilidade é outra característica desse banco de dados. Isso significa que os dados armazenados em um *data warehouse* não podem ser editados, apenas consultados ou excluídos. Essas características, além de conferir precisão e consistência aos dados, permitem uma visão acurada da organização e fornecem um grande conteúdo para análises que resultarão em importantes informações estratégicas[479].

O *data warehouse* permite a transformação de dados sem valor estratégico em conhecimento, bem como a sua disponibilização em tempo hábil para fazer a diferença na gestão do negócio. Essa transformação ocorre por meio do chamado *Online Analytical Processing* (OLAP) – Processamento Analítico *Online*.

Para ilustrar, uma rede varejista, fazendo uso de *data warehouse*, pode consultar as transações que um cliente fez num determinado momento para verificar oportunidades de novas vendas, visualizar informações necessárias para a prospecção de clientes ou analisar dados massivos para transformar seu relacionamento com fornecedores.

Em outro exemplo, Jane Laudon e Kenneth Laudon citam que a Receita Federal dos Estados Unidos possuía uma grande quantidade de dados armazenados em diferentes formatos e fragmentados em muitos sistemas criados ao longo dos anos, tornando praticamente impossível a sua consulta e análise. Depois que a Receita norte-americana começou a utilizar *data warehouse*, pôde pesquisar e analisar bilhões de registros de uma vez, oriundos de uma fonte centralizada de dados consistentes, o que resultou na recuperação de bilhões de dólares em declarações de rendimento perdidas no antigo sistema. Além disso, os analistas da Receita puderam determinar padrões de pessoas propensas a mentir em suas declarações, tais como casais divorciados em que ambos declaram os filhos em seus formulários ou recém-formados sobrecarregados com empréstimos estudantis. O tempo necessário à identificação dos erros nas declarações à análise de dados foi reduzido de meses a algumas horas[480].

---

[478] LAUDON, Kenneth; LAUDON, Jane. **Sistemas de Informação Gerenciais.** 9. ed. Pearson Universidades, 2011, p. 154.

[479] NEVES, Fabricia Vancim Frachone Neves. **Uma Análise da Aplicabilidade do Data Warehouse no Comércio Eletrônico, enfatizando o CRM analítico.** 2001.159 f. Dissertação (Mestrado em Engenharia da Produção) – Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos, 2001, p. 55. Disponível em: https://teses.usp.br/teses/disponiveis/18/18140/tde-10042017-160131/en.php. Acesso em: 28 nov. 2020.

[480] LAUDON, Kenneth; LAUDON, Jane. **Sistemas de Informação Gerenciais.** 9. ed., Pearson Universidades, 2011, p. 156.

A coleta e o armazenamento de dados pelas organizações tornaram-se uma exigência da sociedade da informação, mas, para que os dados tenham valor, precisam ser trabalhados e transformados em conhecimento útil. Nesse contexto, os bancos de dados do tipo *data warehouse* permitiram que dados históricos, referentes a operações realizadas durante anos pela entidade, sejam armazenados de maneira integrada e organizados de acordo com os assuntos mais relevantes para a organização, tornando os dados disponíveis para que sejam analisados.

Um *data warehouse* armazena, majoritariamente, dados estruturados, isto é, dados que são organizados numa estrutura bem definida e previamente planejada para armazená-los, tal qual uma planilha de Excel ou um banco de dados que é composto por várias tabelas, em cujas linhas e colunas serão armazenados os dados que correspondam ao tipo de informação antecipadamente pensado para ali ser depositado.

No início do século XXI, surgiu e se popularizou uma série de tecnologias que possuem estruturas flexíveis e dinâmicas, não seguindo um padrão predefinido, como mensagens de texto, fotos, áudios de WhatsApp, gráficos. Na maior parte das redes sociais, uma postagem, por exemplo, não pode ter uma estrutura rígida e preestabelecida, haja vista que o usuário pode escrever textos de diversos conteúdos e com contagem de caracteres inicialmente não definida, quantidades variadas de imagens, as quais terão tamanhos diferentes com números de pixels também distintos. O *post*, por sua vez, receberá respostas que não podem ser previamente mensuradas e nos mais variados formatos, como textos, imagens, *links*, *emojis*, cada um com distintas características. Todos estes são dados não estruturados, e não é difícil perceber a complexidade do armazenamento e processamento dessas informações nas tabelas existentes em um *data warehouse*.

As organizações podem extrair valiosos conhecimentos a partir desses dados. A velocidade e o volume de produção desses dados na sociedade da informação são imensos, de modo que foi preciso criar uma nova infraestrutura capaz de suportar grandes volumes de dados a um baixo custo e que permitisse a utilização de técnicas de análise de dados com bom desempenho e rápido tempo de resposta[481]. Surge, então, o *big data*.

O conceito de *big data* vai além do que sua tradução sugere, podendo ser definido como um conjunto massivo de dados que demanda ferramentas próprias para o tratamento de grandes volumes de dados, de modo a permitir que as informações processadas possam ser

[481] MARQUESONE, Rosangela. **Big Data –** Técnicas e tecnologias para extração de valor dos dados. Casa do Código, p. 149. [versão digital].

encontradas e analisadas em tempo hábil[482]. Dessa forma, o *big data* possui pelo menos três Vs: volume, variedade e velocidade[483].

No que se refere à primeira característica, o volume de dados armazenado em *big data* é de uma dimensão sem precedentes. São *zettabytes* de dados armazenados em todo o mundo, quantidade esta que continua crescendo, diariamente, em elevada proporção. Saliente-se que, enquanto atualmente o custo para se armazenar um megabyte é de cerca de US$ 0,03, na década de 1990 esse gasto era de aproximadamente US$ 12.000, razão pela qual, à época, ainda que as organizações quisessem aproveitar todo o potencial de extração dos dados, muitas vezes acabavam descartando-os[484].

Com o *big data*, o preço deixou de ser um fator limitante e se tornou possível o armazenamento de grandes quantidades de dados, razão pela qual a ordem é coletar o máximo de informação possível para, posteriormente, decidir sobre a sua utilização ou não. No entanto, o princípio da minimização dos dados pessoais deve refletir, ainda que parcialmente, nesta lógica, haja vista que os agentes de tratamento só poderão coletar os dados efetivamente necessários para a finalidade informada.

Quanto à variedade, este atributo refere-se ao fato de que os dados *do big data* advêm de diversas fontes e são dos mais variados tipos, combinando dados estruturados e não estruturados. Por fim, o terceiro "v" diz respeito à velocidade com que os dados são coletados, analisados e utilizados pela tecnologia *big data,* que chega a ocorrer em tempo real.

Na sociedade da informação, as organizações utilizam, isolada ou integradamente, *data warehouses* e *big data* como importantes ferramentas para a tomada de decisão. Entretanto, para se chegar a conhecimentos que agreguem valor às entidades, os dados precisam passar por uma garimpagem.

Mineração de dados, ou *data mining*, é o processo de extrair informação válida e previamente desconhecida a partir de grandes bases de dados, procurando características ou padrões para previsões acuradas de comportamento e tendências relacionadas a determinados eventos, os quais serão utilizados nas tomadas de decisão. Assim, a mineração de dados "vai muito além da simples consulta a um banco de dados, no sentido de que permite aos usuários

---

[482] CALDAS, Max Silva; SILVA, Emanoel Costa Claudino. Fundamentos e aplicação do Big Data: como tratar informações em uma sociedade de yottabytes, **Bibliotecas Universitárias –** perspectivas, experiências e perspectivas**,** Belo Horizonte, v. 3, n. 1, jan./jun. 2016, p. 73. Disponível em: https://periodicos.ufmg.br/index.php/revistarbu/article/view/3086. Acesso em: 28 nov. 2020.

[483] MARQUESONE, Rosangela. **Big Data –** Técnicas e tecnologias para extração de valor dos dados. Casa do Código, p. 8-9. [versão digital].

[484] MARQUESONE, Rosangela. **Big Data –** Técnicas e tecnologias para extração de valor dos dados. Casa do Código, p. 6. [versão digital].

explorar e inferir informação útil a *partir* dos dados, descobrindo relacionamentos 'escondidos' no banco de dados"[485].

A mineração de dados pode ser utilizada para explicar algum evento, tal como a redução da venda de um determinado produto em uma cidade ou região, para confirmar uma hipótese ou para buscar relacionamentos novos e não previstos. Na seara empresarial, os três maiores usos do *data mining* buscam identificar associações entre produtos e os possíveis proveitos disso; identificar quais clientes têm mais potencial para a aquisição de produtos que proporcionem os maiores lucros; e descobrir os fatores que causam a perda de clientes e aqueles que os fidelizam[486].

O *data mining* é bastante utilizado em diversas áreas. Em vendas, destina-se a identificar padrões de comportamento dos consumidores, encontrar características dos consumidores de acordo com a região demográfica e prever quais consumidores serão alcançados pelas campanhas de *marketing.* No setor de finanças, o *data mining* é usado para detectar padrões de fraudes no uso dos cartões de crédito. Na área de seguros e planos de saúde, a mineração de dados permite determinar quais procedimentos médicos são requisitados ao mesmo tempo, prever quais consumidores comprarão novas apólices e identificar comportamentos fraudulentos. No setor de transportes, seu uso possibilita determinar a distribuição dos horários entre os vários caminhos e identificar padrões de sobrecarga. Na medicina, o *data mining* é capaz de caracterizar o comportamento dos pacientes para prever novas consultas e identificar terapias de sucessos para diferentes doenças[487].

Nesse diapasão, a mineração de dados identifica oportunidades, problemas e ameaças mais rapidamente, minimizando os riscos e aumentando as probabilidades de êxito das decisões tomadas.

---

[485] NEVES, Fabricia Vancim Frachone Neves. **Uma Análise da Aplicabilidade do Data Warehouse no Comércio Eletrônico, enfatizando o CRM analítico.** 2001.159 f. Dissertação (Mestrado em Engenharia da Produção) – Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos, 2001, p. 81-82. Disponível em: https://teses.usp.br/teses/disponiveis/18/18140/tde-10042017-160131/en.php. Acesso em: 28 nov. 2020.

[486] NEVES, Fabricia Vancim Frachone Neves. **Uma Análise da Aplicabilidade do Data Warehouse no Comércio Eletrônico, enfatizando o CRM analítico.** 2001.159 f. Dissertação (Mestrado em Engenharia da Produção) – Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos, 2001, p. 83. Disponível em: https://teses.usp.br/teses/disponiveis/18/18140/tde-10042017-160131/en.php. Acesso em: 28 nov. 2020.

[487] NEVES, Fabricia Vancim Frachone Neves. **Uma Análise da Aplicabilidade do Data Warehouse no Comércio Eletrônico, enfatizando o CRM analítico.** 2001.159 f. Dissertação (Mestrado em Engenharia da Produção) – Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos, 2001, p. 85-86. Disponível em: https://teses.usp.br/teses/disponiveis/18/18140/tde-10042017-160131/en.php. Acesso em: 28 nov. 2020.

No que diz respeito ao titular dos dados pessoais, a mineração de dados é capaz de provocar substancial assimetria da informação entre as entidades, públicas ou privadas, que mineram dados e os indivíduos. Essas organizações podem descobrir correlações acerca dos titulares que estes nem sequer imaginam existir, o que concede muito poder a tais entidades, já que podem tomar uma série de decisões com base num conhecimento que nem o próprio indivíduo a que tal informação se refere tem sobre si mesmo.

Ademais, o *data mining* pode revelar informações a respeito do titular dos dados que este conhece, mas que não fornece e nem quer que o agente de tratamento descubra. Dessa feita, hipoteticamente, uma entidade pode considerar um consumidor como indesejado, pois a mineração de dados revelou seu nível econômico, ou pode aumentar os preços de determinados produtos por verificar que certo consumidor necessita muito do item e irá adquiri-lo mesmo com a elevação do valor de venda.

Em 2012, Duhigg[488] publicou um artigo no *New York Times* detalhando uma situação que demonstra a assimetria da informação gerada pela mineração de dados. Trata-se do caso da *Target*, que desejava identificar suas clientes que estivessem grávidas, pois mulheres até o segundo trimestre da gravidez estão mais suscetíveis a modificar seus hábitos de compra, já que é quando começam a adquirir produtos para o bebê. Para tanto, começou a analisar os dados de seus consumidores, coletados e armazenados durante anos, buscando descobrir como seus hábitos se modificam à medida que se aproximava a data do parto.

Em pouco tempo, a mineração de dados revelou alguns padrões úteis, tal como o fato de que grávidas costumam comprar grandes quantidades de loção sem perfume no início do segundo trimestre, bem como consomem muitos suplementos vitamínicos durante as vinte primeiras semanas de gravidez. Assim, a *Target* identificou 25 produtos que, quando analisados em conjunto, permitiram a atribuição a cada cliente de uma pontuação de "previsão de gravidez", além da estimativa da data de parto, para que a rede varejista pudesse enviar cupons programados para estágios muito específicos de gravidez.

Aproximadamente um ano depois, um pai entrou em contato com a *Target*, reclamando do envio de cupons de roupas de bebês e de berços para a sua filha que ainda estava no ensino médio. A seu ver, a varejista estaria tentando incentivar sua filha a engravidar. O gerente se desculpou e, alguns dias depois, ligou para se desculpar novamente,

[488] DUHIGG, Charles. How Companies Learn Your Secrets. **The New York Times Magazine,** 16 fev. 2012. Disponível em: https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp. Acesso em: 13 set. 2020.

quando ouviu do pai descontente que este havia descoberto que a garota realmente estava grávida.

Esse fato fez a *Target* perceber que o envio de cupons específicos para produtos de bebês poderia passar a impressão às mulheres grávidas de que elas estariam sendo espionadas, o que poderia afugentá-las. A varejista passou então a enviar livretos de anúncios especialmente projetados para cada cliente; estes, no caso das gestantes, passaram a misturar anúncios de produtos que estas mulheres nunca comprariam com anúncios de bebês, fazendo parecer que todos os itens foram escolhidos aleatoriamente. Dessa forma, a grávida presume que todos os seus vizinhos receberam os mesmos anúncios e, por conseguinte, não verá problema em usar os cupons para produtos de bebês que somente ela recebeu.

A mineração de dados tem grande importância na sociedade da informação, e seu uso é fundamental para uma rápida e eficaz tomada de decisão pelas organizações, públicas e privadas, num contexto de imensa produção de dados. Apesar de todas essas vantagens, a mineração de dados também é um processo potencialmente danoso aos titulares das informações.

Além do problema da assimetria da informação, aqui já mencionado, há outros riscos associados a essa atividade. Um dos principais usos do *data mining* verifica-se na construção de perfis, que representa uma séria ameaça aos direitos individuais, consoante se discutirá a seguir.

4.2.2.2 Definição de perfis

Um perfil é um conjunto de dados correlacionados que representa um sujeito, individual ou coletivo[489]. Essas correlações, resultantes principalmente do processo de mineração de dados, fornecem uma probabilidade de que determinado comportamento passado se repita no futuro[490].

Conforme os ensinamentos de Hildebrandt, *profiling* é o processo de "descobrir" correlações entre dados em bancos de dados que podem ser usados para identificar e

[489] BOSCO, Francesca et al. Profiling Technologies and Fundamental Rights and Values: regulatory challenges and perspectives from European Data Protection Authorities. *In:* BOSCO, Francesca et al. **Profiling technologies in practice**: Applications and impact on fundamental rights and values. **Wolf Legal Publishers,** 2015, p. 8. Disponível em: https://research.tilburguniversity.edu/en/publications/profiling-technologies-and-fundamental-rights-an-introduction. Acesso em: 1 out. 2020.

[490] JAQUET-CHIFFELLE, David-Olivier. Reply: direct and indirect profiling in the light of virtual persons. *In:* HILDEBRANDT, Mireille. **Defining Profiling:** A new type of knowledge? Springer, Dordrecht, 2008, p. 18. Disponível em: https://link.springer.com/chapter/10.1007%2F978-1-4020-6914-7_2#citeas. Acesso em: 28 nov. 2020.

representar um indivíduo ou grupo[491]. Tal processamento de dados será utilizado para a tomada de decisões, em muitas situações, até mesmo sem intervenção humana.

O conhecimento produzido pelo *profiling* diferencia-se da produção de conhecimento clássica, uma vez que nesta o pesquisador formula uma hipótese acerca do comportamento social e, em seguida, testa tal conjectura numa amostra da população, ao passo que na construção de perfis, a descoberta se dá a partir dos dados, isto é, a partir do processo de mineração de dados surge uma hipótese que só será testada quando os perfis forem aplicados[492].

Um perfil pode ser individual ou de grupo. O perfil individual é usado para identificar um indivíduo numa comunidade ou apenas para inferir seus hábitos, comportamento, preferências, conhecimentos, riscos ou outras características sociais e econômicas. Já o perfil de grupo é usado para encontrar recursos compartilhados entre membros de uma comunidade definida ou para definir categorias de indivíduos que compartilham algumas características[493].

A partir da análise dos dados coletados, emergem grupos e categorias de sujeitos com propriedades e características semelhantes. Cada grupo tem sua própria identidade definida. Um perfil de grupo possibilita a classificação de indivíduos nessas diferentes categorias. É suficiente identificar um sujeito como um membro do grupo para poder inferir, para este sujeito, conhecimento herdado do próprio grupo: comportamento provável, atributos, riscos etc.[494]

A criação de perfis é uma técnica pela qual um conjunto de características de uma determinada classe de pessoa é inferido a partir de experiências anteriores, para que, em seguida, sejam identificados indivíduos que se enquadrem nesse conjunto de características[495].

---

[491] JAQUET-CHIFFELLE, David-Olivier. Reply: direct and indirect profiling in the light of virtual persons. *In:* HILDEBRANDT, Mireille. **Defining Profiling:** A new type of knowledge? Springer, Dordrecht, 2008, p. 19. Disponível em: https://link.springer.com/chapter/10.1007%2F978-1-4020-6914-7_2#citeas. Acesso em: 28 nov. 2020.

[492] JAQUET-CHIFFELLE, David-Olivier. Reply: direct and indirect profiling in the light of virtual persons. *In:* HILDEBRANDT, Mireille. **Defining Profiling:** A new type of knowledge? Springer, Dordrecht, 2008, p. 18-19. Disponível em: https://link.springer.com/chapter/10.1007%2F978-1-4020-6914-7_2#citeas. Acesso em: 28 nov. 2020.

[493] JAQUET-CHIFFELLE, David-Olivier. Reply: direct and indirect profiling in the light of virtual persons. *In:* HILDEBRANDT, Mireille. **Defining Profiling:** A new type of knowledge? Springer, Dordrecht, 2008, p. 35. Disponível em: https://link.springer.com/chapter/10.1007%2F978-1-4020-6914-7_2#citeas. Acesso em: 28 nov. 2020.

[494] JAQUET-CHIFFELLE, David-Olivier. Reply: direct and indirect profiling in the light of virtual persons. *In:* HILDEBRANDT, Mireille. **Defining Profiling:** A new type of knowledge? Springer, Dordrecht, 2008, p. 35. Disponível em: https://link.springer.com/chapter/10.1007%2F978-1-4020-6914-7_2#citeas. Acesso em: 28 nov. 2020.

[495] CLARKE, Roger. "Profiling: a hidden challenge to the regulation of data surveillance". **Journal of Law, Information and Science,** v. 4, n. 2, 1993, p. 2. Disponível em: https://www.austlii.edu.au/au/journals/JlLawInfoSci/1993/26.html. Acesso em: 12 set. 2020.

A aplicação de perfis é o processo de identificação e representação de um indivíduo específico ou grupo que se enquadra num perfil e a tomada de alguma forma de decisão com base nesta identificação e representação[496].

Ressalte-se que um perfil pode ser criado manualmente, entretanto, na sociedade da informação, a maior parte dos perfis é construída de maneira automatizada. O Regulamento Geral de Proteção de Dados Pessoais da União Europeia despende especial atenção ao perfil automatizado, definindo-o, em seu artigo 4º, alínea 4, como

> qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações[497].

Para a construção de tais perfis, diferentes dispositivos de *hardware*, como biometria, sensores e computadores, são integrados a diferentes técnicas, como agregação e mineração de dados, no intento de descobrir padrões entre os diferentes dados existentes em grandes conjuntos de dados que podem ser usados para perfilização[498]. A LGPD, por sua vez, não traz uma definição para o *profiling.*

Numa sociedade que exige rápidas e eficientes tomadas de decisão, as quais devem passar por adequada avaliação e mitigação de riscos, mas que, para tanto, é necessário processar uma massiva quantidade de dados, a construção de perfis assume importante papel como ferramenta de análise e resposta. No caso da aplicação de perfis de maneira automatizada, a decisão pode ser tomada livre de tendências e preconceitos do ser humano, apenas por critérios objetivos.

No entanto, apesar de tais benefícios, o *profiling* também pode acarretar prejuízos aos titulares dos dados, em especial à sua privacidade.

---

[496] BOSCO, Francesca et al. Profiling Technologies and Fundamental Rights and Values: regulatory challenges and perspectives from European Data Protection Authorities. *In:* BOSCO, Francesca et al. **Profiling technologies in practice**: Applications and impact on fundamental rights and values. **Wolf Legal Publishers,** 2015, p. 8. Disponível em: https://research.tilburguniversity.edu/en/publications/profiling-technologies-and-fundamental-rights-an-introduction. Acesso em: 1 out. 2020.

[497] UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016**. Relativo à proteção de dados pessoais 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 Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679#d1e1554-1-1. Acesso em: 28 jun. 2020.

[498] JAQUET-CHIFFELLE, David-Olivier. Reply: direct and indirect profiling in the light of virtual persons. *In:* HILDEBRANDT, Mireille. **Defining Profiling:** A new type of knowledge? Springer, Dordrecht, 2008, p. 1-2. Disponível em: https://link.springer.com/chapter/10.1007%2F978-1-4020-6914-7_2#citeas. Acesso em: 28 nov. 2020.

4.2.2.2.1 Riscos associados ao *profiling*

Além de contribuir para a assimetria da informação entre titulares dos dados e agentes de tratamento, a definição e a construção de perfis envolvem outras ameaças aos direitos dos indivíduos. Aqui serão examinados dois destes riscos: a discriminação e a influência externa à dimensão decisional da privacidade.

4.2.2.2.1.1 Discriminação

O *profiling* destina-se à classificação e segmentação dos indivíduos de acordo com certas características, predições e correlações. Contudo, muitas vezes essa atividade pode levar à discriminação. Importa dizer que esse termo é utilizado, neste trabalho, no sentido da categorização de pessoas a partir de uma característica ou situação jurídica para, injustamente, atribuir-lhes alguma consequência negativa[499].

A aplicação de perfis, por diversas razões, pode levar a um resultado discriminatório, como se verá. Ressalte-se que tal resultado pode acontecer mesmo em caso de construção e aplicação de perfis de maneira não automatizada, no entanto, os algoritmos potencializam sobremaneira os riscos de discriminação, bem como tornam mais difícil a identificação deste resultado, já que são procedimentos complexos e obscuros, os quais as organizações sempre buscam proteger como segredo de negócio.

É o que se chama de discriminação algorítmica, que já era objeto de estudo desde as últimas décadas do século passado, mas que ganhou ainda mais relevo nos últimos anos, em virtude do crescimento da utilização do *profiling* nos mais diversos campos e do uso da inteligência artificial para tanto.

Como visto, a mineração encontra correlações entre os dados coletados e projeta possíveis comportamentos futuros dos titulares dos dados. A partir dessas predições, são criadas categorias em que os indivíduos serão enquadrados. Nesse cenário, o primeiro ponto a ser considerado é que os perfis são construídos com base em dados anteriores, que podem trazer consigo tendências discriminatórias. Saliente-se que os perfis não levam em consideração relações de causa e efeito, apenas a probabilidade de se verificar determinado evento caso outro evento venha a ocorrer, de modo que, se os dados que serão analisados apresentarem qualquer viés discriminatório, os perfis aprenderão tal tendência.

---

[499] MOREIRA, Adilson José. **O que é discriminação?** Belo Horizonte (MG): Letramento: Casa do Direito: Justificando, 2017, p. 27.

No caso de construção de perfis por meio de algoritmos, como o tratamento é automatizado, o problema torna-se ainda maior, haja vista que é mais difícil identificar esse viés, bem como se retira a possibilidade de integrantes dos grupos discriminados transporem a barreira do respectivo perfil, como poderia acontecer, por exemplo, numa seleção de emprego em que o recrutador, ao entrevistar um indivíduo, resolve contratá-lo, mesmo ele estando fora do perfil procurado pela empregadora.

Um estudo da professora Sweeney revelou que, ao se pesquisar um nome completo no *Google*.com, muitas vezes este provedor de pesquisa veicula anúncios que podem ser diferentes se o nome pesquisado for comumente associado a pessoas negras ou, ao contrário, se o nome frequentemente for associado a pessoas brancas. Nessa senda, 60% dos anúncios para verificação de antecedentes criminais ou anúncios que mencionavam as palavras "prisão" ou "criminal" apareciam quando a pesquisa se referia a nomes negros, ao passo que apenas 48% de tais anúncios eram mostrados quando se pesquisavam nomes brancos[500].

Isso acontece porque o *Google* entende que um anunciante pode não saber qual texto do anúncio funcionará melhor, então este pode fornecer vários modelos para a mesma sequência de pesquisa e, posteriormente, o algoritmo do *Google* aprenderá qual texto do anúncio obtém mais cliques dos visualizadores. No início, todos os textos de anúncio fornecidos possuem a mesma probabilidade de produzir um clique e, por conseguinte, de serem veiculados. Com o tempo, conforme as pessoas clicam numa versão de um anúncio com mais frequência do que em outras versões, as probabilidades mudam e o texto do anúncio que obtém mais cliques passará a ser exibido com mais frequência[501].

Dessa forma, o algoritmo utilizado para veicular anúncios não foi projetado para ser racista, no entanto, ao aprender com os dados com os quais foi alimentado, passa a reproduzir vieses sociais.

Se um dado é incorretamente coletado ou há alguma falha no tratamento desse dado, como um erro na codificação do algoritmo, o perfil que será aplicado ao titular revela-se inadequado, podendo levar a uma injusta discriminação. Assim, um erro no histórico de crédito de um indivíduo pode resultar em condições menos vantajosas na contratação de um financiamento ou até mesmo na sua exclusão das ofertas de crédito.

De igual modo, dados da saúde do indivíduo coletados ou tratados inadequadamente podem trazer grandes prejuízos ao titular, uma vez que tal tratamento pode indicar,

---

[500] SWEENEY, Lataya. Discrimination in online ad delivery. **Search Engines.** Disponível em: https://dl.acm.org/doi/pdf/10.1145/2460276.2460278. Acesso em: 29 dez. 2020, p. 12.

[501] SWEENEY, Lataya. Discrimination in online ad delivery. **Search Engines.** Disponível em: https://dl.acm.org/doi/pdf/10.1145/2460276.2460278. Acesso em: 29 dez. 2020, p. 14-15.

equivocadamente, que o indivíduo possui uma doença preexistente, levando a um aumento na mensalidade ou carência diferenciada para determinados tipos de tratamento.

Nesse diapasão, se, por exemplo, uma pessoa faz todas as compras de medicamentos para ela e sua família numa mesma farmácia e esta, por sua vez, não só armazena tais informações como ainda as compartilha com operadoras de planos de saúde, os medicamentos comprados para familiares – e não para o indivíduo – também serão submetidos a tratamento como se lhe dissessem respeito, predizendo, então, que o indivíduo sofre de enfermidades que, na verdade, são dos seus familiares. Esse processamento poderá aumentar a sua mensalidade do plano de saúde ou até mesmo fazer com que a operadora entenda que o indivíduo cometeu fraude por omissão de informações.

Além disso, se os dados não forem precisos, bem como se as variáveis do perfil não forem escolhidas de maneira representativa, ampla e neutra, os resultados da aplicação de perfil poderão ser enviesados.

Timnit Gebru, cientista da computação que foi colíder da Equipe de Inteligência Artificial do *Google*, afirma que os algoritmos de reconhecimento facial têm mais dificuldade em diferenciar homens e mulheres quanto mais escuro é o tom de pele, de modo que é muito mais provável que uma mulher de pele escura seja confundida com um homem do que outra mulher de pele mais clara. Uma das razões para isso seria que o conjunto de dados originais utilizado para treinar esses algoritmos é, em sua maioria, composto por dados de pessoas brancas e do sexo masculino[502].

Outro fator que pode levar à discriminação é a coleta e o tratamento de dados sensíveis para a construção de perfis. Como já visto, tais dados são assim chamados por, historicamente, possuírem um maior potencial de ser utilizados para fins discriminatórios ou lesivos.

Nos últimos anos, os testes de ancestralidade ganharam inúmeros adeptos, uma vez que são facilmente encontrados na *internet* a preço acessível. Em 2019, a companhia de análise genética *FamilyTreeDNA* admitiu que estava compartilhando as informações genéticas coletadas por meio de tais testes com o FBI e a polícia federal dos Estados Unidos para ajudar a identificar suspeitos de estupros e assassinatos. Posteriormente, surgiram notícias de que outras companhias afins estavam compartilhando os dados genéticos dos

[502] WALL, Matthew. Inteligência artificial: por que as tecnologias de reconhecimento facial são tão contestadas. **BBC News Brasil,** 5 jul. 2019. Disponível em: https://www.bbc.com/portuguese/geral-48889883. Acesso em: 1 out. 2020.

clientes com gigantes farmacêuticas para a realização de pesquisas e o desenvolvimento de novos medicamentos[503].

Segundo essas organizações, as quais possuem dados genéticos de milhões de pessoas, somente foram compartilhadas as informações cujos titulares consentiram na respectiva transferência. Contudo, nos Estados Unidos são comuns fusões de grandes farmacêuticas com fornecedoras de plano de saúde. Em 2018, por exemplo, o Departamento de Justiça autorizou a fusão entre a farmacêutica *CVS Health* e a seguradora de Saúde Aetna por US$ 69 bilhões[504].

Por conseguinte, não é remota a possibilidade de que tais dados sensíveis, cujo tratamento foi permitido pelos seus titulares para ajudar pesquisas de desenvolvimento, sejam utilizados para a construção e a aplicação de perfis por seguradoras de saúde, o que pode levar à discriminação dos indivíduos no tocante a mensalidades e coberturas do plano de saúde.

Acerca da importância da proteção dos dados genéticos, anota Rodotà:

> Parece evidente, a esta altura, que as informações genéticas assumem um valor *constitutivo* da esfera privada bem mais forte do que qualquer outra categoria de informações pessoais. Isso resulta do fato de que elas estão relacionadas à própria estrutura da pessoa, não são modificáveis pela vontade do interessado (como acontece para muitos outros dados, dos nomes às opiniões), não podem ser removidas ou cobertas pelo esquecimento (como acontece com as informações relacionadas aos comportamentos do passado). Exatamente por seu caráter *estrutural* e *permanente*, as informações genéticas constituem a parte mais dura do "núcleo duro" da privacidade, fornecem o perfil mais definido da pessoa e estão, assim, na base de ações discriminatórias. Não foi por acaso que uma das críticas mais preocupantes relacionadas ao "Projeto Genoma" tenha sido a que põe em evidencia o risco de que, utilizando seus resultados, se chegue a um "*gene based castle system*", a uma nova organização por castas da sociedade. (grifos do autor)

Conforme se observa, os dados genéticos são capazes de fornecer o perfil mais preciso de um indivíduo, pois estão relacionados, de maneira imutável, à própria estrutura da pessoa, sendo capazes de revelar informações como as características físicas e genéticas de um indivíduo, sua ascendência, predisposição a doenças, metabolismo, dados relacionados à resposta a tratamentos e medicamentos, probabilidade dos descendentes desenvolverem alguma doença genética. Por essa razão, devem ser especialmente protegidos para que não sejam coletados ou compartilhados sem autorização, ou usados para fins discriminatórios.

---

[503] FOGARTY, Philippa. Como empresas estão ganhando dinheiro com seu DNA. **BBC News Brasil,** 7 mai. 2019. Disponível em: https://www.bbc.com/portuguese/vert-cap-47926294. Acesso em: 1 out. 2020.

[504] ABELSON, Reed. CVS Health and Aetna $69 Billion Merger Is Approved With Conditions. **The New York Times,** 10 out. 2018. Disponível em: https://www.nytimes.com/2018/10/10/health/cvs-aetna-merger.html. Acesso em: 19 set. 2020.

Da mesma forma, os demais dados sensíveis podem gerar práticas tendenciosas. Pessoas com HIV são demitidas ou deixam de ser promovidas se seus empregadores tomarem conhecimento da sua condição de saúde. Segundo dados da Organização Internacional do Trabalho, a porcentagem de demissão por esse tipo de preconceito vai de 13% nas Ilhas Fiji a 100% no Timor Leste. Na Nicarágua, Grécia e Costa Rica, esses percentuais são de 67%, 80% e 53%, respectivamente. A pesquisa da OIT também incluiu relatos de pessoas que não foram aprovadas num processo seletivo para uma vaga de emprego depois que informaram serem soropositivos[505].

É justamente para evitar isso que a proteção de dados pessoais proíbe ou restringe a coleta de dados sensíveis[506]. No entanto, mesmo quando dados considerados sensíveis por natureza são omitidos, a discriminação ainda pode ocorrer, já que, no *profiling*, quando uma determinada variável não é coletada, utilizam-se, em substituição, outras variáveis presumidamente ligadas à variável sensível omitida. São as chamadas variáveis *proxies*.

O *Facebook*, por exemplo, não faz nenhuma pergunta acerca da raça ou etnia dos usuários, contudo, a partir das interações do indivíduo, consegue inferir o *proxy* "afinidade cultural", que se torna uma ferramenta eficaz para anunciantes que desejem apresentar diferentes versões de seus anúncios a grupos distintos[507]. A proibição da coleta de determinados dados pessoais não é suficiente para impedir a discriminação, haja vista que as organizações tendem a preencher tais lacunas na aplicação de perfis com as variáveis *proxies*.

Agan e Starr fizeram um estudo de discriminação na contratação com base em inscrições *online* depois que vários estados dos Estados Unidos proibiram que os empregadores questionassem os candidatos acerca de antecedentes criminais. A pesquisa revelou que, após tal proibição, a diferença entre a quantidade de candidatos com nomes associados a pessoas brancas e candidatos cujos nomes são comumente associados a pessoas negras que foram chamadas para a fase de entrevista cresceu cerca de 40%, uma vez que os

---

[505] ONU News. Pessoas com HIV continuam discriminadas no mercado de trabalho. **Agência Brasil,** 26 jul. 2018. Disponível em: https://agenciabrasil.ebc.com.br/internacional/noticia/2018-07/pessoas-com-hiv-continuam-discriminadas-no-mercado-de-trabalho. Acesso em: 2 nov. 2020.

[506] Como já visto, a disciplina dos dados pessoais sensíveis varia em cada ordenamento jurídico, contudo, de um modo geral, costuma-se proibir o tratamento de tais dados, indicando as exceções em que o tratamento pode ocorrer ou se permite o tratamento desses dados, mas em circunstâncias muito mais restritas que a dos demais dados pessoais e sob regras mais rígidas. Nessa esteira, a LGPD traz, em seu artigo 11, uma seção própria acerca das particularidades no tratamento desses dados, dispondo que o processamento de dados sensíveis somente poderá ocorrer: a) mediante consentimento do titular fornecido de forma específica e destacada, para finalidades específicas, ou b) sem o fornecimento de consentimento do titular, mas em hipóteses mais limitadas que aquelas permitidas para os outros dados pessoais.

[507] WILLIAMS, Betsy Anne; BROOKS, Catherine F.; SHMARGAD, Yotam. How Algorithms Discriminate Based on Data they Lack: challenges, solutions, and policy implications. **Journal of Information Policy,** Penn State University Press**,** v. 8, 4 set. 2018. p. 89-90. Disponível em: https://www.jstor.org/stable/10.5325/jinfopoli.8.2018.0078. Acesso em: 29 dez. 2020.

empregadores passaram a assumir que os negros têm maior probabilidade de possuir antecedentes criminais[508].

Mendes e Mattiuzzo[509], com base nos estudos de Schauer, ensinam que as generalizações podem ser consistentes ou inconsistentes. As consistentes podem ser universais quando se mostram verdadeiras em 100% dos casos, ou não universais, quando determinada característica é compartilhada pela maioria dos indivíduos de certo grupo, tal qual a afirmação de que "os brasileiros possuem ascendência europeia"; em que pese possa ser verdadeira para a maioria dos casos, alguns brasileiros não possuem tal característica.

Há, ainda, um terceiro tipo de generalização consistente, que não é verdadeira para 100% dos casos e tampouco para a maior parte dos membros de um grupo, no entanto, revela que um grupo de integrantes de uma classe maior possui mais frequentemente certo traço do que o restante da classe, ainda que tal atributo não apareça na maioria dos membros tanto do grupo menor quanto da classe inteiramente considerada. O exemplo trazido pelas autoras para ilustrar tal situação é o da afirmação de que "buldogues têm quadris ruins": essa sentença não significa que todos os buldogues ou mesmo a maioria dos integrantes desse grupo tenham quadris ruins, entretanto, a incidência desse problema de saúde é maior nessa raça quando comparada à grande categoria de cachorros. Dessa forma, esse tipo de generalização depende de uma dimensão comparativa.

Por fim, quando não há congruência estatística ou alguma evidência que corrobore a generalização, tem-se uma generalização inconsistente, conforme se verifica em sentenças como "loiras são burras" e "baianos são preguiçosos". Essa categoria de generalização é a que mais reforça estereótipos sociais.

O *profiling* se vale bastante de generalizações. Importa dizer que não somente as generalizações inconsistentes podem gerar discriminação; generalizações consistentes também são capazes disso.

Há situações em que a discriminação é estatisticamente consistente, contudo, dizem respeito a grupos historicamente discriminados e acabam reforçando o tratamento

---

[508] AGAN, Amanda; STARR, Sonja. Ban the Box, Criminal Records, and Racial Discrimination: a field experiment. **The Quarterly Journal of Economics,** v. 13, n. 1, fev. 2018**,** p. 191-235. Disponível em: https://academic.oup.com/qje/article-abstract/133/1/191/4060073?redirectedFrom=fulltext. Acesso em: 2 nov. 2020.

[509] MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. **Revista Direito Público,** v. 16, n. 90, 2019, p. 47-49. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766/Schertel%20Mendes%3B%20Mattiuzzo%2C%202019. Acesso em: 18 set. 2020.

discriminatório[510]. Assim, numa hipótese ilustrativa, o tratamento de dados de determinada companhia revelou que as pessoas do sexo feminino trabalhavam menos horas, por dia, na referida organização e, por isso, ao construir o perfil do próximo contratado para um cargo de gestão, define que este deverá ser do sexo masculino. Nessa situação, há uma evidência estatística a embasar esse perfil, no entanto, esses dados objetivos desconsideram qualquer relação de causalidade. Se a decisão é tomada unicamente com base nesse perfil, reforça-se o preconceito institucional contra as mulheres.

Quando os indivíduos são julgados por características do grupo que eles não possuem como indivíduos, tal fato pode acarretar uma injusta segregação.

> Assim, se uma pessoa mora em uma vizinhança comumente associada à pobreza e o modelo não possui nenhuma outra informação além de seu endereço para decidir se ela é ou não uma boa candidata para um empréstimo, ele a classificará como pertencente a um grupo do qual ela não seja parte, caso ela se apresente como um caso atípico. Isso poderia ocorrer na hipótese de essa pessoa ter uma renda superior ou inferior às pessoas de sua vizinhança, por exemplo. Desse modo, embora o algoritmo esteja correto e as informações também, ainda assim o resultado será uma generalização incorreta, na medida em que mesmo um resultado estatisticamente relevante apresentará um percentual de pessoas que não se encaixam perfeitamente naquela média. Isso se dá pela própria natureza de qualquer exercício probabilístico[511].

De igual forma, uma pessoa que pretende financiar um imóvel e, por conta disso, faz uma pesquisa acerca dos imóveis disponíveis em diferentes construtoras, as quais, por sua vez, realizam várias consultas ao seu CPF, pode acabar sendo encaixada, pelo banco financiador, num perfil de risco e, por conseguinte, ter o crédito negado. Isso porque os dados que deram origem ao perfil revelaram que indivíduos que têm seu CPF consultado com alta frequência têm mais probabilidade de ser inadimplentes, pois tais consultas indicam que estes indivíduos fazem mais uso de diferentes créditos ao mesmo tempo, tornando-se mais endividados. Ainda que esta informação esteja estatisticamente correta, não é a realidade daquela pessoa específica, uma vez que esta não fechará vários contratos de financiamento, mas apenas um.

---

[510] MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. **Revista Direito Público,** v. 16, n. 90, 2019, p. 54. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766/Schertel%20Mendes%3B%20Mattiuzzo%2C%202019. Acesso em: 18 set. 2020.

[511] MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. **Revista Direito Público,** v. 16, n. 90, 2019, p. 52. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766/Schertel%20Mendes%3B%20Mattiuzzo%2C%202019. Acesso em: 18 set. 2020.

As generalizações com base em perfis de grupo desindividualizam os titulares dos dados, que passam a ser julgados não pelo que são enquanto indivíduos, mas como integrantes de um determinado grupo, aos quais, muitas vezes, nem pertencem.

Esse fato faz com que as pessoas que não se encaixam no perfil objetivamente desejado sejam cada vez mais excluídas do acesso a oportunidades e serviços. Conforme Rodotà, a difusão do uso do *profiling* pode discriminar pessoas que não correspondam ao modelo padrão, acentuando a estigmatização dos comportamentos distintos de tal modelo, bem como a penalização das minorias[512].

Nas grandes companhias dos Estados Unidos, é frequente o uso do *profiling* para a contratação de novos empregados. Algoritmos decifram os currículos dos candidatos, verificam seus perfis em redes sociais e até mesmo utilizam inteligência artificial para analisar entrevistas. Não raramente os candidatos são submetidos a testes de personalidade, devendo responder se concordam ou não com afirmações como: "Ao longo do dia, posso experimentar muitas mudanças de humor" ou "Se algo muito ruim acontecer, levo algum tempo até que eu me sinta feliz novamente"[513].

Esses testes são usados para avaliar a personalidade, as habilidades cognitivas e outras características de 60% a 70% dos trabalhadores em potencial nos EUA. O problema é que tais testes são capazes de identificar e discriminar pessoas com provável histórico de doença mental[514].

Em 2012, o estudante universitário Behm, que obteve excelentes resultados nos exames SAT, foi rejeitado em processos seletivos para contratação por sete companhias que utilizavam um teste de personalidade desenvolvido pela Kronos, a qual licencia a contratação de *software* para muitas grandes lojas estadunidenses. Para ele, a razão de tantas rejeições foi o fato de o teste de personalidade aplicado nas seleções identificar sua condição de transtorno bipolar. Diante disso, Kyle processou as sete empresas, o que levou uma das organizações processadas, a Lowe's, a afirmar que mudou seu processo de inscrição *online* para garantir que as pessoas com deficiência mental não sejam excluídas de oportunidades de trabalho[515].

---

[512] RODOTÀ, Stefano. **A vida na sociedade de vigilância –** a privacidade hoje. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 105.

[513] WEBER, Lauren; DWOSKIN, Elizabeth. Are Workplace Personality Tests Fair? **The Wall Street Journal,** 29 set. 2014. Disponível em: https://www.wsj.com/articles/are-workplace-personality-tests-fair-1412044257. Acesso em: 11 out. 2020.

[514]WEBER, Lauren; DWOSKIN, Elizabeth. Are Workplace Personality Tests Fair? **The Wall Street Journal,** 29 set. 2014. Disponível em: https://www.wsj.com/articles/are-workplace-personality-tests-fair-1412044257. Acesso em: 11 out. 2020.

[515] O'NEIL, Cathy. Personality Tests Are Failing American Workers. **Bloomberg Opinion,** 18 jan. 2018. Disponível em: https://www.bloomberg.com/opinion/articles/2018-01-18/personality-tests-are-failing-american-workers. Acesso em: 2 nov. 2020.

Outro exemplo de tratamento discriminatório são as práticas de *geopricing* e *geoblocking*, isto é, respectivamente, ofertar, sem nenhuma justificativa legítima, num mesmo dia, local e para o mesmo produto ou serviço, preços diferentes, ou restringir o acesso a determinado conteúdo da *internet*, ambas as ações com base na localização geográfica do indivíduo.

Em junho de 2018, o Departamento de Proteção e Defesa do Consumidor (DPDC) condenou a Decolar.com ao pagamento de multa de R$ 7.500.000,00 por considerar que

> ao precificar – ou permitir que se precifique – o serviço de acomodação de acordo com a localização geográfica do usuário, a Decolar.com se conduz de forma a extrapolar o direito de precificar (ou permitir que serviço por ele anunciado seja precificado) de acordo com as práticas do mercado. Com efeito, não se justifica, e nem é prática usual, o estabelecimento de preços diferentes de serviços que são prestados no mesmo local e nas mesmas condições a qualquer consumidor que esteja disposto a pagar por esses serviços. Quanto à não exibição da disponibilidade total de acomodações, a infração à ordem jurídica é ainda mais evidente: a Decolar.com extrapola de seu direito de praticar o comércio e de ofertar o produto, prejudicando o consumidor brasileiro, ao não mostrar serviço que não queira vender a determinado consumidor (no caso, o consumidor brasileiro). Isso porque o favorecimento (ou desfavorecimento), bem como a discriminação por conta de etnia, localização geográfica ou qualquer outra característica extrínseca ao ato comercial causa desequilíbrio no mercado e nas relações de consumo[516]. (BRASIL, 2018b).

No caso acima, a informação da localização geográfica do indivíduo foi utilizada para apresentar preços mais caros para as acomodações e até mesmo negar a oferta de vagas para brasileiros, enquanto indivíduos de outros países tinham, nas mesmas condições, acesso a ofertas melhores para a mesma acomodação.

Há, ainda, mais um fator que pode levar à discriminação: é o exercício de direitos pelo titular dos dados. Aqui não se verifica erro quantos aos dados ou à estatística; o que ocorre é que o perfil coleta informações acerca de quais direitos o titular exerceu, bem como quantas vezes o fez, para, então, afetar negativamente os resultados para o indivíduo.

Um exemplo ajudará no entendimento desse tipo de discriminação: na Alemanha, verificou-se que os birôs de crédito estavam considerando o exercício do direito de acesso do indivíduo ao *score* de crédito como um aspecto negativo, de modo que as pessoas que acessavam o seu *score* tinham sua pontuação reduzida[517].

---

[516] BRASIL. Ministério da Justiça e Segurança Pública. **Decolar.com é multada por prática de geo pricing e geo blocking.** 16 ago. 2018b. Disponível em: https://www.justica.gov.br/news/collective-nitf-content-51. Acesso em: 20 abr. 2020.

[517] MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. **Revista Direito Público,** v. 16, n. 90, 2019, p. 54. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766/Schertel%20Mendes%3B%20Mattiuzzo%2C%202019. Acesso em: 18 set. 2020.

Importa dizer que o *profiling* pode prejudicar a coesão social, tendo em vista que quando os perfis de grupo, ainda que corretos, tornam-se publicamente conhecidos, as pessoas podem tratar umas às outras de acordo com tais perfis, como no caso de um processamento de dados indicar que há mais criminosos entre os residentes de uma determinada localidade; apesar de a informação desconsiderar uma série de fatores que poderiam explicar essa estatística, as pessoas podem passar a se comportar como suspeitas entre os moradores dessa região[518].

Além da discriminação, a aplicação de perfis pode intervir fortemente nas escolhas do indivíduo, consoante se verá.

4.2.2.2.1.2 Influências externas à privacidade decisional

O uso de *profiling* pode acarretar várias consequências à dimensão decisional da privacidade de um indivíduo. Ao privilegiar comportamentos que estejam de acordo com determinado padrão, os indivíduos podem passar a se comportar e a fazer suas escolhas de modo a se encaixarem no modelo almejado. Nessa esteira, os perfis podem se tornar obstáculos ao livre desenvolvimento da personalidade.

Uma vez que os perfis analisam as preferências dos usuários, seus hábitos, gostos e comportamentos, os indivíduos são categorizados em diferentes grupos de interesse. Por exemplo, uma pessoa que adquiriu alguns livros de Direito integra a categoria daqueles que têm interesse em produtos dessa área do conhecimento. Da mesma forma, uma pessoa que clicou em alguma notícia favorável ao atual presidente do Brasil é encaixada na categoria daqueles indivíduos interessados nesse tipo de informação, ao passo que outro usuário que clica em uma matéria contrária ao presidente é categorizado no grupo daqueles que preferem notícias mais críticas ao presidente.

O problema é que, ao fazer isso, as organizações passam a mostrar e a sugerir ao indivíduo, quase que em sua totalidade, produtos, anúncios, notícias, serviços, oportunidades e informações relacionados ao perfil daquele grupo de interesse no qual a pessoa foi enquadrada. Assim, o usuário tem um acesso muito mais amplo e facilitado àquilo que esteja de acordo com o modelo estabelecido do que a produtos, serviços e notícias que não estejam em conformidade com o padrão, o que pode limitar suas escolhas.

---

[518]SCHERMER, Bart W. The limits of privacy in automated profiling and data mining. **Computer Law & Security Review,** n. 27, 2011, p. 47. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0267364910001767. Acesso em: 10 out. 2020.

Utilizando-se das hipóteses acima, a pessoa que adquiriu o livro de Direito será exposta a uma quantidade muito maior de propaganda sobre publicações desse ramo do conhecimento do que sobre livros de qualquer outra área, o que tende a influenciar o consumidor a adquirir mais publicações de Direito, ao tempo que conhecer novos autores e livros que não estejam nesse padrão exigirá do consumidor mais esforço para sair de sua zona de conforto e pesquisar sobre outras obras.

Também no que diz respeito aos leitores sobre política, haja vista que os perfis das organizações lhes sugerirão notícias de teor semelhante às já lidas, as pessoas que leram matérias favoráveis ao presidente terão muito mais acesso a outras notícias de conteúdo mais positivo sobre ele, o que tanto reforçará a ideia já formada do leitor acerca do governante, como limitará o acesso do usuário a notícias contrárias ao presidente, as quais poderiam influenciar a opinião do indivíduo e sua escolha no pleito eleitoral. De igual modo, as pessoas enquadradas como leitores com interesse em matérias mais hostis sobre o governante serão expostas a mais informações prejudiciais ao presidente, o que também reforçará sua opinião negativa sobre ele, como também limitará seu acesso a notícias que poderiam influenciar sua opinião e decisões enquanto cidadão.

É esse fenômeno que recebe o nome de "bolha de opinião" ou "filtro-bolha". Mecanismos algorítmicos de determinadas companhias, como o *Google* e o *Facebook*, rastreiam o comportamento e outras informações *online* de cada usuário e, a partir daí, criam um universo que condiciona a navegação do indivíduo na *internet* ao que estes desejam – ou desejariam –, conforme uma predição algorítmica[519].

O fato é que a "premissa do *filter bubble* é que o usuário não decide deliberadamente o que aparece para ele dentro da bolha, nem tem acesso ao que fica de fora". Apesar de os filtros-bolha gerarem comodismo para o usuário, que encontra de forma rápida e eficaz aquilo que deseja, o excesso de filtragem pode fazer com que os indivíduos, sem consciência de tal excesso – que muitas vezes é sutil e imperceptível –, afastem-se dos pontos de vista divergentes, "empobrecendo, assim, o valor do debate na esfera pública virtual", bem como sejam inundados por publicidade direcionada[520].

Dessa forma, os perfis, individuais ou de grupo, podem afetar negativamente a liberdade de escolha. Rodotà já alertava a esse respeito:

---

[519] MAGRANI, Eduardo; OLIVEIRA, Renan Medeiros de. A esfera pública (forjada) na era das fake news e dos filtros-bolha. **Cadernos Adenauer XIX,** n. 4, 2018, p. 21. Disponível em: http://eduardomagrani.com/wp-content/uploads/2019/05/PUBLICACAO-nova-2019-KA-Cadernos-2018.4-site.pdf. Acesso em: 10 out. 2020.

[520] MAGRANI, Eduardo; OLIVEIRA, Renan Medeiros de. A esfera pública (forjada) na era das fake news e dos filtros-bolha. **Cadernos Adenauer XIX,** n. 4, 2018, p. 22. Disponível em: http://eduardomagrani.com/wp-content/uploads/2019/05/PUBLICACAO-nova-2019-KA-Cadernos-2018.4-site.pdf. Acesso em: 10 out. 2020.

> Se, por exemplo, se verifica que a maioria das famílias que habitam em um determinado bairro lê apenas um tipo de publicação, razões econômicas estimularão a distribuição naquela área apenas de livros e jornais correspondentes aos gostos e aos interesses individuados naquele momento particular. Por um lado, portanto, dá-se início a um mecanismo que pode bloquear o desenvolvimento daquela comunidade, solidificando-a no seu perfil traçado em uma situação determinada. Por outro lado, penalizam-se os poucos que não correspondem ao perfil geral, iniciando-se assim um perigoso processo de discriminação de minorias. A "categorização" dos indivíduos e grupos, além disso, ameaça anular a capacidade de perceber as nuances sutis, os gostos não habituais[521].

O *profiling*, mesmo quando não automatizado, pode se constituir num grande obstáculo ao desenvolvimento da personalidade dos indivíduos. Com a *internet*, este risco é ainda maior, já que as pessoas sofrem a influência desses perfis a cada minuto, em qualquer atividade realizada na rede mundial de computadores.

Assim, a partir da coleta de grandes quantidades de dados pessoais, as organizações conseguem identificar características individuais ou grupos de pessoas que serão mais impactadas ou influenciadas por determinado anúncio ou conteúdo. Tais dados são capazes de identificar padrões de comportamento e personalidade dos indivíduos e, assim, associá-los em microgrupos que se tornarão um público-alvo muito mais preciso para certas propagandas e notícias. Essa técnica é o se chama de *microtargeting*[522].

Para ilustrar a capacidade de utilização da mencionada técnica, um estudo realizado por pesquisadores da Universidade de Cambrigde demonstrou que as curtidas no *Facebook* podem ser usadas para prever com precisão atributos pessoais altamente sensíveis, tais como orientação sexual, etnia, pontos de vista religiosos e políticos, traços de personalidade, inteligência, felicidade, uso de substâncias viciantes, idade e sexo. O modelo utilizado para a pesquisa, baseado num conjunto de dados de mais de 58 mil voluntários que forneceram *likes* na referida rede social, foi capaz de identificar corretamente, por exemplo, heterossexuais e homossexuais em 88% dos casos; brancos e negros com precisão de 95%; e democratas e republicanos em 85% dos casos[523].

Técnicas sofisticadas de mineração de dados são capazes de descobrir diversos traços da personalidade do indivíduo, o que permite o direcionamento de anúncios e conteúdos sobre

---

[521] RODOTÀ, Stefano. **A vida na sociedade de vigilância –** a privacidade hoje. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 83.

[522] GUEDES, Paula. Direcionamento de campanhas eleitorais: lições do passado para 2020. **Its Rio,** 09 abr. 2020. Disponível em: https://feed.itsrio.org/direcionamento-de-campanhas-eleitorais-li%C3%A7%C3%B5es-do-passado-para-2020-de58e32e5dbe. Acesso em: 10 out. 2020.

[523]KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. Private traits and attributes are predictable from digital records of human behavior. **PNAS Early Edition,** 29 out. 2012. Disponível em: http://goodtimesweb.org/surveillance/2013/PNAS-2013-Kosinski-1218772110.pdf. Acesso em: 2 nov. 2020.

produtos e questões específicas com um potencial muito maior de influência nas decisões do indivíduo, independentemente de serem de interesse das pessoas em geral.

A técnica de *microtargeting* é bastante utilizada nas campanhas políticas, uma vez que os eleitores podem ser categorizados em microalvos muito mais precisos que a estratificação clássica das pesquisas eleitorais, sendo possível classificar os eleitores não só de acordo com sua renda e escolaridade, mas de acordo com suas emoções e comportamento, surgindo categorias como a do eleitor ambientalista sensível, a do eleitor curioso indeciso e a do eleitor raivoso de direita. Então, são construídas mensagens altamente refinadas, personalizadas e direcionadas aos diversos microgrupos de eleitores[524].

O maior exemplo do uso de *microtargeting* e filtro-bolha foi o aqui já relatado escândalo da *Cambridge Analytica*. Com os dados coletados pelo *Facebook*, foram criados modelos e algoritmos capazes de predizer a qual tipo de postagem cada eleitor estadunidense estava mais suscetível, tanto quanto a forma (vídeos, textos ou imagens) como também quanto ao conteúdo, tom e estilo de cada *post*. Ainda, os modelos matemáticos e algoritmos indicavam quantas vezes uma pessoa precisava ser exposta à postagem para ter sua opinião influenciada. Em seguida, a vasta equipe da *Cambridge Analytica* produzia conteúdos com potencial de influência, os quais, então, eram encaminhados à equipe de *targeting* para fazer com que cada uma das postagens alcançasse o maior número possível de eleitores a ela suscetíveis por meio de *posts* patrocinados, bem como novos *blogs* e *sites*[525].

Hoje, um dos maiores problemas da sociedade da informação, as *fake news*, é alimentado e fortalecido pelo uso de *profiling*, *microtargeting* e filtro-bolha, alcançando muito mais pessoas e potencializando sobremaneira seus efeitos negativos.

Nessa esteira, observa-se que os riscos do *profiling*, máxime na sociedade da informação, não se limitam à restrição de acesso a conteúdo e a oportunidade, mas expandem-se para a própria manipulação do indivíduo, o qual sofre forte influência na dimensão decisional de sua privacidade, na maioria das vezes sem ter o menor conhecimento acerca de como seus dados estão sendo tratados e de quais fatores levam os algoritmos a exporem-no a determinados assuntos e propagandas.

Imagine um indivíduo que todo ano viaje com sua esposa, para Maceió (AL) e, em determinado ano, resolve que fará uma viagem diferente, desta vez para Aracaju (SE),

---

[524] FRAGA, Plínio. Como é feito o uso político dos dados roubados nas redes sociais. **Uol Notícias,** 6 jan. 2020. Disponível em: https://noticias.uol.com.br/colunas/plinio-fraga/2020/01/06/como-e-feito-o-uso-politico-dos-dados-roubados-nas-redes-sociais.htm. Acesso em: 10 out. 2020.

[525] OLHAR DIGITAL. **Cambridge Analytica:** tudo sobre o escândalo do *Facebook* que afetou 87 milhões. 21 mar. 2018. Disponível em: https://olhardigital.com.br/2018/03/21/noticias/cambridge-analytica/. Acesso em: 4 abr. 2020.

passando a empreender buscas na *internet* por passagens aéreas e hospedagem neste estado. Ocorre que o hotel alagoano em que a pessoa costumava se hospedar percebe a mudança de planos de seu cliente por meio do seu monitoramento *online* e, então, começa a lhe enviar vários *e-mails* promocionais para hospedagem no hotel, bem como lhe oferecendo certos brindes, tais como um jantar grátis no restaurante do hotel, precedido de uma massagem para casal igualmente gratuita. Diante de tantos atrativos oferecidos pelo hotel de Maceió, o indivíduo resolve não mais viajar para Aracaju e manter sua viagem anual para a capital alagoana.

Também, em outra situação hipotética, um indivíduo que há dois anos possui um carro da marca X resolve trocar de veículo por algum de outra marca. Para tanto, começa a pesquisar *online* sobre outros automóveis e escolhe um modelo de outro fabricante para fazer um *test drive*. A marca do seu atual carro, que até então não havia lhe enviado mensagem alguma, mas que estava monitorando a sua navegação na *internet*, bem como a localização do seu automóvel, no momento em que percebe que o indivíduo parou numa loja da fabricante concorrente, envia-lhe um SMS com uma oportunidade imperdível para a troca do veículo por um do mesmo modelo, porém novo. Assim, o indivíduo faz o *test drive* do carro que desejava comprar e este corresponde a todas às suas expectativas; no entanto, diante da oportunidade que recebera da fabricante do seu automóvel, o indivíduo prefere aceitá-la e adquirir um veículo do mesmo modelo que já possuía.

Estes dois exemplos mostram como o uso da mineração de dados e do *profiling* pode influenciar a autonomia e a liberdade de escolha dos indivíduos. Tais hipóteses trataram de promoções para um produto que não chegam a afetar o estilo de vida das pessoas, entretanto essas técnicas podem ser aplicadas para situações bem mais sérias.

Zarsky aponta dois casos fictícios que demonstram bem o grau de periculosidade de tais técnicas. No primeiro exemplo, um fumante, que costuma comprar vários produtos em determinada loja virtual, decide parar de fumar. O algoritmo da loja verifica que o indivíduo parou de comprar cigarros e comprou um adesivo de nicotina, concluindo que ele resolveu abandonar o referido hábito. A partir disso, o algoritmo começa a lhe apresentar anúncios de cigarros, bem como lhe envia, junto das compras, um maço de cigarros gratuito, buscando levar o indivíduo a mudar sua resolução[526].

[526] ZARSKY, Tal Z. “Mine Your Own Business!”: making the case for the implications of the data mining of personal information in the forum of public opinion. **Yale Journal of Law and Technology,** 2003. Disponível em: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1008&context=yjolt. Acesso em: 28 set. 2020, p. 20.

No segundo exemplo, um indivíduo carnívoro reduziu os gastos com carne bovina, além de ter diminuído notavelmente suas visitas a churrascarias. Passou a assinar revistas sobre natureza, a ler bastante sobre bem-estar animal e a consumir alguns produtos de soja. Uma indústria de carne, que rastreou o comportamento dos vegetarianos por anos, percebeu que as atitudes do indivíduo em questão se amoldavam aos comportamentos classificados como "sintomas" iniciais de que uma pessoa está se tornando um vegetariano e, por conseguinte, começa a estimular o consumo de carne pelo indivíduo antes que este opte, definitivamente, pelo vegetarianismo.

A organização empresária lhe envia cupons para a churrascaria favorita do indivíduo, certifica-se de que este seja exposto a vários comerciais de restaurantes de *fast food*, bem como a matérias e outros conteúdos que tratam da importância de comer carne e proteína. Ainda, por meio de supermercado afiliado, garante que o indivíduo nunca receba promoções de produtos de soja[527].

Tais situações demonstram como as companhias podem aproximar os indivíduos de produtos em que estes não tinham interesse, por meio da grande exposição a ofertas voltadas ao consumo de tais produtos, bem como a argumentos persuasivos em momentos nos quais as pessoas estejam a eles mais suscetíveis.

Apesar de as organizações sempre terem buscado influenciar os gostos, hábitos e decisões das pessoas, não há dúvidas de que a mineração de dados e o *profiling* aumentaram exponencialmente a capacidade e a eficácia de tais entes impactarem a dimensão decisional da privacidade dos indivíduos, já que as estratégias adotadas passam a ser cada vez mais personalizadas e as pessoas não têm conhecimento de como seus dados pessoais são utilizados para influenciar seu comportamento.

Embora técnicas de mineração de dados e de *profiling* sejam cada vez mais frequentes, os riscos de sua utilização não passam despercebidos. À vista disso, juristas e profissionais da tecnologia da informação têm buscado traçar algumas soluções que ao menos sejam capazes de reduzir os riscos a níveis aceitáveis, considerando-se o contexto da sociedade da informação e a importância de tais técnicas, uma vez que é quase impossível eliminar todos os problemas dessa seara.

---

[527] ZARSKY, Tal Z. "Mine Your Own Business!": making the case for the implications of the data mining of personal information in the forum of public opinion. **Yale Journal of Law and Technology,** 2003. Disponível em: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1008&context=yjolt. Acesso em: 28 set. 2020, p. 39.

4.2.2.3 A importância das legislações sobre proteção de dados pessoais para a mitigação dos riscos à privacidade

Até o momento não há, mesmo na experiência europeia, uma solução única e plenamente eficaz para minimizar os riscos que a mineração de dados e a definição de perfis representam para o indivíduo. Apesar disso, as legislações sobre proteção de dados pessoais, máxime as mais recentes, fornecem alguns mecanismos que podem ajudar a garantir, mesmo que parcialmente, os direitos dos titulares de dados.

Inicialmente, importa dizer que a LGPD, em seu artigo 12, § 2º, prevê que mesmo os dados anonimizados poderão ser considerados como dados pessoais se forem "utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada", hipótese em que, por conseguinte, aplica-se a referida legislação.

Ocorre que, muitas vezes, as informações usadas no *profiling* são anonimizadas, pois, nos casos dos perfis de grupo, não há necessidade de se identificar uma pessoa; é suficiente a identificação apenas da categoria da qual ela faz parte, para que uma série de decisões que irão afetá-la, individualmente, seja tomada[528]. Assim, cumpre apurar se a utilização da expressão "identificada", pelo dispositivo acima mencionado, afasta essas situações da tutela da LGPD.

Nesta pesquisa, adota-se o entendimento defendido por Bioni, segundo o qual, numa interpretação sistemática da Lei Geral de Proteção de Dados Pessoais, tendo em conta seus fundamentos e objetivos e o próprio conceito expansionista por esta adotado:

> As expressões "determinada pessoa" e "identificada", constantes do referido dispositivo da LGPD, devem ser compreendidas com relação aos desdobramentos que o tratamento de dados pode ter sobre um indivíduo, ao contrário de significá-los com os olhos voltados para a base de dados em si, especificamente se o perfil comportamental pode ser ou não atribuído a uma pessoa em específico. Ou seja, o foco não está no dado, mas no seu uso – para a formação de perfis comportamentais – e sua consequente repercussão na esfera do indivíduo[529].

Para o autor, o conceito de dado pessoal deve passar por uma análise consequencialista, isto é, se o tratamento de dados, anonimizados ou pessoais, submeter uma coletividade ou um indivíduo a processos de decisões automatizadas e puder lhes causar

---

[528] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais –** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 80.
[529] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais –** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 81.

efeitos negativos, tal processamento deve ser regulado pelo escopo normativo da proteção dos dados pessoais[530].

De fato, uma interpretação literal do aludido artigo 12, § 2º, retiraria do âmbito de aplicação da LGPD inúmeras situações que oferecem sérios riscos aos direitos dos titulares dos dados. Estes continuarão a sofrer os impactos do *profiling* e das decisões neste baseadas sem ter à sua disposição os mecanismos de proteção conferidos pela Lei 13.709/2018. Caberá à Autoridade Nacional dirimir quaisquer dúvidas a respeito do sentido e do alcance do artigo em questão.

A observância de cada um dos princípios que norteiam a proteção de dados contribui, em algum grau, para estabelecer que o *data mining* e a definição de perfis ocorram de maneira lícita e acarretem o mínimo de consequências negativas ao titular do dados, em especial o princípio da não discriminação, expressamente previsto pela LGPD e que é definido como a "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos". O RGPD, por sua vez, não possui uma disposição semelhante, contudo, numa interpretação sistemática do Regulamento, observa-se que o RGPD tampouco admite o tratamento discriminatório[531].

Além disso, segundo o considerando 71, do RGPD, a "decisão e definição de perfis automatizada baseada em categorias especiais de dados pessoais só deverá ser permitida em condições específicas", de modo que o *profiling* com base em dados sensíveis deve ser, em regra, proibido. Não há, na LGPD, idêntica previsão, no entanto, como visto, essa disposição não minimiza satisfatoriamente os riscos envolvidos nessa prática, haja vista que a existência de variáveis *proxies* pode levar a resultados discriminatórios. Desse modo, mostra-se mais

---

[530] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais –** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 82.

[531] A exemplo do Considerando 75, que ao tratar dos riscos aos indivíduos, engloba a discriminação: (75) O risco para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, em especial quando o tratamento possa dar origem à discriminação, à usurpação ou roubo da identidade, a perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a quaisquer outros prejuízos importantes de natureza económica ou social; quando os titulares dos dados possam ficar privados dos seus direitos e liberdades ou impedidos do exercício do controlo sobre os respetivos dados pessoais; quando forem tratados dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical, bem como dados genéticos ou dados relativos à saúde ou à vida sexual ou a condenações penais e infrações ou medidas de segurança conexas; quando forem avaliados aspetos de natureza pessoal, em particular análises ou previsões de aspetos que digam respeito ao desempenho no trabalho, à situação económica, à saúde, às preferências ou interesses pessoais, à fiabilidade ou comportamento e à localização ou às deslocações das pessoas, a fim de definir ou fazer uso de perfis; quando forem tratados dados relativos a pessoas singulares vulneráveis, em particular crianças; ou quando o tratamento incidir sobre uma grande quantidade de dados pessoais e afetar um grande número de titulares de dados.

efetivo focar no uso que se faz do perfil do que evitar que a sua construção se baseie no tratamento de dados sensíveis.

Ainda conforme o mesmo considerando do RGPD, recomenda-se expressamente que o responsável pelo tratamento das informações pessoais utilize procedimentos matemáticos e estatísticos adequados à definição de perfis, bem como aplique medidas técnicas e organizativas que garantam a correção dos fatores que introduzem imprecisões nos dados pessoais e atenuação do risco de erros. O responsável pelo tratamento deverá, também, 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".

Como demonstrado no capítulo anterior, as duas mencionadas legislações preveem alguns direitos dos indivíduos, os quais são essenciais à tutela do direito fundamental para a proteção de dados pessoais. Isso inclui a salvaguarda dos titulares dessas informações contra os perigos envolvidos no *profiling* e na tomada de decisão com base no processamento de dados pessoais.

O primeiro deles é o direito de acesso, que, como já visto, garante ao titular que obtenha dos agentes de tratamento, de modo facilitado, informações claras, adequadas e ostensivas acerca da finalidade, duração e forma do processamento de dados. Esse direito é essencial para a redução da assimetria de informação entre os agentes de tratamento e os titulares dos dados, assegurando aos indivíduos algum grau de conhecimento sobre o uso de suas informações pessoais. Também o direito à correção de dados incompletos, inexatos ou desatualizados é importante para que ao titular de tais informações seja aplicado o perfil mais adequado. Contudo, somente o exercício desses dois direitos não é suficiente.

Por tal razão, o Regulamento Geral de Proteção de Dados da União Europeia prevê, em seu artigo 21, que o indivíduo tem direito de se opor à submissão de seus dados pessoais a tratamento destinado à definição de perfis, inclusive se tal processamento estiver relacionado com a comercialização direta[532].

---

[532] Artigo 21º - Direito de oposição:
1. O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito com base no artigo 6º, nº 1, alínea e) ou f), ou no artigo 6º, nº 4, incluindo a definição de perfis com base nessas disposições. O responsável pelo tratamento cessa o tratamento dos dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.
2. Quando os dados pessoais forem tratados para efeitos de comercialização direta, o titular dos dados tem o direito de se opor a qualquer momento ao tratamento dos dados pessoais que lhe digam respeito para os efeitos da referida comercialização, o que abrange a definição de perfis na medida em que esteja relacionada com a comercialização direta.

O artigo 22 do mesmo Regulamento estabelece que o titular das informações tem o direito de não se sujeitar a nenhuma decisão tomada unicamente em virtude do processamento automatizado de seus dados, incluindo-se aí a definição de perfis, a menos que: a) a decisão seja necessária para a celebração ou a execução de um contrato entre o titular e o responsável pelo tratamento; b) haja o consentimento explícito do indivíduo; c) a decisão seja autorizada por um Estado-Membro. Mesmo na ocorrência das duas primeiras hipóteses, garante-se ao indivíduo o direito de obter "intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão"[533].

A LGPD, por sua vez, também prevê um direito à oposição. De modo mais genérico, estabelece em seu artigo 18, § 2º, que o titular pode se opor a tratamento realizado com fundamento numa das hipóteses de dispensa de consentimento, em caso de descumprimento das disposições da referida lei.

Quanto às decisões individuais automatizadas, a legislação pátria, em seu artigo 20, estabelece que o indivíduo tem direito a solicitar a revisão de decisões tomadas exclusivamente com base no tratamento automatizado de seus dados pessoais que afetem seus interesses, compreendendo as decisões destinadas à definição de perfil pessoal, profissional, de consumo e de crédito ou de aspectos de sua personalidade. A esse respeito, inicialmente o texto da lei previa a possibilidade de a pessoa solicitar que a revisão fosse feita por pessoa natural, porém a Lei 13.853/2019 retirou tal possibilidade.

A revisão humana das decisões automatizadas deixou de ser uma obrigatoriedade e passou a ser uma faculdade dos agentes de tratamento, o que não tutela de maneira adequada os direitos da personalidade do titular dos dados, haja vista que, consoante demonstrado, não são apenas os erros de codificação que podem levar um algoritmo a um resultado inadequado. Existem diversos fatores que podem levar a isso, como os cálculos probabilísticos e as

---

3. Caso o titular dos dados se oponha ao tratamento para efeitos de comercialização direta, os dados pessoais deixam de ser tratados para esse fim.

[533] Artigo 22º Decisões individuais automatizadas, incluindo definição de perfis. 1. O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar. 2. O nº 1 não se aplica se a decisão: a) For necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento; b) For autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou c) For baseada no consentimento explícito do titular dos dados. 3. Nos casos a que se referem o nº 2, alíneas a) e c), o responsável pelo tratamento aplica medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão. 4. As decisões a que se refere o nº 2 não se baseiam nas categorias especiais de dados pessoais a que se refere o artigo 9º, nº 1, a não ser que o nº 2, alínea a) ou g), do mesmo artigo sejam aplicáveis e sejam aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular.

inconsistências nas amostras, que podem não ser sanados com uma revisão que também ocorre de forma automatizada.

Em suma, a revisão automatizada não garante que os indivíduos sejam julgados com base nas suas próprias características e méritos individuais, e não pelas características do grupo a que pertence, as quais, embora válidas para a categoria em questão, podem não ser válidas para o indivíduo enquanto tal. Entretanto, nada impede que os agentes de tratamento viabilizem que os titulares dos dados solicitem que um reexame conte com intervenção humana. Caso as circunstâncias do caso concreto apontem para a necessidade da revisão humana de uma decisão automatizada, o Judiciário poderá determiná-la com vistas a tutelar os direitos dos titulares dos dados.

É preciso garantir que o exercício desses direitos pelo indivíduo não influenciará, negativamente, na decisão tomada pelos agentes de tratamento. Por essa razão, o artigo 21 da LGPD expressamente prevê que "os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo".

Tendo em vista que, atualmente, o tratamento de dados pessoais para a definição de perfis e para a tomada de decisão ocorre cada vez mais de maneira automatizada, é crescente a preocupação dos estudiosos da privacidade com a obscuridade dos algoritmos que processam essas informações. A literatura costuma apontar a transparência como um importante mecanismo para tutelar os direitos dos indivíduos ante os potenciais riscos que o tratamento de dados por meio de sistemas computacionais implica.

A transparência permite que os indivíduos tomem conhecimento de quais tipos de dados pessoais são coletados, como são gerenciados e analisados, bem como quais decisões são tomadas a partir desses dados e com base em quais fatores[534]. Esse princípio intenta assegurar um conhecimento mais amplo acerca do que ocorre durante o tratamento das informações pessoais e de como se chegou a certo resultado.

Para tanto, a transparência exige que sejam satisfeitos dois requisitos: acessibilidade e compreensibilidade[535]. O primeiro componente é o que mais gera debates. De um lado, existem argumentos contrários à abertura do código-fonte ao público em geral, máxime o segredo comercial. De outro, há autores, como Pasquale e Citron, que defendem que essas

---

[534] CABALLOL, Daniel Contreras; DENDAL, Daniel Pefaur. **Cuaderno de Trabajo nº 17 –** Transparencia Algorítmica: buenas prácticas y estándares de transparencia en el proceso de toma de decisiones automatizadas. Out. 2020. Disponível em: https://www.consejotransparencia.cl/wp-content/uploads/2020/10/Transparencia-Algoritmica.pdf. Acesso em: 29 dez. 2020, p. 9.

[535] MITTELSTADT, Brent Daniel et al. The ethics of algoritms: mapping the debate. **SAGE Journals,** 1 dez. 2016. Disponível em: https://journals.sagepub.com/doi/full/10.1177/2053951716679679. Acesso em: 18 set. 2020, p. 6.

alegações são compensadas pelas ameaças à dignidade, não se podendo tolerar que as decisões sobre os indivíduos sejam tomadas por um sistema secreto que não oferece aos indivíduos nenhuma "chance para desafiar pontuações preditivas que prejudicam sua capacidade de obter crédito, empregos, habitação e outras oportunidades importantes"[536].

A extensão do acesso ao código-fonte de algoritmos deve levar em consideração o objetivo do sistema e os outros interesses envolvidos na questão. A depender do uso a que se destina o algoritmo, a divulgação do seu código fará com que o sistema perca a sua capacidade preditiva, já que os indivíduos poderão utilizar o conhecimento obtido para burlá-lo. Outras vezes, haverá preocupações a justificar a não abertura do código-fonte a toda a população, a exemplo do segredo comercial.

Não incorrendo nessas hipóteses, o ideal é que seja dada a maior transparência possível ao algoritmo e, mesmo quando existirem justificativas legítimas para se atribuir algum nível de segredo ao código do sistema, deve haver algum acesso ao funcionamento interno do sistema.

Os algoritmos não devem ser caixas-pretas, cujo funcionamento interno ninguém conhece. Uma alternativa que conciliaria a proteção dos dados e o segredo empresarial seria a abertura do código apenas à autoridade responsável – no caso brasileiro, a Autoridade Nacional de Proteção de Dados –; esta garantiria o sigilo das informações. Dessa forma, seria assegurada a transparência do sistema, sem comprometer o negócio nele baseado.

A esse respeito, tanto a Lei Geral de Proteção de Dados Pessoais quanto o Regulamento Geral de Proteção de Dados Pessoais levam em consideração os argumentos contrários à divulgação do código-fonte dos algoritmos.

Nesse diapasão, a LGPD, em seu artigo 6º, VI, define a transparência como a "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial".

No intento de verificar se as organizações estão observando a LGPD no tratamento dos dados pessoais, inclusive na mineração de dados e na aplicação de perfis, a LGPD, em seu artigo 20, estabelece que:

---

536 "At the very least, individuals should have a meaningful form of notice and a chance to challenge predictive scores that harm their ability to obtain credit, jobs, housing, and other important opportunities." (CITRON, Danielle Keats; PASQUALE, Frank A. The Scored Society: due process for automated predictions. **Washington Law Review,** v. 89, 8 jan. 2014. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2376209. Acesso em: 18 set. 2020, p. 27).

> § 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.

Sempre que um agente de tratamento utilizar o segredo comercial ou industrial para sonegar informações acerca dos fundamentos e da metodologia utilizados na tomada de decisão, a ANPD poderá auditar o sistema de computação, no intento de identificar o respeito, ou não, aos direitos dos titulares dos dados.

Essa obrigação de fornecer informações sobre uma decisão automatizada a que se refere o artigo 20, § 1º, é o que a doutrina chama de direito à explicação. Também o artigo 13, nº 1, alínea f, do RGPD, prevê tal direito ao dispor que o titular tem direito a obter informações acerca da existência de decisões automatizadas, incluindo a definição de perfis, bem como informações úteis relativas à lógica subjacente, além da importância e das possíveis consequências de tal tratamento para o titular dos dados.

Esse direito é de suma importância para a utilização dos sistemas computacionais de maneira transparente. Entretanto, nem a lei brasileira nem a lei europeia deixam claro qual é o grau de explicação a que os agentes de tratamento devem atender.

O Grupo de Trabalho do Artigo 29º para a Proteção de Dados, em suas "Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679", recomenda que os responsáveis pelo tratamento, em vez de apresentar uma explicação complexa sobre o funcionamento dos algoritmos ou da aprendizagem automática, forneçam, de maneira clara, informações essenciais acerca dos fundamentos da decisão, tais com: a) as categorias de dados que foram ou serão utilizadas no processo de definição de perfis ou de tomada de decisão e suas respectivas fontes; b) o motivo pelo qual essas categorias são consideradas pertinentes; c) o modo como é elaborado qualquer perfil utilizado no processo de decisão automatizada, incluindo eventuais estatísticas utilizadas na análise; d) o motivo pelo qual esse perfil é relevante para o processo de decisão automatizada; e) o modo como é utilizado para uma decisão relativa ao titular dos dados[537].

[537] UNIÃO EUROPEIA. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01).** 22 ago. 2018. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053. Acesso em: 3 nov. 2020, p. 35.

No Brasil, ante a ausência de maiores critérios legislativos, espera-se que a Autoridade Nacional de Proteção de Dados elabore diretrizes básicas a respeito da abrangência do direito à explicação.

Ainda sobre o componente da acessibilidade, assim como a LGPD, em momento algum o Regulamento Geral de Dados da União Europeia exige que tal atributo seja aplicado aos códigos-fontes dos algoritmos que processam dados pessoais. Não que a transparência não possa ser empregada ao funcionamento interno dos sistemas computacionais; caso a divulgação de um código-fonte não traga prejuízos, sua abertura é desejável.

Uma vez que a LGPD não traça maiores critérios a respeito da abrangência da transparência, é possível utilizar alguns parâmetros desenvolvidos no âmbito do RGPD como base para se entender tal amplitude.

O RGPD tampouco ignora que os algoritmos protegidos por segredo comercial não podem ser divulgados ao público em geral, no entanto, estabelece que os responsáveis pelo tratamento não podem abusar dessa proteção para se recusar a fornecer informações aos titulares dos dados. Deve ser fornecido, portanto, o máximo de informação possível e necessária para o atendimento da solicitação do indivíduo, inclusive o que concerne à lógica subjacente ao tratamento automático dos dados pessoais e os critérios aplicados para tomar a decisão[538].

A exigência de transparência prevista no Regulamento é voltada para informações e comunicações relacionadas com tratamento dos dados, em particular, informações sobre a identidade do responsável pelo processamento e os fins a que o tratamento se destina, informações voltadas a assegurar que o tratamento de dados seja efetuado com equidade e transparência, bem como a salvaguardar o direito dos titulares a obter a confirmação e a comunicação dos seus dados pessoais que estão a ser tratados, além de informações sobre riscos, regras, garantias e direitos associados ao tratamento dos dados pessoais e acerca dos

[538] Considerando 63: [...] Por conseguinte, cada titular de dados deverá ter o direito de conhecer e ser informado, nomeadamente, das finalidades para as quais os dados pessoais são tratados, quando possível do período durante o qual os dados são tratados, da identidade dos destinatários dos dados pessoais, da lógica subjacente ao eventual tratamento automático dos dados pessoais e, pelo menos quando tiver por base a definição de perfis, das suas consequências. Quando possível, o responsável pelo tratamento deverá poder facultar o acesso a um sistema seguro por via eletrônica que possibilite ao titular aceder diretamente aos seus dados pessoais. Esse direito não deverá prejudicar os direitos ou as liberdades de terceiros, incluindo o segredo comercial ou a propriedade intelectual e, particularmente, o direito de autor que protege o *software*. Todavia, essas considerações não deverão resultar na recusa de prestação de todas as informações ao titular dos dados. Quando o responsável proceder ao tratamento de grande quantidade de informação relativa ao titular dos dados, deverá poder solicitar que, antes de a informação ser fornecida, o titular especifique a que informações ou a que atividades de tratamento se refere o seu pedido.

meios de que os indivíduos dispõem para exercer os seus direitos relativamente a esse tratamento[539].

O titular dos dados deverá ser informado da definição de perfis e das consequências que daí advêm, bem como da eventual obrigatoriedade de fornecer os dados pessoais e das implicações quanto ao não fornecimento[540].

Quanto ao componente da compreensibilidade, a LGPD prevê que informações sobre o tratamento de dados pessoais devem ser prestadas de maneira clara, precisa e acessível. De igual forma, consoante o RGPD, qualquer informação destinada ao público ou ao titular dos dados deve ser concisa, de fácil acesso e compreensão, bem como formulada numa linguagem clara e simples. Adicionalmente, deve-se recorrer à visualização sempre que for adequado[541].

Entretanto, o emprego cada vez mais comum de *machine learning* dificulta a compreensão do algoritmo, tendo em vista que o código-fonte acaba por conter apenas as regras que ditarão o aprendizado das máquinas, mas não a regra decisória que o sistema efetivamente aprendeu.

---

[539] (39) O tratamento de dados pessoais deverá ser efetuado de forma lícita e equitativa. Deverá ser transparente para as pessoas singulares que os dados pessoais que lhes dizem respeito são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento e a medida em que os dados pessoais são ou virão a ser tratados. O princípio da transparência exige que as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples. Esse princípio diz respeito, em particular, às informações fornecidas aos titulares dos dados sobre a identidade do responsável pelo tratamento dos mesmos e os fins a que o tratamento se destina, bem como às informações que se destinam a assegurar que seja efetuado com equidade e transparência para com as pessoas singulares em causa, bem como a salvaguardar o seu direito a obter a confirmação e a comunicação dos dados pessoais que lhes dizem respeito que estão a ser tratados. As pessoas singulares a quem os dados dizem respeito deverão ser alertadas para os riscos, regras, garantias e direitos associados ao tratamento dos dados pessoais e para os meios de que dispõem para exercer os seus direitos relativamente a esse tratamento. Em especial, as finalidades específicas do tratamento dos dados pessoais deverão ser explícitas e legítimas e ser determinadas aquando da recolha dos dados pessoais. [...]

[540] (60) Os princípios do tratamento equitativo e transparente exigem que o titular dos dados seja informado da operação de tratamento de dados e das suas finalidades. O responsável pelo tratamento deverá fornecer ao titular as informações adicionais necessárias para assegurar um tratamento equitativo e transparente tendo em conta as circunstâncias e o contexto específicos em que os dados pessoais forem tratados. O titular dos dados deverá também ser informado da definição de perfis e das consequências que daí advêm. Sempre que os dados pessoais forem recolhidos junto do titular dos dados, este deverá ser também informado da eventual obrigatoriedade de fornecer os dados pessoais e das consequências de não os facultar. Essas informações podem ser fornecidas em combinação com ícones normalizados a fim de dar, de modo facilmente visível, inteligível e claramente legível uma útil perspectiva geral do tratamento previsto. Se forem apresentados por via eletrônica, os ícones deverão ser de leitura automática.

[541] (58) O princípio da transparência exige que qualquer informação destinada ao público ou ao titular dos dados seja concisa, de fácil acesso e compreensão, bem como formulada numa linguagem clara e simples, e que se recorra, adicionalmente, à visualização sempre que for adequado. Essas informações poderão ser fornecidas por via eletrônica, por exemplo num sítio web, quando se destinarem ao público. Isto é especialmente relevante em situações em que a proliferação de operadores e a complexidade tecnológica das práticas tornam difícil que o titular dos dados saiba e compreenda se, por quem e para que fins os seus dados pessoais estão a ser recolhidos, como no caso da publicidade por via eletrônica. 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.

Assim, se muitas vezes já é difícil compreender algoritmos mais simples, quando se trata de sistemas com inteligência artificial Oterllo chama a atenção para o fato de que, para os humanos, enormes conjuntos de centenas de regras são muito difíceis de inspecionar visualmente, sobremodo quando suas previsões são combinadas probabilisticamente de maneiras complexas[542]. Tornar os algoritmos compreensíveis é um desafio a ser enfrentado na busca por transparência, devendo ser um objetivo almejado desde o início do desenvolvimento do sistema.

Dessa feita, em que pese seja um importante instrumento para avaliar se determinado algoritmo promove a discriminação ou viola outras normas de proteção de dados, Kroll e colaboradores[543] apontam as limitações da transparência como remédio para os riscos que envolvem a mineração dos dados e os sistemas para tomadas de decisão.

Para os autores, muitas situações exigem o segredo dos elementos de uma política de decisão. Como exemplo, citam um algoritmo utilizado para procurar sinais de evasão fiscal nas declarações de imposto de renda a fim de afirmar que se o público sabe exatamente o que é considerado como indício de fraude, as pessoas podem ajustar seu comportamento e os sinais podem perder seu valor preditivo. Outras vezes, o segredo comercial pode mostrar-se incompatível com a transparência total. Se um sistema não foi projetado visando à avaliação futura, os testes de verificação de *software* muitas vezes não serão eficazes.

Ainda para Kroll e coautores, se o processo decisório envolver algum elemento de aleatoriedade, a transparência algorítmica pode não ser tão eficiente, já que, por *design*, o processo produz resultados imprevisíveis. O problema é que um algoritmo pode esconder uma randomização mal elaborada e uma suposta escolha aleatória, e esse fato continuar indetectável mesmo com a transparência, porque, em tese, se uma decisão depende de um valor selecionado aleatoriamente, qualquer resultado consistente com algum valor possível da escolha aleatória, não importa quão improvável, deve ser considerado válido, o que dificulta bastante a percepção, somente com transparência, da falha do sistema.

Os autores argumentam que os sistemas que são constantemente atualizados e modificados não podem ser completamente compreendidos por meio da transparência. Primeiro, porque como dependem da interação com os usuários, ainda que se conheça o código-fonte do algoritmo, isso não explica, por si só, o porquê de qualquer decisão específica

---

[542] OTTERLO, Martijn van. A Machine Learning View on Profiling. **Cognitive Artificial Intelligence,** Radboud University Nijmegen. Disponível em: http://www.martijnvanotterlo.nl/cpdp11-draftversion-ProjectedWorlds-MartijnVanOtterlo-2011.pdf. Acesso em: 12 out. 2020, p. 16.

[543] KROLL, Joshua A. et al. Accountable Algorithms. **University of Pensylvania Law Review,** v. 165, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2765268. Acesso em: 18 set. 2020, p. 23-25.

nem quão justo é o sistema com diferentes bases de usuários ou interações. Em segundo lugar, porque existe o risco de a regra decisória divulgada já ser obsoleta no momento em que é analisada. Os sistemas *online* que utilizam aprendizado de máquina atualizam suas regras de decisão após cada interação, o que significa que qualquer divulgação ficará obsoleta assim que for feita.

Apesar de tais limitações, a transparência é um instrumento fundamental na tutela dos dados pessoais, uma vez que lhes garante, de maneira compreensível, explicações e informações acerca de quais dados são coletados, para quais finalidades serão utilizados, quem processará tais dados, a que tipo de tratamento serão submetidos, com quem serão compartilhados, por quanto tempo serão armazenados e quais as consequências do fornecimento – ou não – dos dados pessoais.

De fato, implementar uma transparência total é praticamente impossível e até inviável numa economia em que muitos modelos de negócio dependem do segredo dos algoritmos que utilizam; entretanto, deve-se buscar algum grau de transparência, de modo que os titulares dos dados e as autoridades de controle recebam a maior quantidade de informação significativa possível, levando-se em conta os interesses de ambas as partes.

Tão ou até mais importante quanto a quantidade de informação deve ser a qualidade e a clareza da informação, haja vista que se o indivíduo leigo tiver acesso a uma série de fórmulas matemáticas e códigos de programação, este não será capaz de identificar se aquilo que ele vê viola seus direitos ou lhe causa prejuízo de qualquer natureza.

Autoridades de controle e profissionais de tecnologia da informação podem ser aptos a entender tais fórmulas e este conhecimento pode ser útil para identificar a conformidade dos algoritmos com as legislações de proteção de dados. Em nome da transparência, é necessário que os agentes de tratamento atentem para as peculiaridades dos diferentes grupos que receberão as informações.

No intento de potencializar a transparência algorítmica, bem como buscando minimizar potenciais danos provocados por sistemas computacionais, a *Association for Computing Machinery* – ACM[544] traçou alguns princípios a serem observados em cada fase do desenvolvimento e implantação dos algoritmos, a saber: a) conscientização, b) acesso e reparação, c) responsabilidade, d) explicabilidade, e) proveniência dos dados, f) auditabilidade, g) validação e testes.

---

[544] CONSELHO DA EUROPA. **Statement on Algorithmic Transparency and Accountability.** 12 jan. 2017. Disponível em: http://www.acm.org/binaries/content/assets/public-policy/2017_joint_statement_algorithms.pdf. Acesso em: 29 dez. 2020, p. 1-2.

O primeiro deles aponta para a necessidade de que todas as partes de alguma forma envolvidas pelo sistema, isto é, incluindo desenvolvedores e usuários, estejam cientes dos possíveis vieses que podem surgir na concepção, implementação e uso do algoritmo, bem como das possíveis consequências individuais e sociais que os preconceitos podem causar[545].

Faz-se necessária a adoção de mecanismos que permitam aos indivíduos questionar e solicitar reparação quando forem afetados injustamente por decisões algorítmicas. As instituições devem ser responsabilizadas pelas decisões tomadas por meio de sistemas computacionais. A esse respeito, a *Fairness, Accountability and Transparency in Machine Learning Organization* – FAT/ML indica a importância de os agentes de tratamento disponibilizarem vias alternativas de reparação das lesões individuais ou sociais causadas pela atividade, bem como designarem uma pessoa ou setor para o recebimento e resolução dessas demandas[546].

De igual forma, é preciso garantir a explicabilidade das decisões tomadas por processos algorítmicos, isto é, assegurar que determinado resultado de um processo decisório possa ser explicado de maneira compreensível, apresentando-se as justificativas que levaram o tratamento daqueles dados fornecidos àquela conclusão. Uma vez que cada indivíduo ou grupo tem objetivos e níveis de compreensão diferentes, pode ser necessária a personalização da explicação para diferentes categorias[547].

Mendes e Mattiuzzo distinguem a explicabilidade da transparência na medida em que entender o processo pelo qual se chegou a uma decisão (explicabilidade) não significa conhecer todos os passos seguidos para se alcançar tal resultado (transparência)[548]. Assim, por exemplo, saber as razões que levaram à negativa de um crédito não é o mesmo que conhecer todo o procedimento envolvido nessa decisão e, assim, verificar que estas explicações, aparentemente neutras, escondem alguma forma de discriminação algorítmica.

---

[545] CONSELHO DA EUROPA. **Statement on Algorithmic Transparency and Accountability.** 12 jan. 2017. Disponível em: http://www.acm.org/binaries/content/assets/public-policy/2017_joint_statement_algorithms.pdf. Acesso em: 29 dez. 2020, p. 2.

[546] DIAKOPOULOS, Nicholas. Principles for Accountable Algorithms and a Social Impact Statement for Allgorithms. **FAT/ML.** Disponível em: https://www.fatml.org/resources/principles-for-accountable-algorithms. Acesso em: 29 dez. 2020.

[547] PHILLIPS, Jonathon et al. **Four Principles of Explainable Artificial Intelligence**. Maryland: National Institute of Standards and Technology, ago. 2020. Disponível em: https://www.nist.gov/system/files/documents/2020/08/17/NIST%20Explainable%20AI%20Draft%20NISTIR8312%20%281%29.pdf. Acesso em: 29 dez. 2020.

[548] MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. **Revista Direito Público,** v. 16, n. 90, 2019, p. 56. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766/Schertel%20Mendes%3B%20Mattiuzzo%2C%202019. Acesso em: 18 set. 2020.

O princípio da proveniência dos dados exige que os desenvolvedores descrevam como os dados de treinamento foram coletados, bem como investiguem os potenciais preconceitos induzidos pelo processo de coleta de dados[549].

A FAT/ML adota um princípio semelhante, o princípio da precisão, segundo o qual as fontes de erro e a incerteza dos algoritmos precisam ser identificadas, registradas e organizadas para que as possíveis consequências possam ser compreendidas e os procedimentos de mitigação possam ser traçados e informados[550].

De acordo com o princípio da auditabilidade, modelos, algoritmos, dados e decisões devem ser registrados para que possam ser auditados por terceiros nos casos em que há suspeita de dano. Por último, o princípio da validação e teste exige que as instituições utilizem métodos rigorosos para validar seus modelos, os quais devem ser documentados, juntamente com seus resultados. Nessa esteira, os agentes de tratamento devem realizar, com frequência, testes para avaliar se o algoritmo gera discriminação. A ACM incentiva que as instituições tornem públicos os resultados destes testes[551].

Esses princípios propostos pela ACM são, com algumas variações, frequentemente apontados como formas de minimizar os riscos da mineração de dados e do uso de algoritmos para tomadas de decisão. Contudo, tais orientações não são capazes, sozinhas, de solucionar todos os problemas.

Faz-se necessário que os agentes de tratamento se comprometam a assegurar os direitos fundamentais dos indivíduos, aplicando métodos de prevenção de discriminação e outras ameaças em todas as fases do tratamento. Nas hipóteses de tratamento automatizado, devem ser aplicadas técnicas de prevenção desde o pré-processamento, buscando-se identificar e remover vieses discriminatórios contidos nos dados, passando pela construção de algoritmos justos e que respeitem os direitos dos titulares dos dados e pela análise do código com o objetivo de identificar e corrigir falhas, discriminação ou qualquer outro potencial dano ao titular dos dados, até o pós-processamento, fazendo testes constantes no sistema.

Nesse particular, Mendes e Mattiuzzo ressaltam a importância de que as equipes responsáveis pelos tratamentos de dados e desenvolvimento dos sistemas de processamento

---

[549] CONSELHO DA EUROPA. **Statement on Algorithmic Transparency and Accountability.** 12 jan. 2017. Disponível em: http://www.acm.org/binaries/content/assets/public-policy/2017_joint_statement_algorithms.pdf. Acesso em: 29 dez. 2020, p. 2

[550] DIAKOPOULOS, Nicholas. Principles for Accountable Algorithms and a Social Impact Statement for Allgorithms. **FAT/ML.** Disponível em: https://www.fatml.org/resources/principles-for-accountable-algorithms. Acesso em: 29 dez. 2020.

[551] CONSELHO DA EUROPA. **Statement on Algorithmic Transparency and Accountability.** 12 jan. 2017. Disponível em: http://www.acm.org/binaries/content/assets/public-policy/2017_joint_statement_algorithms.pdf. Acesso em: 29 dez. 2020, p. 2.

sejam treinadas para compreender os aspectos éticos e morais relacionados à tomada de decisão, bem como que sejam compostas por grupos diversificados, no intento de diminuir as chances de que vieses sociais sejam transpostos para os algoritmos[552].

A LGPD busca incentivar os agentes de tratamento a adotarem mecanismos de mitigação de riscos aos direitos dos indivíduos, o que inclui constante avaliação dos processos envolvidos no tratamento de dados com vistas a identificar e corrigir possíveis falhas e impactos negativos para o titular das informações.

Nesse sentido, em observância ao princípio da prevenção, o artigo 50, § 2º, da referida lei estimula a implementação de programa de governança em privacidade que "estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade", o que será levado em consideração quando da aplicação de eventuais sanções, caso se verifique que a mineração de dados e o *profiling* causaram prejuízo aos indivíduos, mesmo com a adoção de tais práticas.

Além disso, a autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais referente a suas operações de tratamento de dados, o qual deverá conter "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" (art. 38 e art. 5º, XVII). Contudo, o texto normativo sugere a ideia de que a formulação desse relatório não é obrigatória mesmo em caso de operações com elevados riscos aos direitos dos titulares envolvidos, dependendo, pois, da iniciativa da ANPD para requisitá-la[553].

Já o artigo 35º do RGPD prevê a obrigatoriedade da avaliação de impacto das operações de tratamento que impliquem elevado risco para os direitos e liberdades das pessoas singulares sempre que uma decisão que afete a esfera jurídica de um indivíduo for tomada com base na avaliação sistemática, completa e automatizada dos seus aspectos pessoais, incluindo a definição de perfis[554].

---

[552] MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. **Revista Direito Público,** v. 16, n. 90, 2019, p. 60-61. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766/Schertel%20Mendes%3B%20Mattiuzzo%2C%202019. Acesso em: 18 set. 2020.

[553] Art. 38º 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.

[554] Artigo 35° - Avaliação de impacto sobre a proteção de dados.

Compete à ANPD realizar ou determinar a realização de auditorias sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, inclusive para verificar aspectos discriminatórios em tratamento automatizado de dados pessoais (art. 55-J, XVI e art. 20, § 2º).

O RGPD não faz uma previsão explícita acerca da possibilidade de as autoridades de controle poderem auditar algoritmos de definição de perfis e tomadas de decisão, no entanto, uma vez que entre as suas atribuições estão fiscalizar a aplicação do regulamento e investigar o conteúdo das reclamações recebidas sobre a realização de determinado processamento de dados por uma organização, a realização de auditorias se encontra entre as funções das referidas autoridades.

Não há a imposição de uma obrigação, pela LGPD ou pelo RGPD, de os agentes de tratamento empreenderem auditorias periódicas para averiguar criticamente a conformidade dos processamentos que executam com as referidas legislações, identificando falhas ou lacunas na proteção de dados e relatando recomendações para remediá-las. As auditorias podem ser internas, quando efetivadas pelas próprias organizações, ou externas, quando realizadas por um terceiro independente.

Se os mecanismos legislativos acima apresentados não forem suficientes para impedir o tratamento discriminatório ou outros impactos negativos decorrentes da mineração de dados e do *profiling*, caberá a aplicação ao agente de tratamento das sanções administrativas e das regras de responsabilidade civil previstas tanto na lei brasileira como na europeia, o que levará em consideração o empenho ou não do mencionado agente em prevenir e mitigar tais danos.

No que se refere à ingerência externa à dimensão decisional da privacidade, a transparência e o direito à autodeterminação informativa também se fazem extremamente relevantes.

Isso porque, na sociedade da informação, não é mais a pessoa que escolhe qual matéria quer ler, ela recebe uma série de sugestões de notícias que, segundo seu perfil, podem te interessar; suas decisões políticas sofrem forte ingerência de *fake news*, bem como da

---

1. Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação.
[...]
3. A realização de uma avaliação de impacto sobre a proteção de dados a que se refere o nº 1 é obrigatória nomeadamente em caso de:
a) Avaliação sistemática e completa dos aspetos pessoais relacionados com 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; [...]

limitação de conteúdo provocada pelos filtros-bolha; os filmes e músicas que vê e ouve são selecionados por algoritmos, que por meio de sugestões acabam atraindo sua atenção; a necessidade por determinados produtos que consome foi criada pela publicidade comportamental que sabe exatamente o que é preciso para persuadi-la.

Estes algoritmos são educados pelo próprio indivíduo, já que, como visto, todo o comportamento do titular é monitorado *online* e é essa atividade que será utilizada para que o sistema computacional segmente anúncios, matérias e conteúdos que, de acordo com as suas atitudes, são consideradas de seu interesse.

Entretanto, frequentemente o indivíduo não tem conhecimento de que o seu comportamento ao utilizar serviços *online* determinam tal segmentação nem de como isso ocorre. Dessa forma, a transparência dos agentes de tratamento, explicando o porquê e apresentando quais os dados coletados influenciaram a seleção daquele conteúdo para o titular, é fundamental para que o indivíduo possa educar o algoritmo de maneira consciente.

Apesar disso, um tratamento transparente não é suficiente, tendo em vista que o titular pode passar a tolher sua atividade *online* para que determinada atitude não reflita na segmentação do que lhe é mostrado. A título ilustrativo, um usuário pode desejar ler determinada matéria, mas desistir por saber que, ao clicar naquele link, passará diversos dias recebendo vários conteúdos com alguma relação, muitas vezes distante, com a reportagem. Da mesma forma, pode deixar de seguir numa rede social o único comediante que lhe agrada, porque o fato de acompanhar as suas postagens faz com que boa parte dos vídeos que lhe são exibidos sejam de comédia.

Dessa feita, faz-se necessário que os agentes de tratamento disponibilizem meios pelos quais o indivíduo possa influir mais ativamente na seleção de conteúdo, permitindo que a pessoa exerça a sua autodeterminação informativa e selecione informações que ela não quer que sejam utilizadas na formação de seu perfil. Contudo, isso pode afetar o modelo de negócio das grandes companhias de tecnologia, o qual se baseia na publicidade comportamental.

Assim, conciliar a autodeterminação informativa e a economia digital é um grande desafio que se impõe na atualidade, não existindo respostas prontas sobre como fazê-lo. Contudo, os agentes de tratamento devem, pelo menos, fornecer algum grau de transparência aos indivíduos para que estes possam utilizar a *internet* de forma mais racional, reduzindo, ainda que um pouco, ingerências externas na sua privacidade decisional, bem como recebendo mais criticamente os anúncios e notícias que lhe são exibidos.

Nesse particular, a educação digital também adquire relevo para que as pessoas tenham ciência, ainda que em linhas gerais, de como as redes sociais e outros serviços *online* funcionam, de que existe publicidade comportamental, do que são filtros-bolha e de que seu comportamento na *internet* educa os algoritmos de seleção de conteúdo. Isso posto, capacita-se o titular para um uso consciente da tecnologia, bem como para um pensamento crítico concernente aos desafios que a sua liberdade de escolha encontra na sociedade da informação, exigindo, pois, seu esforço para ter acesso a outros assuntos e conhecer outros produtos.

À vista disso, a autoridade nacional em colaboração com o Ministério da Educação deve realizar ações educativas sobre estas temáticas, principalmente voltadas para as crianças e adolescentes, os quais, além de serem boa parte dos usuários das aplicações de *internet*, por estarem em desenvolvimento são mais suscetíveis à manipulação do capitalismo de vigilância.

Importa dizer que a mineração de dados e a definição de perfis não são os únicos processamentos de dados que podem violar os direitos dos titulares das informações, tampouco são as únicas hipóteses reguladas pela Lei Geral de Proteção de Dados Pessoais ou pelo regulamento europeu.

Essa subseção se limitou a investigar os perigos envolvidos na mineração de dados e no *profiling* em razão de, além de ser duas das principais formas de processamento de dados existentes na sociedade da informação, envolverem muitos riscos ao indivíduo, os quais, muitas vezes, passam despercebidos, máxime quando se trata de sistemas automatizados e a transparência não é garantida.

Entretanto, qualquer tratamento de dados que não observe os princípios e as disposições previstas em ambas as legislações, os quais foram analisados no capítulo anterior, tal como o processamento para finalidades distintas daquelas para as quais a informação foi coletada, ofendem o direito fundamental à proteção de dados pessoais do indivíduo, de modo que os agentes de tratamento deverão ser responsabilizados.

As próximas subseções examinarão a potencialidade lesiva dos tratamentos de dados que não oferecem segurança adequada. As chamadas violações de dados podem acarretar inúmeros danos aos titulares dos dados afetados e, por isso, tanto a Lei 13.709/2018 quanto o RGPD despendem especial atenção aos incidentes de segurança, regulando as obrigações preventivas dos agentes de tratamento, bem como dispondo acerca do comportamento que estes deverão adotar tão logo se identifique a ocorrência de uma violação. É a essas questões que se dedicam os subsequentes itens deste trabalho.

4.3 Segurança no tratamento de dados pessoais: consequências da violação de dados e disposições da Lei Geral de Proteção de Dados Pessoais

Entre 2012 e 2016, o Yahoo sofreu uma série de violações de dados. Entre elas, a violação de 2013 atingiu 3 bilhões de usuários; em 2014, a violação afetou mais de 500 milhões de contas. Segundo a empresa, nomes, endereços de *e-mail*, números de telefone, datas de nascimento e respostas para perguntas de segurança foram acessados por *hackers*, mas senhas e informações bancárias e de cartão de crédito não foram alcançadas pelo ataque. Apesar da gravidade do incidente, o Yahoo levou anos para divulgar a ocorrência das violações e para notificar os usuários afetados[555].

Em razão das violações, o Yahoo enfrentou ações coletivas que culminaram num acordo de US$ 117,5 milhões em um fundo de compensação destinado ao reembolso de alguns custos dos serviços *premium* ou de pequenas empresas do Yahoo; na compensação pelo tempo gasto em resposta às violações; em um mínimo de dois anos de monitoramento de crédito para usuários individuais; no pagamento ao usuário de custos resultantes da violação; e no pagamento em dinheiro de US$ 100 a usuários que provassem que já têm pelo menos 12 meses de monitoramento de crédito. O acordo alcançou usuários residentes nos Estados Unidos ou em Israel[556]. O valor da empresa foi reduzido em USL$ 350 milhões após todos os incidentes de segurança[557].

Em novembro de 2016[558], *hackers* conseguiram acessar a nuvem em que estavam armazenadas credencias de acesso ao aplicativo Uber e fizeram o *download* de 16 arquivos em que constavam registros com nomes, números de telefone, *e-mails* e o local de cadastro de 57 milhões de usuários em todo o mundo. Dados pessoais de 3,7 milhões de motoristas também foram expostos, com o vazamento de seus rendimentos semanais, resumos de viagem e, em alguns casos, números de carteira de habilitação.

---

[555] SOUZA, Ramon de. Altaba (ex-Yahoo) vai pagar multa de US$ 35 milhões por vazamento de dados. **Canaltech,** 25 abr. 2018. Disponível em: https://canaltech.com.br/juridico/altaba-ex-yahoo-vai-pagar-multa-de-us-35-milhoes-por-vazamento-de-dados-112588/#:~:text=de%20dados%20%2D%20Canaltech-,Altaba%20(ex%2DYahoo)%20vai%20pagar%20multa%20de%20US%24,milh%C3%B5es%20por%20vazamento%20de%20dados&text=Na%20ocasi%C3%A3o%2C%20criminosos%20cibern%C3%A9ticos%20de,tr%C3%AAs%20anos%20depois%2C%20em%202016. Acesso em: 7 jul. 2020.

[556] SZAFRAN, Vinicius. Yahoo começará a pagar indenizações por violações de dados. **Olhar Digital,** 5 fev. 2020. Disponível em: https://olhardigital.com.br/fique_seguro/noticia/yahoo-comecara-a-pagar-indenizacoes-por-violacoes-de-dados/96378. Acesso em: 9 jul. 2020.

[557] WAKKA, Wagner. Vazamento de dados custa em média R$ 1,24 milhão para empresas no Brasil. **Canaltech,** 11 set. 2018. Disponível em: https://canaltech.com.br/seguranca/vazamento-de-dados-custa-em-media-r-124-milhao-para-empresas-no-brasil-122304/. Acesso em: 7 jul. 2020.

[558] HERN, Alex. Uber fined £385,000 for data breach affecting millions of passengers. **The Guardian,** 27 nov. 2018. Disponível em: https://www.theguardian.com/technology/2018/nov/27/uber-fined-385000-for-data-breach-affecting-millions-of-passengers-hacked. Acesso em: 7 jul. 2020.

Além da falha de segurança que permitiu a violação, a *Uber* pagou US$ 100 aos *hackers* na tentativa de que o ataque não fosse divulgado. Ainda, a Uber não notificou nenhum dos titulares dos dados comprometidos acerca da violação. Somente 12 meses depois do incidente, a organização começou a monitorar as contas, buscando identificar possíveis fraudes.

Pela referida violação, a *Uber* dos EUA foi condenada, em setembro de 2018, a pagar US$ 148 milhões por não notificar os motoristas sobre o incidente. Já na Inglaterra, a empresa foi multada em £ 385.000. A empresa ainda foi multada em outros países.

Em 2017[559] foi lançado, no Brasil, o aplicativo E-Saúde, do Ministério da Sáude, o qual continha uma brecha de segurança que expôs, durante meses, as informações pessoais dos brasileiros, tais como o histórico médico de remédios retirados no Sistema Único de Saúde e as consultas agendadas nos postos de atenção básica.

Para o acesso a estas informações, o aplicativo exigia que fosse realizado um cadastro no qual eram informados, apenas, o número do CPF e a data de nascimento da pessoa a respeito da qual se queria tomar conhecimento dos dados disponibilizados, além de se cadastrar um endereço de *e-mail* qualquer, que poderia ser inexistente, e clicar num botão confirmando ser o titular da conta.

Desse modo, era possível realizar o cadastro de qualquer pessoa no aplicativo, sendo suficiente, para tanto, o conhecimento do número do CPF e da data de nascimento deste indivíduo, dados estes que são facilmente encontrados na *internet*. Feito o cadastro, o aplicativo mostrava o cartão SUS da pessoa e o registro de remédios na rede pública desde 2008, além da agenda com as próximas consultas.

Em 2017[560], o Hospital do Câncer de Barretos sofreu um incidente de segurança provocado por um *ransomware* que embaralhava e criptografava os dados dos computadores infectados, paralisando-os e impedindo o acesso a qualquer informação ali armazenada. Para que o acesso fosse restabelecido, os *hackers* solicitaram o pagamento de um resgate. Nesse caso, foi solicitado um resgate no valor de US$ 300 por máquina, o que totalizaria um custo de US$ 360 mil ao hospital, que não foi pago.

Em razão do ataque, cerca de 3 mil consultas e exames foram cancelados, 350 pacientes ficaram sem radioterapia e até mesmo quimioterapias foram interrompidas, uma vez

---

[559] FELITTI, Chico. Brecha em aplicativo do SUS expôs informações de saúde até de Temer. **Folha de São Paulo,** 26 jan. 2018. Disponível em: https://www1.folha.uol.com.br/cotidiano/2018/01/1953472-brecha-em-aplicativo-do-sus-expos-informacoes-de-saude-ate-de-temer.shtml. Acesso em: 20 jul. 2019.

[560] GUIMARÃES, Keila. Os crimes dos hackers que interrompem até quimioterapia em seqüestros virtuais de hospitais. **BBC News Brasil,** 10 ago. 2017. Disponível em: https://www.bbc.com/portuguese/brasil-40870377. Acesso em: 16 jun. 2020.

que, além de não poder utilizar as máquinas, o hospital também ficou sem acesso aos dados pessoais dos pacientes, como histórico médico e exames. Para contornar o problema, o hospital colheu amostras de sangue de alguns pacientes para os exames necessários antes da sessão de quimioterapia e as enviou, em caráter de emergência, a laboratórios externos. Após horas de atraso, algumas sessões de quimioterapia tiveram início. O problema só foi completamente solucionado seis dias depois.

Em maio de 2019[561], o *WhatsApp* confirmou uma vulnerabilidade no aplicativo de mensagens que vinha sendo explorada por um *malware* espião desenvolvido pela firma de segurança israelense NSO. A falha de segurança permitia que, ao receber uma chamada de voz pelo aplicativo – mesmo sem atendê-la –, o celular fosse infectado pelo *malware*, o qual, por sua vez, poderia vigiar as pessoas por meio do microfone e câmeras do *smartphone*, além de vazar arquivos pessoais.

Após uma investigação interna, o *WhatsApp* identificou até 1,4 mil pessoas espionadas. Além de civis, parcela significativa das vítimas é composta de autoridades governamentais e militares do alto escalão de pelo menos vinte governos. Também há, entre os espionados, jornalistas, advogados, diplomatas e ativistas pelos direitos humanos.

O *malware* espião foi criado pela desenvolvedora israelense NSO Group; esta alega que não deu início aos ataques, uma vez que apenas desenvolve *softwares*, bem como nega que tenha desenvolvido o referido vírus. A NSO afirma que somente comercializa produtos para governos com o objetivo de investigar criminosos. Em outubro de 2019, o WhatsApp entrou com uma ação judicial contra a NSO.

Em 2018[562], *hackers* realizaram um ataque cibernético ao *site* da *British Airways* e tiveram acesso aos dados pessoais dos clientes que realizaram operações no *site* entre 21 de agosto e 5 de setembro daquele ano. Entre as informações vazadas estavam o nome, o endereço de *e-mail* e as informações do cartão de crédito (o número do cartão de crédito, a data de validade e o código de três dígitos [CVV] no verso do cartão de crédito). A organização se comprometeu a compensar qualquer dificuldade financeira que as pessoas cujos dados foram expostos possam ter sofrido em virtude do ato ilícito.

---

[561] ALVES, Paulo. Sete fatos sobre a falha no WhatsApp que foi usada para espionar governos. **TechTudo,** 6 nov. 2019. Disponível em: https://www.techtudo.com.br/noticias/2019/11/sete-fatos-sobre-a-falha-no-whatsapp-que-foi-usada-para-espionar-governos.ghtml. Acesso em: 16 jun. 2020.

[562] READ, Simon. British Airways boss apologises for ‘malicious’ data breach. **BBC News,** 7 set. 2018. Disponível em: https://www.bbc.com/news/uk-england-london-45440850. Acesso em: 20 jul. 2019.

Em dezembro de 2018[563], o Banco Inter assinou um acordo em que se comprometeu a pagar R$ 1,5 milhão após o Ministério Público do Distrito Federal acusá-lo de ter deixado vazar os dados de 19,9 mil correntistas, entre os quais 13.207 tiveram informações bancárias, como número da conta, senhas, endereço, CPF e telefones, indevidamente expostas. O Ministério Público denominou o acordo de "reparação de danos morais coletivos".

Em 2019[564], *hackers* tiveram acesso a fotografias de pessoas e placas de veículos que entraram e saíram dos Estados Unidos por meio de um ataque malicioso realizado na rede de um subcontratado federal. Segundo informações da Alfândega e Proteção de Fronteira do respectivo país – CBP, menos de 100 mil pessoas foram afetadas. As fotografias são de um programa de reconhecimento facial da agência que busca intensificar a vigilância na fronteira.

Ainda conforme a CBP, a violação ocorreu porque o subcontratado teria violado os protocolos obrigatórios de segurança e privacidade descritos em seu contrato e, sem a autorização do órgão, transferido cópias das imagens das placas e dos viajantes para seu sistema interno, o qual, posteriormente, foi comprometido pela ação dos *hackers*.

Em maio do mesmo ano[565], o Instituto Defesa Coletiva ajuizou uma ação na vara cível de Belo Horizonte contra o *Facebook* em virtude de vazamento de dados de milhões de usuários da rede social, requerendo a condenação da empresa ao pagamento de R$ 150 milhões por danos morais coletivos. De acordo com o Instituto, somente a partir de 2018 foram registrados pelo menos três episódios de vazamento de dados, inclusive por invasão de *hackers*, tendo o último atingido dados sensíveis dos usuários, expondo senhas e detalhes sobre a movimentação dos indivíduos na rede social.

Em novembro de 2019[566], pesquisadores de segurança descobriram que um *kit* de desenvolvimento do *software* One Audience permitia que desenvolvedores de terceiros tivessem acesso não autorizado a dados pessoais de centenas de usuários do *Facebook* e do Twitter que utilizavam as contas das redes sociais para acessar aplicativos *Android* baixados na loja da *Globo Play*, como o *Giant Square* e o *Photofy*. As redes sociais afirmaram ser

---

563 LUIZ, Gabriel. Banco Inter fecha acordo para pagar R$ 1,5 milhão após vazamento de dados de clientes. **G1 Notícias,** 19 dez. 2018. Disponível em: https://g1.globo.com/df/distrito-federal/noticia/2018/12/19/banco-inter-fecha-acordo-para-pagar-r-15-milhao-de-indenizacao-apos-vazamento-de-dados-de-clientes.ghtml. Acesso em: 20 jul. 2019.

564 NOGUEIRA, Luiz. Hackers roubam imagens do sistema da agência de fronteira dos EUA. **Olhar Digital,** 11 jun. 2019. Disponível em: https://olhardigital.com.br/fique_seguro/noticia/dados-de-usuarios-que-deixaram-os-eua-sao-roubados/86737. Acesso em: 2 jul. 2020.

565 INSTITUTO pede que *Facebook* seja condenado em R$ 150 milhões por vazamento de dados. **Migalhas,** 14 maio 2019. Disponível em: https://www.migalhas.com.br/Quentes/17,MI302322,71043-Instituto+pede+que+Facebook+seja+condenado+em+R+150+milhoes+por. Acesso em: 20 jul. 2019.

566 VIEIRA, Nathan. *Facebook* e *Twitter* anunciam casos de acesso indevido a dados de usuários. **Canaltech,** 25 nov. 2019. Disponível em: https://canaltech.com.br/seguranca/facebook-e-twitter-anunciam-casos-de-acesso-indevido-a-dados-de-usuarios-156195/. Acesso em: 22 jun. 2020.

possível que uma pessoa tivesse assumido o controle da conta do Twitter de outro usuário por meio da vulnerabilidade, entretanto, não havia evidências de que isso tivesse acontecido.

Em junho de 2020[567], o *DDoSecrets*, um grupo autoproclamado "coletivo da transparência" que publica dados secretos, divulgou milhares de arquivos sensíveis de mais de duzentos departamentos policiais dos Estados Unidos, incluindo relatórios da polícia e do FBI. Segundo afirmado pelo grupo *hacker* em uma rede social, os quase 270 *gigabytes* de dados, apelidados de "*BlueLeaks*", referem-se a mais de dez anos de dados dos referidos departamentos. A maior parte das informações vazadas não é de dados pessoais, mas os documentos também incluem nomes, endereços de *e-mail*, números de telefone, além de documentos PDF, imagens e um grande número de arquivos de texto, vídeo, CSV e ZIP.

Também em 2020[568], uma falha no sistema e-SUS-Notifica expôs os dados pessoais de cerca de 243 milhões de brasileiros – alcançando registros até mesmo de pessoas falecidas –, entre os quais se incluem número do CPF, nome completo e endereço de telefone. Anteriormente, uma falha de segurança nesse mesmo sistema já havia exposto informações sensíveis de 16 milhões de pacientes que tinham sido diagnosticados com Covid-19. A violação foi possível porque as credenciais de acesso – que estavam codificadas, mas por um método facilmente decodificável – constavam num trecho do código do *site* que podia ser visualizado por qualquer pessoa por meio da função "inspecionar elemento," existente em qualquer navegador.

Todas essas situações são violações de dados pessoais, que serão estudadas a seguir.

4.3.1 Incidentes de segurança: consequências para titulares dos dados e agentes de tratamento

Conforme o Guia de Tratamento de Incidentes de Segurança Informática elaborado pelo Instituto Nacional de Padrões e Tecnologia do Departamento de Comércio dos EUA, em um sistema ou em uma rede observa-se uma série de ocorrências, como o recebimento da solicitação de uma página de *web* pelo servidor, o envio de um *e-mail* por um usuário ou o

---

[567] O'DONNELL, Lindsey. Report: 'BlueLeaks' Exposes Sensitive Data From Police Departments. **Threat Post,** 22 jun. 2020. Disponível em: https://threatpost.com/report-blueleaks-exposes-sensitive-data-from-police-departments/156806/. Acesso em: 29 dez. 2020.

[568] PRIVACY TECH. **Mais de 200 milhões de brasileiros têm dados pessoais expostos em nova falha de segurança do Ministério da Saúde.** 8 dez. 2020. Disponível em: https://privacytech.com.br/destaque/mais-de-200-milhoes-de-brasileiros-tem-dados-pessoais-expostos-em-nova-falha-de-seguranca-do-ministerio-da-saude.,381645.jhtml. Acesso em: 2 jan. 2021.

bloqueio de uma tentativa de conexão por um *firewall.* Essas ocorrências são chamadas de eventos[569].

Alguns desses eventos provocam uma consequência negativa e, por isso, são denominados de eventos adversos, tais como falhas no sistema, uso não autorizado de privilégios do sistema, acesso não autorizado a dados confidenciais ou a execução de um *malware* que destrói dados.

Esses eventos podem ser causados por diversos fatores, a exemplo de desastres naturais, falhas de energia e causas outras relacionadas à segurança da computação. Nesse sentido, o Guia define um incidente de segurança de computador como uma violação ou ameaça iminente de violação das políticas de segurança de computadores[570], a exemplo de tentativas ou ganho de acesso não autorizado a sistemas ou dados, desrespeito à política de segurança ou à política de uso aceitável de uma empresa ou provedor de acesso e ataques com o intuito de enviar grandes volumes de solicitações de conexão a um servidor *web*, provocando falhas na conexão[571].

Caso esse incidente atinja informações pessoais, ele será considerado uma violação de dados pessoais. Logo, nem todo incidente de segurança é uma violação de dados pessoais, mas toda violação de dados é um incidente de segurança[572].

Uma violação de dados pessoais consiste numa falha de segurança que pode levar a destruição, perda, alteração, divulgação ou acesso não autorizado a tais dados[573], o que pode causar uma série de danos aos titulares desses dados, tanto de ordem material quanto imaterial, como a perda de controle sobre os seus dados pessoais, a limitação dos seus

---

[569] CICHONSKI, Paul et al. **Computer Security Incident Handling Guide –** Recommendations of the National Institute of Standards and Technology. Maryland: National Institute of Standards and Technology, ago. 2012. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf. Acesso em: 10 jun. 2020, p. 6.

[570] CICHONSKI, Paul et al. **Computer Security Incident Handling Guide –** Recommendations of the National Institute of Standards and Technology. Maryland: National Institute of Standards and Technology, ago. 2012. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf. Acesso em: 10 jun. 2020, p. 6

[571] CERT.BR. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **FAQ:** Perguntas Frequentes ao CERT.br. Disponível em: https://www.cert.br/docs/certbr-faq.html#6. Acesso em: 30 maio 2020.

[572] Conforme revelado pela pesquisa de riscos de segurança de TI da empresa global de segurança cibernética Kaspersky, 40% dos incidentes de segurança que atingem dados corporativos envolvem dados pessoais**. (**KASPERSKY. **40% of data breaches affect customer information –** how can businesses reduce the potential damage. 14 abr. 2020. Disponível em: https://www.kaspersky.com/about/press-releases/2020_40-of-data-breaches-affect-customer-information. Acesso em: 5 jun. 2020).

[573] Artigo 4º, alínea 12, do Regulamento Geral de Proteção de Dados da União Europeia. (UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016**. Relativo à proteção de dados pessoais 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 Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679#d1e1554-1-1. Acesso em: 28 jun. 2020).

direitos, a discriminação, o roubo ou a usurpação da identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação, a perda de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem econômica ou social significativa das pessoas[574]. A violação pode ser acidental ou ilícita.

A Lei Geral de Proteção de Dados Pessoais não utiliza a expressão "violação de dados", ao contrário do que faz o RGDP, entretanto, em seu artigo 46, prevê que os agentes de tratamento devem adotar as medidas de segurança, tanto técnicas quanto administrativas, necessárias à proteção dos 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". Logo, verifica-se que o referido artigo trata do mesmo conceito.

A destruição de dados pessoais não significa apenas que as informações deixaram de existir. A perda de qualquer utilidade dos dados para o agente de tratamento, seja pela alteração de formato, seja por qualquer outro meio, também se qualifica como destruição[575].

Já quando se fala em perda de dados pessoais, tem-se que o dado ainda existe – ou o agente de tratamento não sabe precisar se o dado foi destruído ou não –, mas o responsável pelo tratamento não tem mais a posse, o controle ou o acesso a essas informações, a exemplo de quando um dispositivo que contém uma cópia do banco de dados é perdido ou roubado, ou quando a única cópia desse banco de dados tiver sido cifrada por um *software* de sequestro ou pelo próprio agente de tratamento, que, no entanto, não tem mais acesso à chave para proceder à desencriptação[576].

O acesso ou a divulgação não autorizada de dados pessoais pode se dar não somente por pessoas de fora da organização. Se são estabelecidos níveis de acesso aos dados ou se o acesso a determinadas informações pessoais é restrito a determinados funcionários, medidas estas adequadas para assegurar os direitos dos titulares, mas algum funcionário, por algum

---

[574] Conforme Considerando 85, do Regulamento Geral de Proteção de Dados da União Europeia. (UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016**. Relativo à proteção de dados pessoais 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 Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679#d1e1554-1-1. Acesso em: 28 jun. 2020).

[575] UNIÃO EUROPEIA. **Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679.** 20 ago. 2018. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052. Acesso em: 5 jun. 2020, p. 7.

[576] UNIÃO EUROPEIA. **Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679.** 20 ago. 2018. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052. Acesso em: 5 jun. 2020, p. 7.

erro interno ou em decorrência de um ato ilícito, recebe ou acede a dados cujo acesso não lhe era autorizado, isso também é considerado uma violação de dados pessoais[577].

As violações de dados pessoais podem ser a) de confidencialidade, quando existe uma divulgação ou acesso acidental ou não autorizado a dados pessoais; b) de integridade, que diz respeito a alterações acidentais ou não autorizadas dos dados pessoais; ou ainda, c) de disponibilidade, que ocorre quando há uma perda de acesso ou a destruição acidental ou não autorizada de dados pessoais, ainda que de forma temporária, haja vista que essa indisponibilidade, mesmo de forma não permanente, pode trazer graves prejuízos aos titulares. Importa dizer, ainda, que uma violação pode envolver mais de uma dessas categorias simultaneamente[578].

Não é difícil imaginar os danos que a exposição indevida de dados pessoais pode gerar. Se os dados referentes ao cartão de crédito de um usuário de determinado *site* de compras são expostos, por exemplo, qualquer pessoa pode utilizar esses dados para realizar compras em outros *sites* na rede mundial de computadores. Por sua vez, se os dados de um laboratório médico vazam, revelando as informações sensíveis dos pacientes, como os dados de que determinadas pessoas são portadoras do vírus HIV, é patente que essa situação pode causar efeitos nefastos na vida dos indivíduos que tiveram seus dados expostos.

Infelizmente, são cada vez mais recorrentes os casos envolvendo violação aos dados pessoais. O Relatório de Investigações de Violação de Dados da Verizon Business 2020 (2020 DBIR), que é uma referência mundial quanto à pesquisas de incidentes de segurança, analisou, em sua 13ª edição, 32.002 incidentes de segurança de 81 colaboradores globais de 16 setores de negócios, entre os quais foram confirmadas 3.950 violações de dados.

O relatório identificou que a causa predominante das violações é diferente em cada setor de negócios, contudo, numa perspectiva geral, 70% das violações analisadas foram causadas por atores externos, como organizações criminosas que provocaram 55% de tais incidentes. No que diz respeito às táticas utilizadas, o relatório apontou que 45% das violações apresentaram *hackers* e o erro humano foi evento causal em 22% das violações.

Assim, verifica-se que o erro humano representa uma porcentagem significativa entre as causas dos incidentes de segurança. Segundo o Relatório do Estado da Cibersegurança

---

[577] UNIÃO EUROPEIA. **Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679.** 20 ago. 2018. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052. Acesso em: 5 jun. 2020, p. 7.

[578] UNIÃO EUROPEIA. **Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679.** 20 ago. 2018. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052. Acesso em: 5 jun. 2020, p. 8.

2019, da *Kaspersky*, essa porcentagem chegou a 52% entre os incidentes de segurança sofridos pelas 282 organizações industriais em todo o mundo que participaram da pesquisa[579].

Como pontos em comum entre os incidentes, o DBIR identificou que 86% das violações tiveram motivação financeira e não fins de espionagem ou diversão, bem como 37% das violações roubaram ou utilizaram credenciais por serem fracas ou terem sido expostas, 22% utilizaram *phishing* e 17% das violações envolveram *malware*.

As violações de dados não atingem somente grandes organizações. Das violações analisadas pelo mencionado relatório, 28% delas envolveram pequenos empresários.

Já uma pesquisa realizada pela empresa global de segurança cibernética *Kasperky* mostrou que, em 2019, o número de violações de dados que atingiram pequenas organizações cresceu seis pontos percentuais, de 30% (2018) para 36% (2019)[580].

Outro ponto importante trazido pelo 2020 DBIR foi que 43% das violações atingiram aplicativos da *web*, o que representa um aumento de 100% em relação ao relatório de 2019. Esse crescimento se deve ao fato de que as organizações cada vez mais utilizam a nuvem. Com o fortalecimento do trabalho remoto durante a pandemia de Covid-19, as medidas de segurança relacionadas à nuvem tornam-se ainda mais importantes.

À medida que o trabalho remoto cresce com a pandemia global, a segurança ponta a ponta da nuvem para o *laptop* dos funcionários torna-se fundamental. Além da preocupação com a nuvem, o uso de dispositivos pessoais, como *notebooks* e celulares, no desempenho das atividades laborais também se torna um desafio.

Um estudo da *Oxford Economics* contratado pela *Samsung*, feito com 500 líderes seniores de Tecnologia da Informação, apontou que, embora 80% dos participantes da pesquisa tenham dito que seus funcionários não podem desempenhar efetivamente o seu trabalho sem um telefone celular e 75% tenham respondido que os dispositivos móveis integram seus processos de negócios, 31% dos empresários não fornecem telefones móveis a nenhum de seus empregados, 52% fornecem tais aparelhos a determinados grupos de

---

[579] KASPERSKY. **Man-made disaster:** half of cybersecurity incidents in industrial networks happen due to employee errors. 20 ago. 2019. Disponível em: https://www.kaspersky.com/about/press-releases/2019_man-made-disaster-half-of-cybersecurity-incidents-in-industrial-networks-happen-due-to-employee-errors. Acesso em: 5 jun. 2020.

[580] KASPERSKY. **Beign little make you invincible?** The third of small companies that suffered a data breach wouldn't agree. 10 set. 2019. Disponível em: https://www.kaspersky.com/about/press-releases/2019_third-of-small-companies-suffered-a-data-breach. Acesso em: 5 jun. 2020.

funcionários e apenas 17% colocam telefones corporativos à disposição de todos os trabalhadores[581].

Nesse cenário, é comum que, enquanto a segurança dos servidores e estações de trabalho corporativo seja provida por especialistas em tecnologia da informação, a segurança dos dispositivos pessoais dos funcionários fique a cargo dos próprios empregados. Esses dispositivos são mais propensos a perdas, roubos e incidentes de segurança[582].

Em junho de 2018, a *Michigan Medicine* relatou a possibilidade de vazamento de dados de cerca de 870 pacientes em razão do roubo do *laptop* pessoal de um funcionário no qual haviam sido armazenados alguns dados pessoais para fins de pesquisa[583].

De igual forma, em 2017, um incidente provavelmente iniciado por um ataque cibernético no computador pessoal de um funcionário da *Bithumb*, uma das maiores bolsas de *bitcoin* do mundo, expôs os dados pessoais de 32 mil usuários do serviço, muitos dos quais tiveram suas carteiras digitais esvaziadas. Somente um usuário chegou a perder, em segundos, o equivalente a 10 milhões de won (US$ 8.600)[584].

Embora os modelos de negócios se tornem cada vez mais dependentes da tecnologia e dos dados pessoais, muitas vezes as organizações deixam de adotar as medidas de segurança adequadas para prevenir os incidentes de segurança. Além disso, em que pesem as técnicas de segurança da informação estarem em constante atualização, os ataques criminosos tornam-se cada vez mais sofisticados e adaptados a cada setor e aos momentos por que os empresários estão passando. Esses fatores contribuem para o crescente número de incidentes de segurança.

Nesse sentido, *hackers* já desenvolveram até mesmo uma espécie de "chupa-cabra virtual", que consiste na inserção de códigos maliciosos em metadados de arquivos de imagens enviados por meio de um *plugin* disponibilizado pela plataforma *WordPress.* Este permite a utilização de códigos abertos para a criação de uma loja virtual. Assim, as lojas

---

581 MCCARTY, Eric. The State of Enterprise Mobility in 2018: Five key trends. **INSIGHTS,** 06 jun. 2018. Disponível em: https://insights.samsung.com/2018/06/06/the-state-of-enterprise-mobility-in-2018-five-key-trends/. Acesso em: 5 jun. 2020.

582 GRUSTNIY, Leonid. Personal devices at work. **KASPERSKY Daily,** 29 jul. 2019. Disponível em: https://www.kaspersky.com/blog/personal-devices-at-work/27769/. Acesso em: 5 jun. 2020.

583 MASSON, Mary. Michigan Medicine notifies patients of health information data breach. **Michigan Medicine,** University of Michigan, 25 jun. 2018. Disponível em: https://www.uofmhealth.org/news/archive/201806/michigan-medicine-notifies-patients-health-information-data. Acesso em: 18 jun. 2020.

584 LEYDEN, John. Breached Bitcoin Bithumb bosses blame bod's BYOD. **The Register,** 6 jul. 2017. Disponível em: https://www.theregister.com/2017/07/06/bithumb_hack/. Acesso em: 2 jul. 2020.

virtuais, sem saber, executariam esses arquivos, permitindo que os *hackers* coletassem dados como nome do consumidor, endereço, além de informações de cartões de crédito[585].

Ainda, há ataques direcionados a determinados setores, a exemplo da campanha de *malware Revenge Hotels*, que é destinada à hotelaria. Em tal campanha, vários grupos de *hackers* participam com a intenção de infectar as estações de trabalho das vítimas com *trojans* de acesso remoto. Por meio de *e-mails* bastante convincentes, em virtude de os remetentes serem muito semelhantes aos de organizações legítimas, bem como em razão de o conteúdo dos *e-mails* ser pormenorizado, os empresários do ramo da hotelaria acabam instalando ficheiros maliciosos anexados a documentos em formatos Word, PDF ou Excel nomeados como "cópias de documentos legais", "informação sobre o motivo da reserva" ou nomes de arquivos afins[586].

Uma vez que o *malware* permite o acesso remoto, torna possível o acesso a dados armazenados nos computadores, a *spoolers* de impressora e capturas de tela. Como é prática comum copiar os dados do cartão de crédito dos clientes para o caso de eventual cobrança, inclusive de base de dados de agências de viagens, esses dados também podem ser coletados pelos invasores. A campanha já atingiu hotéis da Europa, América Latina e Ásia.

O número de incidentes de segurança de determinados setores aumentou consideravelmente durante a pandemia da Covid-19. Nessa senda, a equipe de resposta a ameaças de crimes cibernéticos da Interpol detectou um aumento significativo no número de tentativas de ataques cibernéticos contra hospitais e organizações importantes no combate ao coronavírus. Tais eventos intentam bloquear os sistemas dessas organizações, impedindo-as de acessar dados pessoais, arquivos e sistemas vitais até que um resgate seja pago[587]. O número de ataques cibernéticos a plataformas educacionais chegou a triplicar durante a pandemia[588].

Nem mesmo estações de trabalho que utilizam a biometria estão livres de violações de dados. Segundo o relatório "Ameaças para sistemas de armazenamento e processamento de

---

[585] JUNQUEIRA, Daniel. Hackers criam golpe que lembra um 'chupa-cabra' virtual. **Olhar Digital,** 26 jun. 2020. Disponível em: https://olhardigital.com.br/fique_seguro/noticia/hackers-criam-golpe-que-lembra-um-chupa-cabra-virtual/102716. Acesso em: 19 set. 2020.

[586] VEDOR, Luis. Portugal é um dos países mais afetados pela campanha de malware Revenge Hotels. **PC Guia,** jan. 2020. Disponível em: https://www.pcguia.pt/2020/01/portugal-afectados-campanha-malware-revengehotels/. Acesso em: 5 jun. 2020.

[587] INTERPOL. **Cybercriminals targeting critical healthcare institutions with ransomware.** 4 abr. 2020Disponível em: https://www.interpol.int/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware. Acesso em: 5 jun. 2020.

[588] KASPERSKY. **DDoS during the coronavirus pandemic: number of attacks on educational and administrationaal web resources tripled in Q1 2020**. 6 maio 2020. Disponível em: https://www.kaspersky.com/about/press-releases/2020_ddos-during-the-coronavirus-pandemic-number-of-attacks-on-educational-and-administrational-web-resources-tripled-in-q1-2020. Acesso em: 3 jul. 2020.

dados biométricos", da *Kaspersky*, entre os computadores que possuem produtos da empresa instalados, um em cada três servidores ou estações de trabalho utilizados para coletar, processar e armazenar dados biométricos, como impressões digitais, geometria das mãos, voz e íris, enfrentou pelo menos uma tentativa de infecção por *malware* em 2019, o que reforça a necessidade de os empresários adotarem medidas adequadas de segurança[589].

Esses incidentes de segurança não ocorrem sem consequências a eles associadas.

Uma equipe de pesquisa da empresa *Digital Shadows Photon* apontou no relatório *From Exposure to Takeover*[590] que 100 mil violações de dados ocorridas em dois anos renderam um aumento de 300% nas credenciais roubadas. Atualmente já são 15 bilhões de nomes de usuários e senhas para uma variedade de serviços de *internet* que estão à venda em fóruns clandestinos da *dark web*.

Estas credenciais custam, em média, US$ 15,43. As contas de bancos e instituições financeiras são as mais valiosas, vendidas pelo preço médio de US$ 70,91 cada uma; acessos a contas para programas antivírus são oferecidos pelo preço intermediário de US$ 21,67; todos os outros tipos de conta são vendidos por menos de US$ 10. Há, ainda, contas que são cedidas gratuitamente.

Apesar de a maioria dos nomes de usuário e senhas ofertados serem pessoais, credenciais para acesso aos principais sistemas de organizações também são vendidas, por meio de leilões, a um preço médio de US$ 3.139; os lances chegam a US$ 140.000. A pesquisa também encontrou anúncios referentes a dois milhões de endereços de *e-mails* de organizações voltados ao envio de faturas para os consumidores.

O relatório também indicou que o mercado de aluguel de identidade tem crescido consideravelmente. Por menos de US$ 10 é possível alugar, por determinado período, credenciais. Esse mercado também coleta dados das impressões digitais do navegador da vítima, isto é, *cookies*, endereços IP, fusos horários, entre outras informações, o que torna mais fácil o ataque cibernético.

Nessa mesma esteira, pesquisadores da *Kaspersky* indicam que, na *dark web*, é possível comprar a vida digital completa de alguém por menos de US$ 50, o que inclui dados de contas de redes sociais roubadas, detalhes bancários, acesso remoto a servidores ou *desktops* e até dados de serviços populares como *Uber*, *Netflix* e *Spotify*, além de *sites* de

---

589 KASPERSKY. **One-in-three computers processing biometry face attempts to steal data or remote control.** 2 dez. 2019. Disponível em: https://www.kaspersky.com/about/press-releases/2019_one-in-three-computers-processing-biometry-face-attempts-to-steal-data-or-remote-control. Acesso em: 3 jul. 2020.

590 DIGITAL SHADOWS. **From Exposure to Takeover –** The 15 billion stolen credentials allowing account takeovers. Disponível em: https://resources.digitalshadows.com/whitepapers-and-reports/from-exposure-to-takeover. Acesso em: 28 jun. 2020.

jogos, aplicativos de namoro e *sites* pornográficos que podem armazenar informações de cartões de crédito[591].

As organizações que sofreram um incidente de segurança também sofrem consequências negativas. Um estudo conduzido pelo Instituto Ponemon, patrocinado pela IBM Security[592], analisou os custos de violação de dados relatados por 507 organizações em 16 regiões geográficas e 17 setores, e concluiu que uma violação de dados custa, em média, US$ 3,92 milhões. Para o cálculo, a pesquisa considerou diversas despesas diretas e indiretas incorridas pela organização, tais como o envolvimento de especialistas forenses, a adoção de medidas técnicas, a perda de valor da marca, a perda de clientes, as investigações internas e a notificação da violação.

Os custos variam nos diferentes países e indústrias em que ocorrem os incidentes de segurança. No Brasil, por exemplo, uma violação de dados custa US$ 1,35 milhão em média, já nos Estados Unidos o custo é de US$ 8,19 milhões. Organizações do setor público costumam ter um custo menor, uma vez que não experimentam uma perda significativa de clientes como resultado de um incidente, bem como empresários sujeitos a regulações mais rigorosas tiveram um maior custo de violação de dados.

Tratando-se de pequenas e médias empresas, o prejuízo causado por uma violação de dados corresponde a cerca de US$ 2,5 milhões. Já incidentes que atinjam mais de 1 milhão de registros chegam a custar US$ 42 milhões às organizações; se ultrapassarem 50 milhões de registros, o custo chega a US$ 388 milhões.

Embora 67% dos custos ocorram no primeiro ano, o agente de tratamento continua sentindo os custos nos anos seguintes ao do incidente de segurança. O maior responsável por tais custos é a perda de confiança do cliente, o que faz com que a organização empresária perca vários negócios. Segundo o estudo, isso representa US$ 1,42 milhão do custo médio total.

A pesquisa verificou que alguns fatores amplificam o custo de uma violação. A complexidade do sistema de tecnologia da informação foi responsável por um aumento de US$ 290.000 em tal custo, e as violações de dados originadas por ataques maliciosos custaram às empresas cerca de US$ 1 milhão a mais que os incidentes de segurança cuja causa foi acidental, como falha no sistema ou erro humano.

---

[591] KASPERSKY. **Your digital identity could be on sale for less than $50 – new Dark Web research from Kaspersky Lab shows.** 5 nov. 2018. Disponível em: https://www.kaspersky.com/about/press-releases/2018_digital-identity-for-less-than-50-dollars. Acesso em: 3 jul. 2020.

[592] IBM SECURITY. **Cost of a Data Breach Report 2019.** Disponível em: https://www.ibm.com/downloads/cas/ZBZLY7KL. Acesso em: 5 jun. 2020.

O relatório apontou, ainda, o tempo médio para identificar e conter uma violação. Quanto mais rápida uma violação for contida, menos custará à organização: um ciclo de vida de violação inferior a 200 dias custa US$ 1,2 milhão a menos que um ciclo de vida superior.

No que diz respeito aos fatores que reduzem o custo de uma violação de dados, as organizações estudadas que tinham uma equipe de resposta a incidentes e realizavam testes extensivos de resposta com exercícios ou simulações economizaram mais de US$ 1,2 milhão, haja vista que essas atitudes diminuem consideravelmente o ciclo de vida de um incidente. De igual forma, o uso extensivo de criptografia reduz o custo de uma violação de dados em uma média de US$ 360 mil. O custo experimentado por organizações que implantaram soluções automatizadas de segurança, incluindo análise e automação de resposta a incidentes, também foi significativamente menor do que os custos sofridos por empresas que necessitam da intervenção humana direta.

A partir de todos os números e dados apresentados, verifica-se que uma violação de dados é bastante lesiva tanto aos titulares das informações quanto aos agentes de tratamento, razão pela qual as organizações devem procurar evitar a ocorrência de incidentes de segurança e, uma vez detectada uma violação, devem empreender todas as medidas necessárias a solucioná-la o mais rapidamente possível.

A esse respeito, tanto a LGPD quanto o regulamento europeu de proteção de dados exigem uma atitude preventiva dos agentes de tratamento, assim como traçam os procedimentos mínimos a serem adotados quando verificada uma violação de dados.

4.3.2 Respostas à violação de dados conforme a Lei Geral de Proteção de Dados Pessoais

Consoante examinado anteriormente, um incidente de segurança pode acarretar vários prejuízos aos titulares das informações. A adequada tutela dos dados pessoais deve ser construída a partir de uma perspectiva preventiva de tais incidentes, de modo que qualquer tratamento de dados deve se pautar pela lógica da *privacy by design*.

Em seu artigo 46, a LGPD prevê a obrigatoriedade, desde a concepção do produto ou serviço, de os agentes de tratamento adotarem 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. Para isso, a autoridade nacional poderá dispor sobre padrões

técnicos mínimos de segurança, considerando a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia[593].

Também o RGPD exige que o responsável pelo tratamento e o subcontratante apliquem medidas técnicas e organizativas aptas a assegurar um nível de segurança adequado ao risco, o que poderá incluir, sempre que adequado, a pseudonimização, a cifragem dos dados pessoais e um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas a fim de garantir a segurança do tratamento[594].

Entretanto, se mesmo com todas as medidas preventivas adotadas vier a ocorrer um incidente de segurança que possa acarretar risco ou dano relevante aos titulares, ambas as legislações exigem que o controlador ou o responsável pelo tratamento deverá comunicá-lo, em prazo razoável, à autoridade nacional. Esta irá verificar a gravidade do incidente e determinar ao referido agente de tratamento, se necessário, a adoção de providências para reverter ou mitigar os efeitos da violação, bem como para dar ampla divulgação do fato, de modo a permitir que os titulares tomem conhecimento do ocorrido, caso essa medida seja importante para a salvaguarda de seus direitos[595].

---

[593] 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.
Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

[594] Artigo 32° Segurança do tratamento
1. Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado:
a) A pseudonimização e a cifragem dos dados pessoais;
b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;
c) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico;
d) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento. [...]

[595] Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
§ 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;

Ressalva-se que, apesar de a LGPD utilizar a expressão “ampla divulgação do fato em meios de comunicação”, para uma efetiva notificação dos titulares é importante que lhes sejam direcionadas notificações individuais.

O regulamento europeu, ainda, faz expressa previsão da obrigação do subcontratante notificar qualquer violação por este identificada ao responsável pelo tratamento que o contratou[596]. Já a lei brasileira não faz previsão semelhante para a figura do operador, contudo, seja por boa-fé ou previsão contratual, este deve comunicar ao controlador tão logo detecte um incidente de segurança.

Quanto ao termo para a notificação do incidente de segurança à autoridade nacional, a LGPD não fixa o prazo no qual esta deverá ser feita, limitando-se a dizer que a comunicação deverá ocorrer em prazo razoável e que os motivos da demora deverão ser informados no caso de a comunicação não ter sido imediata. Caberá, então, à autoridade nacional definir qual o período de tempo máximo que o controlador poderá levar para notificá-la.

Por sua vez, o RGPD dispõe que a autoridade de controle deverá ser notificada em até 72 horas após o responsável pelo tratamento tomar conhecimento do incidente de segurança. Se a notificação não for feita no referido prazo, o responsável deverá justificar o atraso.

Se o incidente de segurança puder acarretar risco ou lesão relevante aos titulares, isto é, sempre que a violação for suscetível de lhes causar danos físicos, materiais ou imateriais, especialmente se o incidente envolver dados sensíveis, os indivíduos afetados também devem ser informados. Deve-se levar em consideração, ainda, a capacidade de se inferir conhecimento a partir dessas informações, máxime quando combinadas com outros dados.

Essa notificação é importante para que cada titular possa tomar as providências a ele disponíveis e necessárias para proteger a sua privacidade, tal como alterar a sua senha divulgada ou cancelar o seu cartão de crédito exposto. A LGPD não admite que haja uma

---

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 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.

[596] Artigo 33° Notificação de uma violação de dados pessoais à autoridade de controlo
1. Em caso de violação de dados pessoais, o responsável pelo tratamento notifica desse facto a autoridade de controlo competente nos termos do artigo 55°, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. Se a notificação à autoridade de controlo não for transmitida no prazo de 72 horas, é acompanhada dos motivos do atraso.
2. O subcontratante notifica o responsável pelo tratamento sem demora injustificada após ter conhecimento de uma violação de dados pessoais [...].

violação de dados potencialmente lesiva e o controlador omita tal fato, como costumava ocorrer, no intento de não sofrer os impactos negativos advindos da divulgação do incidente.

A adequada tutela da privacidade do indivíduo exige uma conduta transparente dos agentes de tratamento. A esse respeito, o RGPD, em seu artigo 34, nº 2, estabelece que a comunicação ao titular dos dados deverá ocorrer em linguagem clara e simples. A lei brasileira não faz idêntica previsão, no entanto, a partir de uma interpretação sistemática dela, é possível inferir que a compreensibilidade da notificação também é uma exigência da LGPD.

A comunicação deve conter, ainda, as indicações sobre os riscos decorrentes da violação e o que o titular poderá fazer para se proteger de eventuais consequências. No que diz respeito ao prazo para notificação, nem o regulamento europeu nem a lei a brasileira fixam um período de tempo para que esta ocorra: a LGPD apenas diz que a comunicação deverá ocorrer em prazo razoável, ao passo que o RGPD utiliza a expressão "sem demora injustificada".

No que concerne à forma de comunicação, o Grupo de Trabalho do Artigo 29 recomendou que os responsáveis pelo tratamento escolham um meio ou combinem vários métodos de comunicação, de modo a maximizar a possibilidade de todas as pessoas afetadas serem notificadas, o que pode incluir o envio direito de mensagens, notificações em *sites*, comunicações postais e divulgação na mídia. Para ser eficaz, importa que a notificação não fique confinada a um único comunicado ou a um único meio[597].

A LGPD não prevê exceções à obrigação de notificar os titulares dos dados quando verificados potenciais riscos a eles. O regulamento europeu, em seu artigo 34º, nº 3, estabelece que tal comunicação não será exigida se: a) o responsável pelo tratamento tiver aplicado medidas de proteção adequadas a evitar que, em caso de violação, os dados sejam acessados por pessoas não autorizadas, como a cifragem; b) o responsável tiver tomado medidas subsequentes que assegurem que o elevado risco para os direitos e liberdades dos titulares dos dados envolvidos na violação já não é suscetível de se concretizar; ou c) implicar um esforço desproporcionado, situação em que deverá ser feita uma comunicação pública ou tomada uma medida semelhante, por meio da qual os titulares dos dados serão informados de forma igualmente eficaz.

Ressalte-se que as comunicações à autoridade de controle e aos titulares dos dados pessoais serão feitas pela figura do encarregado, quando este existir, já que esta é a pessoa

[597] UNIÃO EUROPEIA. **Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679.** 20 ago. 2018. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052. Acesso em: 5 jun. 2020, p. 22.

indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados[598].

Em seu artigo 33, nº 5, o RGPD estabelece que o responsável pelo tratamento deverá documentar quaisquer violações de dados pessoais, seus respectivos efeitos e a medida de reparação adotada, independentemente de o incidente precisar ou não ter sido notificado à autoridade de controle[599]. Não há idêntica disposição na lei brasileira.

Concomitantemente à notificação, o controlador deverá agir para conter e corrigir a violação. No intuito de aumentar o comprometimento dos agentes de tratamento com a implantação das medidas adequadas à garantia da segurança dos dados, a LGPD os incentiva a formularem regras de boas práticas e de governança que estabeleçam as normas de segurança, os padrões técnicos e os mecanismos internos de supervisão e de mitigação de riscos.

O controlador poderá implementar programa de governança em privacidade, o qual deverá ser constantemente atualizado com base no monitoramento contínuo e em avaliações periódicas de impactos e riscos à privacidade, contando com planos de resposta a incidentes e remediação dos riscos e danos[600].

É de extrema importância que os agentes de tratamento tracem um plano de resposta a incidentes, estabelecendo uma política de gestão de tais violações, inclusive construindo um time de profissionais especializado no referido plano. Para ser eficaz, faz-se necessário que o plano de resposta a incidentes seja regularmente testado.

Consoante a norma ISO/IEC 27035-1:2016, da *International Organization for Standardization*, sobre gestão de incidentes de segurança, tal plano deve ser estruturado com

---

[598] Artigo 5º, VIII, da LGPD.

[599] Artigo 33° Notificação de uma violação de dados pessoais à autoridade de controlo
[...] 5. O responsável pelo tratamento documenta quaisquer violações de dados pessoais, compreendendo os factos relacionados com as mesmas, os respetivos efeitos e a medida de reparação adotada. Essa documentação deve permitir à autoridade de controlo verificar o cumprimento do disposto no presente artigo.

[600] Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, 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. [...]
§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do *caput* do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá: [...]
I - implementar programa de governança em privacidade que, no mínimo:
d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade; [...]
g) conte com planos de resposta a incidentes e remediação; e
h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

providências necessárias para: a) detectar, relatar e avaliar incidentes de segurança da informação; b) responder a incidentes de segurança da informação, o que inclui medidas apropriadas para prevenir, reduzir e reparar os impactos; c) relatar vulnerabilidades de segurança da informação, para que possam ser avaliadas e tratadas de forma adequada; e d) aprender com incidentes e vulnerabilidades de segurança da informação, instituir controles preventivos e fazer melhorias na abordagem geral do gerenciamento de incidentes de segurança da informação[601].

O plano de resposta a incidentes de segurança deve conter processos que possibilitem a rápida detecção e interrupção da violação, avaliem os perigos para os indivíduos e determinem se é necessário notificar a autoridade de controle competente e os titulares afetados. Os relatórios de impacto à proteção dos dados pessoais desempenham importante papel na avaliação dos riscos.

Um bom plano de resposta a incidentes é de substancial importância tanto para os titulares quanto para os agentes de tratamento, pois limitam os danos aos indivíduos afetados, bem como reduzem o tempo e os custos de identificação e a solução da violação, o que, por conseguinte, gera menos impactos negativos a ambas as partes.

Por fim, a ocorrência de um incidente de segurança e a forma como os agentes de tratamento lidaram com a mencionada violação, inclusive se deixaram de notificá-la à autoridade nacional e aos titulares dos dados, quando exigido, poderão acarretar sanções civis e administrativas, conforme será visto no capítulo a seguir.

---

[601] INTERNATIONAL STANDARD. **Information technology – Security techniques – Information security incident management –** Part 1: principles of incident management. 1 nov. 2016. Disponível em: https://www.sis.se/api/document/preview/921093/. Acesso em: 2 nov. 2020, p. 5.

5 PERSPECTIVAS PARA O DIREITO À PRIVACIDADE NO BRASIL COM A EDIÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Nos capítulos anteriores, investigaram-se as principais disposições da Lei Geral de Proteção de Dados Pessoais. Nesta seção, buscar-se-á responder se a referida Lei será capaz de tutelar, adequadamente, a privacidade dos indivíduos na sociedade da informação, apontando-se quais as principais repercussões que esperadas para os próximos anos de vigência da LGPD.

Nessa senda, após o estudo dos principais instrumentos de *enforcement* previstos pela legislação, será feito um mapeamento das principais diferenças e semelhanças entre a Lei 13.709/2018 e o Regulamento Geral de Proteção de Dados da União Europeia, bem como será feita uma breve análise dos impactos provocados pelo RGPD com vistas a se construir subsídios, a partir da experiência estrangeira, para a análise da (in) efetividade da LGPD.

5.1 Sanções administrativas na Lei Geral de Proteção de Dados Pessoais

Na busca por efetividade, a Lei Geral de Proteção de Dados Pessoais prevê dois mecanismos distintos, mas complementares: as sanções administrativas e a responsabilidade civil. A seguir, explanar-se-á sobre o primeiro deles.

Inicialmente, cumpre dizer que não são apenas violações de dados que geram a aplicação de sanções administrativas, mas qualquer infração às disposições da LGPD.

A esse respeito, o artigo 52 da LGPD estabelece que os agentes de tratamento de dados que infringirem as normas previstas na referida Lei ficam sujeitos à aplicação, pela autoridade nacional, de forma gradativa, isolada ou cumulativa, de uma série de sanções administrativas, a saber:

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

> VIII - (VETADO);
> IX - (VETADO)
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Em que pese a aplicação da multa pecuniária seja a mais comentada, são nove as sanções que podem ser aplicadas aos agentes infratores, as quais podem ir da advertência até a proibição do exercício de atividades relacionadas a tratamento de dados. Estas outras penalidades têm o potencial de serem bem mais gravosas aos agentes de tratamento que a multa, haja vista que, se ficar impedido de utilizar seu banco de dados ou de realizar determinado processamento de dados, o desempenho da própria atividade-fim do ente pode ser obstado.

Imagine que o funcionamento do banco de dados do Instituto Nacional de Segurança Social seja temporariamente suspenso em razão de uma infração à LGPD, certamente a concessão de diversos benefícios será prejudicada. Do mesmo modo, um *site* de reservas de acomodações que pratique *geopricing* e sofra, como sanção, a suspensão da atividade de tratamento que permite a exibição das acomodações disponíveis e seus respectivos preços, não terá mais qualquer funcionalidade enquanto perdurar a penalidade, o que, além de poder desvalorizar irreparavelmente a imagem do agente de tratamento, também atingirá seus parceiros, máxime os que, não sendo tão conhecidos, beneficiam-se da exibição proporcionada pelo *site*.

Estes exemplos demonstram o potencial gravoso das sanções previstas na LGPD. Foi por esta razão que as três últimas penalidades – as quais constavam, na redação original, nos incisos VII, VIII e IX – foram vetadas pelo presidente da República:

> Razões dos vetos
> "As sanções administrativas de suspensão ou proibição do funcionamento/exercício da atividade relacionada ao tratamento de dados podem gerar insegurança aos responsáveis por essas informações, bem como impossibilitar a utilização e tratamento de bancos de dados essenciais a diversas atividades, a exemplo das aproveitadas pelas instituições financeiras, dentre outras, podendo acarretar prejuízo à estabilidade do sistema financeiro nacional."

Posteriormente, essas penalidades foram reincluídas pela Lei nº 13.853/2019 e, mais uma vez, vetadas pelo presidente da República, contudo, o veto foi derrubado pelo Congresso

Nacional. A reinclusão de tais sanções foi medida importante, já que os agentes de tratamento levarão em consideração o potencial prejuízo delas decorrente, o que pode servir de estímulo à adoção de medidas de segurança adequadas. Além disso, tais penalidades somente poderão ser impostas se, para o mesmo caso concreto, já tiver sido aplicada ao menos uma das outras sanções previstas pelo mesmo dispositivo legal.[602]

Cumpre dizer que a decisão acerca de qual será a sanção aplicada não ficará ao arbítrio da autoridade nacional, já que dependerá de prévio procedimento administrativo que possibilite a oportunidade da ampla defesa, bem como observará as peculiaridades do caso concreto, a gravidade e a natureza das infrações e dos direitos pessoais afetados, a boa-fé do infrator, a condição econômica e a vantagem auferida ou pretendida pelo infrator, a reincidência e o grau dos danos causados.

Ademais, a autoridade nacional também deverá se atentar à cooperação do infrator, se este adotou reiteradamente mecanismos e procedimentos internos capazes de minimizar o dano, se adotou política de boas práticas e governança e se empregou medidas corretivas tão logo identificou a infração ou violação de dados. Por fim, a ANPD deverá fazer um juízo de proporcionalidade entre a gravidade da falta e a intensidade da sanção[603].

Há, ainda, a possibilidade de não ser imposta penalidade administrativa, quando os vazamentos ou acessos não autorizados forem individuais e houver acordo entre o controlador e o titular dos dados[604].

No que diz respeito à aplicação da multa, o artigo 53, da LGPD, estabelece que a autoridade nacional deverá definir, de maneira objetiva e em regulamento próprio sobre

---

[602] Art. 52. [...]§ 6º As sanções previstas nos incisos X, XI e XII do caput deste artigo serão aplicadas:
I - somente após já ter sido imposta ao menos 1 (uma) das sanções de que tratam os incisos II, III, IV, V e VI do caput deste artigo para o mesmo caso concreto [...]

[603] Art. 52 [...]§ 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:
I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
II - a boa-fé do infrator;
III - a vantagem auferida ou pretendida pelo infrator;
IV - a condição econômica do infrator;
V - a reincidência;
VI - o grau do dano;
VII - a cooperação do infrator;
VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
IX - a adoção de política de boas práticas e governança;
X - a pronta adoção de medidas corretivas; e
XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

[604] Art. 52. [...] § 7º Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo.

sanções administrativas, as metodologias que orientarão o cálculo do valor-base, incluindo a fundamentação detalhada de todos os seus elementos, bem como as circunstâncias e as condições para a adoção de multa simples ou diária[605]. A agenda regulatória da autoridade nacional prevê a elaboração desse regulamento ainda no primeiro semestre de 2021[606].

O valor da multa diária, que deverá ser fundamentado pela autoridade nacional, deverá observar a gravidade da falta e a extensão do dano causado (art. 54) e será destinado ao Fundo de Defesa de Direitos Difusos criado pela Lei nº 7.347/85 – Lei da Ação Civil Pública, e regulamentado pela Lei n.º 9.008/95[607], o qual é vinculado ao Ministério da Justiça e Segurança Pública e à Secretaria Nacional do Consumidor, devendo ser destinado à recomposição dos danos causados[608].

De igual modo, o Regulamento Geral de Proteção de Dados da União Europeia prevê que as autoridades de controle poderão aplicar, isolada ou cumulativamente, as seguintes sanções administrativas no caso de violação às suas disposições: a) advertência e repreensões; b) limitação temporária ou definitiva ao tratamento de dados; c) proibição de tratamento de dados; e d) multa (Arts. 58.° e 83.°).

A aplicação de multa será de até 20 000 000 EUR ou, no caso de uma empresa, até 4% do seu volume de negócios anual, quando a infração disser respeito à violação das normas relacionadas aos princípios, às condições de consentimento, às bases legais de tratamento, aos direitos dos titulares, ao não cumprimento de ordem de limitação de tratamento de dados e outras ordens da autoridade de controle e às transferências internacionais.

Já quando a infração disser respeito à violação das normas referentes ao tratamento de dados de criança e demais disposições do Regulamento que não geram aplicação da

---

[605] Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa. (Vigência)
§ 1º As metodologias a que se refere o caput deste artigo devem ser previamente publicadas, para ciência dos agentes de tratamento, e devem apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, que deverão conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos nesta Lei.
§ 2º O regulamento de sanções e metodologias correspondentes deve estabelecer as circunstâncias e as condições para a adoção de multa simples ou diária.

[606] BRASIL. Autoridade Nacional de Proteção de Dados. **Portaria nº 11, de 27 de janeiro de 2021.** Torna pública a agenda regulatória para o biênio 2021-2022. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313. Acesso em: 26 maio 2021.

[607] § 5º O produto da arrecadação das multas aplicadas pela ANPD, inscritas ou não em dívida ativa, será destinado ao Fundo de Defesa de Direitos Difusos de que tratam o art. 13 da Lei nº 7.347, de 24 de julho de 1985, e a Lei nº 9.008, de 21 de março de 1995. (Incluído pela Lei nº 13.853, de 2019)

[608] BRASIL. Ministério da Justiça e Segurança Pública. **O que é o Fundo de Defesa de Direitos Difusos – FDD.** Disponível em: https://www.justica.gov.br/seus-direitos/consumidor/direitos-difusos/institucional. Acesso em: 03 mar. 2021.

penalidade de multa mais grave, o montante da multa poderá chegar a 10 000 000 EUR ou, no caso de uma empresa, até 2% do seu volume de negócios anual.

Ademais, os Estados-membros poderão estabelecer outras sanções, penais ou administrativas, as quais deverão ser efetivas, proporcionas, dissuassivas e poderão, inclusive, prever a privação dos lucros auferidos em virtude da violação ao Regulamento (art. 84.°).

Por fim, cumpre dizer que, enquanto a Lei Geral de Proteção de Dados Pessoais está em vigor desde setembro de 2020, a Lei nº 14.010/2020 – Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) definiu que os dispositivos que tratam das sanções administrativas somente poderão ser aplicáveis a partir de 1º de agosto de 2021.

Esse adiamento da vigência das sanções administrativas foi fruto das diversas tentativas de prorrogação da *vacatio legis* da LGPD, máxime durante a pandemia, a exemplo do artigo 4º da MP/959/2020, que adiava a entrada em vigor da mencionada Lei para maio de 2021, mas que, posteriormente, foi considerado prejudicado pelo Senado Federal, de modo que a Lei 13.709/2018 passou a ser aplicável desde 18 de setembro de 2020, data da publicação da Lei 14.058/2020, oriunda do Projeto de Lei de Conversão da MP /959.

Frise-se que, inicialmente, a LGPD já contava com uma *vacatio legis* de 18 meses e, em momento ulterior, foi alterada pela lei 13.853/2019, a qual ampliou tal vacância para 24 meses. Apesar disso, uma pesquisa do ICTS Global Services[609], realizada com 296 organizações empresárias de diferentes portes indicou que, até setembro de 2020, isto é, posteriormente a entrada em vigor da LGPD, apenas 24% apresentavam um nível satisfatório de adequação à referida lei, sendo que 1/3 destas entidades entraram em conformidade entre abril e setembro do referido ano. Isso significa que, mesmo com uma *vacatio legis* extensa em comparação às demais legislações, os agentes de tratamento brasileiros deixaram para se adaptar às normas de proteção aos dados pessoais no último momento.

Este fato, juntamente com as diversas tentativas de alargamento da vacância da LGPD, demonstra que o país ainda tem muito a caminhar na construção de uma cultura de privacidade. Felizmente, em que pese a vigência das sanções administrativas tenha sido postergada, a mencionada lei também busca prevenir e compensar danos derivados do tratamento indevido de dados pessoais por meio de outro mecanismo, o qual será estudado na próxima subseção, qual seja, a responsabilização civil.

---

[609] LAW Innovation. **ICTS Protiviti:** 82% das empresas ainda estão despreparadas para cumprir a LGPD. 03 dez. 2020. Disponível em: https://lawinnovation.com.br/icts-protiviti-82-das-empresas-ainda-estao-despreparadas-para-cumprir-a-lgpd/. Acesso em: 24 abr. 2021.

5.2 Responsabilidade Civil na Lei Geral de Proteção de Dados Pessoais

A Lei Geral de Proteção de Dados Pessoais dispõe, em seu artigo 42, que o agente de tratamento que "causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo".

Do referido dispositivo, destaca-se a pluralidade de danos que podem ensejar a reparação civil, inclusive havendo a possibilidade de se responsabilizar os agentes de tratamento por danos coletivos, que são aqueles que atingem interesses que pertencem a toda uma coletividade, sendo indivisíveis entre os titulares. Como exemplo, Schreiber cita a situação hipotética em que dados são tratados não para a finalidade informada para a qual foram coletados, mas para o direcionamento de *fake news* com o objetivo de interferir no resultado eleitoral, o que viola os direitos supraindividuais à informação adequadada e à participação de um processo democrático transparente[610].

Nesse contexto, o § 3º, do mesmo artigo, prescreve que as ações de reparação por estes danos coletivos podem ser exercidas coletivamente em juízo, pelos legitimados, como o Ministério Público e Organizações não Governamentais, a exemplo do Instituto Brasileiro de Defesa do Consumidor, que recentemente venceu uma ação movida em face da concessionária responsável pela linha 4-Amarela do Metrô de São Paulo por coleta de dados sem o consentimento dos usuários por meio de um sistema de câmeras de vigilância[611].

Tal previsão é de extrema relevância, vez que, em muitas situações, a defesa coletiva será a forma mais apropriada de se tutelar o direito à proteção de dados pessoais, mesmo quando for possível identificar os ofendidos, já que estes podem ser em tamanho número que ações individuais assoberbariam o Judiciário. Ademais, uma ação coletiva alcança condenações em montantes significativamente maiores que as ações individuais, por conseguinte, causa maior impacto financeiro aos agentes de tratamento, o que pode compeli-los a se conformarem à LGPD.

Outrossim, o artigo 44, da LGPD, estabelece que será considerado irregular o tratamento de dados que deixar de observar a legislação ou que não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais a) o modo

---

[610] SCHREIBER, Anderson. Responsabilidade civil na Lei Geral de Proteção de Dados Pessoais. *In:* DONEDA, Danilo et al (Coords). **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021, p. 336.

[611] SÃO PAULO. Tribunal de Justiça do Estado de São Paulo. **Ação Civil Pública Cível nº 1090663-42.2018.8.26.0100.** Requerente: Idec – Instituto Brasileiro de Defesa do Consumidor, Requerido: Concessionária da Linha 4 do Metro de São Paulo S.a. (Via Quatro). Juíza de Direito: Patrícia Martins Conceição. 37ª Vara Cível, Foro Central Cível, Comarca de São Paulo. DJE: 07 maio 2021. Disponível em: https://www.conjur.com.br/dl/viaquatro-indenizar-implantar-sistema.pdf. Acesso em: 26 maio 2021.

pelo qual é realizado; b) o resultado e os riscos que razoavelmente dele se esperam; e c) as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado. Prevê, ainda, em seu parágrafo primeiro, que será responsabilizado o agente de tratamento que, ao deixar de adotar medidas de segurança, der causa a danos decorrentes de incidentes.

Como excludentes de responsabilidade, a referida Lei prescreve que os agentes de tratamento só não serão responsabilizados quando provarem que não realizaram o tratamento de dados pessoais que lhes é atribuído ou que não houve violação à legislação de proteção de dados ou, ainda, que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Todas estas disposições da LGPD têm provocado muito debate doutrinário acerca do regime de responsabilidade civil por esta previsto.

Nesse sentido, há autores que defendem que a Lei 13.709/2018 adotou a responsabilidade civil subjetiva. Os principais argumentos dessa corrente se concentram a) nas alterações pelas quais passaram as versões anteriores do Projeto de Lei que deu origem à LGPD, pois a primeira versão expressamente dispunha que o tratamento de dados pessoais era uma atividade de risco e a segunda preceituava uma responsabilidade independente de culpa, ao passo que, depois disso, foram retiradas tais expressões[612]; b) a Lei 13.709/2018 estabelece um *standard* de conduta, de modo que, para se responsabilizar o agente de tratamento, dever-se-ia analisar se este agiu em conformidade com o padrão estabelecido; e c) o artigo 43, I, prescreve que o agente não será responsabilizado se demonstrar que não violou a legislação de proteção de dados pessoais, de modo que a responsabilidade civil perquiriria a conduta culposa do agente, a qual, por sua vez, se fundaria no descumprimento da legislação[613].

Registre-se que as normas de responsabilidade civil previstas no Regulamento Geral de Proteção de Dados da União Europeia[614] são bastante similares às disposições da LGPG,

---

[612] BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. **Civilistica.com**, a. 9, n. 3, 2020, p. 1-23. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/662/506. Acesso em: 26 maio 2021, p. 5.

[613] Nesse sentido: GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau. Término do Tratamento de Dados. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro.** São Paulo: Thomson Reuters Brasil, 2019, p. 235.

[614] Artigo 82.° Direito de indenização e responsabilidade

1. Qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do presente regulamento tem direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos.

2. Qualquer responsável pelo tratamento que esteja envolvido no tratamento é responsável pelos danos causados por um tratamento que viole o presente regulamento. O subcontratante é responsável pelos danos causados pelo tratamento apenas se não tiver cumprido as obrigações decorrentes do presente regulamento dirigidas especificamente aos subcontratantes ou se não tiver seguido as instruções lícitas do responsável pelo tratamento.

tendo sido defendido, na Europa, que tal regramento filiou-se ao modelo de responsabilidade subjetiva[615].

Lado outro, há uma corrente para a qual o regime adotado pela LGPD é o da responsabilidade objetiva, vez que, para estes autores, qualquer tratamento de dados é uma atividade intrinsecamente de risco. Dessa feita, a mencionada Lei, defendem, criou um modelo de proteção de dados que se baseia na ideia de que, na sociedade da informação, não existem dados irrelevantes, tendo em vista que qualquer processamento de informações pessoais pode influenciar na representação da pessoa na sociedade, afetando a sua personalidade e, por conseguinte, com potencial de violar os seus direitos fundamentais[616].

Ademais, não raramente os danos resultantes da atividade de tratamento de dados são quantitativamente elevados, já que atingem um número indeterminado de pessoas, por vezes alcançando toda a coletividade, bem como são qualitativamente graves, pois violam direitos de natureza personalíssima, o que, segundo os defensores deste entendimento, já justificaria um regime de responsabilidade civil objetivo, a exemplo da tutela do meio ambiente e do direito do consumidor[617].

Há, ainda, outra corrente doutrinária, a qual entende que a Lei Geral de Proteção de Dados dispôs dois regimes de responsabilidade civil, o subjetivo e o objetivo, os quais convivem na referida legislação.

Nessa esteira, Schreiber[618] argumenta que a LGPD traria hipóteses em que a responsabilidade do agente de tratamento se funda na inobservância de um dever jurídico, a

---

3. O responsável pelo tratamento ou o subcontratante fica isento de responsabilidade nos termos do n.° 2, se provar que não é de modo algum responsável pelo evento que deu origem aos danos.
4. Quando mais do que um responsável pelo tratamento ou subcontratante, ou um responsável pelo tratamento e um subcontratante, estejam envolvidos no mesmo tratamento e sejam, nos termos dos n.º 2 e 3, responsáveis por eventuais danos causados pelo tratamento, cada responsável pelo tratamento ou subcontratante é responsável pela totalidade dos danos, a fim de assegurar a efetiva indemnização do titular dos dados [...]. (UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016**. Relativo à proteção de dados pessoais 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 Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679#d1e1554-1-1. Acesso em: 28 jun. 2020).

[615] SCHREIBER, Anderson. Responsabilidade civil na Lei Geral de Proteção de Dados Pessoais. *In:* DONEDA, Danilo et al (Coords). **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021, p. 324.

[616] MENDES, Laura Schertel; DONEDA, Danilo. Comentário à Nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. **Revista dos Tribunal Online,** Thomson Reuters, 2018, p. 22. Disponível em: https://www.academia.edu/42740879/Coment%C3%A1rio_%C3%A0_nova_Lei_de_Prote%C3%A7%C3%A3o_de_Dados_lei_13.709_2018_o_novo_paradigma_da_prote%C3%A7%C3%A3o_de_dados_no_brasil?auto=download. Acesso em: 26 maio 2021.

[617] MULHOLLAND, Caitlin. Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018). *In:* MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (Coords.). **Responsabilidade Civil e Novas Tecnologias.** São Paulo: Editora Foco, 2020, p. 121.

[618] SCHREIBER, Anderson. Responsabilidade civil na Lei Geral de Proteção de Dados Pessoais. *In:* DONEDA, Danilo et al (Coords). **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021, p. 323-329.

saber: a) a previsão do artigo 42 de que o controlador ou o operador é obrigado a reparar o dano que causar em razão de uma atividade de tratamento "em violação à legislação de proteção de dados pessoais"[619]; e b) o parágrafo único do artigo 44, que preceitua que o controlador e o operador serão responsabilizados pelos danos decorrentes da violação da segurança dos dados, provocados pelo comportamento do agente de "deixar de adotar as medidas de segurança previstas no art. 46 desta Lei"[620]. Assim, a não adoção dessas medidas seria uma situação que, por si só, atrairia a responsabilização pelos danos causados.

Dessa forma, em tais situações, a Lei 13.709/2018 estabeleceria aos agentes de tratamento um dever de observarem os dispositivos da legislação de proteção de dados, bem como de adotarem as medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de incidentes de segurança ou qualquer forma de tratamento inadequado ou ilícito. Ao deixarem de cumprir com estas obrigações, por conseguinte, controlador e operador incorreriam em culpa, pelo que deveriam responder na ocorrência de danos.

Entretanto, continua o autor, a LGPD ainda prescreve mais uma hipótese de responsabilização dos agentes, a qual se encontra nos incisos do artigo 44 da Lei e que ensejaria a adoção do regime de responsabilidade civil objetiva. Isso porque as situações dispostas nestes incisos seriam suscetíveis de causarem lesões aos titulares, vez que o tratamento a que seus dados foram submetidos não forneceram a segurança esperada pelo titular.

Com efeito, os incisos do artigo 44 foram construídos de forma muito semelhante às hipóteses de responsabilidade civil objetiva por defeito do serviço previsto no artigo 14, § 1°, do Código de Defesa do Consumidor, conforme quadro abaixo:

Quadro 2 – Comparativo entre os artigos 44 da LGPD e 14 do CDC

LGPD	CDC
Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam;	Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos. § 1° O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar,

[619] 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.

[620] Art. 44. [...] Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado. Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.	levando-se em consideração as circunstâncias relevantes, entre as quais: I - o modo de seu fornecimento; II - o resultado e os riscos que razoavelmente dele se esperam; III - a época em que foi fornecido.

Fonte: Elaborado pela autora.

Dessa feita, pela construção análoga com o CDC e pelo risco provocado pelo tratamento de dados que não oferece a segurança adequada, o que é reforçado pelo inciso II, do artigo 44, as situações acima seriam hipóteses de responsabilidade civil objetiva.

Por fim, existe uma última corrente doutrinária, encabeçada por Moraes e Queiroz621, que defende que a LGPD criou um sistema de responsabilidade civil proativo, o qual nem seria subjetivo nem objetivo, mas um sistema especialíssimo de responsabilização.

Para os autores, este modelo de responsabilização é multifuncional, pois não objetiva apenas compensar as vítimas pelas lesões sofridas, mas tem em vista, principalmente, evitar tais danos. Dessa forma, esse sistema vai além da responsabilidade dos agentes e exige que estes, em adição ao cumprimento da lei, atitudes conscientes, diligentes e proativas em relação à utilização de dados pessoais e que sejam capazes de demonstrar a adoção de medidas eficazes à conformação da organização com as normas de proteção de dados pessoais, de modo que não descumprir a lei já não é suficiente.

> Em conclusão, vê-se que o legislador, embora tenha flertado com o regime subjetivo, elaborou a um novo sistema, de prevenção, e que se baseia justamente no risco da atividade. Tampouco optou pelo regime da responsabilidade objetiva, que seria talvez mais adequado à matéria dos dados pessoais, porque buscou ir além na prevenção, ao aventurar-se em um sistema que tenta, acima de tudo, evitar que danos sejam causados[622].

Isso posto, a responsabilidade proativa seria um novo jeito de pensar a responsabilidade civil, visto que, enquanto os modelos de responsabilidade civil tradicionais, isto é, o subjetivo e o objetivo, concentram-se nos efeitos danosos, este sistema especial de responsabilidade se preocupa, primariamente, com a prevenção de tais efeitos.

---

621 MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD. *In:* Proteção de Dados Pessoais: privacidade *versus* avanço tecnológico. **Cadernos Adenauer,** Rio de Janeiro: Fundação Konrad Adenauer, ano XX, n. 3, out. 2019. Disponível em: https://www.kas.de/documents/265553/265602/Caderno+Adenauer+3+Schutz+von+pers%C3%B6nlichen+Daten.pdf/476709fc-b7dc-8430-12f1-ba21564cde06?version=1.0&t=1571685012573. Acesso em: 26 maio 2021, p. 113-135.

622 MORAES, Maria Celina Bodin de. LPGD: um novo regime de responsabilização civil dito "proativo". Editorial à **Civilistica.com,** Rio de Janeiro, a. 8, n. 3, 2019. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/448/377. Acesso em: 26 maio 2021, p. 6.

Dessa forma, para esta corrente, em que pese seja necessária a demonstração de que o agente de tratamento descumpriu as normas previstas na LGPD para que seja responsabilizado, o que poderia sugerir que a lei adotou o regime de responsabilidade civil subjetivo, pelo princípio da responsabilização e prestação de contas previsto no artigo 6º, X, da mencionada Lei, o controlador e o operador deverão ser capazes de comprovar sua conformidade com a Lei 13.709/2018.

Em que pese todos os argumentos defendidos pelas diferentes correntes doutrinárias, entende-se, neste trabalho, que a Lei Geral de Proteção de Dados Pessoais abraçou, como regra geral, a responsabilidade civil subjetiva, mas, em situações específicas, instituiu o sistema de responsabilidade objetiva. Explica-se.

No artigo 42, a LGPD preceitua que os agentes de tratamento de dados pessoais são obrigados a reparar o dano que causarem por exercerem suas atividades em violação à mencionada legislação. Dessa forma, além de este dispositivo não fazer referência a um dever de reparar independentemente de culpa, utiliza expressão que é própria do modelo de responsabilidade subjetiva, já que sugere a avaliação da conduta do agente no que atine à observância da Lei. Em reforço a tal entendimento, o artigo 43, II, estabelece que os agentes não serão obrigados a reparar o dano se demonstrarem "que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados".

Já no artigo 44, ciente de que determinados tratamentos de dados implicam risco muito mais elevado ao titular do que outros, a Lei 13.709/2018 parece prever também regime de responsabilidade civil diverso para tais situações, do contrário, não haveria razão para a existência do referido dispositivo.

Assim, ao estabelecer que o tratamento de dados será irregular quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes tais como o modo pelo qual é realizado, o resultado e os riscos que razoavelmente dele se esperam e as técnicas de processamento disponíveis à época em que foi realizado, a LGPD reconhece que existem atividades de tratamento cujo risco lhe é intrínseco, a exemplo de tratamento de dados de saúde, decisões tomadas com base em *profiling* e tratamento em grande escala de dados sensíveis.

Estas atividades, portanto, atraem a incidência do artigo 927, parágrafo único, do Código Civil, segundo o qual "Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.".

Diante disso, bem como numa interpretação teleológica da Lei Geral de Proteção de Dados Pessoais que intenta assegurar ampla proteção aos titulares dos dados na sociedade da informação e, ainda, tendo em vista que o artigo 44 foi construído de maneira muito similar ao do artigo 14, do Código de Defesa do Consumidor, defende-se uma interpretação do seu parágrafo único no sentido de que o agente de tratamento deverá ser responsabilizado quando, nesse cenário de risco, ocorrer qualquer dano decorrente de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou, ainda, qualquer forma de tratamento inadequado ou ilícito. Esta responsabilidade, por sua vez, deve ser objetiva, entendendo-se que a expressão "ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei" nada mais é do que um reforço à importância de implementação destas medidas.

Conforme se observa, a posição aqui defendida segue a mesma linha dos ensinamentos do professor Schreiber, inclusive fora fortemente por estes influenciada, há, contudo, uma sutil diferença para o sustentado por este autor, pois não se vê, no parágrafo único do artigo 44 da LGPD, uma hipótese adicional de responsabilidade do controlador ou do operador.

Importa dizer que, mesmo nas situações em que o sistema de responsabilidade civil estabelecido pela Lei Geral de Proteção de Dados Pessoais a ser aplicado é o subjetivo, uma interpretação sistemática da legislação revela que caberá ao agente de tratamento comprovar que cumpriu com as normas nela previstas.

Isso porque, pelo alhures mencionado princípio da responsabilização e da prestação de contas, o controlador e o operador devem demonstrar que adotaram "medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas".

Ademais, como visto, a LGPD dispõe, em seu artigo 43, que os agentes de tratamento só não serão responsabilizados quando provarem a) que não realizaram o tratamento de dados pessoais que lhes é atribuído; b) que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou c) que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro. Dessa feita, presume-se que o dano decorreu de uma infração à legislação, cabendo, pois, ao controlador e ao operador demonstrarem que estavam adequados às normas de proteção de dados.

Outrossim, a análise do comportamento do agente de tratamento será feita objetivamente, já que terá como parâmetro a própria Lei 13.709/2018 e os regulamentos da autoridade nacional acerca dos padrões técnicos mínimos que as medidas de segurança implementadas por tais agentes deverão apresentar.

Nesse diapasão, a vítima deverá provar o dano alegado, bem como o nexo de causalidade entre o tratamento de dados pessoais e a lesão. A esse respeito, o conforme previsão do artigo 42, § 2º, da LGPD, o juiz ainda poderá, mediante decisão fundamentada, inverter o ônus da prova a favor do lesado "quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa".

Para além de toda essa discussão doutrinária, cumpre dizer que o artigo 45, da Lei 13.709/2018, prescreve que "As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente". Dessa feita, tendo em vista que a grande maioria das operações de tratamento de dados é realizada no domínio das relações consumeristas, de igual forma, parcela imensamente significativa das ações de reparação de danos atrairá a aplicação da responsabilidade objetiva prevista no Código de Defesa do Consumidor.

Isso posto, seja diante de todo o *standard* de conduta imposto pela LGPD, seja em razão de o ônus da prova do cumprimento da legislação recair sobre o agente de tratamento ou seja, ainda, pelas hipóteses de aplicação da responsabilidade objetiva do controlador ou do processador, uma vez demonstrados os danos e o nexo de causalidade, não será rara a imputação da obrigação do dever de reparar a tais agentes.

Nesse contexto, as maiores dificuldades a serem enfrentadas pelos titulares e pelos tribunais em matéria de responsabilização pela Lei 13.709/2018 serão, pois, a comprovação do liame causal e as delimitações em torno da ocorrência ou não do dano.

Dessa feita, existirão situações em que a própria identificação da infração à Lei Geral de Proteção de Dados Pessoais será difícil. Exemplificativamente, um tratamento de dados pessoais que utilize variáveis proxies para fazer inferências sensíveis acerca de um indivíduo que resultam em sua discriminação frequentemente não será percebido como ilícito, haja vista que o titular não faz ideia das correlações reveladas pela mineração de dados.

De igual forma, nas hipóteses de incidentes de segurança que não são comunicados ou são negados pela organização, de modo que os dados dos titulares são vazados, permanecem quase que eternamente expostos na *deep web*, e, muitas vezes, não há qualquer indício de qual tenha sido a fonte da violação. Em outras hipóteses, especialistas até apontam a provável fonte do vazamento, mas não há como determiná-la com certeza sem que haja uma investigação profunda da conformidade do agente indicado com a legislação e dos eventos registrados em seu sistema de informação.

Aqui, mostra-se ainda mais relevante a atuação da ANPD para averiguar tais denúncias e operações de tratamento, bem como a defesa coletiva dos direitos dos titulares, haja vista que, enquanto para um titular, individualmente, é praticamente impossível ou inviável comprovar o nexo de causalidade nestas hipóteses, o Ministério Público pode determinar as investigações necessárias para apurar o incidente e assim, posteriormente, obter a responsabilização do ofensor.

Há, ainda, situações em que se tem conhecimento da infração à LGPD, mas o dano já ocorreu ou só se verifica num momento futuro, de modo que se revela difícil associar a lesão à referida violação.

Ilustrativamente, uma organização verifica um incidente de segurança em sua base de dados que expôs dados de cartão de crédito de seus clientes. A violação de dados é notificada à autoridade nacional e aos titulares, no entanto, apesar de o incidente só ter sido identificado agora, as informações estavam expostas há um ano. Ocorre que, na sociedade da informação, em que os vazamentos de dados são frequentes, os mesmos dados foram indevidamente divulgados em outro incidente, o qual só foi verificado há dois meses, mas a falha já existia há muito mais tempo. Nesse cenário, um titular sofreu, há cinco meses, um dano patrimonial decorrente da utilização de seus dados de cartão de crédito que foram expostos sem o seu consentimento. Em face disso, não é fácil a identificação do agente de tratamento que deu causa ao dano.

Em outro exemplo, dados pessoais de diversos titulares foram indevidamente compartilhados por uma organização, a qual cumpriu com seu dever de notificação imposto pela LGPD. Entretanto, tais informações só vêm a ser utilizadas dali a um ano. Mais uma vez, nessa situação, a depender dos dados vazados, o indivíduo terá muita dificuldade em comprovar que os danos experimentados foram gerados por este e não por outro compartilhamento ilícito.

Dessarte, a possibilidade de inversão do ônus da prova quanto ao nexo de causalidade será essencial para permitir a reparação do dano do titular que apresentar indícios plausíveis do referido liame, atribuindo-se ao agente de tratamento a incumbência de demonstrar que a lesão decorreu de outro fato e não da sua violação à LGPD.

No que se refere à delimitação do dano, enquanto que o patrimonial deve ser comprovado, indaga-se a lesão extrapatrimonial deve ser provada ou presumida.

A esse respeito, a Lei 13.709/2018 não fornece maiores pistas para a superação da questão. Como regra, no ordenamento jurídico pátrio, aquele que sofre uma lesão, para ser ressarcido, deve comprová-la. Contudo, o Superior Tribunal de Justiça tem reconhecido, em

casos específicos, que existem condutas em que, por ofenderem direitos da personalidade ou a dignidade humana, o dano moral é um resultado natural da situação, razão pela qual a vítima não precisa comprovar nenhum prejuízo de ordem extrapatrimonial, apenas que sua dignidade ou personalidade fora violada pelo evento lesivo[623]. Trata-se do dano moral *in re ipsa.*

Também o dano moral coletivo é presumido, exigindo-se somente a demonstração de conduta antijurídica que, de forma absolutamente injusta e intolerável, viole valores éticos essenciais da sociedade, implicando um dever de reparação, que tem por finalidade prevenir novas condutas antissociais, punir o comportamento ilícito e reverter, em favor da comunidade, o eventual proveito patrimonial obtido pelo ofensor[624].

Sobre o dano moral presumido, Lôbo leciona que:

> De modo mais amplo, os direitos de personalidade oferecem um conjunto de situações definidas pelo sistema jurídico, inerentes à pessoa, cuja lesão faz incidir diretamente a pretensão aos danos morais, de modo objetivo e controlável, não sendo necessária a prova do prejuízo ou o recurso à existência de dor moral ou psíquica, sofrimentos ou incômodos.
> A responsabilidade opera-se pelo simples fato da violação (*damnu in re ipsa*); assim, verificada a lesão a direito da personalidade, surge a necessidade de reparação do dano moral[625].

Diante disso, e uma vez que, conforme estudado neste trabalho, as informações pessoais são projeções da personalidade, sendo tuteladas pelo direito à privacidade, o tratamento ilícito de tais informações, em especial quando atinente aos princípios de proteção de dados pessoais, tem como consequência intrínseca um dano moral. Desse modo, bastaria

---

[623] Nesse sentido: DIREITO CIVIL. RECURSO ESPECIAL. AÇÃO DE COMPENSAÇÃO POR DANOSMORAIS. ACIDENTE EM OBRAS DO RODOANEL MÁRIO COVAS. NECESSIDADE DEDESOCUPAÇÃO TEMPORÁRIA DE RESIDÊNCIAS. DANO MORAL IN RE IPSA. 1. Dispensa-se a comprovação de dor e sofrimento, sempre que demonstrada a ocorrência de ofensa injusta à dignidade da pessoa humana. 2. A violação de direitos individuais relacionados à moradia, bem como da legítima expectativa de segurança dos recorrentes,caracteriza dano moral in re ipsa a ser compensado. 3. Por não se enquadrar como excludente de responsabilidade, nos termos do art. 1.519 do CC/16, o estado de necessidade, embora não exclua o dever de indenizar, fundamenta a fixação das indenizações segundo o critério da proporcionalidade. 4. Indenização por danos morais fixada em R$ 500,00 (quinhentos reais) por dia de efetivo afastamento do lar, valor a ser corrigido monetariamente, a contar dessa data, e acrescidos de juros moratórios no percentual de 0,5% (meio por cento) ao mês na vigência do CC/16 e de 1% (um por cento) ao mês na vigência do CC/02,incidentes desde a data do evento danoso. 5. Recurso especial provido. (BRASIL. Superior Tribunal de Justiça. **REsp: 1292141 SP 2011/0265264-3**, Relatora: Ministra NANCY ANDRIGHI, Data de Julgamento: 04/12/2012, T3 - TERCEIRA TURMA, Data de Publicação: DJe 12/12/2012. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/23027511/recurso-especial-resp-1292141-sp-2011-0265264-3-stj/inteiro-teor-23027512. Acesso em: 26 maio 2021.

[624] BRASIL. Superior Tribunal de Justiça. **REsp: 1539056 MG 2015/0144640-6,** Relator: Ministro Luis Felipe Salomão, Data do Julgamento: 06 abr. 2021, Quarta Turma. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201501446406&dt_publicacao=18/05/2021. Acesso em: 26 maio 2021.

[625] LÔBO, Paulo. **Direito Civil:** v. 2: obrigações. 7. ed. São Paulo: Saraiva Educação, 2019, p. 349.

provar que o tratamento de dados não se deu de acordo com a Lei Geral de Proteção de Dados Pessoais para ensejar o direito à reparação.

Nesse sentido, no julgamento do REsp nº 1.758.799 - MG, a Terceira Turma do STJ entendeu que o consumidor tem o direito de tomar conhecimento de que informações a seu respeito estão sendo arquivadas ou comercializadas por terceiro, sem a sua autorização, de forma que a inobservância dos deveres associados ao tratamento dos dados, dentre os quais o dever de informar, faz nascer a pretensão de indenização pelos danos causados e a de fazer cessar, imediatamente, a ofensa aos direitos da personalidade. Por conseguinte, tem-se uma hipótese em que se configura o dano moral *in re ipsa*[626].

Isso posto, verifica-se a possibilidade de que os tribunais brasileiros reconheçam a ocorrência de dano moral presumido decorrente do processamento de dados que não esteja em

[626] RECURSO ESPECIAL. FUNDAMENTO NÃO IMPUGNADO. SÚM. 283/STF. AÇÃO DE COMPENSAÇÃO DE DANO MORAL. BANCO DE DADOS. COMPARTILHAMENTO DE INFORMAÇÕES PESSOAIS. DEVER DE INFORMAÇÃO. VIOLAÇÃO. DANO MORAL IN RE IPSA. JULGAMENTO: CPC/15. 1. Ação de compensação de dano moral ajuizada em 10/05/2013, da qual foi extraído o presente recurso especial, interposto em 29/04/2016 e atribuído ao gabinete em 31/01/2017. 2. O propósito recursal é dizer sobre: (i) a ocorrência de inovação recursal nas razões da apelação interposta pelo recorrido; (ii) a caracterização do dano moral em decorrência da disponibilização/comercialização de dados pessoais do recorrido em banco de dados mantido pela recorrente. 3. A existência de fundamento não impugnado – quando suficiente para a manutenção das conclusões do acórdão recorrido – impede a apreciação do recurso especial (súm. 283/STF). 4. A hipótese dos autos é distinta daquela tratada no julgamento do REsp 1.419.697/RS (julgado em 12/11/2014, pela sistemática dos recursos repetitivos, DJe de 17/11/2014), em que a Segunda Seção decidiu que, no sistema credit scoring, não se pode exigir o prévio e expresso consentimento do consumidor avaliado, pois não constitui um cadastro ou banco de dados, mas um modelo estatístico. 5. A gestão do banco de dados impõe a estrita observância das exigências contidas nas respectivas normas de regência – CDC e Lei 12.414/2011 – dentre as quais se destaca o dever de informação, que tem como uma de suas vertentes o dever de comunicar por escrito ao consumidor a abertura de cadastro, ficha, registro e dados pessoais e de consumo, quando não solicitada por ele. 6. O consumidor tem o direito de tomar conhecimento de que informações a seu respeito estão sendo arquivadas/comercializadas por terceiro, sem a sua autorização, porque desse direito decorrem outros dois que lhe são assegurados pelo ordenamento jurídico: o direito de acesso aos dados armazenados e o direito à retificação das informações incorretas. 7. A inobservância dos deveres associados ao tratamento (que inclui a coleta, o armazenamento e a transferência a terceiros) dos dados do consumidor – dentre os quais se inclui o dever de informar – faz nascer para este a pretensão de indenização pelos danos causados e a de fazer cessar, imediatamente, a ofensa aos direitos da personalidade. 8. Em se tratando de compartilhamento das informações do consumidor pelos bancos de dados, prática essa autorizada pela Lei 12.414/2011 em seus arts. 4º, III, e 9º, deve ser observado o disposto no art. 5º, V, da Lei 12.414/2011, o qual prevê o direito do cadastrado ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais. 9. O fato, por si só, de se tratarem de dados usualmente fornecidos pelos próprios consumidores quando da realização de qualquer compra no comércio, não afasta a responsabilidade do gestor do banco de dados, na medida em que, quando o consumidor o faz não está, implícita e automaticamente, autorizando o comerciante a divulgá-los no mercado; está apenas cumprindo as condições necessárias à concretização do respectivo negócio jurídico entabulado apenas entre as duas partes, confiando ao fornecedor a proteção de suas informações pessoais. 10. Do mesmo modo, o fato de alguém publicar em rede social uma informação de caráter pessoal não implica o consentimento, aos usuários que acessam o conteúdo, de utilização de seus dados para qualquer outra finalidade, ainda mais com fins lucrativos. 11. Hipótese em que se configura o dano moral in re ipsa. 12. Em virtude do exame do mérito, por meio do qual foram rejeitadas as teses sustentada pela recorrente, fica prejudicada a análise da divergência jurisprudencial. 13. Recurso especial conhecido em parte e, nessa extensão, desprovido. BRASIL. Superior Tribunal de Justiça. **REsp 1758799 MG 2017/0006521-9,** Relatora: Ministra Nancy Andrighi, Data do Julgamento: 12 nov. 2019, Terceira Turma. Disponível em: https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ITA?seq=1888267&tipo=0&nreg=201700065219&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20191119&formato=PDF&salvar=false. Acesso em: 26 maio 2021.

conformidade com a legislação, contudo, resta acompanhar quais serão os parâmetros utilizados para tanto. Isto é, se qualquer ilicitude na atividade de tratamento de dados será hipótese se dano *in re ipsa* ou se, em determinadas situações, a lesão deverá ser comprovada.

Exemplificativamente, nos próximos anos existirão várias demandas relacionadas a incidentes de segurança em que os dados vazados já eram facilmente encontrados na *internet*, como o nome, o e-mail e o CPF dos titulares, ou concernentes a falhas de segurança que foram identificadas pelo próprio agente de tratamento, não havendo qualquer indício de que a referida falha fora explorada por terceiros nem que tenha havido utilização indevida da informação. Nesses casos, a jurisprudência deverá firmar um entendimento acerca da prescindibilidade de se comprovar um dano efetivo ou se tais situações, em que pese violem à privacidade, não tem potencial gravoso para que uma lesão necessariamente delas decorra.

Ainda no intento de assegurar uma efetiva indenização ao titular dos dados, a Lei Geral de Proteção de Dados Pessoais prevê, em seu artigo 42, § 1º, que os controladores que estiverem diretamente envolvidos no tratamento que provocou danos responderão solidariamente[627].

Ressalte-se que responsabilidade solidária não quer dizer que o percentual correspondente a cada um dos controladores será igual, devendo-se apurar as cotas partes de responsabilidade, quando do exercício do direito de regresso, de acordo com a respectiva participação de cada controlador no evento lesivo, haja vista que as decisões tomadas por tais agentes contribuirão de forma proporcionalmente diferente para o resultado. É o que preceitua o § 4º, do mesmo artigo: "Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso".

Ademais, o já mencionado artigo 42, § 1º, da LGPD, também prescreve hipótese de responsabilidade entre controlador e operador:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver

[627] Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:
[...] II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

> seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei [...];

Entende-se, numa interpretação do referido artigo que leve em consideração a finalidade para a qual fora previsto, qual seja, a de assegurar a efetiva indenização do titular, que a solidariedade aí prescrita se refere ao controlador, tendo em vista que já há uma previsão, no *caput* do artigo, de que se o operador descumprir as normas da LGPD deverá ser responsabilizado. Dessa feita, o objetivo do citado dispositivo foi garantir que, mesmo que o dano tenha sido provocado exclusivamente pela conduta do operador, o controlador deverá responder solidariamente, cabendo-lhe, posteriormente, o direito de regresso contra aquele agente de tratamento[628].

Por fim, saliente-se que o objetivo primordial da Lei Geral de Proteção de Dados Pessoais é a garantia da privacidade em todos os procedimentos pelos quais passem as informações pessoais e a prevenção de danos ao titular, não a reparação de tais lesões. Por esta razão, a referida Lei impõe uma série de condutas ao agente que devem ser observadas durante todo o tratamento de dados pessoais, bem como prescreve instrumentos para compelir o controlador e o operador a se adequarem à LGPD, quais sejam, as sanções administrativas e a responsabilização civil, de modo que a função desta última vai além da compensação de danos.

Uma vez estudados os mecanismos previstos pela Lei 13.709/2018 para fazer cumprir as suas disposições, averiguar-se-á, a seguir, se tais normas são suficientes para assegurar o direito à privacidade e se seus instrumentos de *enforcement* são capazes de torná-la efetiva.

5.3 Análise da (In)efetividade da Lei Geral de Proteção de Dados Pessoais

Conforme já mencionado, o estudo da efetividade da Lei 13.709/2018 partirá da identificação do seu nível de convergência com o Regulamento Geral de Proteção de Dados da União Europeia, tendo em vista que este Regulamento já está em vigor há mais de três anos e, desse modo, o exame de sua aplicação pode trazer importantes dados acerca de quais previsões comuns a ambas as legislações são relevantes para a tutela da privacidade, bem como quais diferenças podem aumentar ou reduzir a efetividade da LGPD. É o que se propõe nas subseções abaixo.

---

[628] SCHREIBER, Anderson. Responsabilidade civil na Lei Geral de Proteção de Dados Pessoais. *In:* DONEDA, Danilo et al (Coords). **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021, p. 331-332.

5.3.1 Mapeamento das diferenças e semelhanças entre a Lei 13.709/2018 e o Regulamento Geral de Proteção de Dados da União Europeia

Para possibilitar uma completa apuração das similaridades entre a Lei Geral de Proteção de Dados Pessoais e o RGPD, elaborou-se o quadro abaixo, em que ponto a ponto das legislações são confrontados.

Quadro 3 – Comparativo entre disposições da LGPD e do RGPD

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LGPD	**REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS – RGPD**
Técnica legislativa	**Técnica legislativa**
A Lei Geral de Proteção de Dados possui 65 artigos. A maior parte das disposições é genérica. Além disso, o texto final da LGPD não conta com nenhuma exposição de motivos nem com qualquer orientações interpretativas fornecidas pelo legislador. Apenas o projeto de Lei que deu origem à Lei 13.709/2018 (PL 4060/2012) apresenta uma pequena justificativa expondo brevemente a necessidade de se aprovar uma legislação específica sobre a proteção de dados pessoais, mas não traz nenhum elemento adicional à interpretação da Lei. Tal exposição de motivos não é publicada com o texto final da LGPD, sendo encontrada apenas no inteiro teor do PL 4060/2012[629].	O Regulamento Geral de Proteção de Dados da União Europeia possui 99 artigos. Disposições prescritivas e detalhadas. Ademais, introdutoriamente, o RGPD apresenta 173 considerandos, que são orientações interpretativas robustas e amadurecidas acerca das disposições do Regulamento, oferecendo significativos conceitos, exemplos e explicações que contribuem para a sua escorreita interpretação e aplicação.
Âmbito de aplicação	**Âmbito de aplicação**
Conforme o artigo 3º, a LGPD é aplicável a qualquer operação de tratamento, **independentemente do meio (físico ou eletrônico)**, realizada por **pessoa natural para fins econômicos** ou por **pessoa jurídica** de direito público ou privado, do país de sua sede ou do país onde estejam localizados os dados, independentemente da finalidade econômica, desde que: a) a operação de tratamento seja realizada no território nacional, ou b) tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional ou, ainda, c) se os dados pessoais tiverem sido coletados no território nacional. **Por se referir à pessoa natural ou pessoa jurídica, tem gerado discussões quanto à sua aplicabilidade ou não ao tratamento de dados realizados por entes despersonalizados, como condomínios.** Ainda consoante o artigo 4º, a LGPD não se aplica a	Conforme os artigos 2° e 3°, aplica-se o RGPD ao tratamento de dados pessoais, independentemente do meio (físico ou eletrônico), realizado por pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que processe dados individualmente ou em conjunto com outros, desde que: a) seja efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União, ou b) quando as atividades de tratamento estejam relacionadas com a oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento ou ao controle do seu comportamento, desde que esse comportamento tenha lugar na União; ou c) seja realizado por um responsável pelo tratamento estabelecido não na União, mas num lugar em que se aplique o direito de um Estado-Membro por força do

[629] Para acessar a exposição de motivos do PL 4060/2012, ver: BRASIL. Câmara dos Deputados. **Projeto de Lei nº 4060, de 2012.** Dispõe sobre o tratamento de dados pessoais e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node01bkwy75dp9ctf13g0ctmfpu4zg1645605.node0?codteor=1001750&filename=PL+4060/2012. Acesso em: 30 abr. 2021.

operações de tratamento realizadas a) por pessoa natural para fins exclusivamente particulares e não econômicos e, b) exclusivamente para fins jornalísticos, artísticos, de segurança pública, defesa nacional, segurança nacional e atividades de investigação e repressão de infrações penais. Quanto ao tratamento para fins acadêmicos, aplicam-se apenas os artigos 7º e 11 da Lei, os quais dizem respeito às bases legais de tratamento de dados. **Em determinadas situações, a LGPD será aplicável mesmo ao tratamento de dados anonimizados, já que o artigo 12, § 2º, da Lei prevê que tais dados poderão ser considerados pessoais se utilizados para formação do perfil comportamental de determinada pessoa natural e o tratamento for capaz de afetar sua esfera jurídica.**	direito internacional público. **Pela amplitude de quem é expressamente considerado responsável pelo tratamento, o RGPD não suscita dúvidas quanto a sua aplicabilidade ao tratamento de dados realizados por entes despersonalizados, como condomínios.** Também conforme o artigo 2.°, o RGPD não se aplica ao tratamento de dados: a) efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas; b) efetuado pelas autoridades competentes para efeitos de prevenção, investigação, detenção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública. No que atine ao tratamento de dados efetuado para fins exclusivamente jornalísticos, acadêmicos e a artísticos, o RGPD é aplicável, mas prevê expressamente, em seu artigo 85.°, que os Estados-membros poderão estabelecer isenções ou derrogações das normas que determinadas normas, incluindo as que se referem aos princípios e direitos dos titulares, desde que tais isenções ou derrogações sejam necessárias para conciliar o direito à proteção de dados pessoais com a liberdade de expressão e de informação. **Não se aplica ao tratamento de dados anonimizados (considerando 26).**
Definição de dados pessoais	**Definição de dados pessoais**
Informação relacionada a pessoa natural identificada ou identificável (Artigo 5º, I) **Não define o que deve ser considerado como pessoa identificável.**	Informação relativa a uma pessoa singular identificada ou identificável (Artigo 4.° , 1) **Define pessoa identificável** como 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. (Artigo 4.° , 1)
Definição de dados pessoais sensíveis	**Definição de dados pessoais 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 (Artigo 5º, II). **A Lei Geral de Proteção de Dados traz uma definição de dados sensíveis que não leva em consideração a função que o dado exerce no contexto em que está inserido.** Ao contrário, **traz um rol taxativo de dados** que, historicamente e pela sua natureza, são informações que podem gerar discriminação, desconsiderando-se que, a partir de dados pessoais não sensíveis, podem ser feitas inferências sensíveis, bem como deixando fora do escopo de proteção específica dados outros que, de igual	Dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. (Considerando 51), incluindo-se, aí, dados que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa (Artigo 9.°). **O Regulamento Geral de Proteção de Dados não define, em seu Considerando 51, dados sensíveis a**

forma, podem implicar riscos significativos para os direitos fundamentais do indivíduo. Dessa forma, visando a tutelar, ainda que parcialmente, esse tipo de situação, a Lei Geral de Proteção de Dados Pessoais, em seu artigo 11, §1º**, prevê que as disposições relativas ao tratamento de dados pessoais sensíveis**, ressalvado o disposto em legislação específica, **aplicam-se a qualquer tratamento de dados que, embora isoladamente não sejam sensíveis, acabem por revelar informações pessoais que o sejam e que possa causar dano ao titular**.	**partir de um rol taxativo, como o faz a LGPD, o que permite que os dados referidos no artigo 9º sejam entendidos apenas como exemplos desta categoria, possibilitando que outras informações possam ser consideradas sensíveis.** Além disso**, uma interpretação extensiva do Considerando 51 permite estender as normas acerca do tratamento de categorias especiais de dados pessoais a outros dados que a princípio não são sensíveis, mas cuja utilização acabe revelando informações de tal natureza**, uma vez que o referido Considerando expressamente menciona que os dados sensíveis merecem proteção específica, porque, o contexto de seu tratamento pode implicar riscos aos direitos e liberdades fundamentais. Dessa forma, se o uso que se faz de um dado permite a inferência de um conhecimento sensível do ponto dos direitos fundamentais do indivíduo, tal dado merecerá, de acordo com tal interpretação, o mesmo tratamento que os demais dados sensíveis.
Princípios	**Princípios**
Além da boa-fé, o tratamento de dados deve observar os seguintes princípios: a) Finalidade, b) adequação, c) necessidade, d) livre acesso, e) qualidade dos dados, f) transparência, g) segurança, h) prevenção, i) não discriminação, e j) responsabilização e prestação de contas. (Art. 6º)	Os princípios relativos ao tratamento de dados previstos pelo RGPD são: a) licitude, lealdade e transparência, b) limitação das finalidades, c) minimização dos dados (equivalente ao que a LGPD chama de princípio da necessidade), d) exatidão, e) limitação da conservação, f) integridade e confidencialidade, g) responsabilidade (Art. 5.°).
Bases legais para o tratamento lícito dos dados pessoais	**Bases legais para o tratamento lícito dos dados pessoais**
a) mediante o fornecimento de consentimento pelo titular; b) para o cumprimento de obrigação legal ou regulatória pelo controlador; c) pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas; d) para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; e) quando 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; f) para o exercício regular de direitos em processo judicial, administrativo ou arbitral; g) para a proteção da vida ou da incolumidade física do titular ou de terceiro; h) para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; i) 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; ou **j) para a proteção do crédito** **É dispensada a exigência do consentimento para o**	a) mediante o fornecimento do consentimento do titular para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas; b) para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados; c) para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; d) para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; e) para exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; f) para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança. (Artigo 6.°) O RGPD **não prevê a proteção do crédito como uma base legal autônoma** a permitir o tratamento de dados pessoais. Também **não há previsão expressa de dispensa do consentimento para o tratamento de dados tornados manifestamente públicos pelo titular**.

tratamento de dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei. (Artigo 7º) A LGPD previu que poderá ocorrer o tratamento de dados pessoais mesmo sem o consentimento do titular quando for destinado à proteção do crédito, harmonizando a legislação com a Lei do Cadastro Positivo.	
Condições aplicáveis ao consentimento	**Condições aplicáveis ao consentimento**
Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (Artigo 5º, XII) Deve ser fornecido por escrito, em cláusula destacada das demais cláusulas contratuais, ou por outro meio que demonstre a manifestação de vontade do titular. Tal demonstração de manifestação evidencia a adoção do modelo *opt-in* de consentimento para o tratamento de dados pessoais. Deve se referir a finalidades determinadas, sendo nulas as autorizações genéricas para o tratamento de dados pessoais. Pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado. O ônus da prova do fornecimento do consentimento pelo titular cabe ao controlador. (Art. 8º) Além das condições de consentimento aplicáveis ao tratamento de dados de crianças e adolescentes, **não traz nenhuma outra hipótese em que já se presume que o consentimento não foi dado livremente.**	Manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento (Artigo 4.°, 11) Essa definição deixa expressa a opção do RGPD pela técnica de *opt-in* para fornecimento de autorização para tratamento de dados pessoais. Além disso, conforme o considerando 32, "O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento". Pode ser fornecido por escrito ou por outro meio. Quando for escrito, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente de outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples. Deve ser dado para uma ou umas finalidades específicas. Pode ser revogado a qualquer momento. O ônus da prova do fornecimento do consentimento pelo titular cabe ao responsável pelo tratamento (Art. 7.°) **O consentimento não será considerado livre se a pessoa não puder recusar nem retirar o consentimento sem ser prejudicado, bem como se existir um desiquilíbrio manifesto entre o titular do dado e o responsável pelo tratamento ou se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais ou, ainda, se for exigido o consentimento no tratamento de dados desnecessários como condição prévia à execução de um contrato ou serviço.** (Considerandos 42 e 43 e art. 7º, 4).
Tratamento de dados sensíveis	**Tratamento de dados sensíveis**
Prevê hipóteses mais restritas para o tratamento lícito de dados pessoais sensíveis, estabelecendo um regime mais protetivo para essa categoria de dados que para os demais dados pessoais (Artigo 11). As hipóteses legais de tratamento são semelhantes às aplicáveis ao processamento dos demais dados pessoais, mas quando a base legal para o tratamento for o consentimento, este deve ser fornecido de forma	**Prevê uma proibição geral ao tratamento de dados pessoais sensíveis**, estabelecendo exceções (Artigo 9.°). O processamento pode ocorrer se o titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados pessoais para uma ou mais finalidades específicas. É possível que o direito da União ou de um Estado-Membro disponha que a

específica e destacada, para finalidades específicas. Ademais, não podem ser tratados, sem o consentimento do titular, para atender aos interesses legítimos do controlador ou de terceiro nem para a proteção do crédito. Acrescenta a hipótese de tratamento de dados sensíveis, sem consentimento do titular, quando indispensável para a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. **Não prevê a dispensa de consentimento para os dados sensíveis que tenham sido tornado manifestamente públicos pelo titular.** **A autoridade nacional poderá vedar ou regulamentar a comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica**, já sendo vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde. **Também proíbe o tratamento de dados de saúde pelas operadoras de planos privados de assistência à saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.**	proibição geral não pode ser anulada pelo titular dos dados. Poderá ocorrer, na ausência de consentimento, se o tratamento for necessário para o cumprimento de determinadas obrigações jurídicas pelo responsável, ou para proteger os interesses vitais do titular ou de terceiro, ou por motivos de interesse público importante. **Também será dispensado o consentimento se os dados tiverem sido manifestamente tornados públicos pelo titular**, se forem necessários para efeitos de medicina preventiva ou do trabalho ou para fins de investigação científica ou estatísticos. Também poderá ser efetuado por uma fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais, desde que esse tratamento se refira exclusivamente a pessoas com quem esse organismo tenha mantido contatos regulares relacionados com os seus objetivos. Não podem ser tratados para atender aos interesses legítimos do controlador ou de terceiro. **Os Estados-Membros poderão, ainda, manter ou impor novas condições, incluindo limitações, no que respeita ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde.**
Tratamento de dados de crianças e adolescentes	**Tratamento de dados de crianças e adolescentes**
Deverá observar o melhor interesse da criança ou adolescente (Artigo 14). Exige o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal para o tratamento de dados pessoais de **crianças.** **A participação da criança em jogos, aplicações de *internet* ou outras atividades não pode ser condicionada ao fornecimento de informações pessoais além das estritamente necessárias à atividade.** O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento realmente foi dado pelo responsável pela criança. As informações sobre o tratamento de dados deverão utilizar recursos, inclusive audiovisuais, se adequado, que possibilitem o entendimento do responsável legal e da criança.	Exige o consentimento dos titulares das responsabilidades parentais para o tratamento de dados pessoais **de menores de 16 anos** (Artigo 8.°). **Os Estados-Membros poderão estabelecer uma idade inferior** para os efeitos de validade do consentimento dado pela própria criança, desde que essa idade não seja inferior a 13 anos.
Conservação dos dados após o término do tratamento dos dados	**Conservação dos dados após o término do tratamento dos dados**
Os dados pessoais deverão ser eliminados após o	O princípio da limitação da conservação estabelece

término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação apenas para determinadas finalidades (Art. 16).	que, exceto em determinadas hipóteses, os dados só poderão ser conservados durante o período necessário para as finalidades para as quais são tratados (Art. 5.°, 1, e).
Direitos do titular	**Direitos do titular**
Os artigos 17 a 22, da LGPD, dispõem que o titular tem direito a: a) direito geral de informação sobre o tratamento de dados e seus direitos; b) direito à confirmação da existência de tratamento de seus dados pessoais; c) direito de acesso aos dados pessoais; d) direito à cópia eletrônica integral de seus dados pessoais; e) direito à correção de dados incompletos, inexatos ou desatualizados; f) **direito à anonimização**, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei ou com o consentimento do titular; g) direito à portabilidade dos dados pessoais; h) direito à revogação do consentimento; i) direito de peticionar contra o controlador perante a autoridade nacional; j) direito de se opor a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, **em caso de descumprimento ao disposto na lei**; k) direito de obter informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial (o que a doutrina chama de direito à explicação); l) **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.** Não assegura que o indivíduo obtenha uma revisão humana das decisões automatizadas que o afetem. **Não prevê expressamente o direito ao esquecimento, com tal denominação, assim como o faz o RGPD, mas o direito de eliminação de dados desnecessários ou excessivos ou tratados com o consentimento do titular, disposto no artigo 18, IV, VI diz respeito ao direito ao apagamento, categoria do direito ao esquecimento.** A LGPD se preocupou em fazer com que a maior parte desses direitos realmente possa realmente ser utilizada pelos titulares dos dados, dispondo que o procedimento de acesso deverá ser facilitado e gratuito, bem como que **o requerimento para exercício dos direitos previstos no artigo 18 será atendido sem custos** para o titular (art. 18, § 3º e § 5º). **O exercício regular desses direitos pelo titular não pode ser utilizado em seu prejuízo**.	O RGPD, em seus artigos 12 a 22, estabelece uma série de direitos dos titulares dos dados, a saber: a) direito geral de informação sobre o tratamento de dados e seus direitos; b) direito de obter a confirmação de que seus dados pessoais são ou não objeto de tratamento; c) direito de acesso a seus dados pessoais; d) direito de obter uma cópia dos seus dados pessoais em fase de tratamento; e) direito de obter a retificação dos seus dados pessoais; f) direito de obter a limitação do tratamento de seus dados pessoais; g) direito ao apagamento de seus dados pessoais que deixaram de ser necessários para a finalidade que motivou sua coleta, que foram tratados ilicitamente ou com base no consentimento do titular e este é retirado ou quando o titular exercitar seu direito de oposição (direito a ser esquecido); h) direito de portabilidade de seus dados pessoais; i) direito de apresentar reclamação a uma autoridade de controle; j) **direito de se opor, por motivos particulares, ao tratamento de seus dados pessoais com base no interesse legítimo do responsável ou no exercício de funções públicas, bem como de objetar o processamento de seus dados para efeitos de comercialização direta, o que abrange a definição de perfis na medida em que esteja relacionada com tal comercialização;** k) direito de obter informações acerca da existência de decisões automatizadas, incluindo a definição de perfis, bem como informações úteis relativas à lógica subjacente, além da importância e das possíveis consequências de tal tratamento para o titular dos dados (o que a doutrina chama de direito à explicação); l) **direito de não ficar sujeito a nenhuma decisão tomada** exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar; m) direito de obter **intervenção humana** por parte do responsável, manifestar o seu ponto de vista e contestar uma decisão automatizada. **Não prevê o direito de o titular solicitar a anonimização** de seus dados pessoais, deixando de fora a possibilidade de o titular solicitar a adoção desta que é uma importante medida de segurança. **Apesar de os direitos previstos no RGPD e na LGPD serem bastante semelhantes, o Regulamento europeu faz um detalhamento bem maior de cada um desses**, o que facilitará e uniformizará a aplicação

A defesa desses direitos poderá ser exercida individual ou coletivamente, por meio dos legitimados, como o Ministério Público.	de tais direitos pelos países membros. As informações solicitadas pelo titular e quaisquer comunicações e medidas tomadas no exercício dos direitos do titular deverão ser fornecidas a título gratuito, mas **se os pedidos apresentados por um titular de dados forem manifestamente infundados ou excessivos, nomeadamente devido ao seu caráter repetitivo, o responsável pelo tratamento poderá exigir o pagamento de uma taxa razoável tendo em conta os custos para o atendimento da solicitação ou se recusar a dar seguimento ao pedido** (art. 12º, 5). **Não há previsão expressa de que o exercício de seus direitos pelo titular não poderá ser utilizado em seu prejuízo.** O titular dos dados tem o direito de mandatar um organismo, organização ou associação sem fins lucrativos, para, em seu nome, apresentar reclamação à autoridade de controle ou fazer a defesa de seus direitos na seara judicial. **Os Estados-membros poderão prever a desnecessidade de mandato** do titular para tanto. (Artigo 80.°)
Tratamento de dados pelo Poder Público	**Tratamento de dados pelo Poder Público**
Apresenta regras específicas para o tratamento de dados pessoais pelas pessoas jurídicas de direito público (Art. 23 a 32) Prevê o uso compartilhado de dados pessoais pelo Poder Público para atender finalidades específicas de políticas públicas e atribuição legal pelas entidades públicas. Veda ao Poder Público a transferência de dados pessoais a entidades privadas, mas prevê uma série de exceções a tal proibição, inclusive podendo ser respalda por meio de contratos e convênios, os quais deverão ser informados à autoridade nacional.	**Não há disposições específicas para o tratamento de dados pessoais pelo Poder Público.** Dispõe que quando os dados pessoais sejam tratados para fins de arquivo de interesse público, o direito da União ou dos Estados-Membros poderá prever derrogações aos direitos dos titulares, se tais derrogações forem necessárias para a prossecução desses fins.
Transferência internacional de dados	**Transferência internacional de dados**
Somente é permitida: a) para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei; b) ou quando o controlador comprovar garantias de cumprimento do regime de proteção de dados previsto na LGPD por meio de cláusulas analisadas pela autoridade nacional; c) quando a autoridade nacional autorizar a transferência; d) quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência; e) quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, ou na presença de outra exceção especificada na Lei. O nível de proteção a dados pessoais conferido a país ou organismo internacional será avaliado pela autoridade nacional.	Poderá ocorrer: a) independentemente de autorização específica caso a Comissão Europeia reconheça que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado; b) se um país terceiro ou uma organização internacional tiverem apresentado garantias adequadas, exigindo-se a autorização da autoridade de controle competente em determinados casos; c) quando o titular dos dados tiver explicitamente dado o seu consentimento à transferência prevista; d) quando for necessária para a execução de um contrato entre o titular dos dados e o responsável pelo tratamento, na presença de outra exceção especificada no Regulamento; e) se não for repetitiva, apenas disser respeito a um número limitado de titulares dos dados e for necessária para efeitos dos interesses legítimos visados pelo responsável pelo seu tratamento.

A LGPD estabelece requisitos mais genéricos a serem observados pela autoridade nacional na avaliação do nível de proteção de dados do país estrangeiro ou do organismo internacional. **Não há previsão de que a manutenção da garantia do nível de proteção adequado seja avaliada periodicamente.**	O nível de proteção a dados pessoais conferido a país ou organismo internacional será avaliado pela Comissão Europeia. **Os elementos** a serem observados pela Comissão Europeia na avaliação do nível de proteção de dados do país terceiro ou de organismo **internacional são mais detalhados e incluem a análise do primado do Estado de direito**, bem como o respeito pelos direitos humanos e liberdades fundamentais. Também as disposições sobre as transferências sujeitas a garantias adequadas são mais esmiuçadas que na lei brasileira. **A manutenção da garantia do nível de proteção adequado de um país ou organismo internacional deverá ser avaliada periodicamente, no mínimo de 4 em 4 anos.**
Registro do tratamento de dados pessoais	**Registro do tratamento de dados pessoais**
O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse (Art. 37). Não há detalhamento de quais informações devem constar desse registro. **Não há previsão expressa de dispensa desse registro**.	O responsável pelo tratamento e o subcontratante devem conservar um registro, por escrito, de todas as atividades de tratamento que realizarem ou que estejam sob a sua responsabilidade. (Art. 30.°) São esmiuçadas as informações que devem constar do registro. **Essa obrigação não se aplica às empresas ou organizações com menos de 250 trabalhadores**, a menos que o tratamento efetuado seja suscetível de implicar um risco para os direitos e liberdades do titular dos dados, não seja ocasional ou abranja dados sensíveis.
Representantes de agentes de tratamento estrangeiros	**Representantes de agentes de tratamento estrangeiros**
Não há obrigação de agentes de tratamento estrangeiros designar um representante no país, mas o artigo 61 prevê que, independentemente de procuração ou disposição estatutária, a empresa estrangeira será notificada dos atos processuais na pessoa do agente ou representante ou pessoa responsável por sua filial, agência, sucursal, estabelecimento ou escritório instalado no Brasil.	**Quando o tratamento for realizado por um agente não estabelecido na União Europeia, este deverá designar por escrito um representante seu na União** (Art. 27.°).
Relação entre controlador e operador	**Relação entre responsável pelo tratamento e subcontratante**
A LGPD não faz muitas disposições acerca dessa relação, limitando-se a dizer que o operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, (Art. 37) **Não estabelece a obrigatoriedade da existência de um ato formal** que vincule e estabeleça as obrigações e os direitos do controlador e do operador.	**O RGPD traz uma extensa regulação dessa relação**, estabelecendo que: a) O responsável só deverá recorrer a subcontratantes que apresentem garantias de que cumprem o regulamento; b) **A relação entre responsável e subcontratante deverá ser regulada por contrato ou outro ato normativo que os vincule** e estabeleça seus respectivos direitos e obrigações, instituindo uma série de cláusulas que devem constar no contrato; c) O subcontratante só poderá contratar outro subcontratante se o responsável pelo tratamento tiver dado, previamente e por escrito, autorização específica ou geral para tanto. (Art. 28.°)

Encarregado pelo tratamento de dados pessoais	Encarregado pelo tratamento de dados pessoais
Apenas o controlador deverá indicar encarregado pelo tratamento de dados pessoais (Art. 41). **Não estabelece hipóteses de dispensa de indicação do encarregado, porém prevê que a autoridade nacional poderá fazê-lo**, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados. O encarregado deverá manter comunicação com a autoridade nacional, orientar os funcionários do controlador acerca da proteção de dados, bem como aceitar reclamações e comunicações dos titulares, prestando-lhes esclarecimentos. A autoridade nacional poderá estabelecer outras atribuições. **Não há regras sobre os conhecimentos que o encarregado deve possuir nem há detalhamento sobre sua atuação e sua relação com o controlador.**	**Tanto o responsável pelo tratamento quanto o subcontratante deverão indicar um encarregado sempre que** a) O tratamento for efetuado por uma autoridade ou um organismo público; b) A natureza, âmbito e/ou finalidade de tratamento exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou c) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de dados sensíveis (Art. 37). O encarregado deverá controlar a conformidade do agente de tratamento com o Regulamento, aconselhar o responsável pelo tratamento, o subcontratante e os funcionários acerca da proteção de dados, prestar aconselhamento sobre a avaliação de impacto e manter contato com a autoridade de controle e com os titulares (Art. 39.°). O encarregado **deverá possuir conhecimentos especializados no domínio do direito e das práticas de proteção de dados** (Art. 37.°, 5). **Regula a atuação do encarregado e sua relação com o responsável pelo tratamento e o subcontratante** (Art. 38.°).
Responsabilidade e ressarcimento de danos	**Responsabilidade e ressarcimento de danos**
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 (Art. 42). O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado (Art. 44). Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança, der causa ao dano (Art. 44, parágrafo único) Responsabilidade solidária dos controladores que estiverem diretamente envolvidos no tratamento. Responsabilidade solidária do operador quando se desviar das instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador. Excludentes de responsabilidade: a) quando os agentes de tratamento provarem que não realizaram o tratamento;	O responsável pelo tratamento tem o dever de indenizar qualquer pessoa que tenha sofrido danos materiais ou imateriais causados por um tratamento que viole o RGPD (Art. 82.°). O subcontratante será responsabilizado pelos danos causados pelo tratamento apenas se não tiver cumprido as obrigações decorrentes do presente regulamento dirigidas especificamente aos subcontratantes ou se não tiver seguido as instruções lícitas do responsável pelo tratamento. Solidariedade entre todos os que tenham responsabilidade nos termos do Regulamento, inclusive entre responsável pelo tratamento e subcontratante. Excludente de responsabilidade: O responsável pelo tratamento ou o subcontratante não serão responsabilizados se demonstrarem que o evento que deu origem aos danos não lhes pode ser imputado. **O Estados-membros poderão prever que a ação judicial de indenização seja proposta por organismo, organização ou associação sem fins lucrativo (Artigo 80.°).** **Não há disposição específica sobre inversão do ônus da prova**, mas o responsável pelo tratamento deve aplicar as medidas adequadas para assegurar e poder comprovar que o tratamento é realizado em

b) que, embora tenham realizado o tratamento, não houve violação à legislação de proteção de dados; ou c) que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro (Art. 43). **Poderá haver a inversão do ônus da prova em favor do titular** (Art. 42, § 2º). Além disso, o agente deve demonstrar a observância e o cumprimento das normas de proteção de dados pessoais (Art. 6, X). **As ações de reparação por danos coletivos podem ser exercidas coletivamente em juízo** (Art. 42, § 3º). **Nas relações de consumo, aplicam-se as regras de responsabilidade previstas no Código de Defesa do Consumidor** (Art. 45).	conformidade com o Regulamento (Art. 24.°)
Medidas para garantir a segurança dos dados e o tratamento lícito	**Medidas para garantir a segurança dos dados e o tratamento lícito**
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. A autoridade nacional poderá dispor sobre padrões técnicos mínimos de segurança. (Art. 46). **Não há disposição específica no sentido de que a eficácia das medidas deve ser avaliada periodicamente.**	O responsável pelo tratamento e o subcontratante deverão adotar as medidas técnicas e organizativas adequadas destinadas a aplicar com eficácia os princípios da proteção de dados e a incluir as garantias necessárias para que o tratamento cumpra os requisitos do RGPD e assegure um nível de segurança adequado ao risco (Arts. 25.° e 32.°) **A eficácia dessas medidas deve ser testada, apreciada e avaliada regularmente.**
Privacy by design	***Privacy by design***
As medidas de segurança e tratamento adequado devem ser observadas desde a fase de concepção do produto ou do serviço até a sua execução (Art. 46, §2°).	As medidas de segurança e tratamento adequado devem ser observadas tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento (Art. 25.°, 1).
Privacy by default	***Privacy by default***
A LGPD não prevê, expressamente, a obrigação dos agentes de tratamento de garantirem a privacidade como padrão, contudo, numa análise sistemática da Lei, infere-se que a legislação brasileira também adota essa metodologia, como o próprio princípio da necessidade e da prevenção, que exige do controlador e do operador uma postura proativa e preventiva para evitar a ocorrência de danos aos titulares.	**O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por padrão**, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento (Art. 25.°, 2).
Relatório de Impacto à Proteção de Dados Pessoais	**Avaliação de Impacto sobre a Proteção de Dados**
Apenas faculta à autoridade nacional determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais (Art. 38). Também faculta à autoridade nacional solicitar relatório de impacto quando o tratamento tiver como fundamento o interesse legítimo ou quando for realizado pelo Poder Público (Art. 10, § 3º e art. 32). Deverá ser solicitado quando o tratamento de dados ocorrer para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais. Não estabelece outras hipóteses em que o relatório de	**Exige que o responsável pelo tratamento realize uma avaliação de impacto prévia sempre que o tratamento for suscetível de implicar um elevado risco para as pessoas singulares** (Art. 35). A avaliação de impacto é obrigatória quando o tratamento fizer uma avaliação sistemática, automatizada e completa de aspectos pessoais, servindo de base para a tomada de decisões que afetem o titular ou envolver dados sensíveis ou, ainda, tiver como fim o controle sistemático de zonas acessíveis ao público em grande escala. As autoridades de controle poderão publicar listas com operações de tratamento para as quais é ou não exigida

impacto é obrigatório. **A autoridade nacional poderá editar regulamentos e procedimentos sobre estes relatórios para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais (Art. 55-J, XIII).** **Não condiciona o início do tratamento de dados à consulta à autoridade nacional** a respeito do relatório de impacto em nenhuma hipótese. **Não solicita o parecer do encarregado**.	a avaliação de impacto. O **encarregado da proteção de dados deverá fornecer seu parecer** sobre a avaliação de impacto. **Quando a avaliação de impacto indicar que o tratamento de dados resultaria num elevado risco se não fossem tomadas medidas para atenuar o risco, o responsável deverá consultar a autoridade de controle antes de proceder ao tratamento** (Art. 36.°).
Consulta à autoridade nacional durante a elaboração de medida legislativa relacionada com o tratamento de dados	**Consulta à autoridade de controle durante a elaboração de medida legislativa relacionada com o tratamento de dados**
Não há qualquer exigência de que a autoridade nacional seja consultada sempre que houver uma proposta legislativa que esteja relacionada com o tratamento de dados pessoais.	**Exige que os Estados-Membros consultem a autoridade de controle durante a preparação de uma proposta** de medida legislativa ou de uma medida regulamentar **que esteja relacionada com o tratamento de dados** (Art. 36.°, 4).
Incidente de segurança	**Incidente de segurança**
Deverá ser comunicado à autoridade nacional e ao titular, pelo controlador, se acarretar risco ou dano relevante aos titulares (Art. 48). **A comunicação será feita em prazo razoável**, o qual será definido pela autoridade nacional. **Não há disposição expressa acerca da obrigação do operador comunicar o controlador quando identificar um incidente de segurança**. A comunicação deverá conter, dentre outras coisas, as medidas adotadas para minimizar os danos. **Não há obrigação de documentação de todas as violações de dados.** A LGPD não prevê exceções à obrigação de notificar os titulares dos dados quando verificado potenciais riscos a eles.	O responsável pelo tratamento deverá notificar o incidente à autoridade de controle **em até 72 horas**, se for suscetível de resultar em risco para pessoas singulares (Art. 33.°). **O subcontratante deve notificar o responsável pelo tratamento, sem demora injustificada, após ter conhecimento de uma violação de dados pessoais**. A notificação deverá conter, dentre outras coisas, as medidas adotadas para minimizar os danos. **Toda e qualquer violação de dados deve ser documentada pelo responsável pelo tratamento, ainda que não implique em risco aos titulares**. Quando a violação dos dados pessoais for suscetível de implicar um elevado risco para pessoas singulares, deve ser comunicada também aos titulares, sem demora injustificada e em linguagem clara e simples. Prevê exceções à obrigação de notificar os titulares dos dados quando verificado potenciais riscos a eles.
Regras de boas práticas e programas de governança	**Códigos de Conduta**
Incentiva que os agentes de tratamento, individualmente ou por meio de associações, formulem regras de boas práticas ou códigos de conduta e implementem programas de governança relacionados ao tratamento de dados pessoais, política de privacidade e ao atendimento de reclamações dos titulares (art. 50). Essas regras deverão ser publicadas e atualizadas periodicamente. Poderão ser reconhecidas e divulgadas pela autoridade nacional.	**Prevê que os Estados-Membros, as autoridades de controle, o Comité e a Comissão promoverão a elaboração de códigos de conduta** destinados a contribuir para a correta aplicação do RGPD, tendo em conta as características dos diferentes setores de tratamento e as necessidades específicas das micro, pequenas e médias empresas (Art. 40.°). Incentiva que associações e outros organismos representantes de categorias de responsáveis pelo tratamento ou de subcontratantes também elaborem códigos de conduta, os quais deverão ser aprovados pela autoridade de controle.

A adoção de política de boas práticas e governança será considerada quando da aplicação de sanções administrativas (Art. 52, § 1º, IX). Não estabelece os procedimentos a serem observados quando da elaboração e aprovação dos códigos de conduta, o que deverá ser regulamentado pela autoridade nacional.	Os códigos de conduta serão divulgados pelo Comitê Europeu para a Proteção dos Dados. A supervisão de conformidade com um código de conduta poderá ser efetuada por um organismo acreditado pela autoridade de controle (Art. 41.°). O cumprimento de códigos de conduta pode ser utilizado como elemento para demonstrar o cumprimento das obrigações do responsável pelo tratamento, bem como será considerado quando da aplicação de sanções administrativas (Art. 24.° e art. 41.°). Traz várias disposições acerca dos procedimentos envolvidos na aprovação e supervisão de um código de conduta.
Certificação e selos de proteção de dados	**Certificação e selos de proteção de dados**
Não há disposições acerca de procedimentos de certificação pelos quais os agentes de tratamento poderiam comprovar o cumprimento das normas da LGPD, o que não impede que a autoridade nacional institua esses procedimentos. No que diz respeito a países e organismos internacionais, prevê que estes poderão comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei por meio de selos, certificados e códigos de conduta regularmente emitidos, os quais serão verificados pela autoridade nacional ou por organismo de certificação designado pela autoridade (Arts. 33 e 35).	Os Estados-Membros, as autoridades de controle, o Comité e a Comissão promoverão a criação de procedimentos de certificação em matéria de proteção de dados, bem como selos e marcas de proteção de dados, para efeitos de comprovação da conformidade das operações de tratamento com o RGPD (Art. 42.°) A certificação não diminui a responsabilidade dos responsáveis pelo tratamento e subcontratantes pelo cumprimento do Regulamento. A certificação será emitida por organismos de certificação acreditados, pela autoridade de controle competente ou pelo Comitê Europeu para a proteção de dados. A certificação será emitida por um período máximo de três anos e poderá ser renovada.
Sanções administrativas	**Sanções administrativas**
Prevê uma série de sanções administrativas aplicáveis aos agentes de tratamento em razão de infração à LGPD, a saber: a) advertência; b) publicização da infração; c) bloqueio ou eliminação dos dados pessoais a que se refere a infração; d) suspensão parcial do funcionamento do banco de dados pelo período máximo de 6 (seis) meses, prorrogável por igual período; e) suspensão ou proibição de atividades de tratamento de dados. f) **aplicação de multa simples de até 2%** do faturamento do agente de tratamento limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração (art. 52) ou de multa diária, cujo montante total também deverá ser limitado a esse valor. Poderão ser aplicadas isolada ou cumulativamente, após procedimento administrativo que possibilite a oportunidade da ampla defesa.	As autoridades de controle poderão aplicar as seguintes sanções administrativas no caso de violação ao RGPD: a) advertência e repreensões; b) limitação temporária ou definitiva ao tratamento de dados; c) proibição de tratamento de dados; d) **aplicação de multa de até 20 000 000 EUR ou, no caso de uma empresa, até 4%** do seu volume de negócios anual, quando a infração disser respeito à violação das normas relacionadas aos princípios, às condições de consentimento, às bases legais de tratamento, aos direitos dos titulares, ao não cumprimento de ordem de limitação de tratamento de dados e outras ordens da autoridade de controle e às transferências internacionais. e) **aplicação de multa de até 10 000 000 EUR ou, no caso de uma empresa, até 2%** do seu volume de negócios anual, quando a infração disser respeito à violação das normas referentes ao tratamento de dados de criança e demais disposições do Regulamento que não geram aplicação da penalidade de multa mais grave. (Arts. 58.° e 83.°)

Não substitui a aplicação de sanções administrativas, civis ou penais definidas no Código de Defesa do Consumidor. Com exceção da sanção de multa, todas as demais penalidades poderão ser aplicadas às entidades e órgãos públicos. **Previsão de não aplicação das sanções caso haja acordo entre o controlador e o titular no caso de vazamentos ou acessos não autorizados que sejam individuais.**	**Os Estados-membros poderão estabelecer outras sanções, penais ou administrativas**. As sanções deverão ser efetivas, proporcionas, dissuassivas e **poderão, inclusive, prever a privação dos lucros auferidos em virtude da violação ao Regulamento** (art. 84.° e considerandos 149 e 152). As sanções poderão ser aplicadas isolada ou cumulativamente. Se houver mais de uma disposição do Regulamento violada no âmbito das mesmas operações de tratamento, o montante total da multa não pode exceder 20 000 000 EUR ou, no caso de uma empresa, até 4% do seu volume de negócios anual. **Não há previsão de conciliação direta entre o titular e o responsável pelo tratamento, mas as legislações de execução do RGPD podem possibilitar** que, em determinados casos de reclamações individuais, soluções amigáveis sejam mediadas pelas autoridades de controle e não sejam aplicadas sanções.
Autoridade Nacional de Proteção de Dados - ANPD	**Autoridades de controle**
Apesar de o Art. 55-B assegurar **autonomia técnica e decisória à ANPD**, a autoridade foi criada como **órgão da administração pública federal, integrante da Presidência da República, o que compromete a sua independência** (Art. 55-A). No entanto, a natureza jurídica da ANPD é transitória e poderá ser transformada, em até 2 anos da data da entrada em vigor da sua estrutura regimental, pelo Poder Executivo, em entidade da administração pública federal indireta, de modo que a ANPD ainda poderá vir a ter independência necessária a uma autoridade de controle. **Exige-se dos membros do Conselho Diretor da ANPD que tenham reputação ilibada, nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados** (art. 55-D, §2º). Para assegurar a autonomia de seus membros, aqueles que pertencerem ao Conselho Diretor terão mandato de 4 anos e somente perderão seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar (Arts. 55-D e 55-E). A ANPD tem funções fiscalizatórias, sancionatórias, regulatórias, educativas, de orientação, realização de auditorias e de recebimento e apreciação de reclamações dos titulares (Art. 55-J)	Estados-membros deverão estabelecer uma ou mais autoridades de controle (art. 51.°). **As autoridades de controle agem com total independência, não devendo seus membros ficar sujeitos a influencias externas no desempenho de suas funções** (art. 52.°). Os membros da autoridade de controle não poderão desempenhar qualquer ato ou atividade incompatível com as suas funções, independentemente de remuneração, e só serão exonerados se tiverem cometido uma falta grave ou se tiverem deixado de cumprir as condições exigidas para o exercício das suas funções (Arts. 52.° e 53.°). Cada Estado-membro estabelecerá a duração do mandato dos membros de cada autoridade de controle, mas este não poderá ser inferior a quatro anos (Art. 54.°). **Exigência de que cada membro da autoridade de controle possua os conhecimentos técnicos necessários ao desempenho das suas funções, nomeadamente no domínio da proteção de dados pessoais** (Art. 53.°). As autoridades de controle têm poderes de investigação, poderes de correção, poderes consultivos e de autorização, além de outros que os Estados-membros lhes atribuam (Art. 58.°).
Conselho Nacional de Proteção de Dados Pessoais e da Privacidade	**----------**
É o órgão consultivo da Autoridade Nacional de Proteção de Dados.	----------

Deve propor diretrizes estratégicas para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD e elaborar relatórios anuais de avaliação da execução das ações de tal Política (Art. 58-B). Também deve elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade, além de disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população (Art. 58-B).	
----------	**Comité Europeu para a Proteção de Dados**
----------	O RGPD cria o Comité Europeu para a Proteção de Dados (CEPD), um organismo europeu independente que contribui para a aplicação coerente de regras em matéria de proteção de dados na União Europeia e promove a cooperação entre as autoridades de proteção de dados da União Europeia (Art. 68.° a 76.°). Substitui o antigo Grupo de Trabalho do Artigo 29, que havia sido criado pela Diretiva 95/46/CE, a qual foi revogada pelo RGPD (Art. 94.°).
Avaliação periódica da legislação	**Avaliação periódica do Regulamento**
Não há previsão a esse respeito.	**A Comissão Europeia deverá apresentar, de 4 em 4 anos, ao Parlamento Europeu e ao Conselho, um relatório sobre a avaliação e revisão do RGPD**, apresentando propostas de alteração, se for o caso, que atenderão à evolução das tecnologias da informação e os progressos da Sociedade da Informação (art. 97.°).
Vacacio legis	***Vacacio legis***
Data de sanção: 14 de agosto de 2018. *Vacatio legis* sofreu diversas modificações, as últimas fixaram-na do seguinte modo: a) Em relação às sanções administrativas, a Lei entrará em vigor em 1° de agosto de 2021. b) Quanto às demais disposições, apesar da previsão de *vacatio legis* de 24 meses, a LGPD entrou em vigor um pouco depois disso, em 18 de setembro, data da publicação da Lei 14.058/2020, sem o conteúdo que dilatava a vacância.	Data de aprovação do Regulamento: 27 de abril de 2016. A partir de quando se tornou aplicável: 25 de maio de 2018.

Fonte: Elaborado pela autora.

De um modo geral, como se demonstrou durante todo o trabalho e ficou evidenciado no quadro comparativo, há forte convergência regulatória entre a Lei Geral de Proteção de Dados Pessoais e o Regulamento Geral de Proteção de Dados da União Europeia, mas também há algumas diferenças significativas.

O primeiro ponto a se destacar é que, até a interpretação de seus dispositivos ser amadurecida e consolidada, por meio dos trabalhos desenvolvidos pela doutrina, pela Autoridade Nacional de Proteção de Dados e pela jurisprudência, a LGPD irá suscitar muito mais dúvidas quanto à sua interpretação que o RGPD, vez que não apresenta nenhum norte interpretativo, tal qual o faz a lei europeia, bem como disciplina o tratamento de dados de

maneira mais genérica e principiológica, ao passo que o RGPD faz uma previsão mais detalhista e exaustiva. Essa característica da legislação brasileira, contudo, não é negativa, haja vista permitir que, por meio dos princípios, a LGPD seja aplicada a tecnologias ainda não existentes.

Ressalte-se, ainda, que mesmo com as décadas de discussão sobre privacidade, com as centenas de considerandos e com as disposições mais minuciosas, a aplicação do Regulamento da União Europeia não tem sido uniforme nos Estados-membros e tem levantado uma série de questionamentos quanto aos requisitos exigidos para a conformidade do agente de tratamento com o RGPD. Diante disso, no Brasil, a atuação da ANPD será de fundamental importância para guiar a implementação da Lei Geral de Proteção de Dados Pessoais, de modo a se garantir maior segurança jurídica aos agentes de tratamento e aos titulares dos dados.

Também no âmbito de aplicação das legislações, há uma previsão distintiva relevante. Como discutido na seção 3, ambas as legislações não fornecem a proteção mais adequada ao titular quando se trata dos dados anonimizados, visto que tanto a LGPD quanto o Regulamento europeu excluíram tais dados de sua abrangência material, contudo, diante dos riscos de reidentificação, a tutela da privacidade estaria mais bem garantida se estas leis tivessem se dedicado a fazer algumas poucas, mas essenciais previsões no intento de se minimizar tais riscos.

A título exemplificativo, as mencionadas leis de proteção de dados poderiam estabelecer que a caracterização de um dado como anonimizado deve ser contextual, exigindo a adoção de procedimentos que, periodicamente, reavaliem se, diante dos avanços tecnológicos, as técnicas de anonimização utilizadas ainda são razoavelmente seguras, bem como se, diante das bases de dados com que estes dados anonimizados podem ser combinados, o risco de reidentificação permanece tolerável.

De igual modo, a exigência de transparência no compartilhamento e uso de tais dados permitiria um maior monitoramento das autoridades de controle e da sociedade civil a respeito da possibilidade de reversão da anonimização, em especial por meio da associação de bancos de dados.

Apesar disso, em contraste com o RGPD, a LGPD traz algumas valiosas disposições relacionadas à anonimização. Nesse sentido, enquanto o Regulamento europeu não estimula nem ao menos menciona a anonimização como uma técnica de segurança de dados pessoais, a lei brasileira busca incentivar o uso de tal medida, estabelecendo que a anonimização deve ser garantida, sempre que possível, quando dados pessoais forem tratados para a realização de

estudos por órgãos de pesquisa (art. 7º, IV e art. 11, II) , bem como possibilitando ao titular solicitar a anonimização – se não preferir optar pelo bloqueio ou pela eliminação – de seus dados que sejam desnecessários, excessivos ou tratados em desconformidade com a Lei (art. 18, V).

Ademais, a LGPD, diferentemente do RGPD, prevê que os dados anonimizados poderão ser considerados como dados pessoais se forem utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada (art. 12, §2°), hipótese em que se aplica a lei brasileira. Contudo, uma vez que o referido artigo utilizou a expressão "identificada", haverá, ainda, consoante discutido anteriormente, muita discussão acerca do alcance desse dispositivo, já que, a interpretação literal do aludido artigo retira do âmbito de aplicação da LGPD inúmeras situações em que ao indivíduo são atribuídos perfis de grupo e suas respectivas consequências.

Necessário, pois, adotar uma interpretação sistemática da lei e numa perspectiva civil-constitucional que considere que, de acordo com os fundamentos e objetivos da LGPD, a expressão identificada deve considerar não somente se um indivíduo pode ser identificado a partir daquele dado, mas se o uso do dado para a formação de perfil comportamental será capaz de atingir uma pessoa específica. Nessa senda, mais uma vez se destaca o importante papel da Autoridade Nacional, que poderá firmar sua compreensão sobre o tema, auxiliando a resolução das eventuais dúvidas a esse respeito.

De todo modo, em que pese a aplicação da Lei Geral de Proteção de Dados Pessoais aos dados anonimizados utilizados para a formação de perfis comportamentais ainda precise se firmar, tal disposição, assim como o incentivo ao uso da anonimização, oferece, nesse ponto, uma tutela mais conveniente aos indivíduos que o Regulamento Geral de Proteção de Dados da União Europeia.

No que atine às definições de dados pessoais e de dados pessoais sensíveis, o Regulamento europeu traz conceitos mais detalhados que a LGPD, dando vários exemplos do que pode ser considerado pessoa identificável. Também quanto aos dados sensíveis, conforme demonstrado, uma definição combinada do artigo 9º e do Considerando 51 do RGPD permite, com menos dificuldade que no Brasil, uma interpretação extensiva que acabe por alcançar outras informações pessoais cujo contexto de tratamento possa implicar sérios riscos aos direitos fundamentais do indivíduo, diferentemente das disposições da LGPD.

Ilustrativamente, a simples informação de que um candidato a uma de emprego é morador de comunidade pode levar à sua exclusão do processo seletivo por parte do recrutador, uma vez que ainda há muito preconceito com tais indivíduos. A esse respeito, um

levantamento feito com 3.050 pessoas de 150 cidades do Brasil revelou que 47% das pessoas que não moram em comunidade jamais contratariam uma pessoa que vivesse em favela para trabalhar em sua casa. Por esta razão, há muitos trabalhadores que não informam explicitamente ao empregador que residem em comunidade[630].

Este é um exemplo de um dado que embora, historicamente, não seja considerado suscetível de gerar riscos aos direitos fundamentais do titular, o contexto de seu tratamento possibilita grave discriminação ao indivíduo, razão pela qual esta informação pessoal poderia vir a ser considerada sensível. Contudo, como visto, uma vez que a LGPD traz um rol taxativo do que é considerado dado pessoal sensível, uma interpretação neste sentido se mostra tarefa mais árdua do que exigiria a aplicação do RGPD.

Note-se que o mencionado tratamento de dados é capaz de gerar mais riscos aos direitos individuais que certos tratamentos dos dados considerados sensíveis por natureza. Por exemplo, a coleta de dados relacionados à religião de alunos de uma escola com a única finalidade de incluir conteúdo de diversas crenças nas aulas de religião – e sendo observados os demais princípios e normas da Lei 13.709/2018, inclusive quanto à eliminação de dados pessoais – é menos suscetível de gerar discriminação do que a informação de que o candidato ao posto de trabalho é um morador de comunidade.

Diante disso, vez que a LGPD não dá margem para uma definição funcional de dado sensível, o indivíduo, mesmo em algumas situações que exigiriam o tratamento especial de determinados dados pessoais, não receberá a tutela mais adequada. Melhor seria, pois, que a classificação de um dado como sensível ou não fosse dinâmica e contextual, a partir da consideração do uso que se fará dos dados e de quais as inferências que se pode obter a partir deles.

Ao menos no que atine à possibilidade de se fazer inferências sensíveis a partir do tratamento de dados pessoais que, a princípio, não são considerados sensíveis, consoante discutido na seção 3 deste trabalho, o artigo 11, §1º, da LGPD prevê que as disposições relativas ao tratamento de dados pessoais sensíveis se aplicam a qualquer tratamento de dados que acabem por revelar algum daqueles dados previstos no rol taxativo da Lei do artigo 5º, II, o qual define os dados que integram essa categoria especial, e que possam causar dano ao titular.

---

630 GANDRA, Alana. Moradores do asfalto têm visão preconceituosa de favelas, mostra pesquisa. **Agência Brasil**, Rio de Janeiro, 16 fev. 2015. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2015-02/moradores-do-asfalto-tem-visao-preconceituosa-em-relacao-favelas. Acesso em: 26 maio 2021.

Neste ponto, tutela a questão de uma melhor forma que o Regulamento europeu, tendo em vista que este não traz uma disposição semelhante de modo expresso, cabendo à atividade hermenêutica a possibilidade de extensão das normas voltadas ao tratamento de dados sensíveis aos processamentos de dados pessoais que permitam ao agente de tratamento obter um conhecimento sensível sobre o titular.

No que toca aos princípios previstos em ambas as legislações, há forte similaridade entre estes, decorrente de todo o processo de convergência regulatória exposto na seção 3. Entrentanto, como visto, a LGPD expressamente prevê o princípio da não discriminação, robustecendo a obrigação de os agentes de tratamento observarem se a finalidade para a qual os dados estão sendo processados possuem algum caráter discriminatório, ainda que não intencional, de modo que os controladores, em especial aqueles que não contam com uma assessoria jurídica, são alcançados por esta limitação à sua atividade sem precisarem recorrer à Constituição Federal ou a métodos interpretativos, o que fortalece a proteção do titular. Além disso, tal preceito fortalece o aspecto proativo do princípio: não basta que o fim não seja discriminatório, é preciso testar e avaliar todo o processo de tratamento com o intuito de evitar a discriminação.

Já o RGPD, apesar de uma interpretação sistemática revelar que a legislação também não permite o tratamento discriminatório, ao deixar de trazer previsão semelhante, deixa de fortificar a mensagem de que evitar este tipo de resultado deve ser objetivo de todo agente de tratamento. Neste particular, os considerandos do Regulamento adquirem especial relevância, ao menos quanto às decisões automatizadas baseadas em *profiling*, ao estabelecerem que os responsáveis pelo tratamento deverão corrigir fatores que causem imprecisões nos dados ou eventuais erros, além de prevenir que o tratamento de dados tenha efeitos discriminatórios, máxime no que atine aos dados sensíveis do titular.

Também as bases legais que justificam o tratamento dos dados pessoais, apesar de algumas peculiaridades, são bastante semelhantes. Acerca do consentimento, tanto a LGPD quanto o RGPD trazem disposições bem próximas, com destaque para o fato de que ambas as legislações adotaram o modelo *opt-in* para fornecimento da aquiescência para o tratamento de dados pessoais, privilegiando, assim, a autodeterminação informativa do titular.

O Regulamento europeu, contudo, já assentou alguns critérios relacionados à manifestação e à liberdade do consentimento, estabelecendo, por exemplo, que opções pré-validadas não constituem consentimento, bem como que não há liberdade de consentimento quando o fornecimento deste, apesar de não ser necessário, for condição para a prestação de um serviço. Por seu turno, a LGPD dá um tratamento mais genérico quanto à liberdade e

expressão do consentimento, apesar de enfatizar que as autorizações genéricas não serão consideradas nulas, previsão esta que reforça a proteção do titular.

Dessa feita, o RGPD traz uma disciplina mais rígida sobre a questão que a lei brasileira, deixando menos margem para que os agentes de tratamento utilizem determinados artifícios para que o titular seja sutilmente compelido a fornecer seu consentimento, tal como os mencionados pelo Regulamento. A autoridade nacional, então, deverá emitir diretrizes acerca da aquiescência do titular com o tratamento de dados que servirão de parâmetro para a atuação dos agentes de tratamento, aumentando a segurança jurídica para estes e para o titular dos dados. De toda forma, no Brasil, os agentes de tratamento deverão observar os princípios de proteção de dados, como o da prevenção e o da responsabilidade, para pautar sua conduta relacionada à obtenção da concordância do indivíduo.

A respeito da disciplina dos dados sensíveis, em que pese a lei brasileira e o Regulamento europeu tenham utilizado técnicas legislativas distintas, já que este último estabelece uma proibição geral ao passo que a LGPD apenas estabelece regras mais restritivas para o tratamento desses dados, ambas as legislações fornecem uma tutela semelhante e adequada ao tratamento desses dados, ressaltando-se as limitações proporcionadas pela definição de quais informações integram essa categoria, acima mencionadas.

No entanto, a Lei Geral de Proteção de Dados Pessoais vai além da proteção conferida pelo RGPD, tendo em vista que faz pertinentes proibições relativas ao tratamento de dados de saúde, vedando o seu compartilhamento com a única finalidade de os agentes de tratamento obterem vantagem econômica, bem como o seu uso por operadoras de plano de saúde para fins de seleção de risco, contratação ou exclusão de beneficiários. Ainda, atribui à autoridade nacional poderes para proibir ou regulamentar o compartilhamento entre controladores, com fins predominantemente econômicos, de outros dados sensíveis.

O Regulamento europeu, por sua vez, deixa a cargo dos Estados-membros imporem novas limitações quanto ao tratamento de dados genéticos, biométricos ou relativos à saúde, se assim o desejarem, de modo que as legislações de execução do RGPD dos membros da União Europeia poderão ser mais ou menos protetivos quanto à disciplina aplicável a tais dados sensíveis. Desse modo, além de não garantir que o titular dos dados receba a tutela mais apropriada, máxime quanto ao tratamento de seus dados de saúde, já que o nível de proteção dependerá das legislações internas que forem aprovadas pelos Estados-membros, ao não traçar as restrições, o RGPD permite que as normas sobre o tratamento desses dados sensíveis não sejam uniformes nesses Estados, o que pode dificultar a adequação de agentes de tratamento que processam dados de indivíduos de diferentes países ao Regulamento.

Acerca da proteção às crianças e adolescentes no contexto de tratamento dos dados, verifica-se uma das poucas questões em que a Lei Geral de Proteção de Dados se preocupa em dispensar uma disciplina mais detalhada do que o disposto na RGPD. Nesse sentido, expressamente proíbe que a participação da criança em jogos, aplicações da *internet* ou qualquer outra atividade seja condicionada ao fornecimento de dados pessoais não necessários à atividade, num esforço legislativo para evitar que os controladores exijam a entrega de tais dados, e aleguem, posteriormente, que o responsável pelo menor consentiu com o respectivo tratamento.

Dessa feita, a Lei brasileira reconhece a vulnerabilidade das crianças, as quais, sem estarem plenamente ciente dos riscos e implicações do fornecimento de seus dados pessoais, são mais suscetíveis de cederem a tal exigência – ou de exercerem forte pressão sobre seus pais para que o façam por eles – para poderem ter acesso aquele jogo ou aplicação que faz o maior sucesso entre as pessoas de sua idade. Dessa forma, adequadamente, a LGPD restringe o exercício da autodeterminação informativa, prevendo uma proibição que não pode ser derrogada pelo consentimento. Outrossim, uma vez que a Lei brasileira não traz, de modo expresso, outras hipóteses em que se presume que o consentimento não fora dado livremente, a referida previsão é especialmente relevante.

Já no que concerne ao Regulamento europeu de proteção de dados, não se observa disposição semelhante à proibição trazida pela LGPD e, em que pese preveja que o consentimento não se presume livre quando fornecido sob condição de acesso a um produto ou serviço, esta previsão ainda deixa margem para que os agentes de tratamento contornem essa presunção. Exemplificativamente, um desenvolvedor de jogo pode oferecer uma versão paga do aplicativo, em que não há coleta de dados pessoais além dos necessários, e uma versão gratuita, em que se exige a aquiescência quanto à recolha e ao processamento de informações da criança ou adolescentes que não essenciais à execução do jogo, de modo a alegar que, nesse caso, o consentimento foi dado livremente, já que, podendo escolher, o responsável – ou o próprio adolescente, quando já tiver idade para consentir – optou por participar do jogo por meio da versão em que havia a coleta de diversos dados pessoais. Nesse caso, ainda que o consentimento do responsável possa ser qualificado como livre, verifica-se que não há observância do melhor interesse da criança ou do adolescente.

Isso posto, a proibição estabelecida pela Lei brasileira se mostra mais eficaz para resguardar os direitos dos menores na sociedade da informação que o Regulamento europeu. Ademais, diferentemente deste, a LGPD reforça a necessidade de transparência em relação ao

tratamento de dados de tais indivíduos, com destaque para a previsão de que as informações devem ser compreensíveis pelas crianças.

Também, a LGPD exige que o controlador realize todos os esforços razoáveis para verificar que o consentimento realmente foi dado pelo responsável e não pela criança, exigência esta para a qual não há correspondência no RGPD.

Dessa feita, a LGPD protege mais efetivamente as crianças e adolescentes no que diz respeito ao tratamento de dados pessoais na sociedade da informação do que o Regulamento Geral de Proteção de Dados da União Europeia.

No que se refere aos direitos do titular, como visto, também se verifica forte convergência entre a LGPD e o Regulamento Geral de Proteção de Dados da União Europeia, entretanto, o RGPD faz um detalhamento bem maior de cada um desses, aumentando a compreensão de tais direitos por aqueles que deles farão uso. Outrossim, ao menos quanto ao direito de objeção e de revisão de decisões automatizadas, o Regulamento estabelece mais salvaguardas aos indivíduos que a legislação pátria.

Dessa feita, em que pese sejam bastante semelhantes, a disciplina dos direitos do titular do RGPD se mostra, em algum grau, mais protetiva ao indivíduo que a lei brasileira. Saliente-se que estes direitos são muito importantes, pois são os instrumentos oferecidos aos titulares para a defesa de sua privacidade.

Nessa senda, a LGPD, assim como o Regulamento europeu, prevê um direito à oposição, mas de modo mais genérico, estabelecendo apenas que o titular pode se opor a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento das disposições da referida Lei.

Dessa feita, o direito previsto na legislação pátria restringe consideravelmente as possibilidades do titular dos dados se opor a determinado tratamento, vez que exige que este processamento esteja em desacordo com o disposto pela LGPD, o que, por seu turno, já tornaria o respectivo tratamento ilícito, permitindo, por conseguinte, que o indivíduo tomasse medidas para fazer cessar o processamento de seus dados, mesmo na ausência de previsão do direito à oposição.

Já o Regulamento europeu tutela de maneira mais adequada a autodeterminação informativa do titular, ao lhe garantir maior controle sobre as hipóteses em que seus dados serão tratados, permitindo-lhe, inclusive, opor-se ao processamento de dados com base no legítimo interesse do responsável pelo tratamento, a menos que este apresente razões imperiosas e fundamentadas para o processamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados.

De igual forma, o RGPD expressamente estabelece que o titular pode se opor ao tratamento de seus dados para fins de marketing direto, ao passo que a LGPD não traz idêntica previsão. Por conseguinte, a lei brasileira não deixa claro aos indivíduos nem aos agentes de tratamento que, ainda que a oferta de promoções e de determinados produtos ou serviços tenha base jurídica para o respectivo tratamento diversa do consentimento e mesmo que tal base seja lícita – a exemplo das hipóteses em que seja possível embasar uma ação de marketing direto no legítimo interesse do controlador –, deve ser oportunizado ao titular o direito de oposição.

Isso posto, além de gerar insegurança jurídica a respeito de o indivíduo poder ou não se opor ao tratamento de dados para fins de marketing direto, sendo necessário recorrer a outras previsões da LGPD para tanto, como os direitos à privacidade e à autodeterminação informativa, os quais são objetivo e fundamentos da Lei, a lacuna legislativa pode prejudicar o conhecimento do titular acerca da possibilidade de fazer uso desse remédio. Necessário, pois, a atuação da Autoridade Nacional de Proteção de Dados Pessoais também nesse ponto, orientando os agentes de tratamento a como adequarem suas ações de marketing direto à LGPD, bem como educando os indivíduos acerca de seus direitos.

Também como já estudado, o Regulamento europeu assegura ao indivíduo o direito de não ficar sujeito a uma decisão que o afete de forma significativa e que seja baseada exclusivamente em processamento automatizado, estabelecendo, assim, uma proibição geral a utilização desse tipo de decisão pelos responsáveis pelo tratamento, a qual poderá ser transposta se verificada uma das exceções definidas pelo RGPD.

Ademais, o mencionado Regulamento garante ao titular das informações o direito de obter uma intervenção humana por parte do responsável pelo tratamento – com o objetivo de revisar a decisão ou explicar porque ela é adequada – ou, ao menos, manifestar o seu ponto de vista e contestar a decisão, quando, em decorrência de uma das exceções previstas, este for submetido a uma decisão tomada unicamente com base em um tratamento automatizado de seus dados,

Já a legislação pátria, além de não estabelecer referida proibição, apenas assegura ao indivíduo o direito de solicitar a revisão de decisões tomadas exclusivamente baseadas no tratamento automatizado de seus dados pessoais, mas não garante que tal revisão seja feita por uma pessoa natural. Nessa esteira, não tutela, da forma mais apropriada, o titular dos dados, tendo em vista que, diante de todos os riscos envolvidos nesse tipo de tratamento e dos fatores que podem influenciar negativamente o resultado do processamento automatizado (expostos na seção 4 deste trabalho), uma revisão que ocorra de maneira também automatizada não

assegura que tais fatores sejam corrigidos nem que a decisão seja tomada com fundamento nas caraterísticas e méritos individuais do titular e não pelas características do grupo a que pertence.

Entretanto, para minimizar tais ameaças, a LGPD prevê o direito à explicação, alusivo aos critérios e procedimentos utilizados para a decisão automatizada, bem como prescreve a possibilidade de a autoridade nacional realizar auditorias para a verificação de aspectos discriminatórios no tratamento automatizado de dados pessoais.

Por fim, ainda tratando dos direitos do titular, difere o RGPD da Lei brasileira ao prever expressamente o direito ao esquecimento, enquanto que a Lei Geral de Proteção de Dados Pessoais não utiliza tal denominação, entretanto, a Lei brasileira traz disposições que dizem respeito ao direito ao apagamento, que é uma categoria do direito ao esquecimento. Outrossim, abre margem para o reconhecimento de outros duas categorias desse direito: o direito à desindexação e o direito ao esquecimento dos dados recolhidos na sociedade da informação (conforme discutido na seção 3).

Importa dizer, ainda, que ambas as legislações buscaram tornar os direitos acessíveis aos titulares dos dados, prevendo que estes devem poder ser exercidos sem custo ao indivíduo, mas com duas peculiaridades.

A primeira delas é que o RGPD preceitua que se pedidos forem manifestamente infundados ou excessivos, nomeadamente por serem repetitivos, o responsável pelo tratamento poderá se recusar a dar seguimento à solicitação ou exigir o pagamento de uma taxa razoável para o cumprimento do pleito, enquanto a LGPD se preocupa em fortalecer o uso destes remédios legais pelo titular, não prevendo exceções à gratuidade e evitando que os controladores possam criar obstáculos ao exercício dos direitos previstos sob o argumento de que não teriam fundamento, por exemplo.

A segunda, é que o RGPD estende a gratuidade, nos termos acima, ao exercício de todos os direitos expressamente previstos pelo Regulamento, ao passo que a legislação pátria apenas prevê o requerimento gratuito em relação aos remédios elencados em seu artigo 18, o que deixa de fora dois direitos de suma importância num contexto de tratamento de dados cada vez mais automatizado: o direito à explicação e o direito à revisão de decisões automatizadas que afetem o titular.

Isso posto, embora tanto a LGPD quanto o Regulamento europeu de proteção de dados disponham de modo semelhante acerca dos direitos do titular, estabelecendo praticamente as mesmas garantias, a sua disciplina encontra peculiaridades em ambas as legislações, as quais, em alguns pontos, tornam o RGPD mais protetivo que a lei brasileira no que se refere a

assegurar a autodeterminação informativa do indivíduo, bem como à sua tutela frente aos riscos impostos pelo *profiling* e pelas decisões automatizadas, o que reflete as décadas de amadurecimento do direito à proteção de dados pelo qual passou a Europa.

Com relação à defesa dos interesses e dos direitos dos titulares dos dados em juízo, a LGPD prevê que esta poderá ser exercida individual ou coletivamente, por meio dos legitimados, inclusive sendo possível o pleito de danos coletivos. Esta previsão é de fundamental importância para a efetividade da legislação, tendo em vista o contexto de assimetria técnica, financeira e informacional em que a maior parte das violações à proteção de dados acontecem, de modo que, se somente o próprio titular do dado pudesse demandar o Judiciário, muitas vezes este deixaria de fazê-lo, máxime pela falta de conhecimento. Ademais, nas hipóteses que uma mesma violação de dados pessoais ou infração à LGPD atingisse inúmeros titulares, a defesa individual de cada um deles assoberbaria, ainda mais, o Judiciário.

Nesse diapasão, a defesa coletiva do direito à proteção de dados pessoais será, em muitas situações, o instrumento mais adequado para resguardar a privacidade dos titulares, tendo os legitimados para tanto, como o Ministério Público, meios mais adequados para litigar contra grandes agentes de tratamento, pleiteando tutelas inibitórias, quando for o caso, ou medidas para ressarcir os prejuízos causados.

Outrossim, em mais uma relevante medida para diminuir o desequilíbrio entre as partes, a Lei Geral de Proteção de Dados Pessoais prevê que, no processo civil, o juiz poderá inverter o ônus da prova a favor do titular dos dados quando a alegação for verossímil, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa., reforçando uma garantia já existente no Código de Defesa do Consumidor e no Código de Processo Civil.

Por sua vez, o RGPD também prevê a tutela coletiva dos interesses dos titulares dos dados, mas de forma mais tímida. Assim, poderá ocorrer mediante representação, quando o titular poderá mandatar uma organização ou associação para apresentar uma reclamação à autoridade de controle em seu nome ou para pleitear o exercício de seus direitos, administrativa ou judicialmente, bem como para pedir indenização por danos materiais ou morais, se o direito do Estado-membro permitir tal ação por meio de representante.

De igual forma, o Regulamento dispõe que os Estados-Membros poderão prever que uma organização ou associação apresente uma reclamação à autoridade de controle ou demande judicialmente na defesa do titular, mesmo sem o mandato deste. Não há, contudo, nesta disposição, referência à possibilidade de se pleitear indenização por danos materiais ou

morais, o que não exclui a possiblidade de que as legislações internas dos países membros atribuam tal possibilidade aos seus instrumentos de tutela coletiva.

Isso posto, ao deixar a cargo dos Estados-membros a defesa coletiva dos interesses e direitos dos titulares que não exige representação, o Regulamento europeu deixa de obrigá-los a oferecer este importante instrumento de tutela da privacidade dos indivíduos, permitindo que, em países onde não haja tal previsão, o titular somente seja protegido diante de uma infração ao RGPD se tomar conhecimento do fato e, ainda, procurar uma associação ligada à defesa e liberdades dos direitos dos tilares para mandatá-la ou se, individualmente, acionar os mecanismos administrativos e judiciais que lhe são postos à disposição. Nesse cenário, diante da assimetria informacional e desequilíbrio de poder entre os agentes de tratamento e os titulares dos dados, dificultar a defesa coletiva dos interesses de tais indivíduos significa reduzir a efetividade de aplicação do Regulamento.

Observa-se, assim, que o RGPD é menos robusto neste ponto que a lei brasileira, o que pode prejudicar sua efetividade nos países que não contem com processos de ação coletiva e que não desejem institui-los.

Por fim, ainda no que concerne aos direitos do titular, a LGPD, contrariamente ao Regulamento europeu, traz mais uma importante previsão: a de que o exercício de tais remédios não poderá ser utilizado em seu prejuízo, encorajando os indivíduos a exigir seus direitos, bem como densificando uma faceta do princípio da não discriminação e, por conseguinte, aumentando a segurança jurídica a esse respeito.

No que atine à transferência internacional de dados, há uma distinção relevante entre as duas legislações analisadas: o Regulamento europeu estabelece que a manutenção da garantia do nível de proteção adequado de um país ou de organismo internacional deve passar por uma avaliação periódica, assegurando que, mesmo com todos os avanços tecnológicos e com os novos desafios que se impõem ao direito à proteção de dados, as informações dos titulares não serão enviadas a organismos que não consigam oferecer garantias adequadas de acordo com os parâmetros do RGPD. A mesma segurança ao titular não é conferida pela Lei brasileira, já que esta não estabelece a obrigação de se avaliar regularmente a conservação do nível de proteção adequado de um país ou organismo internacional.

Para possibilitar a fiscalização, pelas autoridades de controle, do tratamento de dados quanto ao cumprimento das normas de proteção de dados pessoais, ambas as legislações impõem aos agentes de tratamento a obrigação de manterem um registro de todas as operações de processamento de informações pessoais que realizarem.

No tocante à contratação do operador, o RGPD disciplina mais detalhadamente a relação entre o responsável pelo tratamento e o subcontratado, no intento de garantir que o responsável apenas recorra a subcontratantes que cumpram o Regulamento. Também há uma preocupação em evitar que as atividades contratadas sejam repassadas a outro subcontratante sem que o responsável possa averiguar o seu nível de conformidade com o RGPD. Estas disposições intentam assegurar uma cadeia de tratamento de dados que, do início ao fim, proteja o titular de tais informações.

Por seu turno, a LGPD não traz regras específicas a esse respeito, entretanto, em respeito ao princípio da prevenção e sob pena de responsabilização solidária se o titular vier a sofrer danos em decorrência da atuação do operador, é prudente que o controlador, antes da contratação, observe o grau de adequação à legislação pátria do contratado para realizar o tratamento de dados em seu nome.

No que tange à figura do encarregado de proteção de dados, tanto a LGPD quanto o RGPD, com suas peculiaridades, estabelecem a obrigação dos agentes de tratamento designarem este profissional, o qual, em razão de suas funções, terá um importante papel na implantação da cultura de privacidade nas organizações, no cumprimento das referidas legislações e no relacionamento dos titulares com estes agentes de tratamento no que se refere às suas reclamações relacionadas à proteção de dados.

Desse modo, esta obrigação é fundamental para o alcance do objetivo de prevenção de danos que ambas as leis carregam, vez que, em que pese prevejam sanções administrativas e responsabilização civil, o objetivo primeiro da LGPD e do Regulamento europeu de proteção de dados é evitar que a privacidade do indivíduo seja violada pelos tratamentos de dados pessoais e, para tanto, é necessário sensibilizar e orientar as organizações quanto aos direitos dos titulares e requisitos das legislações de proteção de dados para que, desde o projeto de cada produto ou serviço, a privacidade do indivíduo seja considerada em todo esse processo.

Ressalte-se que, no Brasil, a autoridade nacional poderá estabelecer normas complementares quanto às atribuições desse profissional, fortalecendo sua relevância no que atine à aplicação da LGPD pelas organizações, enquanto que, no RGPD, já um detalhamento maior acerca das funções do encarregado e da sua relação com o responsável pelo tratamento e com o subcontratado.

No entanto, também diferentemente do Regulamento europeu, a lei brasileira estabelece a obrigação de designar um encarregado da proteção de dados apenas para o controlador, de modo que aos operadores, embora seja aconselhável que o façam, não há essa

imposição, o que pode distanciar esse agente de tratamento da cultura de privacidade que se intenta criar no país.

Acerca da segurança no tratamento dos dados pessoais, a Lei Geral de Proteção de Dados Pessoais e o RGPD impõem aos agentes de tratamento o dever de adotarem medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de incidentes de segurança e qualquer forma de tratamento ilícito, mas o Regulamento europeu vai além, estabelecendo que a eficácia dessas medidas deve ser testada, apreciada e avaliada regularmente, tendo em vista que o surgimento de novas tecnologias podem tornar ineficaz uma medida de segurança anteriormente considerada apta.

Outrossim, de acordo as duas legislações estudadas, tais medidas devem ser empregadas desde o projeto do produto ou serviço até a sua execução (*privacy by design*). Também a ideia de que a privacidade deve ser protegida por padrão (*privacy by default*) é por elas adotada: expressamente, no caso do RGPD e por meio da aplicação dos princípios de proteção de dados, no caso da LGPD. Nesse cenário, o titular é protegido durante todo o tratamento a que seus dados é submetido sem que tenha que tomar nenhuma atitude para proteger sua privacidade, de forma que, independentemente do nível de conhecimento do indivíduo sobre seus direitos e do seu comportamento, o titular deverá estar resguardado pelas garantias previstas em ambas as legislações e pelas obrigações que estas impõem aos agentes de tratamento.

Concernente ao relatório de impacto à proteção de dados pessoais, há uma diferença sobressalente. O RGPD estabelece circunstâncias em que este documento deve ser elaborado de maneira prévia e obrigatória, bem como impõe a obrigação de o responsável consultar a autoridade de controle antes de proceder ao tratamento de dados sempre que a avaliação de impacto indicar que o tratamento poderá resultar em elevado risco aos titulares caso não sejam tomadas medidas para mitigar tal ameaça. Desse modo, na legislação europeia a avaliação de impacto é um importante instrumento para possibilitar que a autoridade de proteção de dados possa fazer um controle preventivo da operação e emitir orientações para que o tratamento se adeque ao Regulamento.

Já a LGPD dispõe que a autoridade nacional poderá solicitar que o controlador elabore o relatório de impacto à proteção de dados pessoais, de modo que, ao menos até que ANPD, no âmbito de suas competências, regulamente as hipóteses em que o controlador deverá preparar esse documento, a elaboração do relatório de impacto, mesmo em caso de operações com elevados riscos aos direitos dos titulares envolvidos, é uma faculdade e dependerá da iniciativa da autoridade nacional para requisitá-la.

Outrossim, não há obrigação de que o relatório de impacto seja prévio à realização do tratamento. Nessa senda, observa-se que o RGPD dispõe que sempre que um tratamento de dados puder implicar um risco para o titular, o responsável pelo tratamento deverá fazer uma avaliação do impacto das operações com o objetivo de verificar se há ou não risco, quais são esses riscos, quais medidas podem ser tomadas para atenuá-los e se essas medidas são eficazes. Somente depois de feita a referida avaliação, se não for o caso de consultar a autoridade de controle, é que o responsável poderá dar início ao tratamento.

Por sua vez, a LGPD, ao dispor sobre esse instrumento, prescreve que o relatório é a 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, sem fazer qualquer menção à necessidade de a elaboração desse documento ser prévia ao tratamento de dados. Da forma como previsto, o relatório de impacto se mostra mais voltado para atender eventual fiscalização da ANPD do que a ser um instrumento de prevenção de danos. Inclusive, o próprio termo "relatório", distintamente do que é utilizado pelo RGPD ("avaliação"), sugere uma exposição de um fato passado, de um tratamento que já ocorreu, do que uma análise acerca de uma operação que ainda virá a ser realizada.

Para reforçar essa ideia, também não há, na Lei Geral de Proteção de Dados Pessoais, qualquer obrigação do controlador consultar a autoridade nacional quando seu relatório identificar elevados riscos para o titular, de modo que, neste ponto, a ANPD não exerce uma atividade preventiva antes de operações de tratamento que representem séria ameaça aos direitos do indivíduo terem início.

É evidente que, uma vez que o controlador deve ser capaz de demonstrar que está em conformidade com a LGPD, o relatório de impacto deverá ser um instrumento muito utilizado por tais agentes de tratamento, inclusive de maneira prévia, com o objetivo de verificarem o nível de adequação do tratamento com a referida lei e, assim, evitarem a aplicação de sanções e a responsabilização civil por eventuais danos, contudo, tal qual disposto, o relatório de impacto se mostra muito mais frágil enquanto recurso de mitigação de riscos que a avaliação de impacto prevista no RGPD. Caberá a ANPD, pois, o relevante papel de, ao editar regulamentos e procedimentos sobre os relatórios de impacto, conforme previsto no artigo 55-J, XIII, robustecer a utilização desse documento pelos agentes de tratamento no intento de prevenir lesões aos titulares dos dados.

Ainda sobre os deveres de consulta à legislação, o RGPD exige que os Estados-Membros consultem a autoridade de controle durante a preparação de uma proposta de

medida legislativa ou de uma medida regulamentar que esteja relacionada com o tratamento de dados, obrigação esta que é essencial para a tutela do indivíduo, vez que assegura que a proposta esteja de acordo com o direito à proteção de dados, além de fazer uma análise prévia de ponderação dos interesses visados pela nova legislação e o direito à privacidade, evitando posterior judicialização caso a nova lei aprovada não observe os princípios de proteção de dados pessoais.

Nesse particular, basta lembrar as várias medidas legislativas em todo o mundo que envolveram o tratamento de dados pessoais no combate à pandemia de COVID-19. Com a exigência de se consultar a autoridade nacional acerca das propostas de lei, há uma maior probabilidade de que as medidas aprovadas pelos Estados-membros respeitaram os princípios aplicáveis ao tratamento de dados, harmonizando o interesse público com os direitos fundamentais dos indivíduos.

No Brasil, embora esta exigência seja de fundamental relevância, não há previsão semelhante, de modo que é possível que, futuramente, sejam aprovadas leis relacionadas ao tratamento de dados sem que a autoridade nacional tenha sido consultada, cabendo a esta última fiscalizar, com base na LGPD, as operações de processamento referentes à legislação aprovada e, ao Judiciário, fazer o controle das novas disposições, declarando-as inconstitucionais, caso violem o direito à proteção de dados pessoais. Dessa feita, como tais ações são a *posteriori,* o indivíduo ficará submetido à aplicação de uma lei que viola seus direitos até que a atuação da ANPD ou do Judiciário faça cessar esta ofensa.

No que diz respeito às violações de dados pessoais, mesmo com algumas particularidades investigadas na seção anterior, a disciplina destes incidentes de segurança é bem semelhante em ambas as legislações, mas, seguindo sua técnica legislativa, o RGPD também é mais detalhista neste ponto.

Além disso, há um ponto que merece destaque especial: o Regulamento europeu exige que toda e qualquer violação de dados seja documentada, ainda que não implique riscos ao titular, o que permite às autoridades de controle manter um maior controle sobre os incidentes relacionados a determinado agente de tratamento, podendo, inclusive, verificar se as violações que não foram notificadas realmente não representaram riscos aos indivíduos. Já a LGPD não faz essa imposição, de modo que a ANPD não terá o mesmo potencial de fiscalização.

No que tange à adoção de códigos de conduta e regras de boas práticas, enquanto a LGPD apenas a incentiva, o RGPD prevê a criação destes códigos, inclusive pelas próprias autoridades de controle, os quais levarão em conta as especificidades dos diferentes setores e as necessidades das micro, pequenas e médias empresas, as quais são as organizações que

mais argumentam dificuldades para se adequarem à legislação diante dos custos da implementação de muitas medidas, razão pela qual merecem uma atenção especial para que estas empresas possam se adequar ao RGPD sem inviabilizarem seus negócios.

Estes códigos de conduta são importantes, pois aumentam e uniformizam a conformidade dos agentes de tratamento com as mencionadas legislações, além de estabelecerem outras práticas que, embora não previstas, estão de acordo com os princípios adotados pela LGPD e pelo RGPD e que significam, por conseguinte, um acréscimo à tutela da privacidade do titular.

Quanto às sanções administrativas, tanto a lei nacional quanto o Regulamento da União Europeia preveem penalidades pecuniárias e não pecuniárias similares, com o RGPD determinando multas um pouco mais gravosas que a legislação brasileira no caso das infrações mais graves.

De igual forma, as disposições de ambas as legislações a respeito da responsabilização civil dos agentes de tratamento são semelhantes, mas há duas distinções relevantes a serem destacadas: a) como já visto, a defesa coletiva dos titulares que sofreram algum dano decorrente do tratamento de dados é prevista de forma mais robusta na legislação nacional que na europeia; e b) a LGPD expressamente assegura aos titulares que, nas relações de consumo, serão aplicáveis as regras de responsabilidade objetiva presentes no Código de Defesa do Consumidor, afastando, assim, as discussões quanto à natureza dessa responsabilidade na maior parte das relações nas quais há tratamento de dados pessoais e, por conseguinte, oferecendo maior proteção jurídica a estes indivíduos.

Acerca das autoridades de controle, existe uma notável diferença entre a Lei Geral de Proteção de Dados Pessoais e o RGPD, a qual diminui o nível de convergência entre ambas as legislações, além de ser suscetível de reduzir a efetividade da LGPD e de obstar o reconhecimento do Brasil pela União Europeia como um país que oferece nível de proteção adequada aos dados pessoais, qual seja, a independência da autoridade nacional.

Como visto, enquanto às autoridades de controle previstas no RGPD é garantida uma atuação independente e sem qualquer ingerência externa, a autoridade nacional foi criada como órgão integrante da Presidência da República, de modo que, ainda que se busque assegurar autonomia técnica e decisória à ANPD e dar algumas garantias de permanência no cargo aos seus diretores, é indubitável que a natureza jurídica de órgão da administração federal compromete a independência da autoridade nacional e aumenta os riscos de sua atuação sofrer influência do Poder Executivo. Isso posto, se a ANPD não for transformada em órgão da administração pública federal, tornando-se independente, conforme a previsão do

artigo 55-A, da § 1º, da LGPD, seu funcionamento enquanto mecanismo institucional verdadeiramente eficaz de fiscalização e aplicação da LGPD pode ser prejudicado.

Por fim, o Regulamento Geral de Proteção de Dados Pessoais ainda traz mais uma relevante disposição e que se diferencia da LGPD, que é a previsão de avalição periódica do Regulamento. Tendo em vista que os avanços tecnológicos podem tornar as normas de proteção de dados obsoletas e ineficientes, a verificação regular acerca da capacidade de tais normas de tutelarem o indivíduo na sociedade da informação com a consequente apresentação de propostas de alteração, quando convenientes, mostra-se necessária. Entretanto, a legislação nacional não prevê um mecanismo de avaliação semelhante, de modo que caberá à doutrina e à ANPD a função de fazer apontamentos referentes à necessidade de alteração legislativa, a qual, por sua vez, passará por todo o moroso trâmite legislativo, deixando os titulares sem garantias adequadas enquanto isso.

5.3.2 Impactos do Regulamento Geral de Proteção de Dados da União Europeia na proteção de dados pessoais dos europeus

Desde que o Regulamento Geral de Dados da União Europeia entrou em vigor, observou-se um grande aumento no número de reclamações de titulares dos dados e seus representantes recebidas pelas autoridades de controle dos países que aplicam o referido Regulamento.

Ressalte-se que, tendo em vista que há décadas a Europa tem criado legislações e mecanismos voltados à proteção dos dados pessoais, os membros da União Europeia já possuíam tais autoridades, as quais, dentre as suas funções, recebiam reclamações relacionadas ao descumprimento de suas leis internas sobre a temática. Com a vigência do RGPD, estas autoridades passaram também a receber reclamações baseadas nas normas previstas em tal Regulamento.

No quadro abaixo, confeccionado a partir das informações encontradas nos *sites* das autoridades de controle dos cinco países mais populosos da União Europeia (com exceção da Alemanha)[631] e da Irlanda, verifica-se que, em 2018, a quantidade de reclamações que estas autoridades receberam cresceu significativamente. Apesar de a Alemanha ter a maior quantidade de habitantes da União Europeia, este país não foi incluído na tabela abaixo, tendo

[631] De acordo com: EUROSTAT. **Data Browser.** Disponível em: https://ec.europa.eu/eurostat/databrowser/view/TPS00001/default/table?lang=en&bookmarkId=c0aa2b16-607c-4429-abb3-a4c8d74f7d1e. Acesso em: 26 maio 2021.

em vista que a Alemanha não tem uma autoridade de proteção de dados central, mas diferentes autoridades de controle para cada um de seus 16 estados. A Irlanda foi incluída neste levantamento, pois é neste país em que se encontram os escritórios de gigantes da tecnologia, tais como o *Google* e o *Facebook*.

Quadro 4 – Reclamações recebidas pelas Autoridades de Controle (2017-2020)

País	Quantidade de habitantes	Número de Reclamações de 2017	Número de Reclamações de 2018	Número de Reclamações de 2019	Número de Reclamações de 2020
França*	67.320.216	8360	11.077	14.137	13.585
Itália*	59.641.488	5.708	7.458	9.689	Ainda não disponibilizado no site da Autoridade
Espanha*	47.332.614	10.500	13.005	11.590	10.324
Polônia*	37.958.138	2.900	5.500	9.300	6.400
Romênia**	19.328.838	3.543	4.822	5.808	5.082
Irlanda**	4.964.440	2.642	4.113	7.215	4.719

* Não informa se inclui ou não os pedidos de informação no número de reclamações

** Não inclui os pedidos de informação no número de reclamações

Fonte: Elaborado pela autora, com base em informações dos relatórios anuais publicados pelas autoridades de proteção de dados dos respectivos países[632]

A despeito da quantidade de reclamações recebidas em 2019 continuar elevado em comparação ao ano de 2017, nota-se um menor crescimento neste número se comparado aos dados de 2018, com a quantidade de reclamações, no caso da Espanha, chegando a ser superada pelos dados do ano anterior.

Outrossim, já em 2019 os números de reclamações começam a se estabilizar numa alta soma, se comparados com o ano de 2017, o que é confirmado pelos dados referentes ao ano de 2020, ainda que os números referentes a este último ano tenham sido impactados negativamente pela pandemia causada pelo COVID-19.

Tal estabilização sugere que a fase de transição experimentada pelos países membros da União Europeia com o advento de uma legislação mais protetiva aos titulares dos dados – em que estes se tornam mais cientes dos seus direitos, ao passo que as organizações ainda

[632] FRANÇA. **Commission Nationale de L'informatique et des Libertés.** Disponível em: https://www.cnil.fr/fr. Acesso em: 30 abr. 2021; ITÁLIA. **Garante per la Protezione dei dati personali.** Disponível em: https://www.garanteprivacy.it/home/attivita-e-documenti/documenti/relazioni-annuali. Acesso em: 30 abr. 2021; ESPANHA. **Agencia Española Protección datos.** Disponível em: https://www.aepd.es/pt-pt. Acesso em: 30 abr. 2021; POLÔNIA. **Urzad Ochrony Danych Osobowych.** Disponível em: https://uodo.gov.pl/pl/138/2059. Acesso em: 30 abr. 2021. ROMÊNIA. Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal. Disponível em: https://www.dataprotection.ro/?page=Rapoarte%20anuale&lang=ro. Acesso em: 30 abr. 2021. IRLANDA. **An Coimisiún um Chosaint Sonraí.** Disponível em: https://www.dataprotection.ie/. Acesso em: 30 abr. 2021.

estão se adaptando às novas exigências – dá lugar à consolidação do novo regramento, com as autoridades de controle trabalhando junto às entidades e ao público em geral para conscientizar a ambos dos direitos dos titulares e do que se considera tratamento lícito de dados. Nesse cenário, a quantidade de reclamações tende a não mais crescer tão significativamente, ao mesmo tempo em que, não se tratando de um mundo ideal e estando os indivíduos mais conscientes e com mais garantias em relação ao seu direito à proteção de dados, esta quantidade se estabiliza num nível superior ao do pré-RGPD.

Conforme dados do Comitê Europeu para a Proteção de Dados, apenas entre 25 de maio de 2018 e 30 de novembro de 2019 as autoridades de controle receberam aproximadamente 275.557 reclamações com base no Regulamento Geral de Proteção de Dados da União Europeia, excluindo-se desse dado os pedidos de informação[633].

Boa parte dessas reclamações se centra em obstáculos ao exercício dos direitos previstos no RGPD, em especial, direito de acesso, direito de exclusão, direito de retificação e direito à eliminação. Nessa senda, a autoridade de controle da Holanda[634] informou que 34% das reclamações por esta recebida dizem respeito a tal temática. No mesmo sentido, as autoridades de controle da Áustria[635] e de Portugal[636] também indicaram que a maior parte das queixas que registram se referem ao exercício dos direitos previstos no Regulamento. Isso demonstra que há certo conhecimento por parte dos titulares dos dados acerca destas garantias.

O Eurobarômetro 487a, que entrevistou, em março de 2019, 27.524 europeus entre residentes com mais de 15 anos de idade de todos os Estados-membros, apontou que, em menos de um ano depois da entrada em vigor do Regulamento Geral da União Europeia, 67% dos entrevistados já tinha ouvido falar do Regulamento: 36% ouviram falar e disseram saber exatamente do que se tratava e 31% não tinha esse conhecimento, apesar de terem escutado algo a respeito do RGPD, o que demonstra que as informações acerca do Regulamento

---

633 UNIÃO EUROPEIA. Comitê Europeu para a Proteção de Dados. **Contribution of the EDPB to the evaluation of the GDPR under Article 97.** Adotado em 18 de fevereiro de 2020. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf. Acesso em: 30 abr. 2021, p. 31.

634 PAÍSES BAIXOS. **Klachtenrapportage:** facts & figures – overzicht 2020. Disponível em: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_klachtenrapportage_2020.pdf. Acesso em: 30 abri. 2021, p. 7.

635 ÁUSTRIA. **Datenschutzbericht 2020.** Disponível em: https://www.dsb.gv.at/dam/jcr:ad90690f-1d10-4e8f-8ed6-b489e888c30f/Datenschutzbericht%202020.pdf. Acesso em: 30 abr. 2021, p. 15.

636 PORTUGAL. Comissão Nacional de Proteção de Dados. **Relatório de Atividades 2019 – 2020.** Disponível em: https://www.cnpd.pt/media/adsndrsf/relato-rio-2019-2020.pdf. Acesso em: 30 abr. 2021, p. 10.

chegaram a boa parte da população europeia, mas ainda é preciso levar mais esclarecimento a esse respeito[637].

Dado importante a ser ressaltado é o de que quase 73% dos entrevistados já ouviram falar de pelo menos um direito garantido pelo RGPD, o que reflete o amadurecimento da tutela da privacidade naquele continente, vez que tal porcentagem é superior a dos que ouviram falar sobre o Regulamento. Ademais, três em cada dez entrevistados afirmaram conhecer todos os direitos que lhe foram questionados, demonstrando um conhecimento significativo da população acerca de tais garantias, mas também um longo caminho de conscientização pública a ser trilhado, já que este nível de informação não atingiu nem metade dos europeus[638].

Outrossim, mais da metade dos entrevistados afirmou saber que existe uma autoridade pública que é responsável pela proteção dos dados pessoais, o que representou um aumento de 20% em relação ao Eurobarômetro realizado em 2015. Este dado evidencia que os esforços das autoridades de controle no intento de se aproximarem da população têm alcançado resultados positivos. Apesar disso, apenas um quinto dos entrevistados soube dizer qual autoridade pública é responsável por proteger seus dados, mais uma vez demonstrando a necessidade de se aumentar o contato destas autoridades com os indivíduos[639].

A Irlanda é um bom exemplo de ações tomadas por autoridades de controle com o objetivo de difundir o conhecimento no que atine ao RGPD, aos direitos dos titulares dos dados, bem como no que se refere à atuação de tais autoridades e dos meios colocados à disposição das pessoas para pedirem informações e registrarem reclamações.

Somente durante o ano de 2020, a autoridade de controle da Irlanda reformulou o seu *site* para torná-lo mais intuitivo e melhorar sua navegabilidade, facilitando o acesso à informação para os indivíduos e para os encarregados de proteção de dados. Ademais, a autoridade buscou diversificar os meios de divulgação do conhecimento, tendo produzido quarenta itens de orientação sobre diversas questões e os divulgado em blogs e podcasts. Além disso, a referida autoridade continuou a expandir seu engajamento nas mídias sociais,

---

637 UNIAO EUROPEIA. Comissão Europeia. **Special Eurobarometer 487a** - Report: The general data protection regulation. Jun. 2019. Disponível em: https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/06/ebs487a_en.pdf. Acesso em: 30 abr. 2021, p. 3.

638 UNIAO EUROPEIA. Comissão Europeia. **Special Eurobarometer 487a** - Report: The general data protection regulation. Jun. 2019. Disponível em: https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/06/ebs487a_en.pdf. Acesso em: 30 abr. 2021, p. 3.

639 UNIAO EUROPEIA. Comissão Europeia. **Special Eurobarometer 487a** - Report: The general data protection regulation. Jun. 2019. Disponível em: https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/06/ebs487a_en.pdf. Acesso em: 30 abr. 2021, p. 3.

tais como o Twitter, Instagram e LinkedIn, triplicando o número de seguidores em tais redes, bem como atingindo um alcance orgânico de quase 2,8 milhões de pessoas[640].

Importa dizer, ainda, que a quantidade de habitantes dos países não parece ser o fator de maior impacto no número de reclamações, haja vista que, enquanto a França, com 67,3 milhões de habitantes registrou 13.585 queixas em 2020 (2 reclamações/10.000 hab.) e a Romênia, com menos de um terço da população francesa, registrou 5.082 queixas no mesmo ano (2,6 reclamações/10.000 hab.), a Irlanda, com apenas 4,9 milhões de habitantes, registrou 4.719 reclamações (10,7 reclamações/10.000 hab.), isto é, somente 363 queixas a menos que a Romênia e, proporcionalmente, possuindo um número de reclamações bem superior em comparação com os dois outros países. Em apoio a esta constatação, a Holanda, que possui 17,4 milhões de habitantes, isto é, possui uma população próxima a da Romênia, registrou 25.590 reclamações (14,7 reclamações/10.000 hab.) somente em 2020[641], o que corresponde a uma quantidade de queixas 5 vezes maior que a recebida pela autoridade de controle romena.

Dessa feita, fatores outros devem influenciar o número de reclamações recebidas pelas autoridades de controle dos diferentes países, os quais não puderam ser identificados nesta pesquisa. Além disso, dos dados acima é possível verificar que, em alguns Estados-membros, o instrumento de reclamações está subutilizado, como no caso da Itália e da Polônia, que receberam pouco mais de 1,5 queixa por 10.000 habitantes. Isso demonstra a necessidade de se fortalecer tal mecanismo, vez que este é de extrema importância para uma efetiva proteção dos titulares dos dados pessoais.

Também as notificações de violações de dados dispararam desde a entrada em vigor do RGPD, tendo em vista que anteriormente, em que pese algumas poucas organizações notificassem às autoridades quando um incidente de segurança era identificado, a cultura organizacional era esconder das autoridades e dos titulares dos dados quando ocorria uma violação de dados diante dos altos custos que tais incidentes representam para as organizações, em especial as empresárias, consoante visto na seção passada.

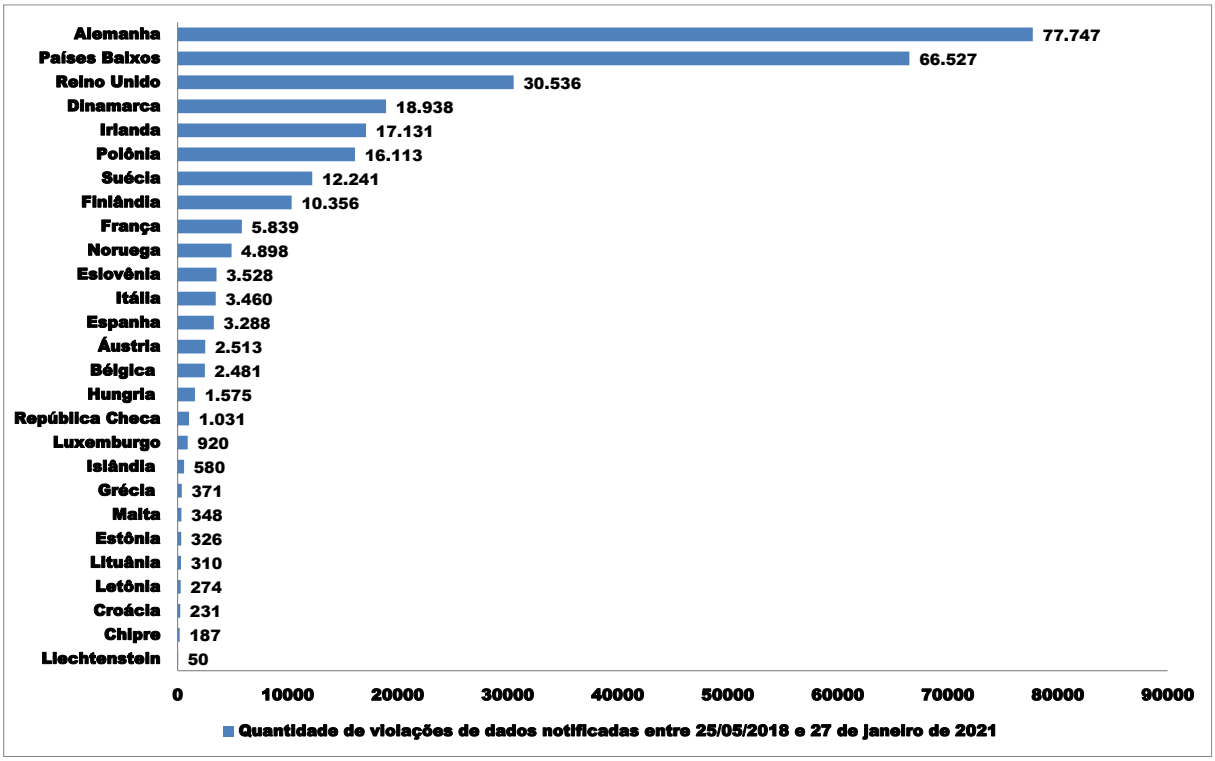
Nessa senda, desde o início da vigência do Regulamento até 21 de janeiro de 2021, 281.799 violações de dados foram notificadas às autoridades de controle dos Estados-membros da União Europeia:

---

[640] IRLANDA. Data Protection Commission. **Data Protection Commission publishes 2020 Annual Report.** 25 fev. 2021. Disponível em: https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-publishes-2020-annual-report. Acesso em: 30 abr. 2021, p. 77.

[641] PAÍSES BAIXOS. **Klachtenrapportage:** facts & figures – overzicht 2020. Disponível em: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_klachtenrapportage_2020.pdf. Acesso em: 30 abri. 2021, p. 1.

Gráfico 1 – Número total de violações de dados pessoais notificados por jurisdição para o período de 25 de maio de 2018 a 27 de janeiro de 2021 inclusive



Fonte: DLA Piper's Cybersecurity and Data Protection Team[642] (tradução nossa).

Importa salientar que este crescimento no número de violações notificadas não significa dizer que mais incidentes de segurança ocorreram, mas que boa parte das organizações tem cumprido com a obrigação imposta pelo Regulamento de informar tal ocorrência à autoridade de controle.

A partir do gráfico acima, é de destacar que a França, a Itália e a Espanha, países que estão dentre os cinco mais populosos da União Europeia, tiveram poucas violações relatadas em comparação a outros países bem menos populosos. Nesse diapasão, os Países Baixos, com 17,4 milhões de habitantes, teve 66.527 incidentes notificados, ao passo que a Itália, com 59,6 milhões de habitantes, teve apenas 3.460 violações relatadas. No mesmo sentido, enquanto a Dinamarca e a Irlanda, com 5,8 e 4,9 milhões de habitantes, respectivamente, registraram mais de 15 mil violações, a Grécia, com 10,7 milhões de habitantes notificou somente 371 violações de dados.

[642] DLA Piper's Cybersecurity and data protection team. **DLA Piper GDPR fines and data breach survey:** january 2021. Disponível em: https://inform.dlapiper.com/10/5202/uploads/data-breach-report-2021.pdf?intIaContactId=P%2bRppLL6Uz7TQ6%2bELU2nbw%3d%3d&intExternalSystemId=1. Acesso em: 30 abr. 2021.

Tais dados evidenciam que, embora o Regulamento Geral de Proteção de Dados da União Europeia tenha buscado uniformizar a proteção de dados pessoais em seus Estados-membros, ainda há muitas divergências no que se refere à aplicação e efetividade do Regulamento. Dessa feita, os esforços das organizações dos diferentes Estados-membros em se conformarem ao RGPD variam bastante. Ademais também a interpretação dos agentes de tratamento e das autoridades de controle acerca das obrigações do Regulamento influencia a quantidade de violações de dados notificadas, haja vista que, como visto, se o incidente de segurança não for capaz de resultar em risco para os direitos e liberdades dos indivíduos não precisa ser notificado, de modo que uma interpretação mais ou menos rígida no que atine ao que pode ser considerado um risco para o titular refletirá em quais violações são entendidas como de notificação obrigatória.

Isso posto, verifica-se a necessidade de desenvolvimento de alguns critérios objetivos relacionados à identificação de quais incidentes de segurança devem ser relatados às autoridades de controle, de modo a garantir aos titulares dos dados uma proteção mais efetiva. Apesar disso, o grande número de notificações de violações de dados a tais autoridades representa uma importante conquista para a privacidade, tendo em vista que uma porcentagem extremamente significativa desses incidentes não chegaria ao conhecimento das autoridades de controle, as quais, por sua vez não poderiam orientar e acompanhar as medidas adotadas no intento de se minimizarem os efeitos das violações, não sendo possível garantir que as organizações tomassem as providências mais adequadas para a proteção dos titulares dos dados envolvidos no incidente.

Uma vez recebida uma reclamação individual, as autoridades de controle podem adotar alguns caminhos, conforme julguem mais adequado para a resolução da demanda de maneira célere e satisfatória. Dessa feita, quando se trata de queixas relacionadas ao exercício de direitos ou a infrações mais leves, boa parte das autoridades busca mediar uma solução entre a organização e o titular do dado, sem a aplicação, *a priori*, de sanções. Entretanto, se entender necessário, a autoridade pode orientar a entidade reclamada a promover certas mudanças no sentido de aumentar a sua conformidade com o RGPD, bem como no intento de que queixas semelhantes não voltem a acontecer.

Além disso, muitas destas reclamações podem exigir uma atuação investigativa das autoridades de controle com vistas a verificar o cumprimento das obrigações impostas pelo Regulamento, especialmente quando a autoridade registra uma série de reclamações contra a mesma organização e pelo mesmo motivo ou quando a queixa diz respeito à ilicitude de um tratamento de dados, a um incidente de segurança ou a qualquer outra circunstância que exija

uma análise da conformidade do processamento de dados realizado por uma entidade com o RGPD. Estas averiguações também podem decorrer de uma notificação de violação de dados, bem como do planejamento anual da autoridade, de questões de interesse e temas prioritários, quando a autoridade dará início à investigação por vontade própria. Sempre que necessário, a autoridade poderá solicitar documentos, fazer visitas ao escritório da organização e a *sites*, realizar auditorias, entre outras ações fiscalizatórias.

A título ilustrativo, em 2020, como visto, a autoridade de controle francesa recebeu 13.585 reclamações, além de diversas notificações de violação de dados, os quais desencadearam 6.500 atos de investigação. Por sua vez, em algumas centenas de casos ou de acordo com as suas prioridades ou questões de interesse, a autoridade nacional entendeu ser necessário abrir um procedimento formal de controle, os quais permitem, principalmente, aprofundar a investigação de reclamações, garantir o cumprimento de medidas corretivas anteriores ou apurar determinados temas considerados prioritários. Em 2020, foram realizados 247 procedimentos de controle[643].

Se a autoridade de controle observar uma violação à legislação de proteção de dados, poderá dar início a um procedimento sancionatório. Nesse particular, as autoridades de controle têm feito uso das diversas sanções previstas no Regulamento Geral de Proteção de Dados e em suas legislações internas. Nessa senda, as autoridade de controle informaram ao Comitê Europeu de Proteção de Dados que, até novembro de 2019, com exceção da retirada de certificação de conformidade com o Regulamento e da ordem para a suspensão do envio de dados para destinatários em países terceiros ou para organizações internacionais, todos os demais poderes de correção previstos no RGPD foram exercidos por ao menos uma delas:

Quadro 5 – Aplicação de sanções pelas Autoridades de Controle

Sanção/Poder corretivo	Quantidade de autoridades que fizeram uso ao menos uma vez do poder corretivo até 30 de novembro de 2019
Advertências de que uma operação de tratamento é suscetível de violar o Regulamento	14 autoridades
Repreensões acerca de violações ao RGPD verificadas em decorrência de um tratamento de dados	24 autoridades
Ordem para o cumprimento de um direito individual do titular	26 autoridades
Ordem para deixar um tratamento de dados em conformidade com o Regulamento	27 autoridades

[643] FRANÇA. Commission Nationale de L'informatique et des Libertés. **Ensemble, voyons le numérique autrement 2020.** Maio 2021. Disponível em: https://www.cnil.fr/sites/default/files/atoms/files/cnil_-_41e_rapport_annuel_-_2020.pdf. Acesso em: 30 abr. 2021.

Ordem para a comunicação do titular acerca de uma violação de dados	10 autoridades
Imposição de limitação temporária ou definitiva ao tratamento de dados, incluindo a sua proibição	13 autoridades
Ordem de retificação ou apagamento de dados pessoais ou restrição de processamento	17 autoridades
Multa administrativa	22 autoridades
Outras sanções ao abrigo da legislação do Estado-membro	6 autoridades

Fonte: Adaptado pela autora, a partir das informações de Comitê Europeu para Proteção de Dados[644]

A análise dos dados acima demonstra que, embora o RGPD tenha contado com uma *vacatio legis* de dois anos, ao menos até novembro de 2019, isto é, um ano e meio após a entrada em vigor do Regulamento, as autoridades de controle estavam mais preocupadas em instituir, nas organizações, uma cultura de privacidade e de conformidade com o RGPD do que em aplicar multas, de modo que as ordens para deixar um tratamento de dados em conformidade com o Regulamento e as ordens para o cumprimento de direito pleiteado por um titular de dados foram os poderes corretivos utilizados por mais autoridades de controle. Ademais, até a mencionada data, 9 autoridades de controle[645] ainda não tinham aplicado nenhuma multa, incluindo a Irlanda, que é sede dos escritórios que comandam as atividades na Europa, Oriente Médio e África de grandes companhias de tecnologia como o *Google*, o *Facebook*, a *Apple*, a *Amazon* e a *Microsoft*[646].

Ressalte-se que as sanções não pecuniárias também são de extrema importância para o cumprimento do RGPD, em alguns casos podendo ser até mais eficaz que a imposição de multas. Como exemplo da utilização de tais medidas, em 2019, a autoridade fiscal do Reino Unido teve que excluir dados de 5 milhões de pessoas que haviam sido coletados por um sistema de reconhecimento de voz criado para confirmar a identidade dos contribuintes. Isso aconteceu depois que a autoridade de proteção de dados do país emitiu um aviso de execução (penalidade prevista em legislação própria), ordenando a exclusão[647]. A decisão da autoridade

[644] UNIÃO EUROPEIA. Comitê Europeu para a Proteção de Dados. **Contribution of the EDPB to the evaluation of the GDPR under Article 97.** Adotado em 18 de fevereiro de 2020. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf. Acesso em: 30 abr. 2021,, p. 32-33.

[645] Os dados dizem respeito a todos os países cobertos pelo RGPD, isto é, 27 Estados-membros da União Europeia, além da Islândia, Lichtenstein e Noruega, que fazem parte do Espaço Econômico Europeu. Ademais, no período a que se refere as informações prestadas ao Comitê Europeu de Proteção de Dados (25/05/2018 a 30/11/2019), o Reino Unido ainda fazia parte da União Europeia.

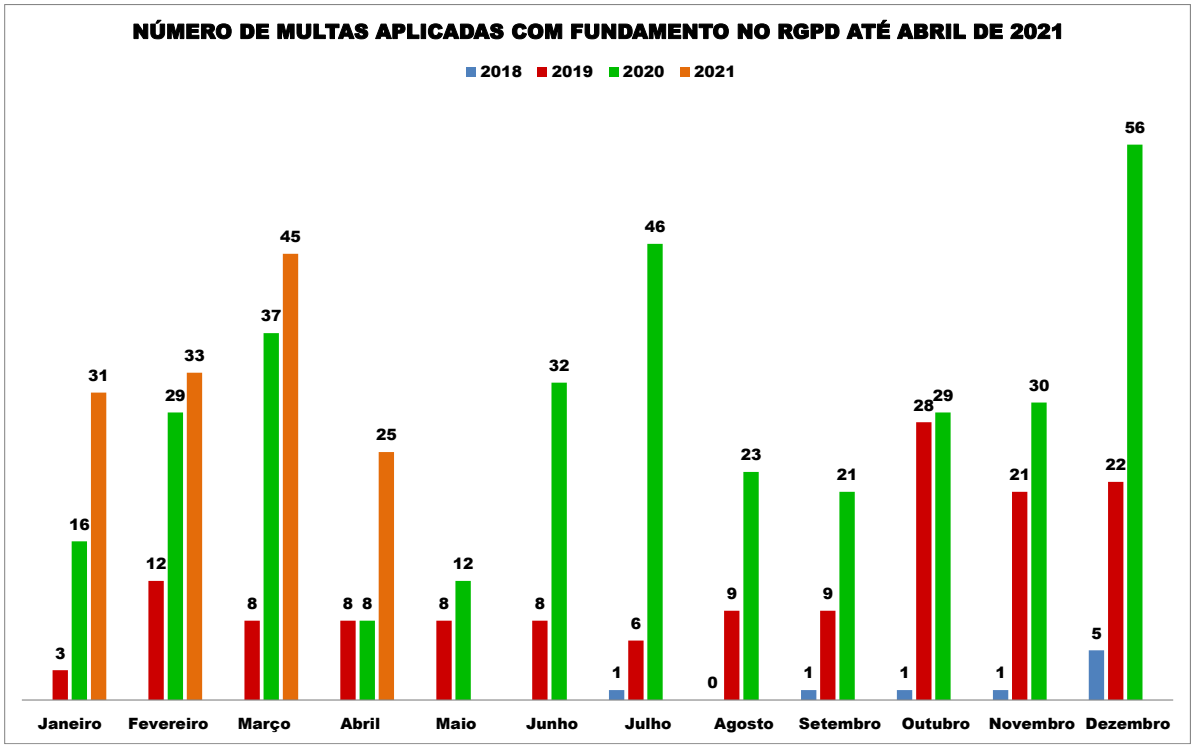
[646] OLHAR DIGITAL. **Com poucos impostos, Irlanda atrai gigantes da tecnologia.** 10 out. 2017. Disponível em: https://olhardigital.com.br/2017/10/13/olhar-digital-internacional/com-poucos-impostos-irlanda-atrai-gigantes-da-tecnologia/. Acesso em: 30 abr. 2021.

[647] PEACHEY, Kevin. HMRC forced to delete five million voice files. **BBC News,** 03 maio 2019. Disponível em: https://www.bbc.com/news/business-48150575. Acesso em: 30 abr. 2021.

de controle do Reino Unido tem um efeito imediato de assegurar o direito dos titulares, pois não só constata a violação ao Regulamento como também impede o uso posterior dos dados indevidamente coletados. Outrossim, transmite uma mensagem clara às organizações, públicas e privadas, de que é preciso se adequar ao RGPD.

Dessa feita, nos dezoito primeiros meses de aplicação do RGPD, as autoridades de controle foram mais lenientes com os agentes de tratamento, focando sua atuação em orientar as organizações a como se adequarem ao Regulamento, bem como fazendo maior uso de sanções não pecuniárias para promover mudanças na atuação destes agentes. Passada essa fase de transição, contudo, as autoridades de controle passaram a aplicar mais multas, as quais também passaram a ter valores maiores. Nessa esteira, o número de multas aplicadas com fundamento no RGPD chegou, em abril de 2021, a 624, o que corresponde a um montante de € 280.356.013, conforme os gráficos a seguir.

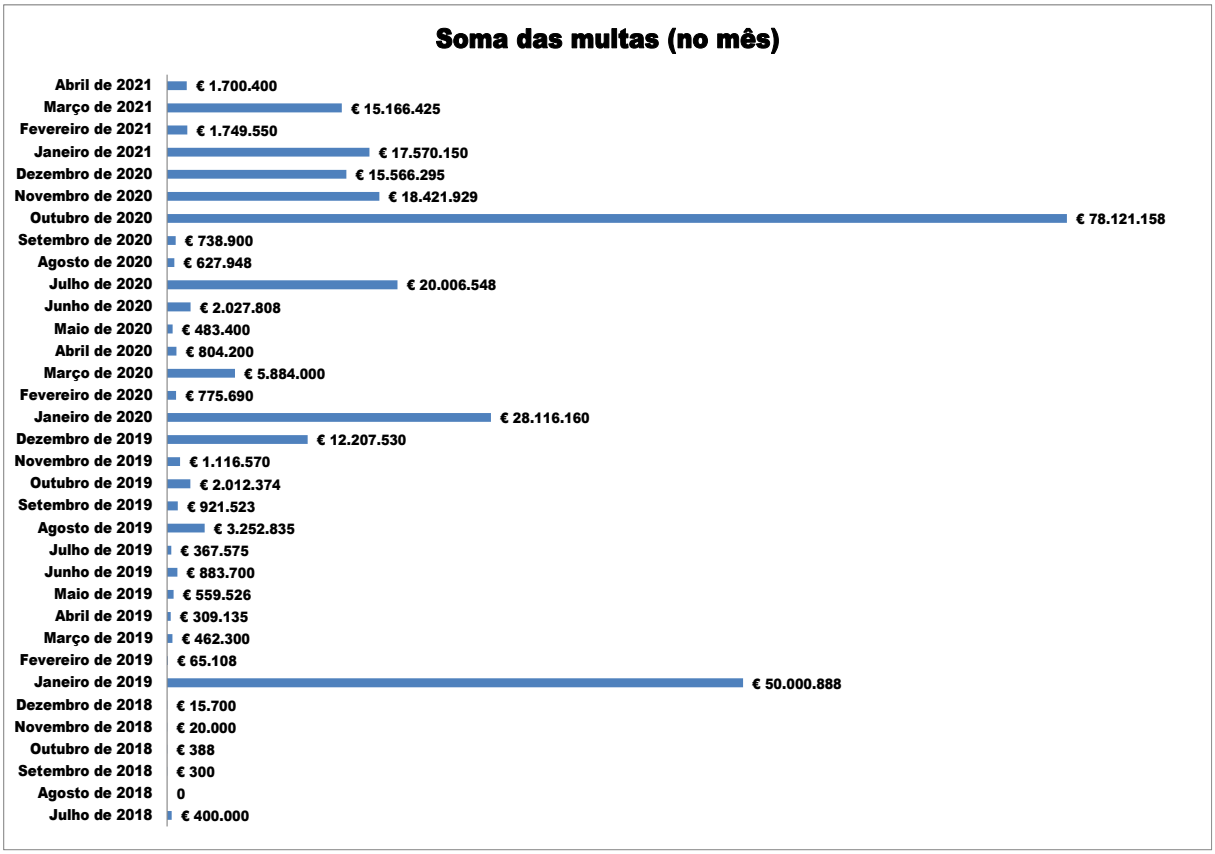
Gráfico 2 – Número de multas aplicadas com fundamento no RGPD até abril de 2021



Fonte: Elaborado pela autora, com base nos dados disponibilizados por GDPR Enforcement Tracker[648].

[648] GDPR Enforcement Tracker. **Fines Statistics.** Disponível em: https://www.enforcementtracker.com/. Acesso em: 30 abr. 2021.

Gráfico 3 – Soma mensal das multas aplicadas com base no RGPD até abril de 2021



Fonte: Elaborado pela autora, com base nos dados disponibilizados por GDPR Enforcement Tracker[649].

Como se observa, no ano de 2018 foram aplicadas apenas 9 multas em sete meses de aplicação, as quais, somadas, não chegaram nem a € 1 milhão, evidenciando a tolerância das autoridades de controle. Já em 2019, 142 multas foram aplicadas, número quase 16 vezes maior que o do ano anterior. Além disso, o montante destas sanções ultrapassou € 72 milhões. Assim, a partir de tal ano as autoridades de controle começaram a intensificar sua atuação sancionatória, num esforço para transmitir a mensagem aos agentes de tratamento de que se adequar ao RGPD é necessário e que a aplicação do Regulamento deve ser levada a sério.

Contudo, é em 2020 que estas autoridades resolvem fortalecer a aplicação de multas, uma vez que já se passou tempo suficiente para as organizações entrarem em conformidade com o RGPD, as quais também tiveram acesso ao conhecimento necessário para tanto, vez que as autoridades de controle emitiram uma série orientações acerca dos mais diversos temas, fizeram uma série de conferências, eventos e *webinars* voltados para os agentes de tratamento e para o público, divulgaram informações sobre o RGPD e sua aplicação em seus

[649] GDPR Enforcement Tracker. **Fines Statistics.** Disponível em: https://www.enforcementtracker.com/. Acesso em: 30 abr. 2021.

sites e ainda estiveram disponíveis, todo este tempo, para responder às consultas e pedidos de informação dos encarregados de proteção de dados das organizações.

Nesse cenário, já não há espaço para tanta condescendência quanto nos anos anteriores. Diante disso, houve a imposição de 339 multas no ano de 2020, número superior ao dobro do aplicado em 2019. Também o somatório destas penalidades foi bastante significativo, ultrapassando os € 170 milhões.

É neste ano que a Irlanda aplica as suas primeiras multas, como a cominada ao Twitter, que foi multado em € 450.000 por não ter cumprido o prazo de 72 horas previsto no RGPD para notificar uma violação de dados à autoridade de controle[650]. Sublinhe-se que esta foi a maior multa aplicada por esta autoridade até agora, em que pese os escritórios das gigantes da tecnologia estejam situados neste país.

Em 2021, a tendência de forte aplicação de multas se confirma, com a imposição de 134 multas apenas nos 4 primeiros meses do ano, as quais totalizaram € 36.186.525. Estas informações foram sintetizadas no quadro abaixo:

Quadro 6 – Total de multas aplicadas com fundamento no RGPD até abril de 2021

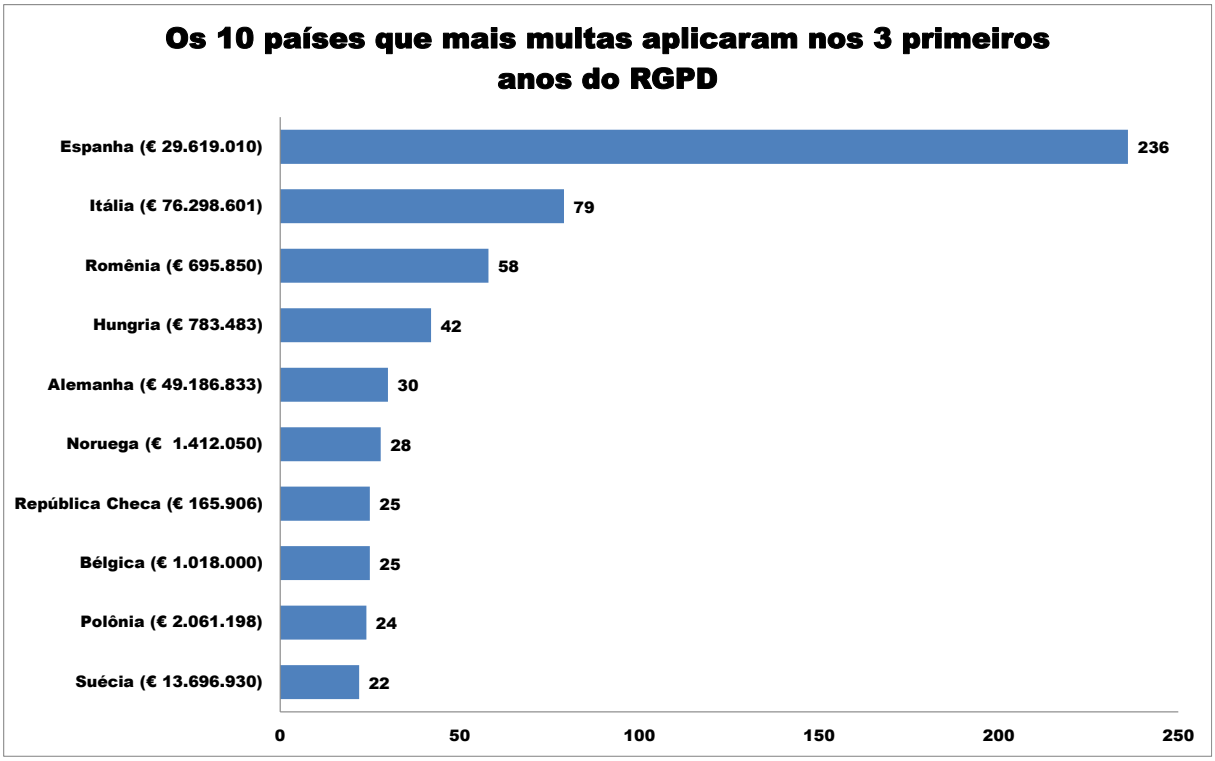
Mês	Número de multas	Soma das multas
2018	**9**	**€ 436.388**
2019	**142**	**€ 72.159.064**
2020	**339**	**€ 171.574.036**
Até abril de 2021	**134**	**€ 36.186.525**
Total de multas aplicadas	**624**	**€ 280.356.013**

Fonte: Elaborado pela autora.

Os 10 maiores responsáveis pela quantidade de multas aplicadas até maio de 2021 estão representados no próximo gráfico[651].

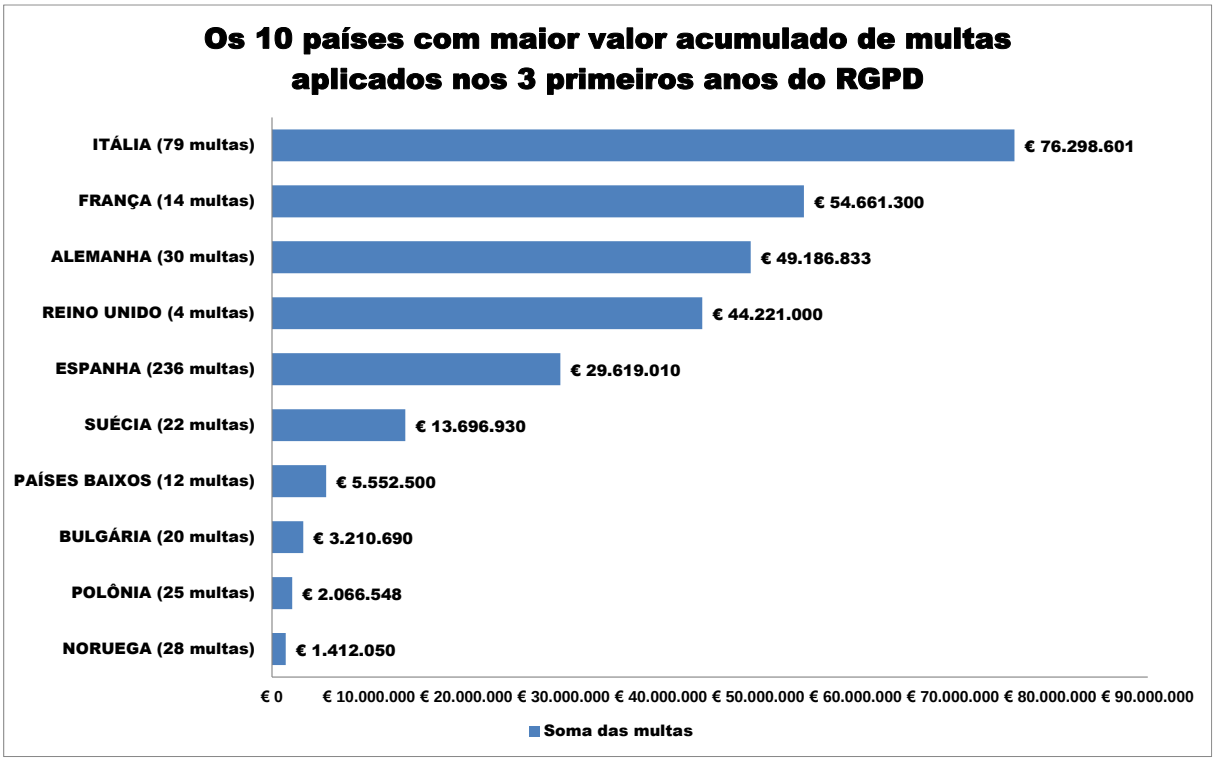
[650] SHIMABUKURO, Igor. *Twitter* é multado na UR por atraso em notificação de violação de dados. **Olhar Digital,** 15 dez. 2020. Disponível em: https://olhardigital.com.br/2020/12/15/noticias/twitter-e-multado-na-ue-por-atraso-em-notificacao-de-violacao-de-dados/. Acesso em: 30 abr. 2021.
[651] GDPR Enforcement Tracker. **Fines Statistics.** Disponível em: https://www.enforcementtracker.com/. Acesso em: 30 abr. 2021.

Gráfico 4 – Os 10 países que mais multas aplicaram nos 3 primeiros anos do RGPD



Fonte: Adaptado pela autora, com base nos dados disponibilizados por GDPR Enforcement Tracker[652].

Gráfico 5 – Os 10 países com maior valor acumulado de multas aplicadas



Fonte: Adaptado pela autora, com base nos dados disponibilizados por GDPR Enforcement Tracker[653].

[652] GDPR Enforcement Tracker. **Fines Statistics.** Disponível em: https://www.enforcementtracker.com/. Acesso em: 30 abr. 2021.

A partir dos gráficos acima, verifica-se que a Espanha é, de longe, o país que mais vezes impôs uma sanção pecuniária, seguida pela Itália e Romênia. No entanto, a quantidade de multas cominadas pelas autoridades de controle não é proporcional ao montante pecuniário resultante da atividade sancionatória destes órgãos.

A França, que é o segundo país mais populoso da União Europeia, emitiu apenas 14 multas, totalizando € 54.661.300. A maior parcela desse montante diz respeito à multa aplicada ao *Google*, de € 50.000.000, em 21 de janeiro de 2019. Esta, que é a maior sanção pecuniária com fundamento no RGPD imposta até agora, decorreu de uma decisão da autoridade de controle francesa que entendeu que a companhia não era transparente e clara no modo como informava aos usuários a respeito da coleta de seus dados pessoais por meio de seus serviços, incluindo o mecanismo de busca, o *Youtube* e o *Maps*, para fins publicitários[654]. Um dia depois da aplicação da multa, o *Google* promoveu mudanças em sua política de privacidade[655].

Outro ponto a se destacar é que a Espanha, que emitiu 236 multas, número absoluto que em muito supera os demais países, somou apenas € 29.619.010, alçando a quinta posição no ranking que considera o valor total das penalidades aplicadas. Assim, a multa média na Espanha é notavelmente mais baixa que em outros Estados-membros, como Alemanha e França, os quais, com quantidade de multas bem menor que a aplicada pela autoridade espanhola, impuseram montante bastante superior que o desta. Estes dados demonstram que, para o valor individual da multa, as circunstâncias de cada caso são decisivas.

Ainda, saliente que os Países Baixos, que receberam o segundo maior número de violações notificadas, apesar de só terem aplicado 12 multas, figura entre as 10 autoridades de controle que impuseram os maiores montantes de penalidades pecuniárias somadas, com a cifra de € 5.552.500. Também merece destaque o fato de que a França, que recebeu, nos últimos 3 anos, quase 40.000 reclamações e mais de 3 mil violações notificadas aplicaram somente 14 multas, ao passo que a Espanha, que registrou quase 35000 reclamações, número muito próximo do informado pelo outro país, impôs 236 multas, o que sugere que há diferentes abordagens e atuação das autoridades de controle.

---

653 GDPR Enforcement Tracker. **Fines Statistics.** Disponível em: https://www.enforcementtracker.com/. Acesso em: 30 abr. 2021.

654 G1 Economia. **França multa *Google* em 50 milhões de euros por violação de lei de privacidade na EU.** 21 jan. 2019. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2019/01/21/franca-multa-google-em-50-milhoes-de-euros-por-violacao-de-lei-de-privacidade-na-ue.ghtml. Acesso em: 30 abr. 2021.

655 A lista de versões arquivadas da política de privacidade do *Google* podem ser encontradas em: GOOGLE. **Política de Privacidade.** Disponível em: https://policies.google.com/privacy/archive?hl=pt-BR&fg=1. Acesso em: 30 abr. 2021.

Desse modo, enquanto algumas autoridades fortalecem o uso de sanções pecuniárias como forma de incentivarem às organizações a entrarem em conformidade com o RGPD, outras podem preferir se utilizar destes poderes corretivos no caso de infrações mais graves, sendo menos rígidos com a aplicação do Regulamento ou fazendo uso das outras penalidades legalmente previstas. Não é possível, contudo, afirmar que esta seja a causa de tamanha discrepância na quantidade de aplicação de multas pelas autoridades de proteção de dados, tendo em vista que não foi feita uma análise minuciosa da atuação de cada uma delas.

Além disso, ressalte-se que a imposição de multa não impede a administração de outras penalidades e medidas necessárias à adequação da organização ao RGPD, sendo possível, por exemplo, ordenar que uma companhia empresária modifique a forma como realiza determinado tratamento de dados e, ao mesmo tempo, multá-la por ter infringido o Regulamento, cabendo às legislações internas e às autoridades de controle de cada Estado-membro traçar critérios mais objetivos para a aplicação das sanções.

Os principais fundamentos para imposição das sanções pecuniárias foram: a) base jurídica insuficiente para processamento de dados; b) medidas técnicas e organizacionais insuficientes para garantir a segurança da informação; c) não conformidade com os princípios gerais de processamento de dados; d) cumprimento insuficiente dos direitos dos titulares dos dados; e) cumprimento insuficiente das obrigações de informação; f) cooperação insuficiente com a autoridade supervisora; g) cumprimento insuficiente das obrigações de notificação de violação de dados; h) ausência de nomeação de oficial de proteção de dados; h) acordo de processamento de dados insuficiente[656].

Como se vê, em que pese o RGPD tenha trazido mudanças significativas para a proteção de dados pessoais e as autoridades de controle tenham se empenhado em orientar as organizações para que estas promovessem as mudanças necessárias para se adequarem ao Regulamento, bem como a despeito de a aplicação de multas e outras penalidades ter se demonstrado uma tendência crescente, verifica-se que os agentes de tratamento continuam testando a autuação destes órgãos de supervisão.

Note-se que o maior ensejador de imposição de multas é a base jurídica insuficiente, demonstrando que muitas organizações não estão seguindo as obrigações do RGPD quanto à obtenção do consentimento livre do titular, assim como ainda estão tendo dificuldades – ou desinteresse – para interpretar adequadamente os requisitos para um tratamento de dados poder ser realizado de acordo com as hipóteses previstas no Regulamento.

---

[656]GDPR Enforcement Tracker. **Fines Statistics.** Disponível em: https://www.enforcementtracker.com/. Acesso em: 30 abr. 2021.

Destaque-se que, até mesmo para as autoridades de controle, há diferenças quanto às bases jurídicas para tratamento de dados pessoais. Ilustrativamente, enquanto o órgão de proteção de dados holandês considera que interesses puramente comerciais não podem ser qualificados como interesse legítimo, a autoridade de supervisão belga entende ser possível tratar dados para fins de marketing direto com base num interesse comercial legítimo[657].

Já no que atine a outras hipóteses legais, há maior uniformidade entre as autoridades de controle. Nesse sentido, quase todos os órgãos de supervisão entendem ser ilegal a imposição ao usuário de aceitar todos os *cookies* para poder navegar num *site*. O uso de *cookies* em conformidade com o RGPD, inclusive, tem sido uma preocupação constante das autoridades de controle, boa parte das quais colocou a questão dentre os seus temas prioritários, o que, por conseguinte, levou, e ainda levará, a ações destes órgãos focadas na orientação, investigação, fiscalização e punição pela utilização inadequada de rastreadores digitais. Espera-se, então, um crescimento no número de multas aplicadas relacionadas a tal uso[658].

Outrossim, os agentes de tratamento também estão deixando de aplicar medidas simples de segurança da informação que evitariam a ocorrência de violações de dados e imposição de multas, a exemplo do uso de criptografia de dados pessoais, especialmente os sensíveis[659].

A não observância dos princípios de proteção de dados durante a coleta e processamento de dados também tem sido outro grande motivo de aplicação de penalidades, evidenciando a necessidade de se criar, nas organizações, uma cultura de respeito a tais princípios, o que, muitas vezes, perpassa pela dificuldade de se interpretar e uniformizar a interpretação destas normas, uma vez que possui conteúdo aberto. Ademais, as novas tecnologias não raramente imporão o desafio hermenêutico de como realizar o tratamento de dados à luz de tais princípios, de modo que as orientações das autoridades de controle serão essenciais. Até lá, novas multas continuarão sendo aplicadas sob este mesmo fundamento, o que também ajudará na evolução da compreensão prática destes princípios.

---

[657] SOMERS, Geert; FITEN, Bernd. 2 years GDPR: na overview of enforcement, warnings and fines. **Timelex.eu,** 11 jun. 2020. Disponível em: https://www.timelex.eu/en/blog/2-years-gdpr-overview-enforcement-warnings-and-fines. Acesso em: 30 abr. 2021.

[658] SOMERS, Geert; FITEN, Bernd. 2 years GDPR: na overview of enforcement, warnings and fines. **Timelex.eu,** 11 jun. 2020. Disponível em: https://www.timelex.eu/en/blog/2-years-gdpr-overview-enforcement-warnings-and-fines. Acesso em: 30 abr. 2021.

[659] DLA Piper's Cybersecurity and data protection team. **DLA Piper GDPR fines and data breach survey:** january 2021. Disponível em: https://inform.dlapiper.com/10/5202/uploads/data-breach-report-2021.pdf?intIaContactId=P%2bRppLL6Uz7TQ6%2bELU2nbw%3d%3d&intExternalSystemId=1. Acesso em: 30 abr. 2021, p. 7.

Por fim, destaque-se que o cumprimento insuficiente dos direitos dos titulares não poderia deixar de ser um fundamento importante na aplicação de multas, tendo em vista que a maior parte das reclamações recebidas pelas autoridades de controle dizem respeito a esta questão. Saliente-se que a imposição de penalidades relacionadas aos obstáculos colocados pelos agentes de tratamento ao exercício dos direitos individuais só não é maior, porque boa parte das autoridades de controle tenta resolver esse tipo de demanda amigavelmente, máxime em razão da celeridade que as medidas consensuais de resolução de conflito proporcionam.

Isso posto, apesar do crescente número de reclamações individuais e de notificações de violações de dados poder sugerir, numa análise mais apressada, que os agentes de tratamento não estão cumprindo o disposto no RGPD ou que os incidentes de segurança aumentaram após a entrada em vigor do Regulamento, na verdade o que se vê é a legislação de proteção de dados surtindo efeito. Isto é, as reclamações cresceram porque os titulares dos dados estão mais conscientes de seus direitos e as notificações de violação de dados aumentaram justamente porque as organizações estão cumprindo com a obrigação imposta pelo RGPD de informar tais incidentes às autoridades de controle.

Desse modo, desde a entrada em vigor do Regulamento e com os órgãos de proteção de dados demonstrando uma atuação forte na aplicação do RGPD, a conformidade dos agentes de tratamento com a legislação tem aumentado, gradativamente.

Uma pesquisa da *Cisco System*[660] revelou que, em 2018, entre os países da União Europeia, a conformidade dos agentes de tratamento participantes da pesquisa com o RGPD variava entre 58% e 76%, sendo os espanhóis aqueles que responderam mais positivamente ao nível de adequação com o Regulamento. De modo geral, o que incluía entrevistados de países de diferentes regiões geográficas, 59% das organizações indicaram que, já naquele ano, atendia a todos ou a maioria dos requisitos do RGPD, enquanto 29% informaram que estimavam estar em conformidade até o final de 2019 e 9% disseram que a adequação levaria mais tempo.

Além disso, o estudo revelou que, embora as mudanças promovidas pelas entidades participantes tenham objetivado afastar as penalidades do RGPD, estas vêm colhendo benefícios que vão além disso, uma vez que os clientes estão mais preocupados com a sua privacidade, o que impacta as vendas daqueles que ainda não se adequaram ao Regulamento, bem como os agentes de tratamento que estão em conformidade com o RGPD registraram

---

[660] CISCO Cibersecurity. **Maximizing the value of your data privacy investments –** data privacy benchmark study. 2019. Disponível em: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/dpbs-2019.pdf. Acesso em: 30 abr. 2021, p. 4.

menos violações de dados quando comparados àqueles responsáveis por processamento de dados pessoais que não observam o Regulamento. Além disso, quando ocorreram incidentes de segurança, menos dados pessoais foram afetados e o tempo de inatividade do sistema foi mais curto entre as organizações devidamente prontas para a aplicação do RGPD, o que diminuiu o custo total das violações para estas companhias.

Apesar disso, ainda há muito a ser feito com vistas a uma tutela efetiva do titular dos dados pessoais. No que diz respeito às políticas de privacidade, por exemplo, mesmo com as mudanças pelas quais estes documentos passaram para se adaptarem ao RGPD, o Eurobarômetro 487a, de 2019, revelou que apenas 13% dos usuários de *sites* entrevistados lêem totalmente tais documentos. As razões apontadas para isso foram que as políticas de privacidade são muito longas (66%) e que são pouco claras ou de difícil compreensão (31%)[661].

Este dado demonstra uma das dificuldades encontradas pelos *sites* para se conformarem ao RGPD: enquanto muitos continuam não sendo transparentes por não fornecerem todas as informações exigidas pelo RGPD, outros apresentam todas estas informações, mas muitas vezes isso torna a política de privacidade tão extensa que raramente será lida. É preciso encontrar caminhos que consigam, de fato, levar ao titular o conhecimento acerca de como seu dado será tratado.

Por oportuno, importa dizer que as autoridades de controle têm sido fundamentais para garantir a efetividade do Regulamento Geral de Proteção de Dados. Seus trabalhos de conscientização têm sensibilizado tanto os agentes de tratamento, acerca da necessidade de estarem em conformidade com o Regulamento, quanto o público em geral, a respeito das obrigações das organizações e dos seus direitos garantidos pelo Regulamento.

Nesse sentido, estes órgãos de supervisão têm realizado uma série de eventos presenciais e online referentes a respeito do direito à proteção de dados, das normas do RGPD e das funções das autoridades de controle. A participação de membros destas autoridades em conferências, seminários e palestras realizados por terceiros também é significativa. A diversidade de canais utilizados para levar a informação também é um ponto a se destacar, tendo sido utilizados, além dos próprios *sites* das autoridades, cartas, redes sociais, blogs, podcasts.

---

[661] UNIAO EUROPEIA. Comissão Europeia. **Special Eurobarometer 487a** - Report: The general data protection regulation. Jun. 2019. Disponível em: https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/06/ebs487a_en.pdf. Acesso em: 30 abr. 2021, p. 3.

A autoridade de controle portuguesa, ainda, anualmente lança pelo menos um número da Revista Fórum de Proteção de Dados, a qual, além de ter uma versão digital no *site* do órgão, também conta com exemplares físicos que são distribuídos por tribunais, universidades, bibliotecas, centros de estudos, advogados, sindicatos e ordens profissionais[662].

Ademais, os órgãos de proteção de dados têm emitido uma série de pareceres, diretrizes e orientações, de modo a esclarecer para os agentes de tratamento como estes devem proceder para realizarem os processamentos de dados em consonância com o disposto no RGDP. Se esta atividade orientadora já é, normalmente, de suma importância, em tempos de pandemia se mostrou essencial.

Nesse sentido, durante o ano de 2020, as autoridades de controle emitiram diversas diretrizes e orientações voltadas a) guiar o poder público quanto ao uso de dados pessoais no enfrentamento ao COVID-19 sem violar os direitos individuais; b) nortear a coleta e tratamento de dados pessoais pelas instituições de ensino, tanto em regime de aula à distância, quanto presencial, com destaque para o uso de câmeras para monitoramento dos alunos e para as aferições de temperatura corporal; c) orientar os empregadores sobre o tratamento de dados de seus funcionários em home office, bem como sobre o processamento de dados de saúde dos trabalhadores, tal como a aferição de temperatura e; d) fornecer informações aos profissionais e estabelecimentos de saúde acerca do tratamento dos dados dos pacientes de COVID-19[663].

Como exemplo dessa atuação, as consultas das autoridades de saúde irlandesa ao órgão de proteção de dados do país resultaram na publicação, por aquela autoridade, da Avaliação de Impacto da Proteção de Dados e do código-fonte do aplicativo de rastreamento de contatos criado para ajudar no combate à pandemia, garantindo maior transparência quanto ao uso dos dados pessoais para este fim e um ano nível de confiança entre a população[664].

---

662 PORTUGAL. Comissão Nacional de Proteção de Dados. **Relatório de Atividades 2019 – 2020.** Disponível em: https://www.cnpd.pt/media/adsndrsf/relato-rio-2019-2020.pdf. Acesso em: 30 abr. 2021.

663 A esse respeito, ver os relatórios anuais de atividade de Portugal - PORTUGAL. Comissão Nacional de Proteção de Dados. **Relatório de Atividades 2019 – 2020.** Disponível em: https://www.cnpd.pt/media/adsndrsf/relato-rio-2019-2020.pdf. Acesso em: 30 abr. 2021, p. 10; dos Países Baixos - PAÍSES BAIXOS. **Klachtenrapportage:** facts & figures – overzicht 2020. Disponível em: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_klachtenrapportage_2020.pdf. Acesso em: 30 abri. 2021; e da Irlanda - IRLANDA. Data Protection Commission. **Data Protection Commission publishes 2020 Annual Report.** 25 fev. 2021. Disponível em: https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-publishes-2020-annual-report. Acesso em: 30 abr. 2021.

664 IRLANDA. Data Protection Commission. **Annual Report 2020**. Disponível em: https://www.dataprotection.ie/sites/default/files/uploads/2021-05/DPC%202020%20Annual%20Report%20%28English%29.pdf. Acesso em: 30 abr. 2021, p. 6.

Saliente-se que desde a vigência do RGPD, as autoridades de controle têm recebido, principalmente por telefone e por e-mail, milhares de pedidos de informação tanto dos indivíduos, que têm dúvidas sobre seus direitos e obrigações dos agentes de tratamento, quanto dos encarregados de proteção de dados, que desejam consultar os órgãos para obter determinado conhecimento sobre a aplicação do Regulamento.

Além dos pedidos de informação, como visto, as autoridades de controle têm recebido milhares de reclamações e notificações de violações de dados, as quais podem impulsionar as atividades fiscalizatória e corretiva desses órgãos, essenciais para garantir o cumprimento do RGPD. Ademais, as próprias autoridades estabelecem temas prioritários e questões de interesse que dão origem a investigações por parte do órgão com vistas a identificar se determinadas organizações estão em conformidade com o RGPD.

Estas investigações, por sua vez, para além da questão das multas aqui já analisada, podem resultar, entre outras coisas, em ordens para que um tratamento de dados seja adequado ao Regulamento, não só fazendo cessar possíveis violações de direitos, como também as impedindo.

Nesse sentido, em fevereiro de 2020, o *Facebook* informou à autoridade de controle irlandesa de que, poucos dias depois, lançaria um serviço de namoro, sem fornecer maiores detalhes de como a rede social garantiria que o serviço estaria em conformidade com os requisitos de proteção de dados. Diante disso, o órgão realizou uma inspeção nos escritórios do *Facebook* para obter a documentação necessária, bem como apresentou uma série de perguntas e preocupações à companhia. Esta, por sua vez, adiou o lançamento do serviço, prestou os esclarecimentos necessários e promoveu todas as mudanças solicitadas pela autoridade antes de o produto ser lançado[665].

A despeito de todo o trabalho desempenhado pelas autoridades de controle, o qual, frise-se, é essencial para a efetividade do RGPD, estes órgãos de proteção de dados têm enfrentado dificuldades estruturais, faltando recursos humanos e financeiros para a maioria deles.

Nesse diapasão, como já analisado, desde a entrada em vigor do Regulamento Geral de Proteção de Dados, o número de pedidos de informação e de reclamações cresceu expressivamente. Outrossim, as autoridades passaram a receber milhares de notificações de violações de dados. Dessa feita, a carga de trabalho dos órgãos de proteção de dados pessoais

---

[665] IRLANDA. Data Protection Commission. **Annual Report 2020**. Disponível em: https://www.dataprotection.ie/sites/default/files/uploads/2021-05/DPC%202020%20Annual%20Report%20%28English%29.pdf. Acesso em: 30 abr. 2021, p. 66.

aumentou de modo significativo, lado outro, o quadro de pessoal e o orçamento destas autoridades não evoluiu ou, em que pese tenha crescido, não aumentou em quantidade suficiente para atender a demanda de maneira célere.

A esse respeito, em dezembro de 2019, 21 autoridades de controle informaram ao Comitê Europeu para a Proteção de Dados que não possuíam recursos humanos, financeiros e técnicos suficientes para desempenharem suas atribuições eficazmente[666]. Essa escassez de recursos tem provocado demora na conclusão de reclamações e de investigações, comprometendo a tutela dos direitos individuais por estes órgãos.

Ilustrativamente, a autoridade de controle dos Países Baixos colocou um aviso em seu *site* de que leva cerca de 6 meses para lidar com a reclamação do titular[667], o que pode dissuadir o indivíduo a procurar o respectivo órgão para resolver uma questão sua sobre proteção de dados, principalmente quando se tratar do exercício de direitos previstos no RGPD, uma vez que este tipo de demanda geralmente necessita de uma resposta rápida.

Em outro exemplo, a Irlanda levou quase dois anos para concluir o processo que levou à imposição de multa ao Twitter[668]. A demora nos processos administrativos não é uma exclusividade deste país, o que pode abalar a credibilidade das autoridades de controle quanto à fiscalização do cumprimento do RGPD, enfraquecendo o sistema de proteção de dados e permitindo que muitas organizações ignorem o Regulamento, em razão da imposição de penalidades pelo seu descumprimento ser muito lenta ou até mesmo inexistente.

Ademais, sem recursos suficientes, os órgãos de proteção de dados podem ser impelidos a realizar acordos não tão adequados com infratores do Regulamento por não terem como arcar com os custos de longos processos judiciais.

Dessa feita, para se garantir a efetividade do Regulamento Geral de Proteção de Dados da União Europeia, faz-se necessária não somente a existência de autoridades de controle independentes, mas também dotadas dos recursos necessários para que possam desempenhas suas funções de maneira rápida e eficaz, transmitindo a mensagem aos agentes de tratamento de que é preciso estar em conformidade com o RGPD para não serem penalizados.

---

666 UNIÃO EUROPEIA. Comitê Europeu para a Proteção de Dados. **Contribution of the EDPB to the evaluation of the GDPR under Article 97.** Adotado em 18 de fevereiro de 2020. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf. Acesso em: 30 abr. 2021, p. 30.

667 PAÍSES BAIXOS. **Autoriteit Persoonsgegevens**. Disponível em: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/gebruik-uw-privacyrechten/klacht-melden-bij-de-ap. Acesso em: 30 abr. 2021.

668 SHIMABUKURO, Igor. *Twitter* é multado na UR por atraso em notificação de violação de dados. **Olhar Digital,** 15 dez. 2020. Disponível em: https://olhardigital.com.br/2020/12/15/noticias/twitter-e-multado-na-ue-por-atraso-em-notificacao-de-violacao-de-dados/. Acesso em: 30 abr. 2021.

Isso posto, o exame das disposições do Regulamento europeu demonstram que a legislação tem notável potencial para resguardar os direitos do indivíduo, mas, pragmaticamente, seu grau de efetividade pode ser maior ou menor, a depender da atuação dos órgãos de proteção de dados pessoais.

Apoiando-se nessa inferência, e tendo sido verificada a existência de uma forte convergência entre o RGPD e a Lei Geral de Proteção de Dados Pessoais, parte-se agora para a análise da LGPD enquanto instrumento de tutela da privacidade.

5.3.3 A Lei nº 13.709/2018 será capaz de assegurar o direito à privacidade na Sociedade da Informação?

Diante de tudo o que se analisou neste trabalho, verifica-se que a Lei Geral de Proteção de Dados Pessoais traz uma série de disposições com grande potencial para provocar mudanças positivas relacionadas à tutela da privacidade na Sociedade da Informação.

Nessa esteira, preocupou-se em proteger o titular desde antes da coleta de seus dados uma vez que obriga que os agentes de tratamento, já durante a fase de projeto de um novo produto ou serviço, tracem estratégias para proteger a privacidade do indivíduo e prevenir que este venha a sofrer qualquer dano.

Por meio dos seus princípios e das bases jurídicas para o tratamento de dados, a LGPD intenta dar efetividade a autodeterminação informativa do titular, de modo a permitir que este possa, na prática, exercer algum controle sobre seus dados pessoais.

Assim, a Lei 13.709/2018 apenas permite a coleta, o processamento e o compartilhamento de dados pessoais se o indivíduo, depois de receber suficientes, claras e adequadas informações acerca do tratamento a que seus dados serão submetidos, com este livremente consentir ou, independentemente de tal aquiescência, na presença de alguma das hipóteses expressamente previstas na LGPD como justificadoras do tratamento de dados. Em qualquer caso, os princípios de proteção de dados e os direitos dos titulares previstos na referida lei deverão ser observados.

Nesse particular, destaca-se que somente poderão ser tratados os dados pessoais que sejam estritamente necessários para a realização da finalidade para a qual foram coletados, finalidade esta que deve ser previamente informada ao titular e deverá orientar todo o tratamento de dados, haja vista que o processamento deve ser compatível e adequado a este fim. Dessa forma, observa-se um considerável impacto no comportamento dos agentes de

tratamento, vez que, até então, a ordem era coletar o máximo de informação possível sobre o titular para depois verificar se tais dados teriam alguma utilidade para a organização.

Ademais, era frequente a coleta destas informações pessoais sem qualquer comunicação ao titular. A partir da vigência da LGPD, os controladores deverão informar ao titular sobre a recolha, mesmo nos casos em que o consentimento deste é dispensável. Este dever de informar, aliás, se estende a todo o ciclo de vida do dado do titular nas operações de tratamento da organização.

Isso posto, a LGPD consagra um direito geral de informação, garantindo que o indivíduo seja informado não somente a respeito da coleta e armazenamento de seus dados, mas também obtenha conhecimento sobre quem tratará e utilizará seus dados, de que forma, com qual objetivo, com quem seus dados serão compartilhados, bem como seja esclarecido acerca de seus direitos e de como exercê-los.

Ainda sobre a autodeterminação informativa do titular, a LGPD se dedica a estabelecer salvaguardas para que de fato este direito seja concretizado. Nesse sentido, prescreve que não é suficiente que o titular não se oponha ao tratamento de seus dados, mas que ele deve fornecer, de forma inequívoca, livre e informada, o seu consentimento. Isso significa que, com o advento da mencionada lei, os controladores devem adotar técnicas *opt-in* de consentimento, ou seja, não mais se pode presumir que o indivíduo concorda com o tratamento de seus dados até que ele solicite o término do processamento e exclusão de suas informações (modelo *opt out*), é necessário que o titular expressamente assinta com o tratamento. Além disso, a obtenção de consentimento por meio de opções pré-validadas, a exemplo de caixas de seleção já marcadas, não é permitida pela LGPD. Autorizações genéricas também são consideradas nulas.

Contudo, um grande desafio que se impõe nesse contexto é como garantir a liberdade do consentimento fornecido pelo titular.

Conforme demonstrado, na sociedade da informação, muitas oportunidades, facilidades e serviços de relevante utilidade para o indivíduo são ofertados em troca do fornecimento de dados pessoais, de modo que o custo de não se consentir com o tratamento de dados pessoais é bastante alto. Nesse particular, a Lei 13.709/2018, de um modo geral, não prevê hipóteses em que se presume que o consentimento não foi dado livremente, mas a experiência europeia deve auxiliar a exegese dessa condição de validade, conforme visto na subseção 5.3.1.

Dessa feita, para ser considerado válido, deve-se evitar que o titular se sinta pressionado de qualquer forma a assentir com o tratamento de seus dados, como as situações

em que a utilização de determinado serviço depende do consentimento do indivíduo com o processamento de dados desnecessários à execução do serviço. Acerca disso, inclusive, a LGPD expressamente dispôs que, na hipótese de tratamento de dados de crianças, o controlador não poderá condicionar a participação destes indivíduos em jogos, aplicações de *internet* ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

A Lei Geral de Proteção de Dados Pessoais, então, impõe aos agentes de tratamento que busquem meios de realmente oferecerem uma escolha aos titulares dos dados. Ilustrativamente, um controlador pode oferecer uma versão "gratuita" de um serviço, cuja utilização depende da entrega de dados pessoais além dos necessários para a sua execução, e uma versão *premium*, em que não há essa coleta, mas o indivíduo paga um valor razoável pela fruição do serviço, de modo que o titular pode escolher entre pagar pela utilização do serviço ou fornecer suas informações pessoais para que sejam monetizadas pela organização empresária e, nesse caso, o consentimento do titular poderá ser qualificado como livre.

Outrossim, existem situações em que os riscos para o indivíduo são de tamanha gravidade ou dizem respeito aos aspectos mais intrínsecos da sua personalidade que uma tutela efetiva da sua privacidade implicará na redução do seu espaço de autonomia, haja vista que, diante da assimetria econômica, técnica e informacional entre agentes de tratamento e titulares dos dados, nem sempre o indivíduo terá consciência completa dos perigos envolvidos no tratamento ou, ainda que tenha, poderá estar num contexto em que não pode deixar de consentir com determinado processamento de dados. Por esta razão, objetivando prevenir eventuais danos, tais situações demandam que a autodeterminação do titular seja parcialmente limitada.

Dito isso, a LGPD veda a comunicação ou o uso compartilhado entre controladores, com finalidade puramente econômica, de dados relacionados à saúde do indivíduo, de modo que o consentimento deste não é capaz de derrogar tal proibição. A mencionada lei, ainda, atribui poderes à autoridade nacional para proibir que outros dados sensíveis sejam compartilhados entre agentes de tratamento com objetivo de obter vantagem econômica.

Assim, as funções de regulamentação, orientação e fiscalização da ANPD serão essenciais para atribuir algum grau de efetividade às disposições da Lei 13.709/2018 referentes ao consentimento e à autodeterminação informativa, emitindo diretrizes interpretativas acerca da liberdade do consentimento, preenchendo as lacunas normativas de acordo com suas competências e fiscalizando a conformação dos controladores à Lei.

Saliente-se que, mesmo o RGPD sendo mais detalhista nestas questões que a LGPD, as autoridades de controle dos Estados-membros têm despendido grande esforço para garantir a adequação dos agentes de tratamento ao Regulamento e, assim, salvaguardar os titulares. Nesse diapasão, por exemplo, além de publicarem, em seus *sites*, orientações sobre a obtenção do consentimento para a utilização de *cookies*, tais órgãos já colocaram ou estão inserindo em suas agendas de temas prioritários ações relacionadas a estes rastreadores digitais, o que inclui a educação do público e das organizações, visitas aos *sites* mais acessados nos respectivos países para verificação do nível de conformidade das páginas, envio de comunicações aos agentes de tratamento, fixando prazo para que se adequem às orientações e, por último, a aplicação de sanções pecuniárias e não pecuniárias a tais agentes.

Para além de todas essas questões alusivas ao consentimento, a Lei Geral de Proteção de Dados Pessoais, assim como o RGPD e as outras leis de quarta geração da proteção de dados pessoais, não desconsidera o desequilíbrio existente entre o indivíduo e os agentes de tratamento e que nem sempre é suficientemente corrigido pelas limitações à liberdade de consentir ou pelas condições que devem ser observadas pelas organizações no momento da coleta de dados pessoais.

Por tal razão, estas leis não se centram exclusivamente no consentimento do titular. Além disso, é preciso considerar que a privacidade ultrapassa a questão da coleta de dados e da segurança da informação. Com efeito, consoante se demonstrou neste trabalho, na sociedade da informação, este direito do indivíduo é constantemente ameaçado, em cada operação de tratamento de dados. Dessa feita, não é porque o controlador obteve o consentimento do titular para a recolha de suas informações, bem como porque tomou as medidas necessárias para evitar situações acidentais ou ilícitas de destruição, perda, alteração ou comunicação desses dados que a tutela da privacidade está satisfeita.

Nessa senda, o principal êxito da LGPD, da mesma forma que o Regulamento europeu, é instituir um sistema de proteção de dados pessoais baseado no dever de prevenção de danos ao titular e no *accountability* dos agentes de tratamento. Inclusive, a Lei 13.709/2018 expressamente impõe a estes agentes a obrigação de observarem os princípios da boa-fé, da prevenção e da responsabilização e prestação de contas nas suas atividades de tratamento. Outrossim, a LGPD também prescreve que as operações destes agentes devem seguir uma abordagem de *privacy by design.*

Isso posto, a Lei Geral de Proteção de Dados Pessoais estabelece um sistema de proteção à privacidade que, sem retirar toda e qualquer possibilidade de o indivíduo exercer sua autodeterminação informativa, num paternalismo exacerbado, bem como sem obstar os

avanços tecnológicos e a nova economia, vez que traz uma série de bases que servirão para os agentes de tratamento, licitamente, justificarem suas atividades de tratamento de dados, exige que os agentes de tratamento pensem e incorporem a privacidade em todo o sistema de negócios ou de execução de atividades no intento de evitar qualquer dano ao titular.

Em outras palavras, a referida Lei impõe que todo o negócio ou atuação da organização seja estruturada levando-se em consideração a perspectiva do titular, de modo que toda a organização e a estrutura de gerenciamento, todos os processos, a rede, as tecnologias e os sistemas de informação da organização devem incorporar a privacidade em seus projetos e desenvolvimento.

Assim, antes de darem início ao processamento dos dados, os agentes de tratamento devem identificar todas as informações pessoais que eles realmente necessitam coletar para as finalidades pretendidas e quais os riscos para o titular envolvidos no tratamento. Além disso, devem buscar formas de mitigar essas ameaças, promovendo diversos testes para garantir que, de fato, os riscos foram reduzidos.

O uso de tecnologias de aprimoramento da privacidade também deve ser avaliado, de modo a verificar se a incorporação ao processo de técnicas que potencializam a privacidade do titular, a exemplo da criptografia e da anonimização, são viáveis em termos de utilidade da informação. Outrossim, medidas de segurança técnicas e administrativas devem ser adotadas durante todo o ciclo de vida do dado na organização, implementando ações de segurança da informação, inclusive definindo-se, desde o projeto do produto ou serviço, os níveis de acesso àquela informação pelos diversos funcionários e administradores da entidade.

Todas essas medidas devem ser tomadas no intento de se identificarem os potenciais danos que o titular pode sofrer e, então, serem adotados comportamentos que possam prevenir, ou ao menos mitigar, tais lesões. Por conseguinte, os agentes de tratamento somente devem dar início a suas operações de processamento de dados depois de implementarem todas essas ações.

Ademais, é imprescindível que as medidas sejam avaliadas regularmente, não apenas com o objetivo de verificar se estão sendo cumpridas pelos diferentes setores da organização, mas também para se analisar se tais ações ainda são capazes de salvaguardarem a privacidade do titular. Por conseguinte, estar em conformidade com a Lei 13.709/2018 exige um esforço constante dos agentes de tratamento, não sendo suficiente a efetuação de mudanças para uma adequação inicial à lei se estas não forem periodicamente testadas.

Isso porque, pelo princípio da responsabilidade e da prestação de contas, o qual, conforme a LGPD, deve nortear toda a atividade do agente de tratamento, este deve ser capaz

de demonstrar, quando solicitado, a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Dessa feita, para além do consentimento, a Lei Geral de Proteção de Dados Pessoais tem como foco uma tutela da privacidade do titular que parte, principalmente, de uma atuação de prevenção, mitigação e controle de dados pelos agentes de tratamento, sem que o indivíduo tenha, pois, que tomar medidas adicionais para a proteção de seus direitos.

Nesse cenário, uma legislação de proteção de dados que exige a proatividade dos agentes de tratamento no mapeamento de problemas é uma grande conquista para o direito à privacidade, máxime quando se tem em vista que, na sociedade da informação, muitos danos sofridos pelo indivíduo são irreversíveis, alcançando uma superexposição de proporções mundiais. Além disso, como estudado, quando ocorre um vazamento de dados estes se espraiam pela *dark web*, onde ficam disponíveis quase que eternamente, possibilitando que um mesmo titular sofra as consequências de um incidente de segurança repetidas vezes.

Também no que atine aos riscos associados ao *profiling*, em especial à discriminação, o comportamento das organizações no sentido de anteverem tais ameaças e buscarem soluções para mitigá-las será fundamental para a proteção do indivíduo, diante das dificuldades existentes para a identificação destes danos, mesmo com outras previsões da LGPD destinadas a permitir esse reconhecimento, como a transparência, o direito à explicação e a possibilidade de realização de auditorias pela ANPD.

À vista disso, a Lei 13.709/2018 se esforça em instituir, no Brasil, uma cultura de privacidade.

Para auxiliar nesse processo, a exemplo do RGPD, cria a figura do encarregado, que é a pessoa, física ou jurídica, designada pelo controlador, que irá orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais, além de receber comunicações da autoridade nacional e adotar providências de aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e tomar as medidas cabíveis relacionadas a tais reclamações. Isto é, o encarregado irá contribuir para a conformidade do agente de tratamento com a LGPD, de modo que a organização como um todo deve seguir suas orientações, além de lhe fornecer o acesso e recursos necessários para a análise do cumprimento das normas da LGPD pelo controlador.

Como visto na subseção anterior, estes profissionais têm sido essenciais no processo de aplicação do Regulamento de Proteção de Dados da União Europeia dentro das organizações, haja vista que as autoridades de controle relataram terem recebido muitas

consultas de encarregados acerca da implementação do RGPD, além de os eventos proporcionados pelos órgãos de proteção de dados ou que contam com a participação destes alcançarem muitos participantes que são encarregados.

Além disso, a LGPD, ciente das limitações próprias da heterorregulação em matéria de proteção à privacidade, estimula que os agentes de tratamento de dados pessoais, individualmente ou por meio de associações, formulem regras de boas práticas e de governança que estabeleçam, pelo menos, 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.

Dessa forma, estes códigos de conduta orientam o comportamento de todos os envolvidos no tratamento de dados, bem como consideram as especificidades de cada setor, contribuindo para a criação de procedimentos que traduzam, para a realidade daquela organização ou setor e em termos de aplicação prática, as disposições genéricas e principiológicas da LGPD, aumentando o grau de conformidade dos respectivos agentes de tratamento à referida Lei.

Busca-se, assim, uma combinação entre heterorregulação e autorregulação, a partir do compromisso das organizações privadas em efetivamente protegerem a privacidade dos titulares dos dados, com a LGPD, inclusive, elencando a adoção destas políticas de privacidade como parâmetro que deve ser observado quando da aplicação de sanções administrativas, podendo, portanto, até amenizar eventuais penalidades.

Contudo, como a previsão em Lei não é capaz de solucionar todos os problemas atinentes à privacidade, é preciso garantir que o indivíduo tenha meios de salvaguardá-la nesse contexto de tratamento de dados. Desse modo, a LGPD estabelece uma gama de direitos do titular, os quais, como demonstrado na seção 3, não são interesses juridicamente tutelados por si mesmos, mas se tratam de remédios que servem a instrumentalizar a tutela da privacidade, a torná-la efetiva, vez que intentam prevenir danos e sanar violações às dimensões informacional e decisional desse direito.

Nessa senda, os direitos previstos pela Lei 13.709/2018 vão desde a simples confirmação pelo titular de que seus dados são tratados por aquele controlador, passando por garantias de que seus dados projetam a sua personalidade de maneira fiel e atual (como o direito à correção e à eliminação de dados desnecessários e excessivos), pela possibilidade de se exigir medidas de segurança (direito à anonimização de dados) ou que se façam cessar

violações à sua privacidade (direito de oposição e direito ao bloqueio ou eliminação dos dados tratados em desconformidade com a lei) até o direito de poder revogar o consentimento e solicitar a eliminação dos dados pessoais com base nele tratados.

Isso posto, tais disposições, além do direito geral de informação, atribuem um maior controle aos titulares sobre seus dados, mesmo nas hipóteses em que o consentimento não seja a base jurídica para o tratamento, permitindo-lhes mapear o fluxo de suas informações pessoais, influenciar a sua representação virtual e, em determinados casos, retirar os seus dados do âmbito de conhecimento e utilização dos agentes de tratamento.

Também o exercício dos direitos do titular recebe atenção da Lei Geral de Proteção de Dados Pessoais, a qual prescreve que este deve ser facilitado e gratuito. Outrossim, se o agente de tratamento obstar o exercício de quaisquer desses direitos, a LGPD possibilita que o titular busque resolver a questão administrativamente, sem precisar recorrer ao Judiciário. Para tanto, é-lhe assegurado direito de peticionar uma reclamação à ANPD.

Ressalte-se que este é um importante instrumento que o indivíduo tem para fazer com que a Lei Geral de Proteção de Dados Pessoais seja aplicada à sua relação com o controlador. A esse respeito, verifica-se que, quando RGPD, que prevê este mesmo direito, entrou e vigor, o número de reclamações dos titulares recebidas pelas autoridades de controle cresceu consideravelmente e, a partir delas, tiveram início procedimentos de solução amigável, bem como processos de fiscalização acerca da conformidade do agente de tratamento com o Regulamento.

Entretanto, no que concerne aos direitos dos titulares, cabe relembrar aqui as críticas feitas alhures e retomadas na subseção 5.3.1 acerca do direito de oposição, o qual abarca poucas hipóteses em que o indivíduo pode fazer uso de tal salvaguarda, e do direito de solicitar a revisão de decisões tomadas exclusivamente baseadas no tratamento automatizado, o qual não assegura ao titular que esta revisão seja feita por uma pessoa natural, o que, conforme visto, não garante que todos os fatores de risco envolvidos nessas decisões sejam identificados e corrigidos, bem como não garante que os indivíduos sejam julgados com base nas suas próprias características e méritos individuais, e não pelas características do grupo a que pertence.

Apesar disso, a Lei 13.709/2018 não deixa o titular completamente sem proteção em face das ameaças da utilização do *profiling* para a tomada de decisões. Além dos princípios que são aplicáveis ao tratamento de dados pessoais, particularmente o da não discriminação, e dos direitos de acesso e correção – que permitirão ao indivíduo proceder às medidas necessárias para que o seu perfil seja construído da forma mais fiel possível à realidade –, a

LGPD estabelece um direito à explicação relacionado às decisões automatizadas, incluindo os critérios e procedimentos utilizados para se chegar à decisão.

De igual forma, prevê o princípio da transparência, o qual, mesmo com todas as limitações de ordem prática, é um instrumento fundamental na tutela dos dados pessoais, uma vez que garante ao indivíduo, de maneira compreensível, explicações e informações relevantes acerca do tratamento de dados. Ainda, dispõe que a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

Também os incidentes de segurança, grandes e constantes problemas da sociedade da informação, recebem disciplina da LGPD, a qual busca, primeiramente, evitá-los, e, não sendo possível, traça diretrizes de atuação para os agentes de tratamento no sentido de minimizar os danos ao titular e notificar tais violações de dados à ANPD e aos titulares, permitindo a fiscalização do incidente e a adoção de providências por parte da autoridade e dos indivíduos no intento de mitigarem as ameaças e lesões provocadas pela violação de dados.

No entanto, todas estas disposições da LGPD até aqui expostas necessitam de instrumentos que levem os agentes de tratamento a se adequarem à lei. A esse respeito, a Lei 13.709/2018, também seguindo o movimento de convergência internacional, cria a Autoridade Nacional de Proteção de Dados com uma série de competências, as quais serão destacadas adiante, bem como prevê a aplicação de sanções administrativas, pecuniárias e não pecuniárias – similares às penalidades do RGPD, como visto –, além da responsabilização civil dos agentes de tratamento que causarem dano aos titulares.

Quanto às sanções administrativas, importa destacar que, após muitas tentativas de prorrogação da *vacatio legis* da Lei Geral de Proteção de Dados Pessoais, esta acabou entrando em vigor em setembro de 2020, contudo, seus dispositivos que tratam da aplicação de penalidades administrativas pela ANPD foram postergados para agosto de 2021. Dessa feita, a LGPD vigerá por quase um ano sem contar com este importante instrumento de *enforcement*.

Apesar disso, a referida Lei permanece aplicável, tanto pelo Judiciário, o qual pode, inclusive, aplicar os dispositivos da LGPD sobre responsabilidade civil, bem como pelos órgãos de proteção do consumidor podendo sancionar agentes de tratamento infratores com as penalidades previstas no Código de Defesa do Consumidor.

Nessa esteira, pouco tempo depois da entrada em vigor da Lei 13.709/2018, a 13ª Vara Cível de São Paulo condenou uma imobiliária que, sem consentimento, teria divulgado os

dados pessoais do autor para parceiros da organização, como firmas de decoração, a se abster de fazer tal compartilhamento, sob pena de multa, bem como ao pagamento de indenização por danos morais no valor de R$ 10.000,00. A fundamentação da sentença fez diversas referências à LGPD e, ao fim, reconheceu que, além desta lei, a imobiliária teria violado o Código de Defesa do Consumidor e a Constituição Federal. Saliente-se que a aplicação dos princípios da proteção de dados independem da aplicação da LGPD, vez que constituem o núcleo desse direito fundamental[669].

Isso demonstra que a aprovação da Lei 13.709/2018 ampliou o conhecimento sobre a proteção dos dados pessoais nos tribunais brasileiros, como também que a referida Lei já está surtindo efeitos desde os primeiros dias que se seguiram ao fim da sua *vacatio legis.* Neste particular, é de se mencionar que os órgãos de proteção do consumidor também estão aplicando a Lei Geral de Proteção de Dados Pessoais, com a primeira ação civil pública nela baseada tendo início um mês após a sua entrada em vigor. A petição inicial, contudo, foi indeferida, porque o juiz entendeu que, estando, à época, o *site* em manutenção e sendo recente a aplicação da LGPD, a página deveria estar se adequando à legislação[670].

Para a aplicação das sanções administrativas, quando estas entrarem vigor, assim como para a fiscalização do cumprimento de suas normas, como visto, a Lei 13.709/2018 criou a Autoridade Nacional de Proteção de Dados Pessoais. Este órgão terá um papel essencial na tutela da privacidade do indivíduo, vez que estão entre as suas competências: a) fiscalizar o cumprimento da legislação, inclusive realizando auditorias, e aplicar sanções, em caso de descumprimento; b) apreciar petições de titular contra o controlador, se este não solucionar a demanda no prazo estabelecido em Lei; c) promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; d) editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais; e) celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade; f) deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos.

---

669 SÃO PAULO. Tribunal de Justiça do Estado de São Paulo. **Processo nº 1080233-94.8.26.0100.** Juíza de Direito: Tonia Yuka Koroku. 13ª Vara Cível, Foro Central Cível, Comarca de São Paulo. Data do Julgamento: 29 set. 2020. Disponível em: https://www.migalhas.com.br/arquivos/2020/9/B05F37C296A643_decisaoLGPD.pdf. Acesso em: 30 abr. 2021.

670 VITAL, Danilo. Primeira ACP baseada na LGPD é indeferida porque *site* da ré está em manutenção. **Consultor Jurídico,** 23 set. 2020. Disponível em: https://www.conjur.com.br/2020-set-23/peticao-inicial-acao-civil-publica-baseada-lgpd-indeferida. Acesso em: 30 abr. 2021.

Isso posto, das várias competências estabelecidas pela LGPD, destacam-se as acima citadas, as quais revelam que a autoridade nacional possui funções regulatórias, de orientação, educativas, fiscalizatórias e corretivas.

Dessa feita, como se demonstrou neste trabalho, a Lei 13.709/2018 é uma lei principiológica, de prescrições genéricas, o que permite que suas disposições se adaptem às novas tecnologias, já que disposições muito específicas a determinado tratamento de dados não assegurariam uma proteção efetiva do titular diante dos avanços tecnológicos.

No entanto, a técnica legislativa utilizada pela Lei Geral de Proteção de Dados Pessoais exige uma atuação contínua e atenta da ANPD para, além de preencher as lacunas com a edição das normas que a Lei, expressamente, deixou a seu turno, editar regulamentos outros que possam fortalecer os instrumentos já previstos na legislação, bem como tutelar o indivíduo frente às novas tecnologias, dando maior efetividade à LGPD. Ilustrativamente, a atividade regulatória da autoridade nacional pode potencializar o relatório de impacto à proteção de dados pessoais enquanto ferramenta de prevenção de danos, superando-se, assim, as críticas apontadas na subseção 5.3.1 e aproximando o referido documento da avaliação de impacto prevista no RGPD.

No desempenho de suas funções de orientação, caberá a ANPD o importante papel de interpretar as disposições da LGPD, garantindo maior segurança jurídica tanto para os agentes de tratamento, nos seus processos de adequação, quanto para o titular, que terá maior substrato para compreender seus direitos e identificar ilicitudes na atuação das organizações. Outrossim, deverá orientar os referidos agentes acerca de como aplicarem a legislação, o que é de suma relevância na instituição da cultura de privacidade e na prevenção de danos ao titular, tendo em vista que as ameaças aos direitos do indivíduo são consideravelmente reduzidas quando a organização implementa, adequadamente, as obrigações que a Lei 13.709/2018 lhe impõe.

A esse respeito, conforme visto na seção anterior, as autoridades de controle dos Estados-membros da União Europeia têm despendido muitos esforços para levarem o máximo de orientação possível e pelos mais diversos meios para os encarregados da proteção de dados, alcançando bons resultados, inclusive recebendo milhares de contatos destes profissionais em busca de orientações para a conformação da organização com o RGPD.

Acerca das atividades fiscalizatórias e corretivas, a ANPD deverá investigar as reclamações que os titulares lhe façam atinentes a determinado tratamento de dados, assim como as notificações de violações de dados que receber, objetivando averiguar se os agentes de tratamento tomaram as medidas técnicas e organizacionais adequadas à proteção dos dados

pessoais e se criaram obstáculos ao exercício dos direitos dos titulares estabelecidos na LGPD. Ainda, a exemplo das autoridades de controle dos Estados-membros da União Europeia, este órgão poderá criar uma agenda fiscalizatória de acordo com suas prioridades, bem como realizar investigações a partir de questões de seu interesse que cheguem a seu conhecimento, como vazamentos em massa noticiados pela mídia.

A importância dessas atividades de fiscalização reside na possibilidade não só de imposição de multas, as quais, por si só e a depender do tamanho da entidade, já podem ser incentivo suficiente para a conformação do agente de tratamento à Lei Geral de Proteção de Dados Pessoais, mas também de penalidades não pecuniárias que podem ter um efeito ainda mais efetivo para fazer cessar a infração, bem como para compelir a organização à adequação.

Isso porque, dentre estas penalidades, estão sanções administrativas que podem ser bastante prejudiciais à execução das atividades do agente de tratamento, tais como a suspensão parcial do funcionamento do banco de dados ou mesmo a proibição total do exercício de operações de processamento de dados pessoais. Desse modo, uma organização empresária cujo modelo de negócio dependa do tratamento de dados pessoais, por exemplo, sofrerá notáveis prejuízos caso lhes seja imposta alguma dessas penalidades, talvez muito maiores dos que os causados pela cominação de multa. O titular, por sua vez, estará resguardado, já que, nessas situações, a entidade estará impedida de tratar seus dados até que se adeque à LGPD.

Nesse cenário, as sanções administrativas são relevantes instrumentos de *enforcement*, atribuindo maior potencial de efetividade à lei.

Outrossim, à LGPD prescreve regras de responsabilidade civil aos agentes que causarem danos aos titulares em suas atividades de tratamento de dados pessoais, as quais, frise-se, não afastam as disposições do Código de Defesa do Consumidor concernente à responsabilização de tais agentes no âmbito das relações consumeristas, que são a maior parte das relações em que se efetuam tratamento de dados.

Nesse diapasão, as indenizações podem ser por danos materiais e morais, além de individuais ou coletivos, salientando-se que a Lei 13.709/2018, além da tutela individual, fortaleceu a defesa coletiva do direito à proteção aos dados pessoais, por meio dos legitimados, o que é fundamental num contexto de infrações em massa, bem como de assimetria técnica, financeira e informacional entre titulares e agentes de tratamento em que a maior parte das violações à proteção de dados acontecem. Assim, esta previsão, bem como a da inversão do ônus da prova a favor do titular, diminuem o desequilíbrio entre as partes, possibilitando uma proteção mais apropriada da privacidade do indivíduo.

Dessa feita, estas prescrições tanto servem como mais um incentivo aos agentes de tratamento para que estes se conformem à Lei Geral de Proteção de Dados como também se prestam à reparação, ou ao menos compensação, ao indivíduo pelas lesões sofridas em seu direito à privacidade.

Ainda, compete à ANPD a indispensável função de fortalecer a tutela individual da privacidade. Nesse sentido, deve não somente receber reclamações dos titulares referentes ao descumprimento da lei, buscando soluções amigáveis e céleres que atendam às necessidades do indivíduo ou fiscalizando e punindo o agente de tratamento, conforme o caso, mas facilitar o registro dessas reclamações, implementando mecanismos simplificados, inclusive por meio eletrônico.

Para além disso, é fundamental que a autoridade nacional promova diversas ações educativas para conscientizar os titulares sobre seus direitos e como exercê-los. Com efeito, uma lei que prescreve uma gama de garantias aos indivíduos, mas que não chega ao conhecimento do público, não pode ser efetiva.

Dessa forma, muito se ouviu falar, nos grandes meios de comunicação, sobre a Lei Geral de Proteção de Dados Pessoais, primeiro quando de sua aprovação e, posteriormente, na ocasião de sua entrada em vigor, entretanto, tais reportagens costumavam ter um enfoque nas obrigações impostas às organizações e nos princípios da proteção de dados, pouco sendo dito a respeito dos direitos colocados à disposição do titular para que este pudesse salvaguardar a sua privacidade e do que este poderia fazer quando identificasse que um controlador estava descumprindo a legislação.

Isso posto, a autoridade nacional deve ser capaz de conscientizar os titulares acerca de seus direitos. Para tanto, observando a experiência brasileira proporcionada pelos órgãos de defesa do consumidor, como o Procon, que sempre se faz presente nos jornais locais levando conhecimento sobre os direitos dos consumidores, e a experiência europeia, em que as autoridades de controle tem se utilizado dos mais diversos meios para difundir informações relativas ao RGPD, a ANPD precisa desenvolver ações de educação que envolvam mídias analógicas e digitais, alcançando, assim, os indivíduos que ainda tem como principal meio de informação as emissoras de rádio e televisão, bem como aqueles que se informam pela *internet*, seja por mídias digitais, seja por redes sociais.

Nessa senda, a sensibilização do público a respeito da Lei Geral de Proteção de Dados Pessoais é essencial para garantir efetividade à legislação, pois, como visto na subseção anterior, em que pese as reclamações individuais recebidas pelas autoridades de controle dos Estados-membros da União Europeia tenham crescido, há uma disparidade na proporção de

reclamações a cada 10.000 habitantes registradas pelos órgãos de proteção de dados pessoais dos diferentes Estados-membros, o que evidencia que apenas a previsão em lei de direitos dos titulares não é suficiente, é preciso fortalecer os instrumentos que as legislações oferecem para que eles possam ser exercidos.

Diante disso, verifica-se que a LGPD institui um sistema que é capaz de tutelar a privacidade do indivíduo na sociedade da informação, contudo, para a sua efetivação necessita de uma atuação forte e independente da Autoridade Nacional de Proteção de Dados. Sobre este último ponto, como aqui já estudado, tendo em vista que a ANPD foi criada como órgão da administração pública federal, integrante da Presidência da República, se a sua natureza jurídica não for transformada consoante a previsão do artigo 55-A, § 1º, a autoridade nacional poderá sofrer influências externas que comprometam o desempenho de suas atividades, a exemplo de pressões indevidas para que não sejam fiscalizadas as operações de tratamento de determinadas organizações ou para que não haja a imposição de penalidades caso se verifique alguma infração à Lei.

Saliente-se que, atualmente, dos cinco membros do Conselho Diretor da ANPD, três são militares, o que aumenta as preocupações quanto à fiscalização das atividades de tratamento do Poder Executivo por este órgão. De fato, esta não é uma composição comum entre as autoridades de controle de países democráticos, máxime quando se tem em consideração os riscos relacionados à vigilância estatal[671].

No entanto, observou-se um esforço legislativo visando a minimizar estes riscos, de modo que o artigo 55-B da LGPD assegura autonomia técnica e decisória à ANPD. De igual forma, os artigos 55-D e seguinte intentaram dar alguma garantia de permanência no cargo aos membros do Conselho Diretor da ANPD, estabelecendo que estes terão mandados de quatro anos e somente perderão seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar. Dessa feita, ainda é cedo para avaliar se tais previsões serão suficientes para reduzir as ingerências externas na autoridade nacional e garantir que esta seja um mecanismo institucional eficaz de fiscalização e aplicação da LGPD, de modo que será necessário analisar a atuação da ANPD nos próximos anos para examinar a eficiência destes dispositivos.

Ademais, para um desempenho efetivo, a autoridade nacional precisa do orçamento e do pessoal necessário para tanto. Como se viu, a maior parte das autoridades de controle dos

---

[671] SOPRANA, Paula. Bolsonaro nomeia três militares para Autoridade de proteção de dados. 15 out. 2020. **Folha de São Paulo,** Disponível em: https://www1.folha.uol.com.br/mercado/2020/10/bolsonaro-nomeia-tres-militares-para-autoridade-de-protecao-de-dados.shtml. Acesso em: 30 abr. 2021.

Estados-membros tem enfrentando dificuldades relacionadas à falta de recursos humanos e financeiros, o que tem prejudicado a efetividade do Regulamento Geral de Proteção de Dados Pessoais, em virtude da morosidade na conclusão de reclamações e investigações, o que impede, muitas vezes, que o indivíduo tenha uma solução rápida para as suas demandas, as quais muitas vezes são urgentes, além de afetar a credibilidade do sistema de proteção de dados instituído pelo RGPD, já que as penalidades pelo seu descumprimento demoram ou nem mesmo são impostas.

Nesse particular, cumpre dizer que o Brasil, além de suas dimensões continentais, possui uma população consideravelmente maior que a dos Estados-membros da União Europeia, de modo que se exige um contingente de servidores e orçamentário ainda maior para poder difundir o conhecimento acerca da LGPD, receber as reclamações de todos os brasileiros interessados em fazê-las, registrar e analisar as notificações de incidentes de segurança e, ainda, fiscalizar o tratamento de dados realizado pelas mais diversas organizações e punir os agentes pelas respectivas infrações, tudo isso de forma rápida e eficiente. Ressalte-se que a própria Lei 13.7092018 prevê que a ANPD poderá criar as unidades administrativas e unidades especializadas necessárias à aplicação da legislação (artigo 55-C, VI).

Por conseguinte, uma vez que será difícil, máxime nos próximos anos, que disponibilizem, à autoridade nacional, recursos humanos e financeiros suficientes, o caminho que a ANPD deve seguir é o da colaboração com a Secretaria Nacional do Consumidor, para que o titular tenha à sua disposição para peticionar contra o controlador, além dos mecanismos próprios para reclamações da ANPD, as centenas de unidades do Procon espalhadas por todo o país, haja vista que muitas destas demandas decorrerão de relações consumeristas.

Nessa perspectiva, em 22 de março de 2021, a autoridade nacional e a Senacon firmaram um acordo de cooperação técnica, o qual prevê ações conjuntas dos respectivos órgãos que incluem apoio institucional, compartilhamento de informações agregadas e dados estatísticos quanto às reclamações dos consumidores concernentes à proteção de dados pessoais, uniformização de entendimento e coordenação de ações relacionadas a incidentes de segurança, promoção de ações de capacitação e sensibilização referentes a temas de proteção de dados, bem como elaboração de materiais informativos, além de cooperação quanto a ações de fiscalização relacionadas à proteção de dados pessoais no âmbito das relações de consumo. Dessa forma, caberá à Senacon dar conhecimento à ANPD de notificações de

incidentes de segurança de grande escala e de práticas que possam representar violações à LGPD[672].

Por fim, conforme ficou demonstrado nesse trabalho, há muitos pontos de convergência entre o Regulamento Geral de Proteção de Dados da União Europeia e a LGPD, mas não há uma identidade das disposições, de modo que, em algumas questões, o Regulamento europeu é mais protetivo já em outras, como no tratamento de dados de crianças e adolescentes, a legislação brasileira estabelece uma disciplina mais adequada à tutela do titular.

Entretanto, a Lei Geral de Proteção de Dados Pessoais possui mais disposições principiológicas e genéricas que o RGPD, com muitos de seus pontos dependendo de futura regulamentação da autoridade nacional para uma aplicação efetiva. Dessa forma, se a ANPD fizer um uso pertinente de sua função regulatória, a LGPD poderá se tornar uma conquista ainda maior para a salvaguarda da privacidade.

A esse respeito, uma das divergências que mais distanciam as duas legislações é o dever de consulta dos agentes de tratamento às autoridades de controle antes de darem início às operações de processamento quando a avaliação de impacto indicar elevado risco aos titulares na ausência de determinadas medidas, o qual é previsto no RGPD. Esta previsão é de suma importância por permitir que tais autoridades façam um controle preventivo do tratamento de dados e, se for o caso, orientem as organizações a como se conformarem ao Regulamento, reduzindo, assim, o perigo de dano ao titular.

A lei brasileira, por sua vez, não traz disposições específicas acerca do controle preventivo da autoridade nacional sobre determinadas operações de tratamento de dados, o que pode reduzir a efetividade da Lei 13.709/2018, já que se perde a oportunidade de a ANPD avaliar se certo tratamento resulta ou não em ameaças aos indivíduos e, por conseguinte, tomar providências para que o dano ao titular seja evitado.

No entanto, ao editar regulamentos sobre os relatórios de impacto à proteção de dados pessoais, a autoridade nacional poderá estabelecer procedimentos de consulta que lhe possibilitem fazer essa avaliação preventiva, a exemplo do que dispõe o Regulamento europeu. Ademais, tendo em vista que a competência fiscalizatória da autoridade nacional prevista na LGPD também abrange uma atividade preventiva, a ANPD poderá regular como

---

672 BRASIL. Secretaria Nacional do Consumidor. **Acordo de Cooperação Técnica nº 1/2021/GAB-SENACON/SENACON.** Acordo de Cooperação Técnica que entre si celebram a Autoridade Nacional de Proteção de Dados – ANPD e a Secretaria Nacional do Consumidor do Ministério da Justiça e Segurança Pública – MJSP. Disponível em: https://www.defesadoconsumidor.gov.br/images/docs2020/acordo_anpd_senacon_assinado.pdf. Acesso em: 30 abr. 2021.

se dará a adoção de medidas preventivas pelo referido órgão, preenchendo, desse modo, essa lacuna legislativa e, portanto, dando maior efetividade à lei enquanto instrumento de tutela da privacidade.

Outrossim, verificaram-se algumas falhas legislativas tanto no regulamento europeu quanto na lei brasileira de proteção de dados pessoais, de forma que a proteção do titular não é completa em nenhuma das legislações, contudo, cada uma com suas particularidades, ambas conseguem oferecer um grau de proteção à privacidade dos indivíduos na sociedade da informação bastante satisfatório.

Nessa senda, no que se refere à efetividade, viu-se que, na Europa, onde o RGPD já é aplicado há três anos, o Regulamento tem se mostrado eficaz socialmente. Dessarte, como resultado do esforço das autoridades de controle dos Estados-membros da União Europeia, o conhecimento acerca da legislação tem alcançado a maior parte da população, com metade dos entrevistados para o Eurobarômetro tendo respondido saber que existe uma autoridade pública que zela pela proteção dos dados pessoais, bem como com parcela considerável destes entrevistados afirmando conhecer ao menos um dos direitos previstos no RGPD.

Aqui, importa dizer que, ao contrário do Brasil, o Regulamento Geral de Proteção de Dados não é a primeira lei sobre a matéria da União Europeia, de forma que, anteriormente à aprovação do referido regulamento, já havia uma cultura de privacidade em seus países-membros, razão pela qual, para alguns europeus, a existência de um órgão de proteção de dados e alguns dos direitos estabelecidos no RGPD não foram uma novidade.

Isso aponta para uma necessidade ainda maior, no Brasil, de a ANPD, sozinha e por meio de colaboração com outros órgãos, dispender esforços na promoção de ações educativas e na difusão do conhecimento da LGPD por variados meios de comunicação, já que, para que os titulares possam exercer seus direitos, é preciso conhecê-los e saber os meios existentes para exercitá-los. Na União Europeia, toda a informação que tem chegado aos indivíduos se reflete nos números de reclamações recebidas pelas autoridades de controle, os quais aumentaram consideravelmente em comparação ao período pré-RGPD.

Por outro lado, estas reclamações, assim como o número crescente de notificações de violações de dados, também evidenciam que os agentes de tratamento ainda não estão plenamente em conformidade com o Regulamento europeu, com muitas destas organizações tendo dificuldades para justificar as operações de tratamento de acordo com as bases jurídicas elencadas pelo RGPD, além de, por vezes, deixarem de aplicarem os princípios de proteção de dados pessoais e medidas simples de segurança da informação que protegeriam o titular na ocorrência de um incidente de segurança.

Lado outro, o aumento das notificações destas violações demonstram que, mesmo com variações nos Estados-membros, as organizações tem buscado cumprir o Regulamento, verificando-se um aumento gradativo na conformidade destes agentes de tratamento desde a vigência do RGPD. De igual forma, as autoridades de controle registram progressos na procura dos encarregados de proteção de dados por orientações destes órgãos, evidenciando um esforço destes profissionais em adequarem os agentes de tratamento de acordo com as interpretações e diretrizes das autoridades de controle.

No Brasil, mais uma vez tendo-se em vista a muito incipiente cultura de privacidade nas organizações do país, o empenho dos agentes de tratamento, dos encarregados e da autoridade nacional deve ser ainda maior, haja vista que vários conceitos e exigências da Lei 13.709/2018 são, até agora, totalmente desconhecidos. Dessa forma, a atividade orientadora da ANPD adquire grande relevância enquanto norte para a conformação destes agentes com a Lei, razão pela qual a autoridade deverá desenvolver vasto, acessível e compreensível material informativo, divulgando-o em seu *site* e redes sociais, bem como deverá criar procedimentos para receber e responder a pedidos de informação dos encarregados em tempo hábil. Outrossim, a organização e a participação da ANPD em eventos voltados para encarregados também devem fazer parte da agenda do órgão.

Toda essa dedicação se mostra ainda mais essencial quando se salienta que, até setembro de 2020, apenas 24% das organizações empresárias tinham se adequado satisfatoriamente à LGPD. Instituir uma cultura de privacidade no país, pois, não será tarefa fácil, o que exigirá, igualmente, forte atuação preventiva da autoridade nacional no sentido de se adotarem medidas que permitam um controle das operações de tratamento que impliquem elevado risco aos titulares antes que estes aconteçam, a exemplo da experiência europeia.

Por outro lado, como se observou na subseção anterior, as organizações precisam compreender que, ao adotarem a privacidade como um importante valor para as suas atividades, colherão benefícios que vão além da não aplicação de penalidades pela ANPD. Tal compreensão será um importante incentivo para a mudança de cultura destes agentes de tratamento.

Ademais, para aumentar o nível de conformação desses agentes com a Lei Geral de Proteção de Dados Pessoais, a ANPD deverá ser capaz de fiscalizar o cumprimento da legislação, bem como de aplicar, com celeridade, as sanções administrativas, pecuniárias e não pecuniárias, fazendo cessar as infrações identificadas e passando a mensagem, para as demais organizações, de que é preciso se adequar à LGPD, pois a autoridade nacional estará vigilante e atuante.

Nesse particular, assim como se observou nos Estados-membros da União Europeia, deve-se esperar que, nos primeiros anos de vigência da referida Lei, a ANPD foque seu desempenho nas atividades orientadora e preventiva, bem como que haja uma maior aplicação das sanções não pecuniárias mais brandas, como a advertência, somente depois é que há de se verificar um enrijecimento nas ações corretivas e, por conseguinte, um crescimento na imposição de multas.

Já o incentivo às soluções consensuais entre controladores e titulares deve ser constante, como sucede com os órgãos de defesa do consumidor, contudo, também é esperado um considerável número de ações judiciais de responsabilidade civil com fundamento na LGPD, máxime no âmbito das relações consumeristas.

Por fim, conforme se demonstrou, o RGPD tem sido efetivo na tutela dos direitos dos titulares, mas ainda há um longo caminho a se percorrer para se garantir que estes estejam adequadamente resguardados, o que inclui os obstáculos estruturais impostos às autoridades de controle.

De igual forma, no Brasil, a Lei 13.709/2018, a primeira lei de proteção de dados pessoais do país, instituiu um sistema de proteção à privacidade muito próximo das disposições do Regulamento europeu, de modo que também deve ser capaz de assegurar esse direito na sociedade da informação.

Contudo, para tanto dependerá sobremaneira de uma atuação efetiva e independente da Autoridade Nacional de Proteção de Dados Pessoais, a qual, por sua vez, enfrentará o imenso desafio de criar uma cultura de proteção de privacidade num país onde até pouco tempo, diferentemente da Europa, quase não se debatia o tema. Ademais, o desempenho desse órgão poderá ser dificultado pela sua natureza jurídica, pelo tamanho do país e de sua população e pela falta de recursos humanos e financeiros.

Nesse contexto, espera-se que as disposições da LGPD que buscaram dar alguma autonomia à autoridade nacional e algumas garantias aos membros do seu Conselho Diretor, bem como que a possibilidade de ações realizadas em colaboração com outros órgãos, em especial com os de defesa do consumidor, sejam suficientes para que a ANPD possa superar estas dificuldades e desempenhar suas funções da maneira necessária à efetividade da Lei Geral de Proteção de Dados Pessoais.

6 CONCLUSÃO

Na sociedade da informação, os dados são utilizados em todas as atividades humanas, inclusive como matéria-prima e ferramenta de tomada de decisão, de modo que o fornecimento de dados pessoais se tornou quase uma exigência da modernidade.

Nessa senda, as possibilidades de utilização da informação são as mais variadas e o seu tratamento adequado pode trazer inúmeros benefícios para o desenvolvimento da sociedade. Contudo, nesse contexto, o direito à privacidade é constantemente ameaçado.

Por conseguinte, surgem, em todo o mundo, legislações voltadas a regular a coleta e o processamento dessas informações, salvaguardando os direitos fundamentos, mas sem impedir o desenvolvimento econômico-social. Nessa esteira, em 2018, o Brasil sancionou a Lei Geral de Proteção de Dados Pessoais.

Por ser a primeira legislação nacional específica sobre a matéria e uma vez que o tratamento de dados pessoais é uma realidade crescente, este trabalho se propôs a estudar se suas disposições serão capazes de tutelar adequadamente a privacidade dos indivíduos na sociedade da informação ou se, ao contrário, tais normas não serão suficientes para enfrentar os desafios impostos pelos avanços tecnológicos, demandando-se, por conseguinte, novas abordagens legislativas.

Dessa feita, na segunda seção buscou-se demonstrar como os variados contextos históricos, econômicos, sociais e culturais refletem na concepção de privacidade, razão pela qual este é um conceito dinâmico que não pode ser entendido separadamente da sociedade em que foi construído.

Nessa senda, verificou-se que, atualmente, o direito à privacidade tem seu âmbito de proteção ampliado para abarcar também o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da esfera privada.

Igualmente, foram analisadas as três dimensões da privacidade: a espacial, que diz respeito à privacidade existente em um determinado espaço físico; a decisional, que tutela o modo de vida e as decisões do indivíduo; e a informacional, que protege as informações pessoais do indivíduo da coleta, tratamento e disseminação não autorizados. Estas dimensões não são excludentes, mas complementares entre si, de modo que, numa mesma situação, é possível verificar uma violação ou interferência externa em mais de uma perspectiva desse direito. No Brasil, a privacidade informacional passou a ser especialmente protegida por meio da Lei Geral de Proteção de Dados Pessoais, a qual entrou em vigor em setembro de 2020 e que é objeto de estudo desse trabalho.

Além disso, a cultura também influencia a regulação do direito à privacidade, de modo que existem 3 principais modelos regulatórios distintos, quais sejam, a privacidade americana, a privacidade europeia e a privacidade oriental.

O modelo jurídico de privacidade brasileiro é híbrido, cuja concepção do direito à privacidade sofre forte influência da compreensão americana, mas a forma de regular a matéria é muito semelhante ao modelo regulatório europeu, além disso, no Brasil assim como na Europa, esse direito se liga à dignidade da pessoa humana e não à liberdade. Entretanto, a vigência da Lei nº 13.709/2018 tem provocado mudanças no modo de se enxergar a privacidade, por conseguinte, a tendência é que este hibridismo se desfaça e dê lugar a uma correspondência, ainda que imperfeita, com o modelo europeu de acepção e tutela da privacidade.

Nesse diapasão, os atores privados não são irrestritamente livres para realizarem suas transações negociais, devendo observar as disposições legais que visam a proteger os indivíduos em suas relações sociais, como a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. Ademais, no que diz respeito à proteção de dados pessoais, a LGPD aproximou o Brasil da Europa no que atine à tutela da dimensão informacional da privacidade, inclusive, a legislação brasileira possui forte inspiração no Regulamento Geral de Proteção de Dados da União Europeia.

Em seguida, na seção 3, intentou-se esclarecer o que é o direito à proteção de dados pessoais e como tem sido a sua disciplina ao longo das décadas, discorrendo-se, a princípio, sobre a adoção de uma concepção ampla de dado pessoal pela LGPD, assim como pelo Regimento europeu, definindo-o como a informação relacionada à pessoa natural identificada ou identificável.

Ainda, verificou-se que a Lei 13.709/2018 atribuiu regras mais rígidas para o tratamento dos chamados dados pessoais sensíveis, que são aqueles que, se conhecidos e submetidos a determinados processamentos, podem ser utilizados com finalidades discriminatórias ou lesivas, representando riscos potenciais muito maiores do que as demais informações pessoais.

Constatou-se, também, que a LGPD definiu os dados sensíveis a partir de um rol de informações que, historicamente, são assim considerados, não estendendo a disciplina especial ao tratamento de outros dados com igual potencial lesivo, bem como desconsidera que inferências sensíveis podem surgir do processamento de dados pessoais não sensíveis. Apesar disso, a Lei 13.709/2018 traz outras disposições capazes de reduzir tal falha, como os princípios da não discriminação e da prevenção, além da previsão de que as normas

concernentes ao tratamento dessa categoria de informações pessoais serão aplicadas a qualquer operação que revele dados sensíveis e que possa causar dano ao titular.

No que se refere à licitude do tratamento de dados pessoais verificou-se a exigência do consentimento do titular para a realização destas operações ou a verificação de uma das demais hipóteses previstas na Lei 13.709/2018, além de que o agente de tratamento deverá adotar medidas adequadas a garantir a proteção dos dados pessoais em todas as fases de processamento.

Ainda na seção 3, investigou-se a natureza jurídica dos dados pessoais, verificando-se que os dados pessoais são atributos da própria personalidade do indivíduo, de modo que não se protegem os dados por si mesmos, mas para se resguardar a pessoa a quem essas informações se referem.

Ademais, analisou-se a proteção de dados pessoais enquanto direito fundamental, adotando-se, neste trabalho, o entendimento de que o direito à privacidade é gênero do qual são espécies vários direitos da mesma família, dentre eles, o direito à proteção dos dados pessoais.

Outrossim, constatou-se que, para oferecer o nível de salvaguarda que as legislações mais recentes proporcionam, as normas referentes à proteção de dados aprovadas pelo mundo, em especial na Europa, passaram por um desenvolvimento geracional, evidenciando que a disciplina da matéria nem sempre foi a mesma e que o direito vem buscando acompanhar os avanços tecnológicos no intento de garantir efetividade aos direitos dos titulares dos dados.

Também se demonstrou que há um movimento de convergência internacional que busca por soluções comuns concernentes à proteção de dados pessoais, razão pela qual a disciplina da matéria encontra semelhanças em todo o mundo, inclusive na Lei brasileira nº 13.709/2018 e no RGPD, máxime no que diz respeito aos princípios de práticas justas de informação (*Fair Information Practice Principles – FIPPs*), os quais formam o núcleo da proteção dos dados pessoais.

Esse esforço por certa padronização foi fortalecido quando a OCDE emitiu suas Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais no intento de se estabelecer um ambiente regulatório uniforme mínimo por meio de oito princípios, entre os quais se destaca o da responsabilidade, que já continha a ideia de prestação de contas pelo controlador acerca da licitude do tratamento de dados. Isso evidencia que o *accountability*, o qual é visto como uma grande inovação da LGPD, não é recurso tão inovador assim, o que, de modo algum, reduz a importância de sua previsão na legislação brasileira.

Além disso, como efeito do movimento de tendência internacional da tutela dos dados pessoais, também se verifica um padrão referente aos direitos dos titulares nos diferentes ordenamentos jurídicos, os quais, de um modo geral, são: a) direito geral de informação; b) direito de acesso; c) direito de notificação; d) direito de retificação, cancelamento e bloqueio dos dados; e e) direito de não ficar sujeito a uma decisão individual automatizada.

Os direitos dos titulares elencados na LGPD são basicamente os mesmos verificados na maior parte das legislações sobre proteção de dados, os quais, além de intentarem sanar violações ao direito à privacidade, tutelam ativamente este direito, buscando prevenir danos. Dessa feita, não são interesses juridicamente tutelados por si mesmos, mas se tratam de remédios que servem a instrumentalizar a tutela da privacidade, garantindo a sua eficácia.

Além dos princípios e direitos dos titulares em comum previstos nas diferentes legislações sobre proteção de dados, há outro ponto convergente e que tem se mostrado essencial para a efetividade de tais normas: a existência de órgãos administrativos de proteção de dados pessoais independentes.

O Brasil seguiu a experiência internacional e criou a Autoridade Nacional de Proteção de Dados, que deverá ter um papel essencial para a construção da cultura de privacidade no país. Entretanto, a ANPD foi criada como órgão integrante da Presidência da República, prejudicando a sua independência e, por conseguinte, a existência de um mecanismo institucional verdadeiramente eficaz de fiscalização e aplicação da LGPD, já que poderá sofrer influências externas que comprometam o desempenho de suas atividades.

Dessa forma, apesar das previsões da LGPD que asseguram autonomia técnica e decisória à ANPD e oferecem algumas garantias de manutenção no cargo aos membros do Conselho Diretor, para que a autoridade nacional possa desempenhar suas atribuições com a independência necessária, é importante que seja transformada em autarquia, conforme possibilidade prevista no artigo 55-A, § 1º, da Lei 13.709/2018.

Na sequência, na seção 4, examinaram-se as principais ameaças que o tratamento de dados pessoais na sociedade da informação oferece à privacidade e qual a importância das legislações de proteção de dados nesse contexto.

A esse respeito, a Lei 13.709/2018 deve provocar importantes mudanças no comportamento dos agentes de tratamento, posto que, até então vigorava o modelo *opt out* de obtenção da informação, isto é, o consentimento do titular era presumido até que este se manifestasse em contrário, entretanto, com o advento da Lei 13.709/2018, o país passou a adotar o regime *opt in* de coleta dos dados pessoais, o qual exige que a aquiescência seja expressa. Entretanto, ainda há muitos desafios a serem enfrentados no campo do

consentimento para permitir que o titular realmente possa livremente exercer sua autodeterminação informativa, a exemplo de como tornar as políticas de privacidade mais curtas, ao mesmo tempo que contém todas as informações indispensáveis, e de como assegurar que a concordância não sofreu pressões motivadas pelo desejo de se utilizar o serviço.

Além disso, verificou-se que com o surgimento de tecnologias de armazenamento e análise que permitem a extração de conhecimento dos dados pessoais num curto tempo de resposta e a um preço acessível, as organizações passaram a coletar ainda mais informações, mesmo sem ainda terem decidido se tais dados seriam ou não utilizados.

Nesse particular, as legislações mais recentes, como a Lei n° 13.7809/2018, têm reconhecido que o direito fundamental à proteção de dados exige que só sejam coletados os dados estritamente necessários para a finalidade informada ao titular, o que se traduz no princípio da minimização de dados, o qual também deve modificar o comportamento dos controladores nos próximos anos.

De igual forma, demonstrou-se que, de um modo geral, a não observância dos princípios e demais disposições da Lei Geral de Proteção de Dados Pessoais ofendem o direito à privacidade, mas existem determinados tratamentos de dados que se destacam pela gravidade dos riscos ao indivíduo neles envolvidos, os quais, muitas vezes, passam despercebidos, máxime quando são realizados de maneira automatizada e a transparência não é garantida, como a mineração de dados e a definição de perfis.

Dessarte, vez que o *data mining* permite a descoberta de padrões de comportamento até então desconhecidos, amplifica a assimetria informacional entre os agentes de tratamento e os titulares de dados, por vezes chegando a revelar um conhecimento que nem a própria pessoa tem sobre si mesma. Já por meio do rastreamento do comportamento do indivíduo e sua posterior categorização, as organizações conseguem identificar a melhor forma de influenciá-lo, moldando suas atitudes sem que ele nem perceba.

Outrossim, a definição e a aplicação de perfis, por diversas razões, pode levar a um resultado discriminatório. Nos casos em que o *profiling* é automatizado, este risco é acentuado, haja vista que, além de os algoritmos não raramente serem procedimentos complexos e obscuros, ao se retirar qualquer componente humano, subtrai-se também qualquer possibilidade de integrantes dos grupos discriminados transporem a barreira do respectivo perfil, já que isso somente ocorreria por meio de algum aspecto subjetivo do tomador de decisão.

Diante disso, as legislações sobre proteção de dados pessoais, máxime as mais recentes, são de extrema importância por fornecer alguns mecanismos que podem ajudar a mitigar os riscos à privacidade a exemplo dos direitos dos titulares de dados e do princípio da transparência, previsto tanto na LGPD quanto no Regulamento europeu de proteção de dados, uma vez que garante aos seus titulares, de maneira compreensível, explicações e informações acerca do *profiling*. No entanto, é praticamente impossível implementar uma transparência total, principalmente quando muitos modelos de negócio dependem do segredo dos sistemas computacionais que utilizam.

Apesar disso, os algoritmos não devem ser caixas pretas, cujo funcionamento interno ninguém conhece. Uma alternativa que conciliaria a proteção dos dados e o segredo empresarial seria a abertura do código apenas à autoridade responsável, como a ANPD, a qual garantiria o sigilo dessas informações. Então, assegurar-se-ia a transparência do sistema sem comprometer o negócio nele baseado. De todo modo, as autoridades de controle, inclusive a brasileira, poderão realizar auditorias para verificar aspectos discriminatórios no tratamento automatizado de dados pessoais.

Ainda, pela metodologia do *privacy by design* que a Lei nº 13.709/2018 impõe aos agentes de tratamento, estes devem aplicar métodos de prevenção de discriminação e outras ameaças em todas as fases do tratamento, inclusive por meio de análise do código e testes recorrentes no sistema no intento de identificar e corrigir qualquer potencial tendencioso.

Outrossim, apurou-se que conciliar a autodeterminação informativa e a economia digital é um grande desafio que se impõe na atualidade, não existindo respostas prontas sobre como fazê-lo. Contudo, os agentes de tratamento devem, pelo menos, fornecer algum grau de transparência aos indivíduos para que estes possam utilizar a *internet* de forma mais consciente. Igualmente, a educação digital adquire relevo para que as pessoas tenham ciência, ainda que em linhas gerais, de como seu comportamento na *internet* educa os algoritmos de segmentação de conteúdo, capacitando-se, assim, o titular para um uso racional da tecnologia, bem como para um pensamento crítico concernente aos desafios que a sua liberdade de escolha encontra na sociedade da informação.

A LGPD também obriga que os agentes de tratamento adotem medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de incidentes de segurança em que se verifiquem acessos não autorizados ou outras situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Outrossim, traça procedimentos mínimos a serem adotados quando verificados tais incidentes.

Isso porque uma violação de dados é bastante lesiva tanto aos titulares das informações quanto para os agentes de tratamento, razão pela qual as organizações devem procurar evitar a ocorrência de incidentes de segurança e, uma vez detectada uma violação, devem empreender todas as medidas necessárias a solucioná-la o mais rápido possível.

Por fim, na seção 5 analisou-se se as disposições da LGPD instituem um sistema adequado de proteção à privacidade e quais os principais desafios a serem enfrentados para que a Lei 13.709/2018 seja efetiva.

Nesse sentido, investigaram-se os mecanismos de *enforcement* que a Lei Geral de Proteção de Dados Pessoais prevê, a saber, as sanções administrativas e a responsabilidade civil, bem como se procedeu a um mapeamento das semelhanças e diferenças entre a LGPD e o Regulamento Geral de Proteção de Dados da União Europeia com o propósito de, a partir da experiência europeia, traçar algumas prováveis perspectivas para o direito à privacidade com a vigência da Lei n° 13.709/2018.

À vista disso, os resultados da pesquisa demonstram que a Lei Geral de Proteção de Dados Pessoais, assim como toda legislação, tem algumas falhas e lacunas, de modo que não resolve, sozinha, todas as ameaças ao direito à privacidade existentes na sociedade da informação. No entanto, apesar disso, a LGPD consegue instituir, com êxito, um sistema de proteção de dados pessoais cujo objetivo primordial é a prevenção de danos e não a sua reparação, de forma que esta só deve ocorrer em último caso, se o agente de tratamento falhar em adotar as disposições da Lei 13.709/2018 ou se estas não forem suficientes para evitarem a lesão.

Nessa esteira, disciplina desde a coleta até a eliminação das informações pessoais, impondo uma série de obrigações aos agentes de tratamento a serem observadas durante todo o ciclo de vida do dado na organização, prescreve direitos aos titulares, estabelece mecanismos para compelir o controlador e o operador à conformidade com suas normas e atribui diversas competências à autoridade nacional essenciais ao cumprimento da lei, dentre as quais se destacam as funções de orientação, de fiscalização e de punição.

Ademais, ainda objetivando oferecer a tutela mais apropriada aos titulares dos dados e instituir uma cultura de privacidade no país, a Lei 13.709/2018 estimula a autorregulação, incentivando a elaboração de códigos de conduta que observem as especificidades dos diferentes setores e organizações e a implementação de programas de governança em privacidade.

Este sistema de proteção à privacidade previsto na LGPD é bastante convergente com o Regulamento Geral de Proteção de Dados da União Europeia, mas não há uma identidade

entre as legislações, cada uma possuindo peculiaridades que as tornam mais ou menos protetivas em determinados pontos.

Dessarte, verificou-se que, ao contrário do que um cotejo apressado possa sugerir, o RGPD não fornece uma tutela muito mais forte que a Lei brasileira nº 13.709/2018. De fato, principalmente no que se refere aos direitos dos titulares, ao regramento da avalição de impacto e às hipóteses de consulta prévia obrigatória aos órgãos de proteção de dados, o Regulamento europeu oferece uma tutela mais apropriada aos titulares dos dados, entretanto, de um modo geral, muitas diferenças apenas decorrem da técnica legislativa empregada, já que a LGPD é mais genérica que o RGPD.

Desse modo, a aplicação correta dos princípios previstos na lei pátria, uma atividade hermenêutica adequada e a atuação eficaz da ANPD para regular, interpretar, orientar e fiscalizar o cumprimento das disposições legais são capazes de aproximar bastante o nível de proteção de dados de ambas as legislações. Ademais, em alguns aspectos, a Lei Geral de Proteção de Dados proporciona mais salvaguardas aos indivíduos que o Regulamento europeu, a exemplo das normas atinentes ao tratamento de dados de crianças e adolescentes.

Ainda, para se analisar a efetividade da Lei Geral de Proteção de Dados Pessoais, investigaram-se os impactos que a vigência do RGPD provocou nos Estados-membros da União Europeia, o que revelou que as disposições do Regulamento são aptas a resguardar os direitos do indivíduo, mas sua eficácia social depende da atuação dos órgãos de proteção de dados pessoais, muitos dos quais, por sua vez, têm enfrentado escassez de recursos humanos e financeiros, o que repercute negativamente nas ações de fiscalização, na aplicação de penalidades e na apreciação das reclamações dos titulares, ameaçando, por conseguinte a credibilidade do sistema de proteção de dados.

Igualmente, observou-se que, embora o nível de adequação das organizações com o Regulamento europeu esteja crescendo, bem como estejam aumentando os números de notificações de violações de dados e de reclamações dos titulares, os agentes de tratamento ainda estão tendo algumas dificuldades no processo de conformidade, especialmente para justificarem suas operações de acordo com as bases jurídicas previstas no RGPD, aplicarem os princípios de proteção de dados, adequarem suas políticas de privacidade, obterem o consentimento dos titulares conforme os requisitos previstos na legislação e testarem com regularidade a eficiência das medidas de segurança implementadas.

Por todas estas razões, os efeitos pragmáticos do Regulamento Geral de Proteção de Dados da União Europeia são proporcionais à capacidade das autoridades de controle dos seus Estados-membros em, de maneira ampla e rápida, fiscalizar as entidades para,

preventivamente, determinar e orientar quanto à adequação das operações com o Regulamento ou, já tendo ocorrido a infração, impor as sanções estabelecidas pelo RGPD e pelas legislações internas, além de exigir providências no intento de sanar a ilicitude.

De igual forma, verificou-se que a Lei Geral de Proteção de Dados Pessoais traz uma série de disposições com grande potencial para provocar mudanças positivas relacionadas à tutela da privacidade na sociedade da informação, entretanto, a exemplo da experiência europeia, sua efetividade em muito dependerá da aptidão da autoridade nacional em desempenhar com celeridade e eficiência as suas funções de orientação, educação, fiscalização e correção, destacando-se, também, que muitas disposições da Lei nº 13.709/2018 dependem de regulação do referido órgão.

Nesse diapasão, para além das críticas relacionadas à falta de independência da ANPD já apresentadas, constatou-se que a atuação da autoridade nacional encontrará dificuldades relacionadas às dimensões do Brasil e à sua numerosa população, o que também demandará um considerável número de servidores e de disponibilidade orçamentária.

Isso posto, para viabilizar suas ações educativas, bem como o recebimento de reclamações dos titulares, é provável que a ANPD se valha de acordos de colaboração com outros órgãos, sobretudo com a Secretaria Nacional do Consumidor, já que muitas das demandas da autoridade nacional decorrerão de relações consumeristas. Dessa feita, estes acordos permitirão que a ANPD conte com a cooperação das centenas de unidades do PROCON difundidas por todo o país. Para corroborar com tal expectativa, em maio deste ano já fora firmado um ajuste de colaboração entre a autoridade nacional e a Senacon.

Essa sensibilização dos agentes de tratamento e dos brasileiros a respeito das normas de proteção de dados exigirá um esforço por parte da ANPD ainda maior que o realizado pelas autoridades europeias, tendo em vista que, enquanto na Europa há leis de proteção de dados há mais de quatro décadas, no Brasil, o debate sobre a matéria ainda é incipiente. Dessa forma, espera-se que, nos próximos anos, a ANPD se faça presente em meios analógicos e digitais para propalar o conhecimento sobre a Lei Geral de Proteção de Dados Pessoais, bem como mantenha canais de comunicação operantes para sanar as dúvidas dos encarregados de proteção de dados e dos titulares de dados.

Outrossim, vez que boa parte das organizações brasileiras ainda não se adequou completamente à Lei nº 13.709/2018, é vital que a autoridade nacional proceda a bem-sucedidas ações de fiscalização, punindo os agentes de tratamento quando verificadas infrações. Para tanto, mais uma vez, urge a imprescindibilidade de que a ANPD seja dotada da independência e dos recursos humanos e financeiros necessários.

Ademais, para que os titulares possam ter respostas rápidas e satisfatórias às suas demandas, espera-se que a autoridade nacional incentive soluções consensuais entre controladores e titulares, assim como ocorre nos órgãos de defesa do consumidor. De igual modo, é aguardado considerável ajuizamento de ações judiciais de responsabilidade civil com fundamento na Lei Geral de Proteção de Dados Pessoais, de forma que o Judiciário deverá estar atualizado e preparado para lidar com essas demandas, especialmente no que se refere às questões de maior dificuldade, tal como o dano moral presumido e a comprovação do nexo causal.

Por fim, este trabalho não pretendeu esgotar o tema nem fazer predições exatas acerca dos impactos à privacidade que a Lei nº 13.709/2018 irá proporcionar, mas sim traçar algumas expectativas para a proteção de dados no Brasil a partir da vigência da referida Lei, assentando-se na análise das suas disposições legais, na experiência europeia e na própria experiência brasileira no que se refere ao sistema de tutela do consumidor, bem como trazer algumas luzes concernentes ao que é preciso para que a Lei Geral de Proteção de Dados Pessoais não represente meramente um discurso político e sim tenha efeitos práticos e relevantes.

Desse modo, buscou servir de ponto de partida para o estudo da efetividade da proteção de dados pessoais no direito pátrio, permanecendo necessárias as pesquisas acerca das normas da LGPD e da sua aplicação pragmática, não apenas para investigar que as perspectivas esperadas se concretizaram, mas também para avaliar se a Lei n° 13.709/2018 permanecerá eficaz diante dos futuros avanços tecnológicos, bem como se o desenvolvimento das legislações internacionais sobre a matéria revelará que as disposições da Lei Geral de Proteção de Dados Pessoais merecem modificações legislativas ou se a edição de regulamentos específicos pela ANPD já seriam suficientes para resguardar a privacidade dos indivíduos.

Ademais, existem questões que somente serão respondidas nos próximos anos, como qual o verdadeiro impacto que a LGPD provocou no comportamento dos agentes de tratamento, em especial no que diz respeito à obtenção do consentimento, e quais os entendimentos que os tribunais brasileiros firmaram sobre a natureza jurídica da responsabilidade civil e as hipóteses de dano moral *in re ipsa*.

Isso posto, o debate acadêmico e doutrinário acerca do tema da proteção de dados pessoais que, além de estar em constante evolução, ainda é tão incipiente no país, continuará se fazendo imprescindível.

REFERÊNCIAS

ABELSON, Reed. CVS Health and Aetna $69 Billion Merger Is Approved With Conditions. **The New York Times,** 10 out. 2018. Disponível em: https://www.nytimes.com/2018/10/10/health/cvs-aetna-merger.html. Acesso em: 19 set. 2020.

ADJEI, Joseph K. Monetization of Personal Identity Information: Technological and Regulatory Framework. **IEEE Computer Society Washington,** Washington DC/EUA, 14 dez. 2015. Disponível em: https://www.researchgate.net/profile/Joseph_Adjei3/publication/325142873_Monetization_of_personal_digital_identity_information_Technological_and_regulatory_framework/links/5be99f48a6fdcc3a8dd1b2a1/Monetization-of-personal-digital-identity-information-Technological-and-regulatory-framework.pdf. Acesso em: 2 abr. 2020.

AGAN, Amanda; STARR, Sonja. Ban the Box, Criminal Records, and Racial Discrimination: a field experiment. **The Quarterly Journal of Economics,** v. 13, n. 1, fev. 2018**,** p. 191-235. Disponível em: https://academic.oup.com/qje/article-abstract/133/1/191/4060073?redirectedFrom=fulltext. Acesso em: 2 nov. 2020.

ALECRIM, Emerson. *Facebook* encerra VPN Onavo após polemica de privacidade. **Tecnoblog,** mar. 2019. Disponível em: https://tecnoblog.net/279912/facebook-fim-onavo-protect-vpn/. Acesso em: 12 jul. 2019.

ALEMANHA. Bundesministerium der Justiz und für Verbraucherschutz. **Federal Data Protection Act de 30 de junho de 2017 (Federal Law Gazette I, p. 2097),** com a última redação que lhe foi dada pelo artigo 12 da Lei de 20 de novembro de 2019 (Federal Law Gazette I, p. 1.626). Disponível em: https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html. Acesso em: 15 mar. 2020.

ALI. The American Law Institute. **Restatement of the Law Second, Torts.** 2020. Disponível em: https://www.ali.org/publications/show/torts/. Acesso em: 5 jan. 2020.

ALVES, Paulo. Sete fatos sobre a falha no *WhatsApp* que foi usada para espionar governos. **TechTudo,** 6 nov. 2019. Disponível em: https://www.techtudo.com.br/noticias/2019/11/sete-fatos-sobre-a-falha-no-whatsapp-que-foi-usada-para-espionar-governos.ghtml. 16 jun. 2020.

AMAZONAS. Governo do Estado. **Wilson Lima anuncia monitoramento remoto de pessoas que chegam pelo aeroporto e aquisição de testes rápidos.** 25 mar. 2020. Disponível em: http://www.amazonas.am.gov.br/2020/03/wilson-lima-anuncia-monitoramento-remoto-de-pessoas-que-chegam-pelo-aeroporto-e-aquisicao-de-testes-rapidos/. Acesso em: 6 abr. 2020.

APPLE. **Política de Privacidade**. 2020. Disponível em: https://www.apple.com/br/privacy/. Acesso em: 5 jan. 2020.

ARENDT, Hannah. **A Condição Humana.** 10. ed. Rio de Janeiro: Forense Universitária, 2007.

ÁUSTRIA. **Datenschutzbericht 2020.** Disponível em: https://www.dsb.gv.at/dam/jcr:ad90690f-1d10-4e8f-8ed6-b489e888c30f/Datenschutzbericht%202020.pdf. Acesso em: 30 abr. 2021.

BAIÃO, Kelly S; GONÇALVES, Kalline C. A garantia da privacidade na sociedade tecnológica: um imperativo à concretização do princípio da dignidade da pessoa humana. **Civilistica.com**, a. 3, n. 2, 2014. Disponível em: http://civilistica.com/a-garantia-da-privacidade-na-sociedade-tecnologica-um-imperativo-a-concretizacao-do-principio-da-dignidade-da-pessoa-humana/. Acesso em: 12 dez. 2019.

BAMBAUER, Jane R. Tragedy of the Data Commons. **Harvard Journal of Law and Technology,** vol. 25, 19 mar. 2011.Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1789749. Acesso em: 15 mar. 2020.

BBC BRASIL. **Entenda o escândalo de uso político de dados que derrubou valor do *Facebook* e o colocou na mira de autoridades.** 20 mar. 2018. Disponível em: https://www.bbc.com/portuguese/internacional-43461751. Acesso em: 17 mar. 2020.

BBC NEWS. **Coronavirus privacy:** Are South Korea's alerts too revealing? 5 mar. 2020. Disponível em: https://www.bbc.com/news/world-asia-51733145. Acesso em: 6 abr. 2020.
BELMUDES, Guilherme. Impactos do julgamento do STF sobre o direito ao esquecimento. **Jota – Opinião e Análise,** 18 fev. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/impactos-do-julgamento-do-stf-sobre-o-direito-ao-esquecimento-18022021. Acesso em: 23 fev. 2021.

BERALDO, Ana de M. S. Ponderações constitucionais sobre a autonomia psicofísica. *In*: **Civilistica.com**, a. 3, n. 1, 2014. Disponível em: http://civilistica.com/ponderacoes-constitucionais-sobre-a-autonomia-psicofisica/. Acesso em: 13 dez. 2019.

BIONI, Bruno R. Xeque-Mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. **Privacidade e Vigilância,** USP, 2015. Disponível em: https://www.academia.edu/28752561/Xeque-Mate_o_trip%C3%A9_de_prote%C3%A7%C3%A3o_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil. Acesso em: 17 abr. 2020.

BIONI, Bruno R.; MENDES, Laura S. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral brasileira de Proteção de Dados: mapeando convergências na direção de um nível de equivalência. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coords.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** São Paulo: Thomson Reuters Brasil, 2019.

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

BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. **Civilistica.com**, a. 9, n. 3, 2020, p. 1-23. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/662/506. Acesso em: 26 maio 2021.

BITTAR, Carlos Alberto. **Reparação Civil por Danos Morais**. 4. ed. São Paulo: Saraiva, 2015.

BOFF, Salete O; FORTES, Vinícius B; FREITAS, Cinthia O. de A. **Proteção de Dados e Privacidade:** do Direito às novas Tecnologias na Sociedade da Informação. Rio de Janeiro: Lumen Juris, 2018.

BOLESINA, Iuri. **O "Direito à Extimidade" e a sua Tutela por uma Autoridade Local de Proteção de Dados Pessoais:** as inter-relações entre identidade, ciberespaço, privacidade e proteção de dados pessoais em face das intersecções jurídicas entre o público e o privado. 2016. Tese (Doutorado – área de concentração em Demandas Sociais e Políticas Públicas – eixo temático Diversidade e Políticas Públicas) – Programa de Pós-Graduação em Direito da Universidade de Santa Cruz do Sul – UNISC, Santa Cruz do Sul. Disponível em: https://unisc.br/images/curso-24/teses/2016/rosane_porto.pdf. Acesso em: 2 dez. 2019.

BOLÍVIA. **Declaración de Santa Cruz de la Sierra.** XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno. 14 y 15 de noviembre 2003. Disponível em: https://www.segib.org/wp-content/uploads/DeclaraciondeSantaCruz.pdf. Acesso em: 15 abr. 2020.

BOSCO, Francesca et al. Profiling Technologies and Fundamental Rights and Values: regulatory challenges and perspectives from European Data Protection Authorities. *In:* BOSCO, Francesca et al. **Profiling technologies in practice**: Applications and impact on fundamental rights and values. **Wolf Legal Publishers,** 2015. Disponível em: https://research.tilburguniversity.edu/en/publications/profiling-technologies-and-fundamental-rights-an-introduction. Acesso em: 1 out. 2020.

BRASIL. Autoridade Nacional de Proteção de Dados. **Portaria nº 11, de 27 de janeiro de 2021.** Torna pública a agenda regulatória para o biênio 2021-2022. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313. Acesso em: 26 maio 2021

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 4060, de 2012.** Dispõe sobre o tratamento de dados pessoais e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node01bkwy75dp9ctf13g0ctmfpu4zg1645605.node0?codteor=1001750&filename=PL+4060/2012. Acesso em: 30 abr. 2021.

BRASIL. **Constituição Federal de 1988.** Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 13 dez. 2019.

BRASIL. **Lei Complementar nº 105,** de 10 de janeiro de 2001**.** Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm. Acesso em: 13 dez. 2019.

BRASIL. **Lei nº 10.406,** de 10 de janeiro de 2002**.** Institui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 13 dez. 2019.

BRASIL. **Lei nº 12.414**, de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 13 dez. 2019.

BRASIL. **Lei nº 12.737**, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providencias. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 13 dez. 2019.

BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 13 dez. 2019.

BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 abr. 2020.

BRASIL. **Lei nº 5.172,** de 25 de outubro de 1966**.** Dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l5172.htm. Acesso em: 13 dez. 2019.

BRASIL. **Lei nº 8.078,** de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 13 dez. 2019.

BRASIL. **Lei nº 9.296,** de 24 de julho de 1996**.** Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 13 dez. 2019.

BRASIL. Ministério da Defesa. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. **Portaria DECEA nº 224/DGCEA,** de 20 de novembro de 2018. Aprova a edição da ICA 100-40, Instrução sobre "Aeronaves não tripuladas e o Acesso ao Espaço Aéreo Brasileiro. Disponível em: https://publicacoes.decea.gov.br/?i=publicacao&id=4944. Acesso em: 12 dez. 2019.

BRASIL. Ministério da Justiça e Segurança Pública. **Decolar.com é multada por prática de geo pricing e geo blocking.** 16 ago. 2018b. Disponível em: https://www.justica.gov.br/news/collective-nitf-content-51. Acesso em: 20 abr. 2020.

BRASIL. Ministério da Justiça e Segurança Pública. **O que é o Fundo de Defesa de Direitos Difusos – FDD.** Disponível em: https://www.justica.gov.br/seus-direitos/consumidor/direitos-difusos/institucional. Acesso em: 3 mar. 2021.

BRASIL. **Proposta de Emenda à Constituição nº 17, de 2017.** Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1567535523044&disposition=inline. Acesso em: 15 abr. 2020.

BRASIL. Secretaria Nacional do Consumidor. **Acordo de Cooperação Técnica nº 1/2021/GAB-SENACON/SENACON.** Acordo de Cooperação Técnica que entre si celebram a Autoridade Nacional de Proteção de Dados – ANPD e a Secretaria Nacional do Consumidor do Ministério da Justiça e Segurança Pública – MJSP. Disponível em: https://www.defesadoconsumidor.gov.br/images/docs2020/acordo_anpd_senacon_assinado.pdf. Acesso em: 30 abr. 2021.

BRASIL. Superior Tribunal de Justiça. **REsp 1758799 MG 2017/0006521-9,** Relatora: Ministra Nancy Andrighi, Data do Julgamento: 12 nov. 2019, Terceira Turma. Disponível em: https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ITA?seq=1888267&tipo=0&nreg=201700065219&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20191119&formato=PDF&salvar=false. Acesso em: 26 maio 2021.

BRASIL. Superior Tribunal de Justiça. **REsp: 1292141 SP 2011/0265264-3**, Relatora: Ministra NANCY ANDRIGHI, Data de Julgamento: 04/12/2012, T3 - TERCEIRA TURMA, Data de Publicação: DJe 12/12/2012. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/23027511/recurso-especial-resp-1292141-sp-2011-0265264-3-stj/inteiro-teor-23027512. Acesso em: 26 maio 2021.

BRASIL. Superior Tribunal de Justiça. **REsp: 1539056 MG 2015/0144640-6,** Relator: Ministro Luis Felipe Salomão, Data do Julgamento: 06 abr. 2021, Quarta Turma. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201501446406&dt_publicacao=18/05/2021. Acesso em: 26 maio 2021.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 4.815/Distrito Federal**. Requerente: Associação Nacional dos Editores de Livros – ANEL. Intimados: Presidente da República e Presidente do Congresso Nacional. Relatora: Ministra Cármen Lúcia. Brasília/DF, 10 de Junho de 2015. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=10162709. Acesso em: 8 mar. 2018.

BRASIL. Tribunal Superior do Trabalho. **RR 61300-23.2000.5.10.0013,** 1ª Turma, Relator: Ministro João Oreste Dalazen, DEJT 10/06/2005. Disponível em: https://jurisprudencia.tst.jus.br/#19f32e7a289f9dc436bceeadc762069e. Acesso em: 12 dez. 2019.

BRIGATTO, Gustavo. Acesso à *internet* cresce no Brasil, mas 28% dos domicílios não estão conectados. **Valor Econômico,** 26 maio 2020. Disponível em: https://valor.globo.com/empresas/noticia/2020/05/26/acesso-a-internet-cresce-no-brasil-mas-28percent-dos-domicilios-nao-estao-conectados.ghtml. Acesso em: 28 jun. 2020.

BSA. Qual é o "x" da questão em relação a dados? **BSA.org – The Software Aliance.** Disponível em: https://data.bsa.org/wp-content/uploads/2015/10/BSADataStudy_br.pdf. Acesso em: 11 jun. 2019.

CABALLOL, Daniel Contreras; DENDAL, Daniel Pefaur. **Cuaderno de Trabajo nº 17 –** Transparencia Algorítmica: buenas prácticas y estándares de transparencia en el proceso de toma de decisiones automatizadas. Out. 2020. Disponível em: https://www.consejotransparencia.cl/wp-content/uploads/2020/10/Transparencia-Algoritmica.pdf. Acesso em: 29 dez. 2020.

CALDAS, Max Silva; SILVA, Emanoel Costa Claudino. Fundamentos e aplicação do Big Data: como tratar informações em uma sociedade de yottabytes, **Bibliotecas Universitárias –** perspectivas, experiências e perspectivas**,** Belo Horizonte, v. 3, n. 1, jan./jun. 2016. Disponível em: https://periodicos.ufmg.br/index.php/revistarbu/article/view/3086. Acesso em: 28 nov. 2020.

CALIFORNIA. **The California Privacy Rights Act of 2020.** Disponível em: https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf. Acesso em: 5 jan. 2020.

CARVALHO, Victor M.B. de. **O Direito Fundamental à Privacidade ante a Monetização de Dados Pessoais na *Internet*: apontamentos legais para uma perspectiva regulatória**. 2018. Dissertação (Mestrado em Direito) – Programa de Pós-Graduação em Direito, Universidade Federal do Rio Grande do Norte, Natal, 2018. Disponível em: http://bdtd.ibict.br/vufind/Record/UFRN_9ee764a6de69a62f84e93f1356e90adb. Acesso em: 2 abr. 2020.

CASTELLS, Manuel. **A galáxia da *internet*:** reflexões sobre a *internet*, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar Ed., 2003.

CASTELLS, Manuel. **A Sociedade em Rede.** (A era da informação: economia, sociedade e cultura; v. 1). São Paulo: Paz e Terra, 1999.

CASTELLS, Manuel. **La era de la información:** Economía, sociedad y cultura. (Fin del Milenio; v. 3), 1999 [versão digital].

CASTRO, Thamis D. V. de. Notas sobre a teoria tríplice da autonomia, paternalismo e direito de não saber na legalidade constitucional. **OpenAccess**, ano. Disponível em: https://openaccess.blucher.com.br/download-pdf/404/21235. Acesso em: 12 dez. 2019.

CATALA, Pierre. Ebauche d'une théorie juridique de l'information**. Informatica e Diritto,** n. 01, v. 15, 1983. Disponível em: http://www.ittig.cnr.it/EditoriaServizi/AttivitaEditoriale/InformaticaEDiritto/1983_01_015-031_Catala.pdf. Acesso em: 15 mar. 2020.

CERT.BR. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **FAQ:** Perguntas Frequentes ao CERT.br. Disponível em: https://www.cert.br/docs/certbr-faq.html#6. Acesso em: 30 mai. 2020.

CICHONSKI, Paul et al. **Computer Security Incident Handling Guide –** Recommendations of the National Institute of Standards and Technology. Maryland: National Institute of Standards and Technology, ago. 2012. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf. Acesso em: 10 jun. 2020.

CISCO Cibersecurity. **Maximizing the value of your data privacy investments –** data privacy benchmark study. 2019. Disponível em: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/dpbs-2019.pdf. Acesso em: 30 abr. 2021.

CITRON, Danielle Keats; PASQUALE, Frank A. The Scored Society: due process for automated predictions. **Washington Law Review,** v. 89, 8 jan. 2014. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2376209. Acesso em: 18 set. 2020.

CLARKE, Roger. "Profiling: a hidden challenge to the regulation of data surveillance". **Journal of Law, Information and Science,** v. 4, n. 2, 1993. Disponível em: https://www.austlii.edu.au/au/journals/JlLawInfoSci/1993/26.html. Acesso em: 12 set. 2020.

COHEN, Max E. Alguns aspectos do uso da informação na economia da informação. **Ciência da Informação,** v. 31, n. 3, 2002. Disponível em: http://www.scielo.br/scielo.php?pid=S0100-19652002000300003&script=sci_abstract&tlng=pt. Acesso em: 2 abr. 2020.

CONSELHO DA EUROPA PARA A PROTEÇÃO DAS PESSOAS SINGULARES. **Convenção nº 108, de 1981.** Tratamento Automatizado de Dados Pessoais. Disponível em: https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm. Acesso em: 25 abr. 2020.

CONSELHO DA EUROPA. **Chart of signatures and ratifications of Treaty 108.** Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=GGLmmfdZ. Acesso em: 20 abr. 2020.

CONSELHO DA EUROPA. Committee of Ministers. **Resolution (73) 22, On The Protection of the Privacy of Individuals Vis-a-Vis Electronic Data Banks in the Private Sector**. 26 set. 1973. Disponível em: https://rm.coe.int/1680502830. Acesso em: 17 mar. 2020.

CONSELHO DA EUROPA. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.** Strasbourg, 28 jan. 1981. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37. Acesso em: 20 abr. 2020.

CONSELHO DA EUROPA. Corte Europeia de Direitos Humanos. **Convenção Europeia dos Direitos do Homem.** Roma, 4 nov. 1950. Disponível em: https://www.echr.coe.int/Documents/Convention_POR.pdf. Acesso em: 20 abr. 2020.

CONSELHO DA EUROPA. **Directiva 95/46/CE do Parlamento Europeu do Conselho, de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT. Acesso em: 20 abr. 2020.

CONSELHO DA EUROPA. **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/HTML/?uri=CELEX:32016R0679&from=EN. Acesso em: 15 mar. 2020.

CONSELHO DA EUROPA. **Statement on Algorithmic Transparency and Accountability.** 12 jan. 2017. Disponível em: http://www.acm.org/binaries/content/assets/public-policy/2017_joint_statement_algorithms.pdf. Acesso em: 29 dez. 2020.

CONSTINE, Josh. Facebook pays tens to install VPN that spies on them. **Tech Crunch,** fev. 2019. Disponível em: https://techcrunch.com/2019/01/29/facebook-project-atlas/. Acesso em: 12 jul. 2019.

COOLEY, Thomas M. **A Treatiseonthe Law of Torts or the Wrongs Which Arise Independent of Contract**. Chicago: Callaghan, 1879. Disponível em: https://repository.law.umich.edu/books/11/. Acesso em: 13 dez. 2019.

CORTE EUROPEIA DE DIREITOS HUMANOS. **Case of Barbulescu v. Romania.** Strasbourg, 5 set. 2017. Disponível em: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22barbulescu%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-177082%22]}. Acesso em: 8 dez. 2019.

CRAWFORD, Susan. The Origin and Development of a Concept: the information society. **Bull. Med. Libr. Assoc.,** v. 71, n. 4, out. 1983. Disponível em: https://europepmc.org/backend/ptpmcrender.fcgi?accid=PMC227258&blobtype=pdf. Acesso em: 28 nov. 2020.

CUDD, Ann E; NAVIN, Mark C. (Edit.). **Core Concepts and Contemporary Issues in Privacy**. Boston: Springer, 2018.

D'SOUZA, Chris; WILLIAMS, David. The Digital Economy. **Bank of Canada Review,** 2017. Disponível em: https://www.bankofcanada.ca/wp-content/uploads/2017/05/boc-review-spring17-dsouza.pdf. Acesso em: 2 abr. 2020.

DIAKOPOULOS, Nicholas. Principles for Accountable Algorithms and a Social Impact Statement for Allgorithms. **FAT/ML.** Disponível em: https://www.fatml.org/resources/principles-for-accountable-algorithms. Acesso em: 29 dez. 2020.

DIGITAL SHADOWS. **From Exposure to Takeover –** The 15 billion stolen credentials allowing account takeovers. Disponível em: https://resources.digitalshadows.com/whitepapers-and-reports/from-exposure-to-takeover. Acesso em: 28 jun. 2020.

DLA Piper's Cybersecurity and data protection team. **DLA Piper GDPR fines and data breach survey:** january 2021. Disponível em: https://inform.dlapiper.com/10/5202/uploads/data-breach-report-2021.pdf?intIaContactId=P%2bRppLL6Uz7TQ6%2bELU2nbw%3d%3d&intExternalSystemId=1. Acesso em: 30 abr. 2021.

DONEDA, Danilo. A Proteção dos Dados Pessoais como um Direito Fundamental. **Espaço Jurídico,** Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: https://dialnet.unirioja.es/descarga/articulo/4555153.pdf. Acesso em: 17 abr. 2020.

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.

DUBY, Georges (Org.). **História da Vida Privada.** São Paulo: Companhia das Letras, 2009.

DUHIGG, Charles. How Companies Learn Your Secrets. **The New York Times Magazine,** 05 jan. 2012. Disponível em: https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp. Acesso em: 13 set. 2020.

DWORKIN, Ronald. **Domínio da Vida –** aborto, eutanásia e liberdades individuais. São Paulo: Martins Fontes, 2003.

EHRHARDT JÚNIOR, Marcos A. A; TORRES, Marcio R. Direitos Fundamentais e as Relações Privadas. Superando a (pseudo) tensão entre aplicabilidade direta e eficácia indireta para além do patrimônio. **Revista Jurídica**, v. 4, n. 53, 2018, p. 343. Disponível em: http://revista.unicuritiba.edu.br/index.php/RevJur/article/view/3222/371371738. Acesso em: 1 abr. 2019.

ESPANHA. **Agencia Española Protección datos.** Disponível em: https://www.aepd.es/pt-pt. Acesso em: 30 abr. 2021.

EUROSTAT. **Data Browser.** Disponível em: https://ec.europa.eu/eurostat/databrowser/view/TPS00001/default/table?lang=en&bookmarkId=c0aa2b16-607c-4429-abb3-a4c8d74f7d1e. Acesso em: 26 maio 2021.

FACEBOOK. ***Cookies* e outras tecnologias de armazenamento.** Disponível em: https://www.facebook.com/policies/cookies/. Acesso em: 29 dez. 2020.

FACEBOOK. **Log in.** Disponível em: https://www.facebook.com/. Acesso em: 29 dez. 2020.

FELITTI, Chico. Brecha em aplicativo do SUS expôs informações de saúde até de Temer. **Folha de São Paulo,** 26 jan. 2018. Disponível em: https://www1.folha.uol.com.br/cotidiano/2018/01/1953472-brecha-em-aplicativo-do-sus-expos-informacoes-de-saude-ate-de-temer.shtml. Acesso em: 20 jul. 2019.

FLORIDI, Luciano. Information Ethics: on the philosophical foundation of computer ethics. **Ethics and Information Technology,** mar. 1999. Disponível em: https://link.springer.com/article/10.1023/A:1010018611096. Acesso em: 2 dez. 2019.

FLORIDI, Luciano. The Ontological Interpretation of Informational Privacy. **Ethics and Information Technology,** dez. 2005. Disponível em: https://link.springer.com/article/10.1007/s10676-006-0001-7. Acesso em: 2 dez. 2019.

FOGARTY, Philippa. Como empresas estão ganhando dinheiro com seu DNA. **BBC News Brasil,** 7 maio 2019. Disponível em: https://www.bbc.com/portuguese/vert-cap-47926294. Acesso em: 1 out. 2020.

FORBES. **O que representa um minuto na *internet* em 2019.** 3 abr. 2019. Disponível em: https://forbes.com.br/colunas/2019/04/o-que-representa-um-minuto-na-internet-em-2019/. Acesso em: 17 jun. 2020.

FORD FOUNDATION. Advice to my younger self: Latanya Sweeney. **Ford Foundation,** 12 mar. 2019. Disponível em: https://www.fordfoundation.org/ideas/equals-change-blog/posts/advice-to-my-younger-self-latanya-sweeney/. Acesso em: 17 mar. 2020.

FRAGA, Plínio. Como é feito o uso político dos dados roubados nas redes sociais. **Uol Notícias,** 6 jan. 2020. Disponível em: https://noticias.uol.com.br/colunas/plinio-fraga/2020/01/06/como-e-feito-o-uso-politico-dos-dados-roubados-nas-redes-sociais.htm. Acesso em: 10 out. 2020.

FRANÇA. **Commission Nationale de L'informatique et des Libertés.** Disponível em: https://www.cnil.fr/fr. Acesso em: 30 abr. 2021.

FRANÇA. Commission Nationale de L'informatique et des Libertés. **Ensemble, voyons le numérique autrement 2020.** Maio 2021. Disponível em: https://www.cnil.fr/sites/default/files/atoms/files/cnil_-_41e_rapport_annuel_-_2020.pdf. Acesso em: 30 abr. 2021.

FRANÇA. Le Service Public de La Diffusion Du Droit. **Loi nº 78/17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertes.** Version consolidée au 25 ma 2020. Disponível em: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460. Acesso em: 17 maio 2020.

G1 Economia. **França multa *Google* em 50 milhões de euros por violação de lei de privacidade na EU.** 21 jan. 2019. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2019/01/21/franca-multa-google-em-50-milhoes-de-euros-por-violacao-de-lei-de-privacidade-na-ue.ghtml. Acesso em: 30 abr. 2021.

G1 MUNDO. **Suprema Corte dos EUA decide a favor de confeiteiro que se recusou a fazer bolo para casal gay.** 4 jun. 2018. Disponível em: https://g1.globo.com/mundo/noticia/suprema-corte-dos-eua-decide-a-favor-de-confeiteiro-que-se-recusou-a-fazer-bolo-a-casal-gay.ghtml. Acesso em: Acesso em: 8 dez. 2019.

G1 PE. **Recife rastreia 700 mil celulares para monitorar isolamento social e direcionar ações contra coronavírus.** 24 mar. 2020. Disponível em: https://g1.globo.com/pe/pernambuco/noticia/2020/03/24/recife-rastreia-700-mil-celulares-para-monitorar-isolamento-social-e-direcionar-acoes-contra-coronavirus.ghtml. Acesso em: 6 abr. 2020.

GALILEU. **Vai um café grátis, em troca dos seus dados pessoais?** 2019. Disponível em: https://revistagalileu.globo.com/Tecnologia/noticia/2018/09/vai-um-cafe-gratis-em-troca-dos-seus-dados-pessoais.html. Acesso em: 12 jul. 2019.

GANDRA, Alana. Moradores do asfalto têm visão preconceituosa de favelas, mostra pesquisa. **Agência Brasil**, Rio de Janeiro, 16 fev. 2015. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2015-02/moradores-do-asfalto-tem-visao-preconceituosa-em-relacao-favelas. Acesso em: 26 maio 2021

GDPR Enforcement Tracker. **Fines Statistics.** Disponível em: https://www.enforcementtracker.com/. Acesso em: 30 abr. 2021.

GLANCY, Dorothy J. The invention of the right to privacy. **Arizona Law Review**. v. 21, n. 1, 1979. Disponível em: https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1318&context=facpubs. Acesso em: 8 dez. 2019.

GOOGLE. **Ajuda do Conta do *Google* – Gerenciar o Histórico de localização.** 2019. Disponível em: https://support.google.com/accounts/answer/3118687?hl=pt. Acesso em: 12 ago. 2019.

GOOGLE. **Política de Privacidade.** Disponível em: https://policies.google.com/privacy?hl=pt-BR. Acesso em: 25 mar. 2021.

GOOGLE. **Política de Privacidade.** Disponível em: https://policies.google.com/privacy/archive?hl=pt-BR&fg=1. Acesso em: 30 abr. 2021.

GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29º. **Parecer 05/2014 sobre as técnicas de anonimização.** 10 abr. 2014. Disponível em: https://www.gpdp.gov.mo/uploadfile/2016/0831/20160831042518381.pdf. Acesso em: 17 mar. 2020

GRUSTNIY, Leonid. Personal devices at work. **KASPERSKY Daily,** 29 jul. 2019. Disponível em: https://www.kaspersky.com/blog/personal-devices-at-work/27769/. Acesso em: 5 jun. 2020.

GUATEMALA. **Declaración de La Antigua.** II Encuentro Iberoamericano de Protección de Datos. 2003. Disponível em: https://www.redipd.org/sites/default/files/inline-files/declaracion_2003_II_encuentro_es.pdf. Acesso em: 17 abr. 2020.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau. Término do Tratamento de Dados. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro.** São Paulo: Thomson Reuters Brasil, 2019.

GUEDES, Paula. Direcionamento de campanhas eleitorais: lições do passado para 2020. **Its Rio,** 09 abr. 2020. Disponível em: https://feed.itsrio.org/direcionamento-de-campanhas-eleitorais-li%C3%A7%C3%B5es-do-passado-para-2020-de58e32e5dbe. Acesso em: 10 out. 2020.

GUIMARÃES, Keila. Os crimes dos hackers que interrompem até quimioterapia em seqüestros virtuais de hospitais. **BBC News Brasil,** 10 ago. 2017. Disponível em: https://www.bbc.com/portuguese/brasil-40870377. Acesso em: 16 jun. 2020.

GUIMARÃES, Nathália. Bistrô troca dados pessoais de clientes por café grátis. **LeiaJa,** 3 set. 2018. Disponível em: https://m.leiaja.com/tecnologia/2018/09/03/bistro-troca-dados-pessoais-de-clientes-por-cafe-gratis/. Acesso em: 12 jul. 2019.

HARGITAI, Viktor; SHKLOVSKI, Irina; WASOWSKI, Andrzej. Going Beyond Obscurity: organizational approaches to Data Anonymization.**Proceedings of the ACM on Human-Computer Interaction,** vol. 2, n. XSCW, nov. 2018. Disponível em: https://dl.acm.org/citation.cfm?id=3274335. Acesso em: 17 abr. 2020.

HERN, Alex. Uber fined £385,000 for data breach affecting millions of passengers. **The Guardian,** 27 nov. 2018. Disponível em: https://www.theguardian.com/technology/2018/nov/27/uber-fined-385000-for-data-breach-affecting-millions-of-passengers-hacked. Acesso em: 7 jul. 2020.

HUBERMAN, Leo. **História da Riqueza do Homem.** Zahar Editores, 1981 [versão digital].

HYEON OH, Se. *Facebook* obtém receita de US$ 15 bilhões no 1º trimestre de 2019. **Canaltech**, 24 abr. 2019. Disponível em: https://canaltech.com.br/resultados-financeiros/facebook-obtem-receita-de-us-15-bilhoes-no-1o-trimestre-de-2019-137867/. Acesso em: 15 abr. 2020.

IBM SECURITY. **Cost of a Data Breach Report 2019.** Disponível em: https://www.ibm.com/downloads/cas/ZBZLY7KL. Acesso em: 5 jun. 2020.

IGNÁCIO, Sérgio Aparecido. Importância da estatística para o processo de conhecimento e tomada de decisão. **Revista Paranaense de Desenvolvimento,** Curitiba, n. 118, jan./jun. 2010. Disponível em: http://www.ipardes.pr.gov.br/ojs/index.php/revistaparanaense/article/view/89/645. Acesso em: 11 jun. 2019.

INSTITUTO pede que *Facebook* seja condenado em R$ 150 milhões por vazamento de dados. **Migalhas,** 14 maio 2019. Disponível em: https://www.migalhas.com.br/Quentes/17,MI302322,71043-Instituto+pede+que+Facebook+seja+condenado+em+R+150+milhoes+por. Acesso em: 20 jul. 2019.

INTERNATIONAL STANDARD. **Information technology – Security techniques – Information security incident management –** Part 1: principles of incident management. 1 nov. 2016. Disponível em: https://www.sis.se/api/document/preview/921093/. Acesso em: 2 nov. 2020.

INTERPOL. **Cybercriminals targeting critical healthcare institutions with ransomware.** 4 abr. 2020Disponível em: https://www.interpol.int/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware. Acesso em: 5 jun. 2020.

IRLANDA. **An Coimisiún um Chosaint Sonraí.** Disponível em: https://www.dataprotection.ie/. Acesso em: 30 abr. 2021.

IRLANDA. Data Protection Commission. **Annual Report 2020**. Disponível em: https://www.dataprotection.ie/sites/default/files/uploads/2021-05/DPC%202020%20Annual%20Report%20 %28English%29.pdf. Acesso em: 30 abr. 2021.

IRLANDA. Data Protection Commission. **Data Protection Commission publishes 2020 Annual Report.** 25 fev. 2021. Disponível em: https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-publishes-2020-annual-report. Acesso em: 30 abr. 2021.

ITÁLIA. **Garante per la Protezione dei dati personali**. Disponível em: https://www.garanteprivacy.it/home/attivita-e-documenti/documenti/relazioni-annuali. Acesso em: 30 abr. 2021.

JAQUET-CHIFFELLE, David-Olivier. Reply: direct and indirect profiling in the light of virtual persons. *In:* HILDEBRANDT, Mireille. **Defining Profiling:** A new type of knowledge? Springer, Dordrecht, 2008. Disponível em: https://link.springer.com/chapter/10.1007%2F978-1-4020-6914-7_2#citeas. Acesso em: 28 nov. 2020.

JUNQUEIRA, Daniel. Hackers criam golpe que lembra um ‘chupa-cabra’ virtual. **Olhar Digital,** 26 jun. 2020. Disponível em: https://olhardigital.com.br/fique_seguro/noticia/hackers-criam-golpe-que-lembra-um-chupa-cabra-virtual/102716. Acesso em: 19 set. 2020.

KARVALICS, László Z. Information Society – what is it exactly? (The meaning, history and conceptual framework of an expression). **Leonardo da Vinci,** Budapeste, jan. 2007. Disponível em: https://www.researchgate.net/publication/237332035_Information_Society_-_what_is_it_exactly_The_meaning_history_and_conceptual_framework_of_an_expression. Acesso em: 15 set. 2020.

KASPERSKY. **40% of data breaches affect customer information –** how can businesses reduce the potential damage. 14 abr. 2020. Disponível em: https://www.kaspersky.com/about/press-releases/2020_40-of-data-breaches-affect-customer-information. Acesso em: 5 jun. 2020.

KASPERSKY. **Beign little make you invincible?** The third of small companies that suffered a data breach wouldn’t agree. 10 set. 2019. Disponível em: https://www.kaspersky.com/about/press-releases/2019_third-of-small-companies-suffered-a-data-breach. Acesso em: 5 jun. 2020.

KASPERSKY. **DDoS during the coronavirus pandemic: number of attacks on educational and administrational web resources tripled in Q1 2020**. 06 maio 2020. Disponível em: https://www.kaspersky.com/about/press-releases/2020_ddos-during-the-coronavirus-pandemic-number-of-attacks-on-educational-and-administrational-web-resources-tripled-in-q1-2020. Acesso em: 3 jul. 2020.

KASPERSKY. **Man-made disaster:** half of cybersecurity incidents in industrial networks happen due to employee errors. 20 ago. 2019. Disponível em: https://www.kaspersky.com/about/press-releases/2019_man-made-disaster-half-of-cybersecurity-incidents-in-industrial-networks-happen-due-to-employee-errors. Acesso em: 5 jun. 2020.

KASPERSKY. **One-in-three computers processing biometry face attempts to steal data or remote control.** 2 dez. 2019. Disponível em: https://www.kaspersky.com/about/press-releases/2019_one-in-three-computers-processing-biometry-face-attempts-to-steal-data-or-remote-control. Acesso em: 3 jul. 2020.

KASPERSKY. **Your digital identity could be on sale for less than $50 – new Dark Web research from Kaspersky Lab shows.** 5 nov. 2018. Disponível em: https://www.kaspersky.com/about/press-releases/2018_digital-identity-for-less-than-50-dollars. Acesso em: 3 jul. 2020.

KIM, Nemo. 'More scary than coronavirus': South Korea's health alerts expose private lives. **The Guardian.** 6 mar. 2020. Disponível em: https://www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives. Acesso em: 6 abr. 2020.

KOKOTT, Juliane; SOBOTTA, Christoph. The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR **International Data Privacy Law,** Oxford Academic**.** v. 3, n. 4, 15 set. 2013. Disponível em: https://academic.oup.com/idpl/article/3/4/222/727206. Acesso em: 17 abr. 2020.

KOOPS, Bert-Jaap et al. A Typology of Privacy. **U. Pa. J. Int'l L.** v. 38, a. 2, p. 485-575. Disponível em: https://scholarship.law.upenn.edu/jil/vol38/iss2/4/. Acesso em: 2 dez. 2019.

KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. Private traits and atributes are precictable from digital records of human behavior. **PNAS,** Califórnia, vol. 110, n. 15, 9 abr. 2013. Disponível em: https://www.pnas.org/content/pnas/110/15/5802.full.pdf. Acesso em: 17 mar. 2020.

KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. Private traits and attributes are predictable from digital records of human behavior. **PNAS Early Edition,** 29 out. 2012. Disponível em: http://goodtimesweb.org/surveillance/2013/PNAS-2013-Kosinski-1218772110.pdf. Acesso em: 2 nov. 2020.

KROLL, Joshua A. et al. Accountable Algorithms. **University of Pensylvania Law Review,** v. 165, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2765268. Acesso em: 18 set. 2020.

LAUDON, Kenneth; LAUDON, Jane. **Sistemas de Informação Gerenciais.** 9. ed., Pearson Universidades, 2011.

LAW Innovation. **ICTS Protiviti:** 82% das empresas ainda estão despreparadas para cumprir a LGPD. 03 dez. 2020. Disponível em: https://lawinnovation.com.br/icts-protiviti-82-das-empresas-ainda-estao-despreparadas-para-cumprir-a-lgpd/. Acesso em: 24 abr. 2021.

LEVIN, Avner; ABRIL, Patricia Sánchez. Two Notions of Privacy Online. *In:* **Vanderbilt J. of Ent. And Tech. Law,** v. 11, n. 4. Disponível em: *In:* POST, Robert C. Three Concepts of Privacy. *In:* **The Georgetown Law Journal,** v. 89, n. 2.089, 2000-2001, p. 2.087-2.098. Disponível em: https://digitalcommons.law.yale.edu/fss_papers/185/. Acesso em: 13 dez. 2019.

LEYDEN, John. Breached Bitcoin Bithumb bosses blame bod's BYOD. **The Register,** 6 jul. 2017. Disponível em: https://www.theregister.com/2017/07/06/bithumb_hack/. Acesso em: 2 jul. 2020.

LI, Wendy C. Y.; NIREI, Makoto; YAMANA, Kazufumi. Value of Data: There's no such thing as a free lunch in the digital economy. **VOX CEPR Policy Portal,** 23 jul. 2019. Disponível em: https://voxeu.org/article/no-such-thing-free-lunch-digital-economy. Acesso em: 2 abr. 2020.

LIMINAL. **Fim dos *cookies* no *Google Chrome*:** o impacto no marketing. 5 fev. 2020. Disponível em: https://liminal.pt/martech-magazine/fim-cookies-chrome-impacto-no-marketing/. Acesso em: 20 out. 2020.

LÔBO, Paulo. Direito à Privacidade e sua Autolimitação. *In*: EHRHARDT JÚNIOR, Marcos; LOBO, Fabiola Albuquerque (Coord.). **Privacidade e sua Compreensão no Direito Brasileiro.** Belo Horizonte: Fórum, 2019.

LÔBO, Paulo. **Direito Civil:** v. 2: obrigações. 7. ed. São Paulo: Saraiva Educação, 2019.

LUIZ, Gabriel. Banco Inter fecha acordo para pagar R$ 1,5 milhão após vazamento de dados de clientes. **G1 Notícias,** 19 dez. 2018. Disponível em: https://g1.globo.com/df/distrito-federal/noticia/2018/12/19/banco-inter-fecha-acordo-para-pagar-r-15-milhao-de-indenizacao-apos-vazamento-de-dados-de-clientes.ghtml. Acesso em: 20 jul. 2019.

MACHADO, Diego. **Tutela jurídica da privacidade, anonimização de dados e anonimato na *internet***. 2018. Disponível em: https://www.researchgate.net/publication/328784970_Tutela_juridica_da_privacidade_anonimizacao_de_dados_e_anonimato_na_internet. Acesso em: 17 abr. 2020.

MACHADO, Diego; DONEDA, Danilo. Proteção de Dados Pessoais e Criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. **Revista dos Tribunais**, v. 998, Caderno Especial, p. 99-128, São Paulo: RT, dez. 2018. Disponível em: https://www.researchgate.net/publication/330401277_Protecao_de_dados_pessoais_e_criptografia_tecnologias_criptograficas_entre_anonimizacao_e_pseudonimizacao_de_dados. Acesso em: 17 abr. 2020.

MAGRANI, Eduardo; OLIVEIRA, Renan Medeiros de. A esfera pública (forjada) na era das *fake news* e dos filtros-bolha. **Cadernos Adenauer XIX,** n. 4, 2018. Disponível em: http://eduardomagrani.com/wp-content/uploads/2019/05/PUBLICACAO-nova-2019-KA-Cadernos-2018.4-site.pdf. Acesso em: 10 out. 2020.

MARQUESONE, Rosangela. **Big Data –** Técnicas e tecnologias para extração de valor dos dados. Casa do Código [versão digital].

MARR, Bernard. Big Data At Caesars Entertainment – A one billion dollar asset? **Forbes,** 18 maio 2015. Disponível em: https://www.forbes.com/sites/bernardmarr/2015/05/18/when-big-data-becomes-your-most-valuable-asset/#318235b61eef. Acesso em: 28 jun. 2020.

MARTÍNEZ, Andrés García. **La Tutela Multinivel del Derecho a la Protección de Datos Personales del Contribuyente: TEDH-TJUE. AFDUAM,** n. 22, 2018. Disponível em: https://repositorio.uam.es/bitstream/handle/10486/690020/AFDUAM_22_19.pdf?sequence=1&isAllowed=y. Acesso em: 22 abr. 2020.

MASSON, Mary. Michigan Medicine notifies patients of health information data breach. **Michigan Medicine,** University of Michigan, 25 jun. 2018. Disponível em: https://www.uofmhealth.org/news/archive/201806/michigan-medicine-notifies-patients-health-information-data. Acesso em: 18 jun. 2020.

MAYER, Jonathan; MUTCHLER, Patrick. **MetaPhone:** The Sensivity of Telephone Metadata. 12 mar. 2014. Disponível em: http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/. Acesso em: 17 mar. 2020.

MAYER-SCHÖNBERGER, Viktor. Generational Development Data Protection in Europe**.** *In:* AGRE, Philipe E.; ROTENBERG, Marc. **Technology and Privacy:** The New Ladscape. Londres, Inglaterra: MIT Press, 2001. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=H2KB2DK4w78C&oi=fnd&pg=PA219&dq=Generational+development+of+data+protection+in+Europe&ots=1X0evcYsOo&sig=tsO6DFUyVQdFjfI2JkJLetz8WmM#v=onepage&q=Generational%20development%20of%20data%20protection%20in%20Europe&f=false. Acesso em: 20 abr. 2020.

MCCARTY, Eric. The State of Enterprise Mobility in 2018: Five key trends. **INSIGHTS,** 06 jun. 2018. Disponível em: https://insights.samsung.com/2018/06/06/the-state-of-enterprise-mobility-in-2018-five-key-trends/. Acesso em: 5 jun. 2020.

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

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à Nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. **Revista dos Tribunal Online,** Thomson Reuters, 2018, p. 22. Disponível em: https://www.academia.edu/42740879/Coment%C3%A1rio_%C3%A0_nova_Lei_de_Prote%C3%A7%C3%A3o_de_Dados_lei_13.709_2018_o_novo_paradigma_da_prote%C3%A7%C3%A3o_de_dados_no_brasil?auto=download. Acesso em: 26 maio 2021.

MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. **Revista Direito Público,** v. 16, n. 90, 2019, p. 60-61. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766/Schertel%20Mendes%3B%20Mattiuzzo%2C%202019. Acesso em: 18 set. 2020.

MENEZES NETO, Elias J; MORAIS, José Luis B; BEZERRA, Tiago José S. L. O projeto de Lei de Proteção de Dados Pessoais (PL 5.276/2016) no mundo do Big Data: o fenômeno da Dataveillance em relação à utilização de metadados e seu impacto nos direitos humanos. **Revista Brasileira de Políticas Públicas,** v. 7, n. 3, 2017. Disponível em: https://www.publicacoesacademicas.uniceub.br/RBPP/article/view/4840. Acesso em: 17 mar. 2020.

MHADHBI, A. Estudo da ONU revela que mundo tem abismo digital de gênero. **ONU News**, 06 nov. 2019. Disponível em: https://news.un.org/pt/story/2019/11/1693711. Acesso em: 28 jun. 2020.

MIRANDA, Francisco Cavalcanti Pontes de. **Tratado de Direito Privado.** Tomo VII – Parte Especial – Direito de Personalidade. Direito de família: direito matrimonial. São Paulo: Bookseller, 2003. [Livro Digital].

MITTELSTADT, Brent Daniel. et al. The ethics of algoritms: mapping the debate. **SAGE Journals,** 1 dez. 2016. Disponível em: https://journals.sagepub.com/doi/full/10.1177/2053951716679679. Acesso em: 18 set. 2020.

MONTJOYE, Yves-Alexandre; RADAELLI, Laura; SINGH, Vivek; PENTLAND, Alex. Unique in the shopping mall: On the reidentifiability of credit card metadata. **Science,** v. 347, n. 6221, jan. 2015. Disponível em: https://www.researchgate.net/publication/271591449_Unique_in_the_shopping_mall_On_the_reidentifiability_of_credit_card_metadata. Acesso em: 15 abr. 2020.

MOORE, Nick. The Information Society**.** *In:* MOORE, Nick. **World Information Report.** UNESCO Reference Books, Bernan Assoc. Geneva, 1998. [Versão digital].

MORAES, Maria Celina Bodin de. LPGD: um novo regime de responsabilização civil dito "proativo". Editorial à **Civilistica.com,** Rio de Janeiro, a. 8, n. 3, 2019. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/448/377. Acesso em: 26 maio 2021.

MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD. *In:* Proteção de Dados Pessoais: privacidade *versus* avanço tecnológico. **Cadernos Adenauer,** Rio de Janeiro: Fundação Konrad Adenauer, ano XX, n. 3, out. 2019. Disponível em: https://www.kas.de/documents/265553/265602/Caderno+Adenauer+3+Schutz+von+pers%C3%B6nlichen+Daten.pdf/476709fc-b7dc-8430-12f1-ba21564cde06?version=1.0&t=1571685012573. Acesso em: 26 maio 2021.

MORAES, Maria Celina Bodin. A constitucionalização do direito civil e seus efeitos sobre a responsabilidade civil. *In:* **Direito, Estado e Sociedade**, v. 9, n. 29, jul./dez. 2006.

MOREIRA, Adilson José. **O que é discriminação?** Belo Horizonte (MG): Letramento: Casa do Direito: Justificando, 2017.

MULHOLLAND, Caitlin Sampaio. 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 Direitos e Garantias Fundamentais**, Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018. Disponível em: http://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603. Acesso em: 17 abr. 2020.

MULHOLLAND, Caitlin. Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018). *In:* MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (Coords.). **Responsabilidade Civil e Novas Tecnologias.** São Paulo: Editora Foco, 2020.

MUMFORD, Lewis. **A Cidade na História** – suas origens, transformações e perspectivas. 4. ed. São Paulo: Martins Fontes, 2004.

NAKASHIMA, Ryan. AP Exclusive: Google tracks your movements, like it or not. **AP News,** 13 ago. 2018. Disponível em: https://www.apnews.com/828aefab64d4411bac257a07c1af0ecb. Acesso em: 12 jul. 2019.

NARAYANAN, Arvind; SHMATIKOV. Privacy and Security: myths and fallacies of "Personally Identifiable Information". **Comunicationofthe ACM,** vol. 53, n. 6, jun. 2010. Disponível em: https://pdfs.semanticscholar.org/44f3/2957fd4cdd2633b6d0cb744b3461f1b73124.pdf. Acesso em: 15 mar. 2020.

NEVES, Fabricia Vancim Frachone Neves. **Uma Análise da Aplicabilidade do Data Warehouse no Comércio Eletrônico, enfatizando o CRM analítico.** 2001. 159 f. Dissertação (Mestrado em Engenharia da Produção) – Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos, 2001. Disponível em: https://teses.usp.br/teses/disponiveis/18/18140/tde-10042017-160131/en.php. Acesso em: 28 nov. 2020.

NOGUEIRA, Luiz. Hackers roubam imagens do sistema da agência de fronteira dos EUA. **Olhar Digital,** 11 jun. 2019. Disponível em: https://olhardigital.com.br/fique_seguro/noticia/dados-de-usuarios-que-deixaram-os-eua-sao-roubados/86737. Acesso em: 2 jul. 2020.

O GLOBO. **Casal processa publicação e critica invasão grotesca de sua privacidade**. 19 set. 2012. Disponível em: https://oglobo.globo.com/mundo/revista-francesa-publica-fotos-de-kate-middleton-de-topless-6090825. Acesso em: 8 dez. 2019.

O GLOBO. **Psicólogo que criou aplicativo da Cambridge Analytica acreditava que sistema era legal.** 21 mar. 2018. Disponível em: https://oglobo.globo.com/mundo/psicologo-que-criou-aplicativo-da-cambridge-analytica-acreditava-que-sistema-era-legal-22510640. Acesso em: 15 abr. 2020.

O'DONNELL, Lindsey. Report: 'BlueLeaks' Exposes Sensitive Data From Police Departments. **Threat Post,** 22 jun. 2020. Disponível em: https://threatpost.com/report-blueleaks-exposes-sensitive-data-from-police-departments/156806/. Acesso em: 29 dez. 2020.

O'NEIL, Cathy. Personality Tests Are Failing American Workers. **Bloomberg Opinion,** 18 jan. 2018. Disponível em: https://www.bloomberg.com/opinion/articles/2018-01-18/personality-tests-are-failing-american-workers. Acesso em: 2 nov. 2020.

OCDE**. Declaration on Transborder Data Flows.** Disponível em: https://legalinstruments.oecd.org/public/doc/108/108.en.pdf.. Acesso em: 20 abr. 2020.

OCDE. **OECD Guidelines o the Protection of Privacy and Transborder Flows of Personal Data.** 2013. Disponível em: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Acesso em: 20 abr. 2020.

OEA. Comissão Interamericana de Direitos Humanos. **Convenção Americana sobre Direitos Humanos,** assinada na Conferência Especializada Interamericana sobre Direitos Humanos, San José, Costa Rica, em 22 de novembro de 1969. Disponível em: https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm. Acesso em: 8 dez. 2019.

OHM, Paul. Broken Promises of Privacy: responding to the surprising failure of anonymization. **UCLA Law Review,** n. 1.701, 2010. Disponível em: https://www.uclalawreview.org/pdf/57-6-3.pdf. Acesso em: 17 abr. 2020.

OLHAR DIGITAL. **Cambridge Analytica:** tudo sobre o escândalo do *Facebook* que afetou 87 milhões. 21 mar. 2018. Disponível em: https://olhardigital.com.br/2018/03/21/noticias/cambridge-analytica/. Acesso em: 4 abr. 2020.

OLHAR DIGITAL. **Com poucos impostos, Irlanda atrai gigantes da tecnologia.** 10 out. 2017. Disponível em: https://olhardigital.com.br/2017/10/13/olhar-digital-internacional/com-poucos-impostos-irlanda-atrai-gigantes-da-tecnologia/. Acesso em: 30 abr. 2021.

ONAVO. **Onavo Protect Will no Longer be Availabe**. 2019. Disponível em: https://www.onavo.com/. Acesso em: 12 jul. 2019.

ONU News. Pessoas com HIV continuam discriminadas no mercado de trabalho. **Agência Brasil,** 26 jul. 2018. Disponível em: https://agenciabrasil.ebc.com.br/internacional/noticia/2018-07/pessoas-com-hiv-continuam-discriminadas-no-mercado-de-trabalho. Acesso em: 2 nov. 2020.

ONU. Assembleia Geral. **Declaração Universal dos Direitos Humanos.** 10 dez. 1948. Disponível em: https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf. Acesso em: 8 dez. 2019.

ONU. **Pacto Internacional de Direitos Civis e Políticos,** adoptado e aberto à assinatura, ratificação e adesão pela Assembleia Geral das Nações Unidas pela Resolução nº 2.200-A (XXI), de 16 de dezembro de 1966. Disponível em: http://www.cidadevirtual.pt/cpr/asilo2/2pidcp.html. Acesso em: 8 dez. 2019.

OTTERLO, Martijn van. A Machine Learning View on Profiling. **Cognitive Artificial Intelligence,** Radboud University Nijmegen. Disponível em: http://www.martijnvanotterlo.nl/cpdp11-draftversion-ProjectedWorlds-MartijnVanOtterlo-2011.pdf. Acesso em: 12 out. 2020.

PAÍSES BAIXOS. **Autoriteit Persoonsgegevens**. Disponível em: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/gebruik-uw-privacyrechten/klacht-melden-bij-de-ap. Acesso em: 30 abr. 2021

PAÍSES BAIXOS. **Klachtenrapportage:** facts & figures – overzicht 2020. Disponível em: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_klachtenrapportage_2020.pdf. Acesso em: 30 abri. 2021.

PALMER, Michael. Data is the new oil. **ANA Marketing Maestros,** 3 nov. 2006. Disponível em: https://ana.blogs.com/maestros/2006/11/data_is_the_new.html. Acesso em: 28 jun. 2020.

PASSOS, Bruno Ricardo dos Santos. **O Direito à Privacidade e a Proteção aos Dados Pessoais na Sociedade da Informação:** uma abordagem acerca de um novo direito fundamental. 2017. Dissertação (Mestrado em Direito Público) – Programa de Pós-Graduação em Direito da Universidade Federal da Bahia, Salvador. Disponível em: https://repositorio.ufba.br/ri/handle/ri/22478. Acesso em: 17 mar. 2020.

PEACHEY, Kevin. HMRC forced to delete five million voice files. **BBC News,** 03 maio 2019. Disponível em: https://www.bbc.com/news/business-48150575. Acesso em: 30 abr. 2021.

PEIXOTO, Erick L. C; EHRHARDT JÚNIOR, Marcos. Breves Notas sobre a Ressignificação da Privacidade. **Revista Brasileira de Direito Civil,** Belo Horizonte, v. 16, jan./jun, 2018. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/230. Acesso em: 12 jun. 2019.

PEIXOTO, Erick L. C; EHRHARDT JÚNIOR, Marcos. Os Desafios da Compreensão do Direito à Privacidade no Sistema Jurídico Brasileiro em face das Novas Tecnologias. *In*: EHRHARDT JÚNIOR, Marcos; LOBO, Fabiola Albuquerque (Coord.). **Privacidade e sua Compreensão no Direito Brasileiro.** Belo Horizonte: Fórum, 2019.

PEREIRA, Caio Mário da Silva. **Instituições de Direito Civil**. Rio de Janeiro: Forense, 2010.

PEZZELLA, Maria Cristina Cereser; GHISI, Silvano. A manipulação de dados pessoais nas relações de consumo e o sistema "*crediscore*". **Civilista.com,** ano 4, n. 1, 2015. Disponível em: http://civilistica.com/a-manipulacao-de-dados-pessoais/. Acesso em: 17 abr. 2020.

PHILLIPS, Jonathon et al. **Four Principles of Explainable Artificial Intelligence**. Maryland: National Institute of Standards and Technology, ago. 2020. Disponível em: https://www.nist.gov/system/files/documents/2020/08/17/NIST%20Explainable%20AI%20Draft%20NISTIR8312%20%281%29.pdf. Acesso em: 29 dez. 2020.

PINHO, Frederico A. S. O. **Anonimização de bases de dados empresariais de acordo com a nova Regulamentação Europeia de Proteção de Dados.** 2017. Dissertação (Mestrado em Segurança Informática), Departamento de Ciência de Computadores, Faculdade de Ciências, Universidade do Porto. Disponível em: https://cracs.fc.up.pt/sites/default/files/MSI_Dissertacao_FINAL.pdf. Acesso em: 17 mar. 2020

PIRES, Lucas de Almendra Freitas. **Direito à Privacidade no Âmbito da Sociedade da Informação:** reflexões em torno da questão nos inícios do século XXI. 2014. Dissertação (Mestrado Científico em Ciências Jurídico-Políticas) – Faculdade de Direito da Universidade de Coimbra, Portugal. Disponível em: https://eg.uc.pt/bitstream/10316/34844/1/Direito%20a%20privacidade%20no%20ambito%20da%20sociedade%20da%20informacao%20reflexoes%20em%20torno%20da%20questao%20nos%20inicios%20do%20seculo%20XXI.pdf. Acesso em: 12 jun. 2019.

POLÔNIA. **Urzad Ochrony Danych Osobowych**. Disponível em: https://uodo.gov.pl/pl/138/2059. Acesso em: 30 abr. 2021.

PORTAL DE NOTÍCIAS G1. **A Globo respeita e protege sua privacidade.** Disponível em: https://privacidade.globo.com/pdf/Vers%C3%A3o%20Publica%C3%A7%C3%A3o_Pol%C3%ADtica%20de%20Privacidade_Globo.pdf. Acesso em: 29 dez. 2020.

PORTAL DE NOTÍCIAS G1. **Home.** Disponível em: https://g1.globo.com/. Acesso em: 29 dez. 2020.

PORTUGAL. Comissão Nacional de Proteção de Dados. **Relatório de Atividades 2019 – 2020.** Disponível em: https://www.cnpd.pt/media/adsndrsf/relato-rio-2019-2020.pdf. Acesso em: 30 abr. 2021.

POSNER, Richard A. **A Economia da Justiça.** São Paulo: WMF Martins Fontes, 2010.

POST, Robert C. Three Concepts of Privacy. **The Georgetown Law Journal,** v. 89, n. 2.089, 2000-2001, p. 2.087-2.098. Disponível em: https://digitalcommons.law.yale.edu/fss_papers/185/. Acesso em: 2 dez. 2019.

PRIVACY TECH. **Mais de 200 milhões de brasileiros têm dados pessoais expostos em nova falha de segurança do Ministério da Saúde.** 8 dez. 2020. Disponível em: https://privacytech.com.br/destaque/mais-de-200-milhoes-de-brasileiros-tem-dados-pessoais-expostos-em-nova-falha-de-seguranca-do-ministerio-da-saude.,381645.jhtml. Acesso em: 2 jan. 2021.

PROSSER, William L. Privacy. **California Law Review,** v. 48, n. 3, ago. 1960. Disponível em: https://heinonline.org/HOL/LandingPage?handle=hein.journals/calr48&div=31&id=&page=. Acesso em: 2 dez. 2019.

PUCCINELLI, Oscar Raúl. Evolución histórica y análisis de las diversas espécies, subespécies, tipos y subtipos de habeas data en América Latina: um intento clasificador con fines didácticos. Pontifícia Universidad Javeriana. Bogotá, Colômbia: **Vniversitas,** n. 107, 2004. Disponível em: https://www.redalyc.org/pdf/825/82510714.pdf..Acesso em: 20 abr. 2020.

RAAB, Charles; SZEKELY, Ivan. Data Protection Authorities and Informations Technology. **Computer Law & Security Review,** v. 33, n. 4, ago. 2017. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0267364917301619. Acesso em: 20 abr. 2020.

READ, Simon. British Airways boss apologises for 'malicious' data breach. **BBC News,** 7 set. 2018. Disponível em: https://www.bbc.com/news/uk-england-london-45440850. Acesso em: 20 jul. 2019.

REINSEL, David; GANTZ, John; RYDNING, John. The Digitization of the World: from edge to core. **IDC White Paper,** nov. 2018. Disponível em: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf. Acesso em: 15 set. 2020.

RIBEIRO, Florbela da Graça Jorge da Silva. **O Tratamento de Dados Pessoais de Clientes para Marketing.** 2017. Dissertação (Mestrado em Direito – Especialidade em Ciências Jurídico-Políticas) – Departamento de Direito da Universidade Autônoma de Lisboa, Lisboa. Disponível em: https://www.academia.edu/33292289/O_TRATAMENTO_DE_DADOS_PESSOAIS_DE_CLIENTES_PARA_MARKETING. Acesso em: 15 abr. 2020.

ROCHFELD, Judith. Como qualificar os dados pessoais? Uma perspectiva teórica e normativa da União Europeia em face dos gigantes da *Internet*. **Revista de Direito, Estado e Telecomunicações,** Brasília, v. 10, n. 1, maio 2018. Disponível em: https://periodicos.unb.br/index.php/RDET/article/view/21500/19816. Acesso em: 16 abr. 2020.

RODOTÀ, Stefano. **A vida na sociedade de vigilância –** a privacidade hoje. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

ROHR, Altieres. 'Cookie eterno' pode rastrear internauta e é impossível de apagar. **G1 – Tecnologias e Games,** 25 out. 2010. Disponível em: http://g1.globo.com/tecnologia/noticia/2010/10/cookie-eterno-pode-rastrear-internauta-e-e-impossivel-de-apagar.html. Acesso em: 28 jun. 2020.

ROMÊNIA. **Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal.** Disponível em: https://www.dataprotection.ro/?page=Rapoarte%20anuale&lang=ro. Acesso em: 30 abr. 2021.

RUBIO, Isabel. *Facebook* lança aplicativo para acessar dados de usuários em troca de dinheiro. **El País – Tecnologia,** 12 jun. 2019. Disponível em: https://brasil.elpais.com/brasil/2019/06/12/tecnologia/1560347825_866607.html. Acesso em: 12 jul. 2019.

RUIZ, Bruno. Web Storage – HTML5. **Tableless,** 28 jan. 2014. Disponível em: https://tableless.com.br/web-storage-html5/. Acesso em: 28 jun. 2020.

SALDANA, María N. The rigth to privacy: la genesis de la proteción de la privacidad em el sistema constitucional norteamericano, el centenario legado de Warren y Brandeis. **Revista de Derecho Político** n. 85, set./dez. 2012, p. 195-240. Disponível em: http://revistas.uned.es/index.php/derechopolitico/article/view/10723. Acesso em: 12 dez. 2019.

SÁNCHEZ-TORRES, Jenny Marcela; GONZÁLEZ-ZABALA, Mayda Patrícia; MUÑOZ, María Paloma Sánchez. La Sociedad de la Información: Génesis, Iniciativas, Concepto y su Relación con Las TIC. **UIS Ingenierías –** Revista de La Facultad de Ingenierías Fisicomecánicas, v. 11, n. 1, Bucaramanga/Colombia, jan./jun. 2012, p. 113-129. Disponível em: https://www.redalyc.org/pdf/5537/553756873001.pdf. Acesso em: 28 jun. 2020.

SANTINO, Renato. *Google* recebeu mais de US$ 15 bilhões com anúncios do YouTube em 2019. **Olhar Digital**, 3 fev. 2020. Disponível em: https://olhardigital.com.br/noticia/google-recebeu-mais-de-us-15-bilhoes-com-anuncios-do-youtube-em-2019/96248. Acesso em: 15 abr. 2020.

SÃO PAULO. Tribunal de Justiça do Estado de São Paulo. **Ação Civil Pública Cível nº 1090663-42.2018.8.26.0100.** Requerente: Idec – Instituto Brasileiro de Defesa do Consumidor, Requerido: Concessionária da Linha 4 do Metro de São Paulo S.a. (Via Quatro). Juíza de Direito: Patrícia Martins Conceição. 37ª Vara Cível, Foro Central Cível, Comarca de São Paulo. DJE: 07 maio 2021. Disponível em: https://www.conjur.com.br/dl/viaquatro-indenizar-implantar-sistema.pdf. Acesso em: 26 maio 2021.

SÃO PAULO. Tribunal de Justiça do Estado de São Paulo. **Processo nº 1080233-94.8.26.0100.** Juíza de Direito: Tonia Yuka Koroku. 13ª Vara Cível, Foro Central Cível, Comarca de São Paulo. Data do Julgamento: 29 set. 2020. Disponível em: https://www.migalhas.com.br/arquivos/2020/9/B05F37C296A643_decisaoLGPD.pdf. Acesso em: 30 abr. 2021.

SARLET, Ingo Wolfgang. **A Eficácia dos Direitos Fundamentais –** uma teoria geral dos direitos fundamentais na perspectiva constitucional. 10. ed. rev. atual. e ampl. Porto Alegre: Livraria do Advogado, 2009.

SARLET, Ingo Wolfgang. **Dignidade da Pessoa Humana e Direitos Fundamentais na Constituição Federal de 1988**. Porto Alegre: Livraria do Advogado, 2002.

SAWARIS, Adriana. **A Tutela do Direito à Reserva sobre a Intimidade da Vida Privada no Regulamento nº 2016/679 da União Européia.** 2017. Dissertação (Mestrado em Ciências Jurídico-Civilistas – Direito Civil) – Faculdade de Direito da Universidade de Coimbra, Coimbra. Disponível em: https://eg.uc.pt/bitstream/10316/81104/1/Dissertac%CC%A7a%CC%83o%20Adriana%20S..pdf. Acesso em: 8 dez. 2019.

SCHERMER, Bart W. The limits of privacy in automated profiling and data mining. **Computer Law & Security Review,** n. 27, 2011, p. 47. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0267364910001767. Acesso em: 10 out. 2020.

SCHREIBER, Anderson. Direito ao Esquecimento e Proteção de Dados Pessoais na Lei 13.709/2018: distinções e potenciais convergências. *In:* FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro.** São Paulo: Thomson Reuters Brasil, 2019.

SCHREIBER, Anderson. **Direitos da Personalidade.** 3. ed. São Paulo: Atlas, 2014.

SCHREIBER, Anderson. Responsabilidade civil na Lei Geral de Proteção de Dados Pessoais. *In:* DONEDA, Danilo et al (Coords). **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021.

SCHREIBER, Mariana. Após reação negativa, *WhatsApp* adia para maio 'ultimato' para usuário compartilhar dados com *Facebook*. **BBC News Brasil,** 15 jan. 2021. Disponível em: https://www.bbc.com/portuguese/brasil-55680262. Acesso em: 16 jan. 2021.

SCHWARTZ, Paul M. ***Internet* Privacy and the State.** 5 nov. 2000. Disponível em: https://paulschwartz.net/wp-content/uploads/2019/01/SCHWARTZ-CK1A-1.pdf. Acesso em: 15 abr. 2020.

SHIMABUKURO, Igor. Twitter é multado na UR por atraso em notificação de violação de dados. **Olhar Digital,** 15 dez. 2020. Disponível em: https://olhardigital.com.br/2020/12/15/noticias/twitter-e-multado-na-ue-por-atraso-em-notificacao-de-violacao-de-dados/. Acesso em: 30 abr. 2021.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo.** 25. ed. São Paulo: Malheiros, 2005.

SIMÕES, Cristina. **O direito a autodeterminação das pessoas com deficiência**. Porto: Associação do Porto de Paralisia Cerebral; Faculdade de Direito da Universidade do Porto, 2016. Disponível em: https://www.appc.pt/_pdf/eBook_FDUP_Dir_PessoasDeficiencia.pdf. Acesso em: 13 dez. 2019.

SIQUEIRA JÚNIOR, Paulo Hamilton. **Teoria do Direito.** 3. ed. São Paulo: Saraiva, 2011.
SOLOVE, Daniel J. A Taxonomy of Privacy. **University of Pennsylvania Law Review,** v. 154, n. 3, jan. 2006. Disponível em: https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf. Acesso em: 2 dez. 2019.

SOLOVE, Daniel J. **Understanding privacy.** Londres: Harvard University Press, 2008.

SOMERS, Geert; FITEN, Bernd. 2 years GDPR: na overview of enforcement, warnings and fines. **Timelex.eu,** 11 jun. 2020. Disponível em: https://www.timelex.eu/en/blog/2-years-gdpr-overview-enforcement-warnings-and-fines. Acesso em: 30 abr. 2021.

SOPRANA, Paula. Bolsonaro nomeia três militares para Autoridade de proteção de dados. 15 out. 2020. **Folha de São Paulo,** Disponível em: https://www1.folha.uol.com.br/mercado/2020/10/bolsonaro-nomeia-tres-militares-para-autoridade-de-protecao-de-dados.shtml. Acesso em: 30 abr. 2021.

SOUZA, Carlos Affonso Pereira de. Segurança e Sigilo dos Dados Pessoais: primeiras impressões à luz da Lei 13.709/2018. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coords.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** São Paulo: Thomson Reuters Brasil, 2019.

SOUZA, Eduardo Nunes de; SILVA, Rodrigo da Guia. Direitos do titular de dados pessoais na Lei 13.709/2018: uma abordagem sistemática. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coords.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** São Paulo: Thomson Reuters Brasil, 2019.

SOUZA, Ramon de. Altaba (ex-Yahoo) vai pagar multa de US$ 35 milhões por vazamento de dados. **Canaltech,** 25 abr. 2018. Disponível em: https://canaltech.com.br/juridico/altaba-ex-yahoo-vai-pagar-multa-de-us-35-milhoes-por-vazamento-de-dados-112588/#:~:text=de%20dados%20%2D%20Canaltech-,Altaba%20(ex%2DYahoo)%20vai%20pagar%20multa%20de%20US%24,milh%C3%B5es%20por%20vazamento%20de%20dados&text=Na%20ocasi%C3%A3o%2C%20criminosos%20cibern%C3%A9ticos%20de,tr%C3%AAs%20anos%20depois%2C%20em%202016. Acesso em: 7 jul. 2020.

SULLIVAN, Bob. Privacy Lost: EU, U.S. laws differ greatly. **NBC NEWS: Technology & Science – Privacy Lost,** 19 out. 2006. Disponível em: http://www.nbcnews.com/id/15221111/ns/technology_and_science-privacy_lost/t/la-difference-stark-eu-us-privacy-laws/. Acesso em: 2 dez. 2019.

SUPREMA CORTE AMERICANA. **Case Bowers v. Hardwick.** v. 478, 1986. Disponível em: https://supreme.justia.com/cases/federal/us/478/186/. Acesso em: 13 dez. 2019.

SUPREMA CORTE AMERICANA. **Case Griswold v. Connecticut.** v. 381, 1965. Disponível em: https://supreme.justia.com/cases/federal/us/381/479/. Acesso em: 13 dez. 2019.

SUPREMA CORTE AMERICANA. **Case Lawrence v. Texas.** v. 539, 2003. Disponível em: https://supreme.justia.com/cases/federal/us/539/558//. Acesso em: 13 dez. 2019.

SUPREMA CORTE AMERICANA. **Case Roe v. Wade.** v. 410, 1973. Disponível em: https://supreme.justia.com/cases/federal/us/410/113/. Acesso em: 13 dez. 2019.

SWEENEY, Latanya. Simple Demographics Often Identify People Uniquely. **Carnegie Mellon University,** Pitsburgh, 2000. Disponível em: https://dataprivacylab.org/projects/identifiability/paper1.pdf. Acesso em: 17 abr. 2020.

SWEENEY, Lataya. Discrimination in Online Ad Delivey. **Search Engines.** Disponível em: https://dl.acm.org/doi/pdf/10.1145/2460276.2460278. Acesso em: 29 dez. 2020.

SZAFRAN, Vinicius. Yahoo começará a pagar indenizações por violações de dados. **Olhar Digital,** 5 fev. 2020. Disponível em: https://olhardigital.com.br/fique_seguro/noticia/yahoo-comecara-a-pagar-indenizacoes-por-violacoes-de-dados/96378. Acesso em: 9 jul. 2020.

TAVANI, Herman T. Informational Privacy: concepts, theories, and Controversies.. *In:* HIMMA, Kenneth E; TAVANI, Herman T. (Edt.). **The Handbook of Information and Computer Ethics.** Wiley, 2008.

TEPEDINO, Gustavo. A tutela da personalidade no ordenamento civil constitucional brasileiro. *In*: TEPEDINO, Gustavo. **Temas de Direito Civil.** 2. ed. Rio de Janeiro:Renovar, 2001.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coords.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** São Paulo: Thomson Reuters Brasil, 2019.

TERRA, Aline de Miranda Valverde; MULHOLLAND, Caitlin. A utilização econômica de rastreadores e identificadores on-line de dados pessoais. *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 Brasil, 2019.

TODD, Steve. O valor dos dados em um mundo impulsionado por informações. **CANALTECH,** 23 out. 2015. Disponível em: https://canaltech.com.br/big-data/o-valor-dos-dados-em-um-mundo-impulsionado-por-informacoes-51425/. Acesso em: 2 abr. 2020.

TOFFLER, Alvin. **La Tercera Ola.** Colombia: Plaza & Janes S.A. Editores, 1980.

TSCHENTSCHER, A; BROICHHAGEN, Seven. **Urteil des Ersten Senats vom 15 Dezember 1983 auf die mündliche Verhandlung vom 18 und 19 oktober in den Verfahren über die Verfassungsbeschwerden.** 1983. Disponível em: http://www.servat.unibe.ch/dfr/bv065001.html. Acesso em: 18 mar. 2020.

TSUKAYAMA, Hayley. Don’t want Google tracking you? You have almost no choice, according to a study. **The Washington Post,** 21 ago. 2018. Disponível em: https://www.washingtonpost.com/technology/2018/08/22/dont-want-google-tracking-you-you-have-almost-no-choice-according-new-study/?noredirect=on&utm_term=.a644e5215606. Acesso em: 12 jul. 2019.

ULMA CONSTRUCTION. **Home.** Disponível em: https://www.ulmaconstruction.com.br/pt-br/ulma. Acesso em: 29 dez. 2020.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia.** 7 jun. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR. Acesso em: 15 mar. 2020.

UNIAO EUROPEIA. Comissão Europeia. **Special Eurobarometer 487a** - Report: The general data protection regulation. Jun. 2019. Disponível em: https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/06/ebs487a_en.pdf. Acesso em: 30 abr. 2021.

UNIÃO EUROPEIA. Comitê Europeu para a Proteção de Dados. **Contribution of the EDPB to the evaluation of the GDPR under Article 97.** Adotado em 18 de fevereiro de 2020. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf. Acesso em: 30 abr. 2021.

UNIÃO EUROPEIA. **Communication from the Comission to the European Parlament, the Council, the Economic and Social Committee and the Committee of the Regions:** a comprehensive approach on personal data protection in the European Union. Disponível em: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52010DC0609. Acesso em: 20 abr. 2020.

UNIÃO EUROPEIA. **Directiva 2009/136/CE do Parlamento Europeu e do Conselho de 25 de Novembro de 2009.** Que altera a Directiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações electrônicas, a Directiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações electrônicas e o Regulamento (CE) n.º 2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor. Disponível em: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:PT:PDF. Acesso em: 28 jun. 2020.

UNIÃO EUROPEIA. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01).** 22 ago. 2018. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053. Acesso em: 3 nov. 2020.

UNIÃO EUROPEIA. **Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679.** 20 ago. 2018. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052. Acesso em: 5 jun. 2020.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016**. Relativo à proteção de dados pessoais 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 Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679#d1e1554-1-1. Acesso em: 28 jun. 2020.

UOL NOTÍCIAS. **Norte-Americana quer ser chamada de "sexy".** 30 jan. 2014. Disponível em: https://noticias.uol.com.br/tabloide/ultimas-noticias/2014/01/30/norte-americana-quer-ser-chamada-de-sexy.htm?cmpid=copiaecola. Acesso em: 5 jan. 2020.

VASCONCELOS, Beto; PAULA, Felipe de. A autoridade nacional de proteção de dados: origem, avanços e pontos críticos. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coords.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** São Paulo: Thomson Reuters Brasil, 2019.

VEDOR, Luis. Portugal é um dos países mais afetados pela campanha de *malware* Revenge Hotels. **PC Guia,** jan. 2020. Disponível em: https://www.pcguia.pt/2020/01/portugal-afectados-campanha-malware-revengehotels/. Acesso em: 5 jun. 2020.

VIEIRA, José Ribas et al. (Coords.). **Direitos à Intimidade e à Vida Privada.** Curitiba: Juruá, 2008.

VIEIRA, Nathan. *Facebook* e Twitter anunciam casos de acesso indevido a dados de usuários. **Canaltech,** 25 nov. 2019. Disponível em: https://canaltech.com.br/seguranca/facebook-e-twitter-anunciam-casos-de-acesso-indevido-a-dados-de-usuarios-156195/. Acesso em: 22 jun. 2020.

VITAL, Danilo. Primeira ACP baseada na LGPD é indeferida porque *site* da ré está em manutenção. **Consultor Jurídico,** 23 set. 2020. Disponível em: https://www.conjur.com.br/2020-set-23/peticao-inicial-acao-civil-publica-baseada-lgpd-indeferida. Acesso em: 30 abr. 2021.

VOSS, W. Gregory; CASTETS-RENARD, Céline Casters. Proposal for an international taxonomy on the various forms of the "Right to be Forgotten": a study on the convergence of norms. **Colo Tech L. J.,** v. 14, n. 2, p. 298, 23 maio 2016. Disponível em: https://ctlj.colorado.edu/wp-content/uploads/2016/06/v.3-final-Voss-and-Renard-5.24.16.pdf. Acesso em: 19 mar. 2020.

WAKKA, Wagner. Vazamento de dados custa em média R$ 1,24 milhão para empresas no Brasil. **Canaltech,** 11 set. 2018. Disponível em: https://canaltech.com.br/seguranca/vazamento-de-dados-custa-em-media-r-124-milhao-para-empresas-no-brasil-122304/. Acesso em: 7 jul. 2020.

WALL, Matthew. Inteligência artificial: por que as tecnologias de reconhecimento facial são tão contestadas. **BBC News Brasil,** 5 jul. 2019. Disponível em: https://www.bbc.com/portuguese/geral-48889883. Acesso em: 1 out. 2020.

WARE, W. H. **Records, Computers and the Rights of Citizens.** Ago. 1973. Disponível em: https://www.rand.org/content/dam/rand/pubs/papers/2008/P5077.pdf. Acesso em: 20 abr. 2020.

WARREN, Samuel D; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review,** v. 4, n. 5, 15 dez. 1890, p. 193-220. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em: 2 dez. 2019.

WEBER, Lauren; DWOSKIN, Elizabeth. Are Workplace Personality Tests Fair? **The Wall Street Journal,** 29 set. 2014. Disponível em: https://www.wsj.com/articles/are-workplace-personality-tests-fair-1412044257. Acesso em: 11 out. 2020.

WEBSTER, Frank. What information society? **The Information Society: an international journal**, v. 10, n. 1, 3 mai. 2013. Disponível em: http://dx.doi.org/10.1080/01972243.1994.9960154. Acesso em: 15 set. 2020.

WHITMAN, James Q. The Two Western Cultures of Privacy: dignity versus liberty. **The Yale Law Journal,** v. 113, n. 1.151. Disponível em: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1647&context=fss_papers. Acesso em: 2 dez. 2019.

WILLIAMS, Betsy Anne; BROOKS, Catherine F.; SHMARGAD, Yotam. How Algorithms Discriminate Based on Data they Lack: challenges, solutions, and policy implications. **Journal of Information Policy,** Penn State University Press**,** v. 8, 4 set. 2018. Disponível em: https://www.jstor.org/stable/10.5325/jinfopoli.8.2018.0078. Acesso em: 29 dez. 2020.

YAMAGATA, Nicolas. Monetizando você e seus dados com a função de inteligência. **Intelligence Hub,** 5 nov. 2017. Disponível em: http://www.intelligencehub.com.br/monetizando-voce-e-seus-dados-com-funcao-de-inteligencia/. Acesso em: 2 abr. 2020.

ZARSKY, Tal Z. “Mine Your Own Business!”: making the case for the implications of the data mining of personal information in the forum of public opinion. **Yale Journal of Law and Technology,** 2003. Disponível em: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1008&context=yjolt. Acesso em: 28 set. 2020.