Sarah Helena Linke

SOCIEDADE DE VIGILÂNCIA E CONSUMO: PROTEÇÃO DE DADOS PESSOAIS RELACIONADOS À SAÚDE EM PROGRAMAS DE FIDELIZAÇÃO DE REDES DE FARMÁCIA

Dissertação apresentada à Banca Examinadora do Programa de Pós-Graduação em Direito da Universidade Federal de Santa Catarina, como requisito à obtenção do título de Mestra em Direito, sob a orientação da Professora Dra. Carolina Medeiros Bahia

Florianópolis
2019

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Linke, Sarah Helena
SOCIEDADE DE VIGILÂNCIA E CONSUMO : PROTEÇÃO DE DADOS PESSOAIS RELACIONADOS À SAÚDE EM PROGRAMAS DE FIDELIZAÇÃO DE REDES DE FARMÁCIA / Sarah Helena Linke ; orientador, Carolina Medeiros Bahia, 2019.
258 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas, Programa de Pós-Graduação em Direito, Florianópolis, 2019.

Inclui referências.

1. Direito. 2. Privacidade, Proteção de Dados Pessoais, Vigilância. I. Bahia, Carolina Medeiros. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Direito. III. Título.

Ata nº 19 da sessão de julgamento da dissertação da mestranda **Sarah Helena Linke** do Curso de Mestrado do Programa de Pós-Graduação em Direito da Universidade Federal de Santa Catarina.

Aos vinte e oito dias do mês de fevereiro de dois mil e dezenove, às catorze horas, reuniu-se na Sala 302 do Centro de Ciências Jurídicas da UFSC a banca examinadora designada pela Portaria nº 32/PPGD/2019, composta pelos professores: Dra. Carolina Medeiros Bahia (Presidente), Dr. Sérgio Vieira Branco Junior - videoconferência – IBMEC, Dra. Liz Beatriz Sass – UFSC (Membros), Dr. Guilherme Coutinho Silva – USP (Suplente) e Dra. Heloísa Gomes Medeiros – UEMA (Suplente), para exame da Defesa de Dissertação da aluna *Sarah Helena Linke*, intitulada **"SOCIEDADE DE VIGILÂNCIA E CONSUMO: PROTEÇÃO DE DADOS PESSOAIS RELACIONADOS À SAÚDE EM PROGRAMAS DE FIDELIZAÇÃO DE REDES DE FARMÁCIA"**. Abertos os trabalhos, a Senhora Presidente cumprimentou os presentes e, após se referir às normas regulamentares, deu a palavra à Mestranda para que, no prazo de cinquenta minutos, expusesse o seu trabalho, o que foi feito. Terminada a exposição, passou-se às arguições. Os componentes da banca fizeram suas observações pelo prazo de vinte minutos cada, obedecida à seguinte ordem: Dr. Sérgio Vieira Branco Junior - videoconferência e Dra. Liz Beatriz Sass. Concluída cada arguição, a mestranda dispôs de vinte minutos para responder ao examinador. Uma vez esgotado o prazo deferido para a mestranda responder à última arguição, a Senhora Presidente suspendeu a sessão para que fosse feita a avaliação. A decisão da banca examinadora, conforme previsto nos artigos 87 e 87-A do Regimento Interno, foi de considerar a Dissertação de Mestrado APROVADA.
Reabertos os trabalhos, a Senhora Presidente deu conhecimento dos resultados aos presentes, esclarecendo que a mestranda tem, a contar desta data, os prazos regimentais para realizar o depósito definitivo da Dissertação. Findos os trabalhos, a Senhora Presidente agradeceu a presença de todos e deu por encerrada a sessão, da qual eu, Maria Aparecida de Oliveira, Secretária do PPGD, lavrei a presente Ata que vai devidamente assinada pela banca examinadora e pela mestranda.

Dra. Carolina Medeiros Bahia – Presidente

Dr. Sérgio Vieira Branco Junior - videoconferência (IBMEC)

Dra. Liz Beatriz Sass (UFSC)

Mestranda: ***Sarah Helena Linke***

AGRADECIMENTOS

Não cheguei até aqui sozinha. Acho que, no final das contas, ninguém chega. Apesar do processo solitário de escrita, apenas com o suporte e a compreensão das pessoas que estiveram ao meu redor, que foi possível perpassar todos os percalços enfrentados.

Primeiramente, gostaria de agradecer à minha família, especialmente à minha mãe, que, ainda quando criança despertou em mim o gosto pela leitura e pelo saber, que carrego ainda em mim até hoje. Depois na vida adulta sempre esteve ao meu lado: aceitou minhas renúncias, apoiou minhas decisões, entendeu minhas angústias. Todas as minhas conquistas eu lhe devo, inclusive esta.

À equipe do Juizado Especial Cível da Comarca de São José pelo apoio institucional e pelo apoio dos colegas com quem convivi diariamente nesse último ano, essenciais para que eu pudesse terminar esta jornada. Apenas posso agradecer pela amizade, pela compreensão e por todo o aprendizado. Que nossos *lattes* sejam tão extensos quanto nossas *playlists.*

Às pessoas que, mesmo longe, fizeram-se tão presentes nesse processo.

À Babi, por nossa sincera amizade, que subsiste ao tempo e à distância de maneira intacta, que me ajudou a manter a sanidade e o equilíbrio emocional tantas vezes nesses últimos anos. Não poderia de mencionar também sua contribuição com a revisão parcial deste trabalho.

Ao CGR, eternamente em meu coração (prometo que voltarei a estar presente), em especial, ao João, com quem pude compartilhar as experiências acadêmicas e as de vida, de maneira tão próxima nesses últimos anos; e ao Davi, pela contribuição social advinda da representação feita ao Ministério Público de Minas Gerais, e por ter me auxiliando no acesso à íntegra do processo administrativo instaurado.

Ao GEDAI, responsável por ter despertado o interesse pela pesquisa e pela vida acadêmica e por ter proporcionado muitos encontros na minha vida, em especial ao prof. Marcos, ao Allan, ao Gui e ao Pedro.

Ao TPEV por ser o melhor grupo que poderíamos formar. Obrigada a todas as meninas e ao Vitor (responsável por esse encontro de almas) por fazerem meus dias mais leves e engraçados, bem como por terem compartilhado momentos inesquecíveis nesse último ano.

À Lígia, com que convivi intensamente no primeiro ano de mestrado, companhia acadêmica impecável, saudade eterna de nossas tardes recheadas com café, bolo, carinho, amor e apoio incondicional.

Às minhas amigas Nathi, Dayse, Luana e Gabi por estarem ao meu lado, cada uma a sua maneira, nessa caminhada.

À Théta e ao Luca, por me ensinarem o que os livros não conseguem.

À Liz Sass, que além de professora e amiga, sempre me incentivou na minha evolução acadêmica, acompanhando-me a cada novo passo dado.

À minha orientadora, Carolina Bahia, que me acolheu nessa empreitada com muito zelo e dedicação. Agradeço imensamente pela convivência e por toda a oportunidade de aprendizado que tive no âmbito da elaboração deste trabalho, nas aulas da pós-graduação e no estágio de docência.

Por último, à Universidade Federal de Santa Catarina, instituição que me acolheu há exatos dez anos, na graduação, e passou a fazer parte indissociável da minha vida. Agradeço aos professores, aos servidores e aos colegas que passaram pelo meu caminho e contribuíram para minha formação acadêmica, profissional e pessoal.

RESUMO

Devido à rápida evolução de tecnologias de informação e comunicação, novos desafios em matéria de privacidade e proteção de dados pessoais surgiram nas últimas décadas. A coleta e o tratamento de dados pessoais permitem às empresas privadas e às entidades públicas sua utilização numa escala sem precedentes no exercício das suas atividades. O objetivo deste trabalho é investigar o nível de proteção do consumidor e de seus dados pessoais relacionados à saúde oferecido, no Brasil, e, em especial na Grande Florianópolis, pelos programas de fidelidade de redes de farmácias, considerando a recente Lei Geral de Proteção de Dados, no âmbito da sociedade de vigilância e do consumo. Para a realização de tal escopo, adotou-se o método de abordagem dedutiva e a técnica de pesquisa bibliográfica e documental. A pesquisa está subdividida em três diferentes capítulos. O primeiro se dedica a estudar o contexto social em que se inserem a vigilância e o consumo, que atuam de maneira simbiótica para manutenção da ordem social, ou seja, associando-se para que ambos tirem proveito um do outro: o consumo gera cada vez mais dados para alimentar bases, consequentemente, aumentando o conhecimento e o poder das empresas que atuam sobre o indivíduo, de forma que possam intervir com o desígnio de instigar e manipular o consumo de produtos. O segundo discorre sobre a evolução e as correlações entre o direito à privacidade e o direito à proteção de dados pessoais, tanto no plano teórico, quanto no plano normativo, descrevendo-se o *General Data Protection Regulation* da União Europeia, e a Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, com as modificações implementadas pela Medida Provisória nº 869/2018. Finalmente, o terceiro capítulo analisa as disposições da Lei Geral de Proteção de Dados Pessoais no que atine aos dados relacionados à saúde, enquanto dado sensível, conforme classificação normatia e examina-se os regulamentos e políticas de privacidade que regem os programas de fidelidade de algumas farmácias atuantes na Grande Florianópolis, como substrato para examinar o nível de proteção ofertado atualmente aos consumidores.

Palavras-chave: Vigilância. Privacidade. Proteção de dados pessoais.

ABSTRACT

Due to the rapid evolution of information and communication technologies, new challenges in privacy and personal data protection have emerged in recent decades. The collection and processing of personal data allow private companies and public entities to use the data on an unprecedented scale in the exercise of their activities. The aim of this study is to investigate the level of protection of the consumer and of their health-related personal data in Brazil, especially in Greater Florianópolis, by the loyalty programs of pharmacy chains, considering the recent Brazilian General Data Protection Law, within the surveillance and consumption society. The deductive approach method and the bibliographic and documentary research technique were adopted for this scope. The study is subdivided into three different chapters. The first one is dedicated to studying the social context in which surveillance and consumption are inserted. These act in a symbiotic way for the maintenance of social order, and are associated so that both benefit from each other. The consumption generates more and more data to feed bases, consequently increasing the knowledge and power of the companies that act on the individual, so that the companies can instigate and manipulate product consumption. The second one discusses the evolution and correlations between the right to privacy and the right to personal data protection, both theoretically and normatively, describing the European Union General Data Protection Regulation and the Brazilian General Data Protection Law, Law No. 13,709/2018, with the modifications implemented by provisional measure No. 869/2018. Finally, the third chapter analyzes the provisions of the Brazilian General Data Protection Law concerning health-related data, as sensitive data, according to the normative classification. The chapter also examines the regulations and privacy policies that govern the loyalty programs of some pharmacies in Greater Florianópolis, as a substrate to examine the level of protection currently offered to consumers.

Keywords: Surveillance. Privacy. Personal Data Protection**.**

SUMÁRIO

INTRODUÇÃO

Lenina Crowne, frequentemente, faz compras em uma mesma farmácia localizada perto de sua residência. Quando vai fazer o pagamento de suas compras no caixa, o atendente, de maneira automática, fala o seguinte: “CPF?!”, em resposta, Lenina desata a falar a sequência de números que a identifica. Em seguida, o sistema lhe concede um pequeno desconto pelos produtos que está comprando, quais sejam, um teste de gravidez, remédio para dor cefaleia e diversos artigos de higiene.

Essa cena faz parte do cotidiano de redes de farmácia que condicionam valores de produtos à identificação do consumidor, os chamados programas de fidelidade. A prática já fora normalizada: a maioria dos consumidores, irrefletidamente, repassa seu CPF com o intuito de economizar dinheiro, com pouco conhecimento acerca do uso dos dados coletados.

Em geral, pensa-se que o objetivo da coleta de dados é tão somente para marketing segmentado. Ocorre, contudo, que, conforme será visto: (i) não se trata apenas de estratégia de publicidade, existem potencialidades, compartilhamentos e usos de seus dados para outras finalidades, cujos consumidores sequer imaginam; (ii) ainda que seu uso fosse apenas para publicidade, que os produtos, os serviços, as expectativas oferecidas moldam o contexto e a realidade em que se vive e, consequentemente, a própria subjetividade.

Por exemplo, na hipótese descrita, toda transação realizada irá compor o banco de dados da farmácia, que já contém todo o histórico de compras da personagem. A partir da análise deste, de maneira sintética, é possível inferir: sua capacidade econômica, tanto pelos valores gastos, quanto pela localização de sua residência; seus horários e hábitos de compra; as marcas de cosméticos de sua preferência; prováveis doenças que a acometeram; o uso de produtos de higiene; etc. Tais dados, aparentemente, são inofensivos, apenas servindo para venda aos fornecedores de localização de produtos nas gôndolas; e para publicidade.

Veja-se, no entanto, as informações sobre o teste de gravidez: se no histórico de compra de Lenina Crowne não houver registro recente de compra de anticoncepcionais ou outros métodos contraceptivos, é possível concluir que ela está tentando engravidar. Por outro lado, se o teste de gravidez foi adquirido de maneira esporádica, com outros apontamentos de aquisição de contraceptivos de emergência, é possível

concluir que não está tentando engravidar, e que se submeteu a comportamento considerado de risco.

Evidentemente essa informação é valiosa para o mercado destinado a gestantes e a bebês recém-nascidos, afinal, as empresas do segmento já sabem de antemão onde devem empregar seus esforços e a quem é interessante apresentar sua publicidade, a fim de conquistar as futuras mamães.

De maneira não tão óbvia, todavia, são os diversos destinos e usos possíveis dessas informações. Por exemplo, uma empresa que passa a identificar dentro de seu quadro de pessoal as mulheres que desejam engravidar no futuro próximo e anteriormente rompem o contrato de trabalho, a fim de que não tenha que arcar com licença-maternidade; ou uma empresa destinada a recrutamento de pessoal terá conhecimento prévio sobre as mulheres que estão tentando engravidar, podendo, desde já, preteri-las nos processos de seleção.

O suposto comportamento de risco, por sua vez, poderá influenciar direta e negativamente no seu *health score* (fator matemático, que tem o intuito de auferir o valor de um consumidor individual como cliente, ou seja, predizer a sua probabilidade de dar lucro ou prejuízo), utilizado por planos de saúde para subsidiar decisões refentes aos termos e valores contratuais e até mesmo a não contratação.

Como poderá a consumidora saber o peso desse suposto comportamento de risco? E se a compra do contraceptivo de emergência foi realizada não para consumo próprio, mas sim de terceira pessoa? Como obter acesso aos bancos de dados das farmácias, como se opor aos registros ali consignados? Como saber com quais empresas estão sendo compartilhado esses dados pessoais?

É quimera crer que o fluxo de dados cessará, pelo contrário, a tendência é que continue aumentando de maneira exponencial nos próximos anos. Dessa forma, torna-se imperioso compreender como os sistemas de vigilância operam, o que os controladores de dados fazem com os dados pessoais dos indivíduos e quais as consequências pessoais e sociais desse ecossistema, a fim de reduzir a assimetria de poder entre os cidadãos-consumidores e os detentores dos meios de tratamento de dados.

Diante dessas circunstâncias fatuais se insere o objetivo geral deste trabalho, qual seja, investigar o nível de proteção do consumidor e de seus dados pessoais relacionados à saúde oferecido, no Brasil, e, em especial na Grande Florianópolis, pelos programas de fidelidade de redes de farmácias, considerando a recente Lei Geral de Proteção de Dados, no âmbito da sociedade de vigilância e do consumo.

Como objetivos específicos, pretende-se, em primeiro lugar, contextualizar a relação estabelecida entre vigilância e consumo, enquanto instrumentos hábeis para o controle social. Em segundo lugar, propõe-se traçar o panorama normativo no que se refere à privacidade e a proteção de dados pessoais, tanto no âmbito da União Europeia, quanto no Brasil. E, finalmente, em terceiro lugar, examinar as disposições normativas específicas relacionadas à proteção de dados referentes à saúde constantes na recente Lei Geral de Proteção de Dados, bem como as políticas de privacidade que respaldam os programas de fidelidade de redes de farmácia da Grande Florianópolis.

Para tanto, o método adotado foi o dedutivo, partindo-se do marco sociológico, perpassando pelo panorama normativo e teórico referente à proteção de dados pessoais que embasaram a avaliação proposta neste trabalho. Empregou-se o método de procedimento monográfico e adotou-se a técnica de pesquisa bibliográfica e documental.

Correspondente aos três objetivos específicos, a pesquisa está subdivida em três diferentes capítulos. No primeiro capítulo, situa-se a vigilância como fenômeno transfronteiriço e transtemporal, penetrando-se com capilaridade de forma inevitável em todos os campos da vida contemporânea e a superação da arquitetura panóptica pelos bancos de dados. O exercício do poder deixa de atuar diretamente sobre os corpos dos indivíduos, passando a operar indiretamente sobre suas mentes: o controle social passa a ser realizado por técnicas de manipulação e desejo.

Essas técnicas são operadas com destreza dentro da sociedade de consumo. Na moda, por exemplo, que pode ser manejada em qualquer âmbito da vida, adota-se a estratégia do efêmero e da inovação para a renovação das vontades, invadindo o psicológico das pessoas.

Por seu turno, a vigilância e o consumo podem agir conjuntamente de maneira simbiótica, ou seja, associando-se para que ambos tirem proveito um do outro: o consumo gerando cada vez mais dados para alimentar as bases e, consequentemente, o conhecimento das empresas que atuam sobre o indivíduo, de forma que possam intervir com técnicas avançadas de marketing com o desígnio de instigar e manipular o consumo de produtos.

No capítulo seguinte, discorre-se sobre a evolução histórica e o desenvolvimento teórico do direito à privacidade, perpassando pela autodeterminação informativa e culminando na proteção de dados pessoais, analisando-se os diferentes posicionamentos doutrinários sobre a relação e a natureza jurídica desses direitos: (i) a proteção de dados e à

privacidade como direitos separados, mas complementares, como instrumentos de proteção à dignidade da pessoa humana; (ii) a proteção aos dados pessoais como uma faceta da privacidade; e (iii) a proteção aos dados pessoais como um direito fundamental independente, o qual não se limita à proteção da privacidade.

No aspecto normativo, são apresentadas as diferentes gerações de leis de proteção de dados propostas por Mayer-Schonberger (1997), incluindo a recente normativa *General Data Protection Regulation* da União Europeia; e, a Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, com as alterações promovidas pela Medida Provisória nº 869/2018.

Finalmente, no terceiro capítulo, abordam-se questões relacionadas a dados de saúde e programas de fidelidade, com o intuito de compreender a dinâmica mercadológica empregada pelas redes de farmácias, apresentando-se matérias jornalísticas, investigações e pesquisas que tratam de tal prática no âmbito brasileiro.

Segue-se a análise das disposições da Lei Geral de Proteção de Dados Pessoais no que atine aos dados relacionados à saúde, enquanto dado sensível, conforme classificação normativa. E, finalmente, o exame dos regulamentos e políticas de privacidade que regem os programas de fidelidade de algumas farmácias atuantes na Grande Florianópolis, como substrato para examinar o nível de proteção ofertado atualmente aos consumidores. Para compor a amostra da análise documental, foram escolhidas cinco diferentes redes que atuam comercialmente na Grande Florianópolis, variando-se sua participação no mercado, com abrangência local, regional e nacional. Em todas, adotou-se o seguinte procedimento: (i) análise inicial do regulamento do programa e identificação da presença de políticas de privacidade presentes no *site* institucional; (ii) contato com o Sistema de Atendimento ao Consumidor, questionando-se acerca do funcionamento do programa e de sua política de privacidade; (iii) visita na loja física, solicitando aos atendentes regulares acesso ao regulamento.

1 VIGILÂNCIA E CONSUMO: UMA SIMBIOSE

"Era a segunda vez em três semanas que faltava a um sarau no Centro Comunal: gesto audacioso, pois podia ter a certeza de que era cuidadosamente verificado o número de presenças no Centro. Em princípio, um membro do Partido não tinha horas vagas, e não ficava nunca só, exceto na cama". Esse trecho, da obra 1984, de autoria de George Orwell é transcrito com o objetivo de contextualizar a reflexão inicial sobre um tema bastante abrangente: a vigilância.

Quando uma pessoa sabe que está sendo observada, notada ou gravada, suas ações tendem a ser censuradas por ela mesma, que se torna menos propensa a falar livremente e agir individualmente, e sim de acordo com as expectativas que recaem sobre ela. Do mesmo modo acontece quando alguém está diante de situações de avaliação, crítica, julgamento, correção por atitudes próprias: passa-se a prestar atenção às impressões causadas e a possíveis registros realizados que possam, ainda que no futuro, trazer alguma implicação ou complicação. Diante deste cenário, Schneier (2015) assevera que são evitadas ações que estejam fora do esperado ou do ordinário daquele contexto, porquanto o que foge ao padrão pode acarretar efeitos como o de exclusão social. Nesse ambiente, portanto, a individualidade cede lugar à obediência e à submissão; o poder não é mais questionado ou desafiado.

Segundo ensina Gary Marx (2016), o termo *surveillance* advém da aglutinação de termos do latim e do francês. No latim, *vigilare* significa "continue observando", enquanto o prefixo *sur* quer dizer "para baixo", ou seja, "continuar observando aqueles abaixo".[1] Todavia, a partir de uma interpretação linguística diversa, no francês, o prefixo "sur" pode remeter a "super", ganhando um sentido como: as novas dinâmicas de vigilância envolvendo um sistema supercarregado, com tecnologias que proporcionam a superobservação; que sondam, armazenam e analisam grande quantidade de dados de forma cada vez mais rápida, precisa, ampla e barata. Para Marx (2016), essa união linguística de múltiplos significados ajuda a capturar o tópico

1 Conforme explica Han (2014) em inglês, o substantivo "*surveillance*" vem do verbo francês "*surveillir*"; por sua vez, no português, o vocábulo vigilância está relacionado ao termo latim "*vigilare*" que denota que algo vagamente estranho ou ameaçador estaria à espreita, para além da torre de vigia e das muralhas da cidade.

contemporâneo acerca da vigilância - tanto de seu poder técnico avançado quanto de seu fator frequente nas relações de poder.

Gary Marx (2016, p. 61) define vigilância como um "escrutínio de indivíduos, grupos, e contextos através de técnicas para extrair dados e criar informação." Com efeito, essa definição abre margem a diferentes interpretações, imprimindo uma fluidez necessária quando se busca fixar um conceito ubíquo e transtemporal, visto que o emprego da vigilância está intimamente ligado a técnicas que envolvem formas de manipulação, sedução, coerção, bem como infiltrações, informantes e habilidades especiais de observação, no caso, tecnologias de informação e comunicação. Além disso, segundo recorda Fernanda Bruno (2013, p. 19), a vigilância também tem ligação com "discursos, medidas legais e administrativas, instituições e corporações, enunciados e empreendimentos científicos, midiáticos, comerciais, políticos etc.".

Também merece destaque o conceito funcional de vigilância desenvolvido por Wood *et al*. (2006, p. 9) e citado por Bruno (2015, p. 85), no qual se lê o seguinte: "Onde encontramos uma atenção proposital, regular, sistemática e focada em dados pessoais tendo em vista controle, direito, administração, influência ou proteção, estamos olhando para vigilância".

Fernanda Bruno (2016) ensina que atividades de vigilância envolvem três elementos centrais: a) observação; b) conhecimento; e c) intervenção. Em outras palavras, segundo a autora, a observação (a) consiste na coleta sistemática dos indivíduos ou grupos, com o intuito de obter informações e dados sobre aspectos corporais, psíquicos e sociais, com o fito de produzir (b) conhecimento acerca dos próprios vigiados: extração de padrões, regularidades ou cadeias causais, por exemplo, tornando possível (c) intervir e controlar ações, escolhas, subjetividades e comportamentos do vigiado.

Já Lyon (1994) entende que a vigilância por si só não pode ser valorada, pois os mesmos processos de vigilância que podem ser utilizados para garantir a eficiência também podem ser utilizados em um contexto diferente com o fito de exercer a opressão e o constrangimento. Por exemplo, se uma pessoa pede para que um vizinho "fique de olho" no filho dela durante um período de tempo, a vigilância é considerada positiva. No entanto, se a polícia local requerer que o vizinho fique de olho na mesma pessoa, por conta de alguma dissidência política, o contexto transforma a vigilância em indesejada e inapropriada.

Todavia, a vigilância já foi incorporada na vida das pessoas, transpondo com facilidade limites espaciais, temporais, financeiros etc. Se antes ela estava relacionada à investigação de suspeitos, a escutas

policiais ou à inteligência nacional, agora se transforma em fenômeno transfronteiriço e transtemporal: ocorre cotidiana, local e globalmente, como um aspecto inevitável da vida contemporânea.

Lyon (2013) explica em outra obra que organizações de todos os tipos estão engajadas em vigiar cidadãos, consumidores e empregados. Também pontua a existência de bases de dados com capacidade para armazenar e processar dados pessoais de diferentes populações, de forma célere e barata. E essa coleta de dados acontece em todos os campos da vida: em lugares de compra, votação, telefonemas e trabalho. Participar da vida moderna já depende das relações estabelecidas com bases de dados. Antes, as maiores preocupações sobre vigilância estavam ligadas à privacidade e à liberdade, ou seja, à defesa do espaço privado onde se é livre para "ser você mesmo", em consonância com o "*right to be alone*", de construção de Warren e Brandeis[2]. Hodiernamente, embora essas questões ainda sejam significantes, outros direitos e outras esferas da vida estão sendo atingidas porque as tecnologias de análise de dados possuem a capacidade de predizer, com alto grau de probabilidade, as decisões de uma determinada pessoa e classificá-la em categorias pré-determinadas, com o propósito de atribuir valor ou risco. Por consequência, situações de discriminação ocorrem de maneira velada. A vigilância deixa de centralizar o debate somente em privacidade e proteção de dados pessoais, alcançando discussões acerca de isonomia e de justiça social: as bases de dados podem ser digitais, mas suas consequências são reais.

É diante deste contexto que Lyon (2013) afirma que o fato de que os dados pessoais podem ser classificados e verificados para interesses empresariais é uma característica- chave da vigilância atualmente[3]. Além disso, enquanto a Internet se torna cada vez mais importante para o marketing, esforços são empregados para combinar dados da vida *off-line* com bases de dados *on-line*. Desta forma, ao classificar pessoas ou populações de acordo com critérios variáveis, mas predeterminados, é possível avaliar e julgar quem deve ser alvo de especial tratamento e quem deve ser excluído.

---

2 WARREN, Samuel; BRANDEIS, Louis. **The Right to Privacy**. Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890), p. 193-220.

3 O autor traz o exemplo de que quando publicitários conseguem individualmente identificar informações como localização de domicílio cruzando com hábitos de compra ou de procuras realizadas em bases de dados, eles conseguem criar um relacionamento mais próximos com consumidores considerados relevantes (LYON, 2013, p. 19).

Fernanda Bruno (2015) entende que os processos de vigilância contemporâneos não obedecem a nenhum princípio unificado: são ações distribuídas por diferentes setores, de maneira ramificada, com interesses e perspectivas diversas, sendo esta heterogeneidade e a natureza reticular dos seus elementos os pontos-chaves para a compreensão da dinâmica. A mesma autora alerta que, em alguns casos, a vigilância acaba sendo uma externalidade de dispositivos que são projetados inicialmente para outras finalidades, como, por exemplo, para "controle de fluxos e acessos, comunicação, publicidade, geolocalização, entretenimento, sociabilidade etc., e ainda que não previstos inicialmente podem ser decisivos para os efeitos que se produzem" (BRUNO, 2015, p. 32).

Fernanda Bruno ainda afirma que:

> [...] a vigilância contemporânea não está restrita aos circuitos de controle, segurança e normalização, mas se faz também intensamente presente nos circuitos de entretenimento e prazer. [...] Não por acaso, vemos crescer o impulso participativo e colaborativo não apenas na produção de conteúdos na Internet, mas também nas práticas de vigilância, que vêm sendo associadas, nesse contexto, ao exercício da cidadania (BRUNO, 2015, p. 34 - 35).

Para ela, neste momento entram em cena os regimes de legitimação, que operam "tornando toleráveis ou desejáveis as práticas de vigilância" (BRUNO, 2015, p. 36).

É nesta toada que Lyon (2013) entende que o exercício da vigilância, em seus moldes atuais, vai além da Sociedade Disciplinar de Foucault, que busca a normalização dos indivíduos (onde pessoas são "normalizadas"), enquadrando-se na Sociedade do Controle de Deleuze , onde similaridades e diferenças são reduzidas a códigos de programação, com o propósito de tornar as pessoas socialmente integradas, ou seja, consumidoras dependentes do mercado, fato este que é alimentado em parte pela vigilância comercial.

Eis aqui o ponto de interseção a ser explorado neste trabalho: vigilância e consumo, fatores existentes para a manutenção da ordem social atuando em simbiose, ou seja, associando-se para que ambos tirem proveito do "outro" organismo: o consumo gerando cada vez mais dados para alimentar as bases e, consequentemente, o conhecimento das

empresas que atuam sobre o indivíduo, de forma que possam intervir com o desígnio de instigar e manipular o consumo de produtos.

1.1 DISTOPIAS LITERÁRIAS EM ORWELLL E HUXLEY: O FUTURO ANUNCIADO

Em que pese haver algumas divergências conceituais, sociólogos, filósofos e juristas reconhecem, em sua grande maioria, a existência de um ponto de inflexão a partir da década de 1970, fruto da crença científica positivista, da ascensão do neoliberalismo, do desenvolvimento de tecnologias de informação e comunicação. Trata-se da chamada pós-modernidade.

Para David Harvey, a modernidade se identificava “com a crença no progresso linear, nas verdades absolutas, no planejamento racional de ordens sociais ideais, e com a padronização do conhecimento e da produção” (2008, p. 19). Por sua vez, o pós-moderno privilegia "a heterogeneidade e a diferença como forças libertadoras na redefinição do discurso cultural" (2008, p. 19).

Sob o ponto de vista de Bauman (2001, 36), a modernidade persiste com as seguintes características:

> [...] a compulsiva e obsessiva, contínua, irrefreável e sempre incompleta modernização; a opressiva e inerradicável, insaciável sede de destruição criativa (ou de criatividade destrutiva, se for o caso: de "limpar o lugar" em nome de um "novo e aperfeiçoado" projeto; de "desmantelar" "cortar" "defasar" "reunir" ou "reduzir' tudo isso em nome da maior capacidade de fazer o mesmo no futuro - em nome da produtividade ou da competitividade).

Para o referido autor (2001), dois fatores distinguem a modernidade sólida e a chamada modernidade líquida, termo por ele cunhado. A primeira diferença seria o fim da crença de que estamos na vida terrena para percorrer um caminho após o qual dias melhores chegarão; dias da perfeita ordem social, do equilíbrio de mercado, em suma, “do completo domínio sobre o futuro - tão completo que põe fim a toda contingência, disputa, ambivalência e consequências (sic) imprevistas das iniciativas humanas” (BAUMAN, 2001, p. 38). A segunda diferença pontuada diz respeito à sociedade como pluralidade

de indivíduos, os quais passam a ser protagonistas de tarefas e deveres em evidente desregulamentação e privatização.

Em outras palavras, cada indivíduo se transforma em uma empresa de si mesmo, se inserindo em um ambiente concorrencial com o desiderato de aumentar sua eficiência diária a fim de ocupar posição de vantagem em relação aos outros concorrentes. Dessa forma, passa a viver em permanente competição em relação às outras pessoas. Ademais, em uma sociedade vigiada, o chamado "marketing pessoal" passa a ser uma prática rotineira, trata-se de um personagem destacado da própria subjetividade a fim de maximizar todo e qualquer tipo de retorno que puder obter.

Esta mutação acerca da percepção coletiva de encarar o futuro foi percebida no campo literário, *locus* capaz de refletir, a partir da ficção, os anseios e medos sociais. Desta forma, as utopias literárias deram lugar às distopias, haja vista o fim da fé cega no progresso e da ciência como um local infalível, que traria a verdade inabalável. Stefano Rodotá explica que o principal fator desta mudança, "além da percepção dos riscos do progresso tecnológico, está a consciência da impossibilidade de deter tal progresso, ainda que traga angústia e temor" (RODOTÁ, 2008, p. 41).

Neste debate, existem dois autores que foram além de seu tempo: Aldous Huxley e George Orwell. Ambos, ainda na década de 1930 e 1940, respectivamente, fizeram prenúncios acerca do futuro - que guarda semelhanças com o presente que vivemos. A influência de suas obras ultrapassou o âmbito literário e ambas são rememoradas até hoje nos debates e obras que versam sobre vigilância.

François Ost (2006) relata que enquanto o Direito seleciona, estabelece hierarquia e cria regras, a narrativa literária satisfaz um infinito de "variações imaginativas", explora um amplo espectro de posições, valores e representações. Para ele, o Direito só se desenvolve por meio de generalidades e abstrações; ao invés disso, a literatura se encontra em constante movimento, avançando sobre a singularidade do individual, podendo ser utilizada como crítica subversiva com a função de criação transformativa, ou seja, como um guia para revisar ideias, valores e preconceitos.

A narrativa de "1984" foi escrita na década de 1940 por George Orwell (pseudônimo de Eric Artur Blair) e ambientada na Grã-Bretanha (no ano que intitula a obra), que geográfica e politicamente fazia parte da Oceania, continente em guerra com outros dois continentes, a Letásia e a Eurásia.

"O Grande Irmão Está de Olho em Você": em "1984", essa mensagem era repetida exaustivamente pelo Partido Ingsoc, cujo poder era hegemônico, nutrido e exercido através de mecanismos de vigilância, tais como a espionagem e a teletela. A teletela consistia em uma TV bidirecional na qual o espectador não apenas assistia à programação, mas também era "assistido" pelo partido. Porém, se os indivíduos eram de fato observados o tempo todo, de forma intermitente ou quiçá se realmente eram observados não era o aspecto mais relevante. O que de fato importava para a eficácia do dispositivo era que as pessoas se sentissem vigiadas, mantendo o autocontrole de suas atitudes e diminuindo, com isso, os riscos de atuar contra os interesses do partido.

O regime dominante era o totalitário, o que tornava o controle dos cidadãos imprescindível para que se mantivesse no poder, sendo a vigilância um importante aspecto de sua estratégia, ainda que não a única. O protagonista da novela Winston Smith, por exemplo, trabalhava para o Ministério da Verdade, responsável pela propaganda e pelo revisionismo histórico. Sua função era reescrever os artigos de jornais já publicados, de modo que o registro final estivesse de acordo com os anseios do partido.

De nome no mínimo irônico, essa pasta ministerial fazia parte da estratégia do "duplipensar", correspondente a um conceito segundo o qual seria possível ao indivíduo conviver simultaneamente com duas crenças diametralmente opostas e aceitar a ambas. O "duplipensar" é uma das palavras elaboradas pela "novilígua", uma manipulação da linguagem visando à redução dos termos utilizados pelas pessoas. O objetivo com isso era o de limitar o espaço das consciências, eliminando o conceito de liberdade a ponto de tornar impossível qualquer crítica ao referido partido, uma vez que não existiriam expressões que pudessem ser utilizadas com esse fim: se não fosse possível definir algo, então seria como se este algo não existisse.

Proibição, repressão, disciplina, vigilância e punição são as formas de exercício do poder encontradas nessa ficção: "Guerra é paz, Liberdade é escravidão, Ignorância é força.", esse é o lema do partido, que emprega seus recursos para garantir a sua permanência incontestável.

Por sua vez, "Admirável Mundo Novo" foi escrito na década de 1930 por Aldous Huxley. A trama se passa em 632 d.f (depois de Ford), na cidade de Londres, e apresenta uma divisão geopolítica entre os "selvagens" e os "civilizados". Os dois grupos são estruturados em uma sociedade de castas, cujo objetivo é o de que todos os indivíduos sejam

felizes, independentemente da posição social que ocupem. No entanto, a felicidade somente seria possível na ordem, imperativo dos civilizados. Por conta disso, as pessoas eram controladas desde o nascimento por sistemas que combinavam controle genético (predestinação da casta) e condicionamento mental.

A hierarquia social e funcional da sociedade criada por Huxley segue o seguinte padrão "de cima para baixo": Alfas, Gamas, Betas, Deltas, Ipsílons e grupos Bokanovsky. A determinação de casta acontece pelo nascimento. Com base em engenharia genética, frutos de uma escolha rigorosa de genes, os humanos do Admirável Mundo Novo são concebidos e desenvolvidos em provetas. Às castas nobres são destinados os óvulos e espermas biologicamente superiores, os quais recebem e o melhor tratamento pré-natal possível. Já aos indivíduos de castas baixas, bem mais numerosas, as fertilizações são de qualidade inferior e o tratamento pré-natal é baseado em álcool e em outros venenos proteicos.

Desde a decantação *in vitro* até o fim de suas vidas, esses seres humanos são objeto de formação psicológica, com destaque para a "hipnopedia", que consiste em instruções aplicadas durante o sono, com o intuito de moldar as convicções de cada casta, fazendo-as aceitar sua condição e serem felizes com ela, por mais indigna que esta seja.

A sociedade apresentada por Huxley extingue a família, a religião, a história, a monogamia e, sobretudo, as emoções. Neste espaço, faz-se necessário manter a serenidade de todo e qualquer indivíduo a fim de que se mantenha a estabilidade social. No despontar de desequilíbrios internos, basta consumir a "soma", uma droga cuja finalidade é entorpecer e restabelecer o controle psíquico. Em outras palavras, uma fuga protetora contra a súbita manifestação de pensamentos abominados pelo sistema. [4]

---

4 A crônica da autora Eliane Brum oferece uma ponte com a realidade: Exaustos e correndo. Exaustos e correndo. E a má notícia é que continuaremos exaustos e correndo, porque exaustos-e-correndo virou a condição humana dessa época. E já percebemos que essa condição humana um corpo humano não aguenta. O corpo então virou um atrapalho, um apêndice incômodo, um não-dá-conta que adoece, fica ansioso, deprime, entra em pânico. E assim dopamos esse corpo falho que se contorce ao ser submetido a uma velocidade não humana. Viramos exaustos-e-correndo-e-dopados. Porque só dopados para continuar exaustos-e-correndo. […] Os cliques da internet tornaram-se os remos das antigas galés. Remem remem remem. Cliquem cliquem cliquem para não ficar para trás e morrer. Disponível em: https://brasil.elpais.com/brasil/2016/07/04/politica/1467642464_246482.html.

Os cidadãos de Admirável Mundo Novo não oferecem mais resistência, estão passivos e, mais do que isso, tornam-se cúmplices e receptivos à própria condição de servidão na qual vivem. A obediência e a cumplicidade cegas impedem a criação de qualquer desejo ou autonomia, uma vez que são podados antes que possam vir a obter qualquer tipo de consciência a respeito da renúncia que fazem. Nessa sociedade não há espaços para questionamento, dúvidas, conflitos: apenas a felicidade pode reinar.

Fazendo um paralelo entre as duas obras aqui trazidas, verifica-se que as tramas possuem dois pontos de contato importantes, quais sejam: o cenário distópico e o controle social. Esse controle, no entanto, é exercido de maneiras diversas em cada uma delas: enquanto em "1984" temos a centralidade do controle pelo governo, com artifícios de disciplina, vigilância, punição e exclusão, em "Admirável Mundo Novo" esse controle é difuso e disperso, sendo fruto do seu sucesso justamente a dispensabilidade de controle governamental central sobre os indivíduos, uma vez que são estes que exercem sobre si o autocontrole e se entorpecem com auxílio da "soma".

Para Bauman (2001, p. 64), cada um dos autores, à sua época, descreveu o futuro que acreditava ser inevitável, mas com divergências entre seus mundos. Enquanto Orwell visualizava um mundo de miséria e destituição, de escassez e necessidade, Huxley desenhava uma terra de opulência e devassidão, de abundância e saciedade. Os habitantes do mundo de Orwell, pontua Bauman, eram tristes e assustados, já os de Huxley eram despreocupados e alegres.

Para o referido autor, o fio que une as duas visões proporcionando o diálogo entre as obras é o seguinte:

> [...] o que elas compartilhavam era o pressentimento de um mundo estritamente controlado; da liberdade individual não apenas reduzida a nada ou quase nada, mas agudamente rejeitada por pessoas treinadas a obedecer a ordens e seguir rotinas estabelecidas; de uma pequena elite que manejava todos os cordões - da Individualidade de tal modo que o resto da humanidade poderia passar toda sua vida movendo-se como marionetes; de um mundo dividido entre administradores e administrados, projetistas e seguidores de projetos. O fato de o

Acesso em: 30 de março de 2018.

> futuro trazer menos liberdade, mais controle, vigilância e opressão não estava em discussão. Orwell e Huxley não discordavam quanto ao destino do mundo; eles apenas viam de modo diferente o caminho que nos levaria até lá se continuássemos suficientemente ignorantes, obtusos, plácidos ou indolentes para permitir que as coisas seguissem sua rota natural (Bauman, 2001, p. 64 - 65).

Em outras palavras, a visão do mundo do futuro encontrada em ambos os autores era a de que a grande maioria das pessoas não mais estaria direcionando as suas próprias vidas. Na realidade, quem designaria um roteiro seria uma minoria da elite que deteria o poder de excluir da sociedade aqueles que não seguissem seu papel pré-determinado. [5]

É neste ponto que diversos autores defendem a proximidade dos tempos atuais com aquele descrito por Huxley. O sociólogo David Lyon (2003), por exemplo, disserta que, semelhante ao que se vê no Admirável Mundo Novo, atualmente persiste o domínio consensual em que as pessoas são seduzidas em conformidade pelos prazeres oferecidos pelo "soma", encarado como o prazer do consumo: as necessidades e os desejos do tempo atual não são reprimidos, mas sim estimulados, afinal, o imperativo do consumo é o de que estes sejam constantemente renovados e de que a intensidade da recompensa seja máxima no menor espaço de tempo, como uma droga, para que o viciado volte a consumir novamente em uma frequência cada vez maior.

Em resumo, do *Big Brother* ao *Big Data* ou aos *Little Brothers*, da "soma" ao "curtir", a sociedade é vigiada tanto pelo governo, quanto por empresas e organizações, as quais possuem aparato tecnológico e de

---

5 Mark Poster transcreve em sua obra excerto de carta escrita por Huxley para Orwell, em 1969, acerca de sua visão do futuro: *Within the next generation I believe that the world's rulers will discover that infant conditioning and narco-hypnosis are more efficient as instruments of government, than clubs and prisons, and that the lust for power can be just as completely satisfied by suggesting people into loving their servitude as by flogging and kicking them into obedience. In other words, I feel that the nightmare of Nineteen Eighty-Four is destined to modulate into the nightmare of a world having more resemblance to that which I imagined in Brave New World. The change will be brought about as a result of a felt need for efficiency [and as viewed 60 years later, we can add seduction and fear*] (HUXLEY, 1969, não p. *apud* MARX, 2016, p. 215).

recursos humanos para armazenamento de dados e tratamento de informações com objetivo comercial, influenciando e moldando cidadãos em consumidores “ideais”.

1.2. PANÓPTICO E ARQUITETURA DE VIGILÂNCIA

Saindo da seara literária, um dos autores mais relevantes que investiga o tema é Michel Foucault, que se debruçou sobre a estrutura panóptica proposta por Bentham para descrever a arquitetura ideal de vigilância a ser empregada em locais que possuíssem a demanda de disciplina e controle.

Deve-se, inicialmente, ressaltar que panóptico e vigilância, embora se correlacionem, não são sinônimos. Na realidade, o panóptico é uma organização para o controle social, sendo uma das possíveis tecnologias burocráticas para exercício da vigilância.

A obra Vigiar e Punir, de Michel Foucault, publicada originariamente em 1975, identifica a inexistência de um poder único[6] - centrado somente no Estado, enquanto uno e onipotente - mas sim de diversas relações de poder descentralizadas, exercidas em campos diversos da vida, tal como na fábrica, na escola, nas relações privadas etc. Para Foucault, o poder não se detém enquanto propriedade ou privilégio adquirido ou conservado de uma classe dominante, mas é, antes disso, “o efeito de conjunto de suas posições estratégicas, efeito manifestado e às vezes reconduzido pela posição dos que são dominados” (FOUCAULT, 2005, p. 26).

Neste contexto, insere-se a vigilância como tecnologia de poder que incide sobre os corpos dos indivíduos, controlando seus gestos, suas atividades, sua aprendizagem e sua vida cotidiana, visando à docilidade dos corpos: “É dócil um corpo que pode ser submetido, que pode ser

6 O estudo desta microfísica supõe que o poder nela exercido não seja concebido como uma propriedade, mas como uma estratégia; que seus efeitos de dominação não sejam atribuídos a uma ‘apropriação’, mas a disposições, manobras, táticas, técnicas, funcionamentos; que se desvende nele antes uma rede de relações sempre tensas, sempre em atividade, do que um privilégio que se pudesse deter; que se seja dado como modelo antes a batalha perpétua do que o contrato que faz uma cessão ou uma conquista que se apodera de um domínio. Em suma, é preciso admitir que esse poder é algo que se exerce mais do que se possui. Não é ‘privilégio’ adquirido ou conservado da classe dominante, mas o efeito de conjunto de suas posições estratégicas, efeito manifestado e, às vezes, reconduzido pela posição dos que são dominados. (1975, p.29)

utilizado, que pode ser transformado e aperfeiçoado" (FOUCAULT, 2005, p.118).

Para o autor, saber é poder e, consequentemente, poder é saber:

> O poder produz saber (...), não há relação de poder sem constituição correlata de um campo de saber, nem saber que não suponha e não constitua ao mesmo tempo relações de poder. Essas relações de "poder-saber" não devem ser analisadas a partir de um sujeito de conhecimento que seria ou não livre em relação ao sistema de poder; mas é preciso considerar ao contrário que o sujeito que conhece, os objetos a conhecer e as modalidades de conhecimento são outros tantos efeitos dessas implicações fundamentais do poder-saber e de suas transformações históricas. Resumindo, não é a atividade do conhecimento que produziria um saber, útil ou arredio ao poder, mas o poder-saber, os processos e as lutas que o atravessam e o constituem, que determinam as formas e os campos possíveis do conhecimento (FOUCAULT, 2005, p. 30).

De acordo com Foucault (2005), por meio da normatização, a Sociedade Disciplinar almeja a normalização dos corpos e a assemelhação dos indivíduos. A estratificação social deixa de possuir o aspecto de *status*, privilégios, filiações, para possuir um grau de normalidade, mantendo, no entanto, o seu papel: de diferenciação, de classificação e de hierarquização. Assim, enuncia o caráter dicotômico da norma: ao mesmo tempo em que homogeneíza, também individualiza:

> [...] permitindo medir os desvios, determinar os níveis, fixar as especialidades e tornar úteis as diferenças, ajustando-as umas às outras. Compreende-se que o poder da norma funcione facilmente dentro de um sistema de igualdade formal, pois dentro de uma homogeneidade que é a regra, ele introduz, como um imperativo útil e resultado de uma medida, toda a gradação das diferenças individuais. Para tanto, as normas referentes à individualidade disciplinar permitem homogeneizar os traços individuais, indicando a

> "formalização" do individual dentro de relações de poder (FOUCAULT, 2005, p. 164).

Identifica-se o poder disciplinar enquanto técnica e dispositivo de poder cujo fim é justamente o controle dos corpos, de modo a assegurar a sujeição dos indivíduos e a sua docilidade-utilidade.

Para tanto, a vigilância se torna uma peça-chave na dinâmica de saber-poder, considerada no âmbito do capitalismo como uma forma de se manter a engrenagem da produção a rodar, um poder exercido em tantos sistemas e de forma tão ramificada que é incorporado à vida dos indivíduos, exercendo-se de forma automática e anônima. "A disciplina faz 'funcionar' um poder relacional que se autossustenta por seus próprios mecanismos e substitui o barulho das manifestações pelo jogo ininterrupto dos olhares calculados" (FOUCAULT, 2005, p. 170).

Era possível, assim, identificar os habitantes que não se enquadravam nos padrões de normalidade delineados na sociedade desenhada por Foucault e excluí-los dessa sociedade, confinando-os fisicamente em locais apartados da vida social e fazendo com que ocorresse a morte cívica do indivíduo. Nesse local, a vigilância e a disciplina eram ainda mais evidentes. "O panoptismo é o princípio geral de uma nova 'anatomia política' cujo objeto e fim não são a relação de soberania, mas as relações de disciplina" (FOUCAULT, 2005, p.172).

Conforme descreve o referido autor, o panóptico é uma máquina de vigilância que possibilita que poucos indivíduos possam vigiar eficientemente o comportamento de muitos. Para tanto, funciona a partir de três elementos arquitetônicos principais: a) um espaço circular e fechado, com controle das pessoas que entram e saem; b) uma divisão em celas, sem qualquer possibilidade e forma de comunicação entre os vigiados; e c) uma torre central, cujo plano de observação está em um nível mais alto que o das celas. Uma das mais importantes características desse dispositivo é que ele instaura um princípio de visibilidade permanente:

> [...] cada um, em seu lugar, está bem trancado em sua cela, de onde é visto de frente pelo vigia; mas os muros laterais impedem que entre em contato com seus companheiros. É visto, mas não vê; objeto de uma informação, nunca sujeito numa comunicação. A disposição de seu quarto, em frente da torre central, lhe impõe uma visibilidade axial; mas as divisões do anel, essas celas bem separadas, implicam uma invisibilidade lateral. E

> esta é a garantia da ordem (FOUCAULT, 2005, p. 167).

Prosseguindo com Foucault (2005, p. 166), o sucesso do panóptico se resumiria em:

> [...] induzir no detento um estado consciente e permanente de visibilidade que assegura o funcionamento automático do poder. Fazer com que a vigilância seja permanente em seus efeitos, mesmo se é descontínua em sua ação; que a perfeição do poder tenda a tornar inútil a atualidade de seu exercício; que esse aparelho arquitetural seja uma máquina de criar e sustentar uma relação de poder independente daquele que o exerce; enfim, que os detentos se encontrem presos numa situação de poder de que eles mesmos são os portadores. Para isso, é ao mesmo tempo excessivo e muito pouco que o prisioneiro seja observado sem cessar por um vigia; muito pouco, pois o essencial é que ele se saiba vigiado; excessivo, porque ele não tem necessidade de sê-lo efetivamente. [...]o panóptico é uma máquina de dissociar o par ver-ser visto: no anel periférico, se é totalmente visto, sem nunca ver; na torre central, vê-se tudo, sem nunca ser visto.

Por meio da vigilância, é possível saber tanto quais as palavras utilizadas quanto quais as atitudes tomadas e qual o rendimento de cada indivíduo, assim como exercer poder sobre eles, por conta da possível intervenção, enquanto método de dominação, como processo de objetivação e de sujeição, e não de construção de subjetividade. Desta forma, a disciplina tem por efeito a padronização e a normatização de condutas quistas, fundamental para o sistema de produção.

Muito embora se reconheça a relevância da obra de Foucault, alguns autores ressalvam que é necessário ter cautela ao interpretar a vigilância atual aos olhos do panóptico. Por exemplo, David Lyon (2003) alerta que a concepção e a ideia do panóptico chegaram à tona no debate e na crítica por meio da releitura feita pelo autor francês, e não diretamente por Bentham.

Outra crítica, esta realizada por Gary Marx (2016), seria a de que Foucault direciona sua análise para o controle realizado por organizações hierárquicas, deixando de lado outras formas de vigilância,

tais como a interorganizacional e a não-organizacional, aquela na qual indivíduos realizam a vigilância uns sobre os outros.

Sugerem Bauman e Lyon (2012) que o trabalho de Foucault acerca do panóptico apresenta "limites históricos, assim como lógicos, à utilização das imagens do panóptico hoje" (não p.)[7], isso porque, sendo o espelho da modernidade, não mais persiste o contexto no qual se insere, havendo a necessidade releituras que o adaptem à realidade, com as novas tecnologias e as diferentes práticas sociais. Este novo momento é chamado por Bauman de "vigilância líquida", onde o panóptico "persiste até o momento e está cada vez mais forte, mas ele claramente deixou de ser o padrão ou a estratégia universal de dominação na qual esses dois autores acreditavam em suas respectivas épocas" (não p).

De forma semelhante, em outra obra, Bauman (2008a) disserta que o panóptico, nos arranjos contemporâneos do poder, persiste com novas e melhoradas versões técnicas, visto que as estratégias ortodoxas, por conta de seu rigor excessivo, revelar-se-iam irrelevantes ou inteiramente contraproducentes na atualidade.

Segundo explica Han (2013), no século XVII, o poder soberano significava o poder da espada, que se transformou no poder disciplinar, enquanto imposição completa sobre a vida: o velho poder de morte cede diante da administração dos corpos e da gestão da vida. Um dos principais motivos para a transição do poder soberano ao disciplinar foi a mudança da forma de produção agrária para a industrial, que requer a disciplina do corpo e o seu ajuste à produção mecânica. O poder disciplinar, então, descobre a população como uma massa de produção e reprodução que deve administrar meticulosamente, sendo imprescindível o poder disciplinar normativo, visto que fixa preceitos e proibições com o fito de eliminar desvios e anomalias.

Han (2013) pontua que o intuito do panóptico, em uma sociedade disciplinar, é o de impor um padrão uniforme ao comportamento dos internos, ou seja, trata-se de uma arma contra a diferença, a opção e a variedade. Ademais, tem por função garantir que ninguém escape do espaço estreitamente vigiado. As torres de observação, no entanto, são substituídas por bancos de dados: os indivíduos passam a estar "amarrados informaticamente", sem qualquer refúgio à observação ou barreira em torno da qual se possa traçar uma linha de resistência.

[7] Adotou-se neste trabalho a expressão "não p." para se referenciar obras em formato *e-book* não estão devidamente paginadas, cuja diagramação apenas mostra a posição no dispositivo de leitura, variável de acordo com a tipo e o tamanho de fonte configurada.

O objetivo do panóptico e do uso de banco de dados difere: empresas de crédito e marketing visam garantir que se trate de um consumidor de credibilidade com fulcro no conhecimento gerado a partir das informações obtidas. Desde já, os considerados incapazes de procederem a escolhas no âmbito do mercado são peneirados antes que possam causar danos ou desperdiçar recursos. Nos termos de Bauman (1999), estar "fixado" em um banco de dados se transforma em condição primordial para participação social, sendo este o meio de acesso à "melhor oportunidade local":

> [...] o banco de dados registra os consumidores confiáveis e dignos de crédito, eliminando todo o restante que não deve ser levado em conta no jogo do consumo simplesmente pelo fato de não haver nada a registrar sobre suas atividades. A principal função do Panóptico era garantir que ninguém pudesse escapar do espaço estreitamente vigiado; a principal função do banco de dados é garantir que nenhum intruso entre aí sob falsas alegações e sem credenciais adequadas. O banco de dados é um instrumento de seleção, separação e exclusão. Ao contrário do Panóptico, o banco de dados é um veículo de mobilidade, não grilhões a imobilizar as pessoas (BAUMAN, 1999, não p.).

Com o desenvolvimento de tecnologias da informação e comunicação, o espaço se estreita com o tempo: a informação pode viajar independentemente de seus portadores físicos. Os dados são intangíveis e seu deslocamento acontece imediatamente, sem qualquer vinculação à velocidade do transporte e a movimentos físicos. Novas formas de interação e contenção sociais ramificadas, incorporadas sutilmente, passam a fazer parte do cotidiano pessoal e organizacional e fizeram com que o panóptico precisasse "evoluir" para manter sua existência.

1.3 DA SOCIEDADE DISCIPLINAR À SOCIEDADE DO CONTROLE

Se na Sociedade Disciplinar os indivíduos deviam ser moldados para aumentar o sistema de produção, na Sociedade do Controle o que deve ser expandido é o consumo, a fim de criar uma demanda que tenha capacidade de absorver a incessante produção de bens e serviços, com a

eliminação de estoques e o estímulo ao descarte. O controle social passa a ser realizado por técnicas de manipulação e desejo, ou seja, deixa de atuar diretamente sobre os corpos, mas passa a atuar indiretamente sobre as mentes (HAN, 2014).

A primeira elaboração teórica acerca da Sociedade do Controle da qual se tem registro é a de Deleuze, em pequeno ensaio intitulado "Post-Scriptum sobre as Sociedades de Controle", inserido na compilação "Conversações" e originariamente publicado em 1990.

Deleuze (1992) identifica dois polos que se contrapõem nas Sociedades Disciplinares: o indivíduo e a sociedade de massa: a assinatura que indica o indivíduo versus o número de matrícula que indica sua posição na multidão indeterminada. Nas Sociedades de Controle, ao contrário, o essencial não se refere mais a assinaturas ou a números, mas a uma cifra, que marca o acesso aos bens e à informação - ou à rejeição - e, consequentemente, à possibilidade de participação da vida pública. Os indivíduos tornaram-se "dividuais", divisíveis, e as massas se tornaram amostras, mercados ou bancos de dados.

Para o autor (1992), este novo arranjo social não decorre apenas da evolução tecnológica, mas, principalmente, do capital. Neste compasso, a lógica e a proeminência das fábricas são substituídas pelas empresas, enquanto alma e enquanto razão de ser, inclusive para os seres "dividuais". O capitalismo abandona sua direção exclusivamente para a produção a fim de se dirigir à venda e ao mercado. Em outras palavras, ele passa a ser voltado para o consumo.

Além disso, Deleuze (1992) já reconhecia o marketing como instrumento de influência social: sua configuração contínua e ilimitada, de curto prazo e de rotação rápida, tendo como alvo o ciclo de formação do desejo, consumo e descarte, repetido indefinidamente, em evidente contraponto às táticas de controle disciplinar, com caráter de longa duração, infinitas e descontínuas.

Para Bauman (2008a), o mérito da Sociedade do Controle foi atingir seus fins por meios coercitivos sutis, motivando condutas comportamentais desejadas à necessária e pretendida manipulação, de forma antagônica às antigas técnicas disciplinares e de punição: "o que por sua maneira de intervir era incômoda, custosa e tendia ao conflito, visto que impunha constrangimentos severos e inegociáveis à sua própria liberdade de manobra" (BAUMAN, 2008a, p. 96).

O que de fato ocorreu após a superação da sociedade disciplinar "foi a descoberta, invenção ou emergência de um método alternativo de manipular as probabilidades comportamentais necessárias para sustentar

o sistema de dominação reconhecido como ordem social" (BAUMAN, 2008a, p. 97).

Conforme explica Han (2014), o regime disciplinar, para Deleuze, se organiza como um corpo, ou seja, trata-se de um regime biopolítico. Por seu turno, a sociedade do controle se insere no regime neoliberal, comportando-se como alma, sendo a psicopolítica sua nova forma de governo. Institui a lógica da competição empresarial aos indivíduos, sendo inerentes a esta técnica de dominação a motivação, o projeto, a competência, a otimização e a iniciativa. Em outras palavras, o poder inteligente e amável não opera contra a vontade dos sujeitos. É mais afirmativo do que denegador, mais sedutor do que repressivo, esforça-se para gerar emoções positivas e explorá-las. Não proíbe, seduz, não enfrenta o sujeito, mas lhe oferece facilidades.

Neste diapasão, de acordo com Fernanda Bruno (2015, p. 63), o sofrimento se desloca do corpo para a alma; é o sentimento de culpa que julga e condena: "ainda que muitas vezes um dispositivo intangível na pós-modernidade, os efeitos da vigilância e sua intervenção são reais".

Schneier (2015) alerta que a tecnologia oferece aos governos e às corporações capacidades robustas para uma vigilância massificada e, ao mesmo tempo, individualizada, permitindo que se proceda à discriminação com base em qualquer tipo de critério elegível: raça, religião, classe, política. Desta forma, a vigilância pode ser utilizada para controlar o que se vê, o que se faz e até mesmo o que se diz, tendo em vista sua influência e manipulação. O mesmo autor percebe que inexiste, atualmente, qualquer mecanismo significativo de *checks and balances* ou oportunidade real de sair dessa dinâmica: as leis promulgadas com o objetivo de proteger a sociedade de perigos advindos de regimes tecnológicos são insuficientes.

Na Sociedade de Controle, desta forma, o indivíduo deixa de ser moldado por ameaças, pelo medo, pela mão de ferro, tornando-se impossível identificar um poder central, não é mais o seu corpo o artifício de controle. A manipulação acontece por meio da própria psique: o autocontrole, a autopunição e a aparente liberdade da criação e de exercício do desejo dominam os indivíduos, que se tornam incapazes de reconhecer essa dinâmica.

1.4 AS FORMAS DE PERSISTIR DO PANÓPTICO

David Lyon (2013) pontua que os estudos de vigilância lançam combustível no fogo do debate sobre a pós-modernidade, exigindo a

revisão da teoria da vigilância, que ainda é dominada por modelos e metáforas decorrentes da era moderna.

Numa tentativa de localizar os esforços teóricos empregados desde o panóptico de Bentham acerca da vigilância, o autor Gary Marx (2016) oferece uma trama de ensaios teóricos cujos autores elaboraram conceitos considerados relevantes para o estudo atual da vigilância:

> *[...] disciplinary society, the gaze, and biopower* (Foucault 1977, 1988) *surveillance society, the new surveillance, and maximum security society* (Marx 1985, 1988, 2002) *net widening* (S. Cohen 1985) *dossier society* (Laudon 1986b) *dataveillance* (Clarke 1988) *superpanopticon* (Poster 1990) *society of control* (Deleuze 1990) *l'anamorphose de l'état-nation* (Palidda 1992) *panoptic sort* (Gandy 1993) *minimum security society* (Blomberg 1987) *synopticon* (Mathiesen 1997) *securitization* (Waever 1995) *telematic society* (Bogard 1996) *techno-policing* (Nogala 1995) *transparent society* (Brin 1998) *liquid modernity* (Bauman 2000) *information empire* (Hardt and Negri 2000) *surveillant assemblage* (Haggerty and Ericson 2000) *postpanopticon* (Boyne 2000) *glass cage* (Gabriel 2004) *ban-opticon* (Bigo 2006a) *high policing* (Brodeur and Leman-Langlois 2006) *ubiquitous computing* (Greenfield 2006) *überveillance* (Michael, Fusco, and Michael 2008) *safe society* (Lyon 2007) *ambient intelligence* (Wright et al. 2010) *thick and thin surveillance* (Torpey 2007) *cryptopicon* (Vaidhyanathan 2011) (MARX, 2016, p. 97 - 98).

O referido autor explica que, embora não haja unanimidade, a construção de tais conceitos é um primeiro passo imprescindível para a compreensão do fenômeno da vigilância. Também reconhece que esses estudos se baseiam em dados empíricos restritos, os quais abrangem contextos específicos, países ou tecnologias, logo, são incapazes de desenredar as múltiplas dimensões que compõem o tipo ideal de vigilância e, consequentemente, de explorar distribuições, correlações e inter-relações.

No entanto, Bauman e Lyon (2012) pontuam que, se existe um consenso, uma espinha dorsal que liga os teóricos que se debruçam ao estudo de vigilância, este diz respeito ao abandono do entendimento da

vigilância enquanto um dispositivo sólido e estável, uma vez que se torna "muito mais móvel e flexível, infiltrando-se e se espalhando em muitas áreas da vida sobre as quais sua influência era apenas marginal" (BAUMAN; LYON, 2012, não p.).

Deveras, é possível visualizar a superação do paradigma do panóptico e a ascensão de uma vigilância rizomática, que penetra em todos os campos da vida, proporcionando novas armas de controle social por mediação tecnológica de dispositivos que coletam dados indiscriminadamente.

Diante disso, o presente estudo irá pincelar alguns dos conceitos trazidos por esses autores, a fim de localizar esta guinada teórica, com a mudança da estrutura de produção e consumo de bens, de controle social e do desenvolvimento de tecnologias de informação e comunicação que auxiliam na vigilância maciça e integral dos indivíduos.

O termo *dataveillance* foi primeiramente cunhado pelo cientista australiano de computação Roger Clarke, em 1988, diz respeito à aglutinação e à abreviação de dois termos em inglês, quais sejam: *data* e *surveillance*, podendo ser conceituado como o uso sistemático de dados pessoais para a investigação ou monitoramento de ações ou comunicação de uma ou mais pessoas.

Para Clarke (1988), a vigilância diz respeito à sistemática investigação ou monitoramento de ações ou comunicação de uma ou mais pessoas, sendo seu intuito primário coletar informações e, o secundário, influenciar pessoas ou mesmo toda uma população a agir de forma predeterminada.

Àquela época a vigilância física estava se expandindo (telescópios, câmeras, lentes fotográficas, áudio-gravação), mas a vigilância eletrônica também estava, mas de forma exponencial e de modo a tomar o lugar daquela.

Outro conceito de relevância trazido por Clarke (1994) está ligado à construção de personas[8] digitais, se referindo à elaboração de modelos de indivíduos considerados ideais, ou seja, a partir da representação digital de aspectos da realidade.

---

8 Conforme explica o autor, Jung entende como "persona" a projeção de uma pessoa sobre o outro, cuja habilidade de construção está não apenas no próprio indivíduo, mas também em outras pessoas ou organizações. Neste sentido, o indivíduo possui algum grau de controle sobre a persona projetada por outrem, mas dificilmente tem influência acerca da persona criada pelos outros. Cada observador capta diferentes dados sobre cada pessoa com quem se relaciona, criando diferentes impressões. (CLARKE, 1994, não p.)

Clarke (1994) já anunciava que *dataveillance* era uma técnica muito mais barata e eficiente do que aquela até então conhecida, a vigilância física. Além disso, com a ideia de "persona" e de Internet, já denunciava a possibilidade de monitoramento e predição com base nos rastros deixados digitalmente, que poderiam vir a ser de interesse de governos e de companhias de marketing. Para ele, a TV bidirecional descrita por Orwell em 1984 já era algo obsoleto, pois o ambiente de coleta de dados são tecnicamente e economicamente superiores.

Thomas Mathiesen, em seu artigo intitulado "*The Viewer Society: Michel Foucault's Panopticon Revisited*" (1997), faz uma revisitação à teoria de Foucault, reconhecendo a mudança de eixo de vigilância ao longo da história, que estabelece novos nexos entre o ver, o ser visto e o poder. Para o autor, controle é mais do que vigilância, implicando a regulação do comportamento ou das atitudes.

De acordo com esse estudo, na idade pré-moderna dominava a lógica do espetáculo: muitos vigiavam poucos. Os plebeus observavam, seja com espanto ou admiração, o poder soberano. O poder moderno, por sua vez, inverte essa situação: o soberano fica na sombra e observa os súditos em vez de ser observado por eles. Ulteriormente, com o desenvolvimento de tecnologias e novas técnicas de poder, ocorre uma nova mudança de perspectiva: não são mais poucos que vigiam muitos, mas também muitos vigiam poucos. Essa nova relação seria fruto da ascensão dos veículos de comunicação de massa (jornais, rádio, televisão), que agora possuem o poder de noticiar qualquer pessoa, deslocando a possibilidade de ver e de ser visto.

Mathiesen (1997) denomina "sinóptico" - do grego *syn*, que significa "estar junto" ou "ao mesmo tempo"; e "óptico", que remete ao visual - à via de mão dupla concernente à vigilância massiva, seja pelo aparato de poder panóptico, seja pela atuação da mídia. O autor reconhece que ambas andam juntas, servindo como dispositivos de controle social, algumas vezes em paralelo e outras com íntimas interações, sendo utilizadas por instituições como parte de uma só dinâmica. O exemplo que Mathiesen oferece se refere à Igreja Católica Romana: a confissão das pessoas ao padre (poder panóptico, em que um ator vigia muitos) e suas igrejas e catedrais, construídas para serem locais sinópticos de admiração e arquitetadas para permitir que muitos pudessem ouvir os sermões ali proferidos.

Além disso, o referido autor (1997) também critica Foucault por não ter dado a devida atenção ao processo moderno paralelo de tecnologias informacionais e burocráticas, bem como à ascensão de

meios de comunicação de massa que permitiam que muitos vigiassem poucos.

Já Bauman (2008a) reconhece que, por conta da transformação existente na relação espaço-tempo, compactada devido às Tecnologias de Comunicação e Informação, que permitem que a distância deixe de ser um problema de tempo e custo, o ato de vigiar desprende os vigilantes e os vigiados de sua localidade. O autor então adota o termo sinóptico em sua obra por conta de sua natureza global, identificando que as pessoas não precisam de coerção, uma vez que seduz as pessoas à vigilância.

A descrição e a análise extensas feitas por Foucault acerca do panóptico demonstram como este pode ser considerado um espelho da modernidade, enquanto forma de moldar comportamento e motivação dos indivíduos. No entanto, defendem Bauman e Lyon (2012) que o sinóptico substitui o panóptico na nova lógica social: as muralhas e as torres de vigilância são despiciendas, bastando supervisores para garantir que os novos vigiados seguirão a rotina prescrita.

Tais supervisores seriam, para Bauman e Lyon (2012, não p.), os engenheiros empregados no "processamento de bases de dados", que preparam o terreno para a aplicação de técnicas de marketing: "Assim é e deve ser, considerando-se que um marketing eficaz exige o conhecimento das clientelas inadequadas para funcionar como alvo, da mesma forma que precisa identificar os 'alvos' mais promissores de seus esforços comerciais".

Sobre o conceito de poder sinóptico desenvolvido por Mathiesen, disserta Stefano Rodotá:

> Os espetáculos tomam o lugar da supervisão sem perder o poder disciplinador do antecessor. A obediência aos padrões (uma maleável e estranhamente ajustável obediência a padrões eminentemente flexíveis, acrescento) tende a ser alcançada hoje em dia pela tentação e pela sedução e não mais pela coerção - e aparece sob o disfarce do livre-arbítrio, em vez de revelar-se como força externa (RODOTÁ, 2008, p. 100 - 101).

Neste enleio, Han (2013) adota o sinóptico como sendo o panóptico digital, que faz desaparecer qualquer distinção estrutural entre centro e periferia, sendo sua eficiência a vigilância sem perspectiva, ou seja, quando se ilumina um cenário sem qualquer ótica perspectivista,

mas a partir de todos os pontos possíveis. Desse modo, a vigilância pode se reproduzir em todos os lados, a partir de todas as partes.

Na arquitetura do panóptico de Bentham, quem está na torre vigia as células, enquanto ele mesmo permanece invisível para os guardados. Por sua vez, no caso do sinóptico ou panóptico digital, sem olho central, nenhuma subjetividade central ou soberania é formada. Enquanto os moradores do panóptico de Bentham estão conscientes da presença constante do observador, aqueles que habitam o panóptico digital acreditam estar em liberdade.

Outra diferença identificada por Han (2013) é a de que as células foram projetadas para que não houvesse qualquer possibilidade de comunicação entre os vigiados, enquanto no sinóptico as pessoas se conectam e se comunicam intensamente umas com as outras. Desta forma, o que garante a transparência do indivíduo não é a solidão, mas a hipercomunicação: a autoexposição do sujeito no mercado panóptico. A sociedade de controle consuma-se onde seu sujeito é despojado, não por coerção externa, mas pela prescrição engendrada em si mesma, ou seja, onde o medo de renunciar à sua esfera privada deixa de ser um fator impeditivo.

Mark Poster (1995), por seu turno, desenvolve o conceito do "superpanóptico", enquanto uma versão cibernética e atualizada do panóptico. O autor afirma já em 1995 que os corpos das pessoas estariam amarrados informaticamente dentro das redes e dos bancos de dados. Identifica os bancos de dados como configurações de linguagem, enquanto forma de escrita com consequências não apenas relacionadas à própria linguagem, mas também às relações variadas com as formas de ação.

Para Poster, a base de dados é uma forma de discurso, porque afeta a própria constituição do sujeito, visto que se trata de uma forma de escrever que interfere e diferencia pessoas, o que se soma à sua transterritorialidade e à sua transtemporalidade.

Conforme o mesmo autor (1995), o aspecto diferenciador do superpanóptico é a voluntariedade: os próprios vigiados fornecem os dados para serem coletados, armazenados, tratados e utilizados por terceiros. A vigilância da escolha pessoal se torna uma realidade com a participação do próprio indivíduo. Em suma, quem está sendo supervisionado fornece as informações necessárias para a vigilância de si mesmo. Um dos maiores exemplos concerne às transações econômicas. O ato da compra que, teoricamente, seria um ato "privado", torna-se parte dos bancos de dados, tendo em vista que, hoje, qualquer

pagamento realizado com cartão de crédito, seja compra *online* ou física, com cartão de fidelidade, é registrado.

Ainda de acordo com Poster (1995), a capilaridade do poder, que foi notada por Foucault, fez com que este fosse sendo cada vez mais ramificado e, por corolário, aperfeiçoado. Os atos individuais se tornaram interesse para exercício do poder governamental e do mercado e foram transformados em um extenso discurso de vigilância; comportamentos privados tornam-se anúncios públicos e, ações individuais, linguagem coletiva.

O autor pontua que o processo de constituição do sujeito até então era de "subjetivação", ou seja, visava produzir indivíduos com (falso) senso de sua própria interioridade. A partir do superpanóptico, ao contrário, a constituição do sujeito adota um curso oposto de "objetificação", caminha para produzir indivíduos com identidades dispersas, identidades essas das quais os indivíduos podem nem mesmo estar cientes. Talvez o escândalo do superpanóptico seja a flagrante violação do grande princípio do indivíduo moderno, de sua interioridade "subjetivada" centrada.

É Fernanda Bruno (2015) quem constrói o conceito de palinóptico. No grego, *palin* significa “processos de dupla via”; enquanto óptico, que remete ao visual.De modo similar ao conceito de sinóptico, para a referida autora, “Ver e ser visto ganham aqui sentidos atrelados à reputação, pertencimento, admiração, desejo, conferindo à visibilidade uma conotação prioritariamente positiva, desejável, que ressoa nos sentidos sociais que a vigilância assume hoje” (BRUNO, 2015, p. 47).

Em outras palavras, Bruno (2015) sinaliza que o jogo da vigilância adquire outras nuances, tornando-se sujeito e objeto de uma dinâmica que se refere à própria percepção de pertencimento social. A exposição pessoal e o *voyerismo* se incorporam não apenas aos meios de comunicação e à mídia, mas ao próprio cotidiano dos indivíduos.

Além das construções sobre o sinóptico, o sociólogo Han também identifica e conceitua uma técnica diversa de vigilância: o “banóptico” (2014). Enquanto o panóptico vigia os excluídos do sistema, o banóptico identifica como não desejadas as pessoas hostis ao sistema, e ele próprio procede à exclusão destas. O panóptico serve para disciplinar e, paralelamente, o banóptico se ocupa da segurança e da eficiência do sistema capitalista e neoliberal. Nesta toada, as pessoas que não se enquadram nos sistemas, são consideradas “sucatas”: como sujeira e bloqueio dos espaços. A finalidade última do banóptico é a de assegurar

que a “sucata” será separada do produto valioso, ou seja, dos consumidores ideais.

Este assunto será visto detidamente no próximo tópico, cabendo assinalar que a destruição de objetos e a exclusão de sujeitos se tornam fatores substanciais em uma sociedade cujo consumo passa a ocupar lugar central e onde a vigilância assume um aspecto não apenas catalisador, mas central nesta dinâmica.

1.5 MARKETING, MODA E TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO: AS FERRAMENTAS DISPONÍVEIS PARA O CONSUMO E A VIGILÂNCIA

Vigilância e consumo estão intimamente ligados, David Lyon (2013) defende, inclusive, que a vigilância em si deve ser repensada em face do consumo, visto que deslocou o seu foco de instituições predeterminadas para o mercado em si. O autor declara que, por conta da vigilância, as tecnologias de informação tanto auxiliam na construção de saberes sobre os consumidores quanto oferecem ferramentas nas quais é possível classificar e agrupar esses consumidores, com o objetivo de identificar quem já está apto para o ecossistema do mercado e quem possui algum *déficit*. Neste último caso, é possível intervir com o fito de educar esses consumidores e estimulá-los de acordo com seus próprios interesses.

No entanto, tal intervenção passa despercebida, visto que as técnicas utilizadas não são coercitivas, consistindo em: marketing, seleção de ofertas, variação de preços e de apresentação de resultados, sempre visando moldar os consumidores a um mercado predeterminado.

Baudrillard já denunciava que, no cotidiano, o consumo havia se tornado o foco da vida, sua razão de ser: “enquanto homogeneização integral onde tudo está compendiado e ultrapassado na facilidade, enquanto translucidez de uma ‘felicidade’ abstrata, definida pela simples das tensões” (BAUDRILLARD, 1995, p. 20).

Ademais, o descarte de objetos, a sabotagem tecnológica ou o desuso organizado estariam acobertados sob o manto da moda. Para o autor, a finalidade da publicidade não é agregar valor, mas sim desvalorizar o valor-tempo dos antigos bens em detrimento do valor-moda e da renovação acelerada. A sociedade de consumo sente não apenas o sentimento primordial de obter, mas principalmente de destruir.

Deve-se pontuar que essa dinâmica entre controle, vigilância e consumo insere-se em um ambiente capitalista neoliberal globalizado,

cujo ínterim pode ser recortado a partir do final da década de 1980 e início da década de 1990 até o momento presente. As peculiaridades e impressões desse tempo, de três décadas para cá, são contextualizadas de diferentes maneiras por autores que se debruçam sobre o tema.

1.5.1 Obsolescência programada: a renovação de produtos e de desejos

Lipovetsky e Serroy (2015) fazem um apanhado histórico referente ao capitalismo de consumo. Conforme explicam, a primeira fase, considerada de Produção e Marketing de massa, vai de 1880 ao fim da Segunda Guerra Mundial. O consumo de massa nesse período é considerado imperfeito, com participação predominante apenas da burguesia. É nesta primeira fase que as marcas são criadas: o produto agora pode ser comprado sem a intermediação de um comerciante. A confiança passa de uma relação sujeito-sujeito para uma relação sujeito-objeto. Nesta época, o consumo-sedução, do qual somos legatários, passa a ser também explorado pelo marketing.

A segunda fase é definida como a Sociedade de Consumo de Massa, sendo marcada pela abundância, tendo início na década de 1950 e predominando até a década de 1980. Nessa fase verifica-se um melhoramento econômico e social, no qual há um aumento dos recursos com a difusão do crédito. Assim, a possibilidade de consumir o que se deseja (e não apenas aquilo de que se necessita) não fica mais restrita às elites sociais; ela se expande.

Nesse contexto, a obsolescência programada invade não apenas a lógica dos produtos em si, que passam a ter tempo de vida útil, mas também o psicológico das pessoas: a moda entra também no universo para tornar descartável, pela lógica do efêmero, da inovação, da renovação dos desejos qualquer âmbito da vida das pessoas. Este é o ponto desta segunda fase, que substitui a coerção pela sedução; o dever pelo hedonismo, de acordo com a própria lógica individualista. Para Lipovetsky e Serroy (2015, p. 42), este ciclo também estaria concluído:

> [...] um capitalismo centrado na produção foi substituído por um capitalismo de sedução focalizado nos prazeres dos consumidores por meio das imagens e dos sonhos, das formas e dos relatos. [...] Apostando em novas fontes de criação de valor, as empresas contemporâneas, notadamente através de estratégias focalizadas nos

> gostos estético-afetivos dos consumidores, forjaram o chamado modelo pós-fordiano ou pósindustrial da economia liberal.

Para Lipovetsky (2004) a pós-modernidade altera a percepção temporal: o aqui e o agora ganham primazia em relação ao futuro utópico delineado pela primeira modernidade. Outros fatores relevantes deste período são a rápida expansão do consumo e da comunicação de massa, o enfraquecimento das normas autoritárias e disciplinares, bem como a consagração do hedonismo e do psicologismo.

Porém, para Lipovetsky (2004, p. 52), o rótulo pós-moderno já nasceu natimorto, tendo em vista que mal havia sido anunciado e já teria "esgotado sua capacidade de exprimir o mundo em que se anuncia, quando já também se lançava os primeiros esboços da hipermodernidade".

Assim, para diferenciar a pós-modernidade dos tempos recentes, o autor incorporou o prefixo "hiper" aos conceitos- chaves presentes em sua obra, com o intuito de representar "a fuga para o adiante, de modernização desenfreada, feita de mercantilização proliferativa, de desregulamentação econômica, de ímpeto técnico-científico, cujos efeitos são tão carregados de perigos como de promessas" (LIPOVETSKY, 2004, p. 54). Neste diapasão, Lipovetsky manifesta sua ideia de sociedade da hipervigilância, que substitui a antiga sociedade disciplinar-totalitária. "A escalada paroxística do 'sempre mais' se imiscui em todas as esferas do conjunto coletivo" (LIPOVETSKY, 2004, p. 56).

Por sua vez, o hiperconsumo caracteriza-se pelo fato de que as esferas até então consideradas não-econômicas (família, religião, escola, ética) passam a ser permeadas pela lógica do consumo, ou seja, desconstroem-se antigos referenciais de sociabilidade. Além disso, o hiperconsumo está baseado no sistema-moda, no qual a temporalidade é breve e o movimento é obrigatório, portanto calcado na técnica do efêmero, da sedução e da inovação: é mandatório escolher cada vez mais e de forma o mais veloz possível. Apenas deste modo é possível alcançar maior rentabilidade e desempenho do indivíduo, em uma lógica que ultrapassa a vida do consumo e permeia outros setores da vida coletiva. A forma-moda generalizada institui o eixo do presente como temporalidade socialmente prevalecente (LIPOVETSKY, 2004, p. 64).

A satisfação acontece no ato da compra em si. E quando o indivíduo compra bens baratos e descartáveis podem escolher mais vezes e, consequentemente, obter prazer com mais frequência.

Lipovetsky e Serroy reconhecem que a motivação do consumo também se dá com o fito de diferenciação social, como distinção do outro. No entanto, defendem que cada vez menos se consome para ofuscar o outro e ganhar consideração social e cada vez mais para si mesmo (LIPOVETSKY; SERROY, 2015, p. 173).

Desta forma, a necessidade deixa de ser o ponto de impulso do consumo para dar lugar ao desejo, que além de se configurar como volátil e efêmero, dispensa outra justificativa ou "causa" que não ele mesmo, configurando um fim em si mesmo. O hiperconsumidor precisa se sentir vivo a todo instante, como se comprar fosse uma fonte da juventude que lhe proporciona rejuvenescer e se reinicia constantemente.

Para Lipovetsky (2006), quanto mais o hiperconsumidor detém um poder que há pouco lhe era desconhecido, mais o mercado faz alastrar os seus tentáculos; quanto mais o comprador se encontra em um estado de autoadministração, mais se verifica a extradeterminação ligada à ordem mercantil. Ou seja, se por um lado o hiperconsumidor acredita que está fazendo escolhas racionais, baseadas na relação qualidade-preço de acordo com informações que pesquisou, por outro lado, os modos de vida, os prazeres e os gostos se mostram cada vez mais dependentes do sistema comercial, cada vez mais vulneráveis a um sistema que seduz e implanta desejos nos consumidores cuja felicidade, ainda que instantânea, passa a depender da satisfação destes últimos.[9]

Segundo o autor, a moda representa um importante e decisivo fator na construção desta nova dinâmica mercantil-social, visto que a sua extensão e a sua permeabilidade emergem no pós-moderno. A sociedade burocrática e democrática se submete aos três componentes

9 Em entrevista, Noam Chomsky faz a seguinte crítica: "Até Orwell estaria assombrado. Vivemos a ficção de que o mercado é maravilhoso porque nos dizem que está composto por consumidores informados que adotam decisões racionais. Mas basta ligar a televisão e ver os anúncios: procuram informar o consumidor para que tome decisões racionais? Ou procuram enganar? Pensemos, por exemplo, nos anúncios de carros. Oferecem dados sobre suas características? Apresentam informes realizados por entidades independentes? Porque isso sim que geraria consumidores informados capazes de tomar decisões racionais. Em vez disso, o que vemos é um carro voando, pilotado por um ator famoso. Tentam prejudicar o mercado. As empresas não querem mercados livres, querem mercados cativos". De outra forma, colapsariam". Disponível em: <https://brasil.elpais.com/brasil/2018/03/06/cultura/1520352987_936609.html>. Acesso em: 02 de abril de 2018.

essenciais: efêmero, sedução, diferenciação marginal. “Uma sociedade superficial e frívola, que impõe a normatividade não mais pela disciplina, mas pela escolha e pela espetacularidade” (LIPOVETSKY, 2004, p. 19).

Por fim, Lipovetsky (2004) reconhece que os mecanismos de controle não desapareceram, apenas se adaptaram, com a intenção de serem menos coercitivos por si só, abandonando a imposição em favor da comunicação.

Este mesmo entendimento é compartilhado por David Harvey (2008, p. 285), que observa que a dinâmica do descarte começou a ficar evidente durante os anos 1960:

> Ela significa mais do que jogar fora bens produzidos (criando um monumental problema sobre o que fazer com o lixo); significa também ser capaz de atirar fora valores, estilos de vida, relacionamentos estáveis, apego a coisas, edifícios, lugares, pessoas e modos adquiridos de agir e ser. Foram essas as formas imediatas e tangíveis pelas quais o "impulso acelerador da sociedade mais ampla" golpeou "a experiência cotidiana comum do individuo" (Toffler, p. 40). Por intermédio desses mecanismos (altamente eficazes da perspectiva da aceleração do giro de bens no consumo), as pessoas foram forçadas a lidar com a descartabilidade, a novidade e as perspectivas de obsolescência instantânea.

Edgar Morin (1997, p. 13-14) trata do consumo cultural como instrumento no auxílio do controle social:

> A segunda industrialização que passa a ser a industrialização do espírito, e a segunda colonização que passa a dizer respeito à alma progridem no decorrer do século XX. Através delas, opera-se esse processo ininterrupto da técnica, não mais unicamente voltado à organização exterior, mas penetrando no domínio interior do homem e aí derramando mercadorias culturais. Não há dúvida de que já o livro, o jornal eram mercadorias, mas a cultura e a vida privada nunca haviam entrado a tal ponto no circuito comercial e industrial. [...] Essas novas

> mercadorias são mais humanas de todas, pois vendem a varejo os ectoplasmas da humanidade, os amores, os medos romanceados, os fatos variados do coração e da alma.

Para ele, o que homogeneíza a sociedade é a identidade dos valores de consumo, veiculados e vinculados à *mass media*, sendo esta "o produto de um diálogo entre uma produção e um consumo". Todavia, este diálogo não é equânime: enquanto a produção desenvolve diferentes narrações e histórias, de acordo com seus próprios interesses, a forma de expressão do consumidor se resume tão somente ao sim e ao não; o sucesso ou fracasso. "O consumidor não fala. Ele ouve, ele vê ou se recusa a ouvir ou a ver" (MORIN, 1997, p. 46).

1.5.2 Dados Pessoais: o Principal Mantimento do Marketing

Bauman, em sua vasta obra, também reconhece o antigo período cujo mercado estava voltado à produção, sendo esta fase batizada por ele como a "fase sólida da modernidade", onde o panóptico estava inserido. Nesta fase, buscava-se a segurança, o ambiente confiável, ordenado, regular etc., e os bens de consumo se caracterizavam por sua longevidade e perenidade. Protegidos da depreciação ou dispersão, uma boa compra significava um investimento de longo prazo.

Embora se reconheça o consumo como ato indispensável, quando este passou a assumir lugar central na vida da maioria das pessoas, foi que deixou de ser uma forma de suprir necessidades para se tornar um hábito, ou seja, um fim em si mesmo, como forma de satisfazer desejos e buscar felicidade. Os valores buscados na modernidade sólida, como segurança e estabilidade, não se enquadram na sociedade de consumidores, que se baseia no volume e na intensidade de desejos sempre crescentes, implicando no imediatismo do uso e na acelerada substituição de produtos e serviços com a intenção de se buscar a satisfação. "Novas necessidades exigem novas mercadorias, que por sua vez exigem novas necessidades e desejos; o advento do consumismo augura uma era de 'obsolescência embutida' dos bens oferecidos no mercado" (BAUMAN, 2008a, p. 45).

Não se trata mais da modernidade sólida, mas da modernidade líquida, cujo panóptico cede à vigilância líquida, diluída em novos espaços e em novas situações (BAUMAN; LYON. 2012). A lógica da moda também pode ser identificada no consumismo visto que para ele se trata:

> [...] da reciclagem de vontades, desejos e anseios humanos rotineiros, permanentes e, por assim dizer, "neutros quanto ao regime" transformando-os na principal força propulsora e operativa da sociedade, uma força que coordena a reprodução sistêmica, a integração e a estratificação sociais, além da formação de indivíduos humanos, desempenhando ao mesmo tempo um papel importante nos processos de autoidentificação individual e de grupo, assim como na seleção e execução de políticas de vida individuais. O "consumismo" chega quando o consumo assume o papel-chave que na sociedade de produtores era exercido pelo trabalho. [...] o consumismo é um atributo da sociedade [...] numa força externa que coloca a "sociedade de consumidores" em movimento e a mantém em curso como uma forma específica de convívio humano, enquanto ao mesmo tempo estabelece parâmetros específicos para as estratégias individuais de vida que são eficazes e manipula as probabilidades de escolha e conduta individuais (BAUMAN, 2008a, p. 41).

Bauman assenta que o atual ambiente líquido-moderno é inóspito ao planejamento, ao investimento e ao armazenamento de longo prazo. O imediatismo e a pressa fazem parte do cotidiano do consumidor, que ressignifica o tempo para estar sempre em movimento: "é o desdém e o desprezo pelas necessidades de ontem e a ridicularização e deturpação de seus objetos" (BAUMAN, 2008a, p. 127) e a criação de novas necessidades que constituem as bases da sociedade de consumidores.

O consumidor, passa a ser visto na condição de uma construção jurídica permanentemente, sendo parte da própria natureza humana do indivíduo "como aquele direito humano primordial que fundamenta todos os direitos do cidadão, os tipos de direitos secundários cuja principal tarefa é confirmar esse direito básico, primário, como sacrossanto, e torná-lo plena e verdadeiramente inalienável" (BAUMAN, 2008a, p. 83).

Nesta toada é que, para Bauman, ser consumidor é o principal papel a ser desempenhado na sociedade atual, na qual o objetivo não se resume apenas à satisfação de necessidades, desejos e vontades, mas também à própria comodificação do consumidor, que acaba por se

tornar igualmente uma mercadoria vendável. Sua subjetividade é, de alguma forma, sua própria objetificação, é o que lhe faz se apresentar e permanecer como a melhor compra possível, um trabalho que só pode ser realizado por ele mesmo. Neste ponto:

> "Consumir", portanto, significa investir na afiliação social de si próprio, o que, numa sociedade de consumidores, traduz-se em "vendabilidade": obter qualidades para as quais já existe uma demanda de mercado, ou reciclar as que já se possui, transformando-as em mercadorias para as quais a demanda pode continuar sendo criada (BAUMAN, 2008a, p. 75).

Se um indivíduo não faz parte desta dinâmica, deve ser excluído, e se este está à margem da vida do consumo, não se enquadra sequer no ideal mínimo de exercício de sua "cidadania". É essencial manter o ambiente de manipulação e comportamentos para que seja mantida a chamada "ordem social". Conforme Bauman, a sociedade líquido-moderna de consumidores "provoca quase nenhuma dissidência, ou revolta, graças ao expediente de apresentar o novo compromisso (o de escolher) como sendo a liberdade de escolha" (BAUMAN, 2008a, p. 97).

Ser consumidor é escolher, e a escolha na sociedade de consumidores se torna pressuposto de liberdade. A liberdade só pode ser exercida com a escolha. No entanto, embora seja possível crer que se está no comando, a escolha, dentre todas as opções que são impostas, é obrigatória, o exercício da liberdade é obrigatório. "Todos nós estamos condenados à vida de opções, mas nem todos temos os meios de ser optantes" (BAUMAN, 2008b, não p.).

O autor traça, então, o seguinte paralelo: se, para Carl Schimitt, soberania diz respeito ao direito de excluir, "o verdadeiro detentor do poder soberano na sociedade de consumidores é o mercado de bens de consumo. É lá, no local de encontro de vendedores e compradores, que se realiza todos os dias a seleção e separação entre condenados e salvos, incluídos e excluídos (consumidores adequados e defeituosos)". (BAUMAN, 2008a, p. 86).

Bauman (2008a) defende a ideia de que o mercado exerce a soberania mais do que qualquer outro soberano político, porquanto exclui sem deixar a possibilidade de recorrer à decisão, que é rígida, irrevogável, informal, tácita e, raras vezes. declarada em

público. Conclui o autor que a soberania do Estado, enquanto prerrogativa de estabelecer o limite entre incluídos e excluídos, assim como o direito de reabilitar e readmitir estes últimos está sendo erodida, e arremata com a delegação de funções e prerrogativas aos mercados.

Bauman e Lyon (2012) explicam que são os próprios usuários e consumidores de serviços que produzem as "bases de dados" que posteriormente se transformam em objeto de trabalho para o monitoramento, a verificação e o processamento de dados, a fim de tornar possível a identificação de "categorias-alvo" de compradores, buscando padrões para inculcar desejos "mediante suas ações difusas, em aparências autônomas, embora sinopticamente pré-coordenadas" (BAUMAN; LYON, 2012, não p.).

Logo, a posição exclusivamente passiva do consumidor no ciclo do consumo deixa de existir em detrimento de uma participação ativa dele. A partir desta observação foi que se criou o neologismo *prosumer*. Ou seja, o consumidor não apenas consome (*consumption*), mas também produz o bem de consumo (*production*). (BIONI, 2016, p. 33). Em outras palavras, o consumidor se torna um produto comercializável, ainda que de uma transação econômica paralela, alimentando sistemas de publicidade comportamental e direcionada. Desta forma, a possibilidade de rentabilização não advém somente da venda de um bem ou serviço, mas também da coleta de dados.

Dessa relação é que se alimenta o marketing, segundo Bioni (2016) explica. A vigilância e os dados pessoais dos consumidores se transformam em fator relevante para a sua própria eficiência, aumentando o consumo de bens, visto que passa a ser possível, com base nas preferências do sujeito, direcionar o consumidor no ambiente online. O caráter de publicidade de massa estandartizado perdeu espaço para uma publicidade baseada em monitoramento de potenciais consumidores. Para o referido autor, "a publicidade direcionada é o gênero de uma prática publicitária que procura personalizar, ainda que parcialmente, tal comunicação social, correlacionando-a a um determinado fator que incrementa a possibilidade de êxito da indução ao consumo" (BIONI, 2016, p. 35).

A comunicação com o público-alvo, por sua vez, tende a ser mais eficiente, uma vez que a probabilidade de retorno (ou seja, a indução ao consumo) é maior porque direcionada. Similarmente, tais sistemas permitem visualizar o retorno real de uma prática publicitária, visto ser

possível mensurar a quantidade de cliques x compras. [10]

1.5.3 Tecnologias de Informação e Comunicação: Algoritmos, Máquinas e Organização Social

Este tópico intenciona apenas pincelar o tema acerca da evolução das tecnologias informacionais que se tornaram imprescindíveis para a compreensão do contexto de vigilância e consumo.

Partindo dessa premissa, Fernanda Bruno (2015) comenta que alguns aspectos da vigilância se atualizam na era digital, quais sejam: a) os mecanismos de rastreamento, monitoramento e arquivo de informação; b) os sistemas de classificação e conhecimento dos rastros pessoais; c) os procedimentos de individualização; e d) as formas performativas e proativas de controle sobre as ações e escolhas dos indivíduos.

De forma exponencial, Schneier (2015) relata que, em 2015, o custo de armazenamento em nuvem de um *petabyte* de dados custava 100 mil dólares por ano, 90% a menos que o um milhão cobrado em 2011. Considerando que o armazenamento de dados se torna cada vez mais barato, conclui-se ser possível salvar e registrar maior quantidade de dados e por tempo prolongado. O resultado disso é um volume de dados gigantesco sendo armazenado indeterminadamente. Paralelamente, houve o desenvolvimento de ferramentas de análise de dados com finalidades cada vez mais específicas, desde a criação de perfis até a possibilidade de predição, tal como o *big data.* Em suma, tornou-se cada vez mais rentável e lucrativo armazenar mais informações, proporcionando modelos de negócio baseados em vigilância.

Ademais, questões consideradas triviais agora têm alto valor de mercado, visto que, em grande quantidade ou combinadas com outros dados, passam a fornecer informações e conhecimentos valiosos para quem deseja obter vantagem competitiva, tornando-se importante para o nicho de marketing contemporâneo. Dados e informações são agora *commodities.*

---

10 Este é o objetivo do chamado "*Google Adwords*", que correlaciona as palavras buscadas pelo usuário à publicidade direcionada, sendo devida à contraprestação somente se houver o clique no anúncio correspondente – sendo fácil inferir que, sendo o próprio Google indiretamente beneficiário desta prática, irá produzir ferramentas para instigar tal "clique".

Segundo dissertam Castells et al. (1999), o controle do conhecimento e da informação decide quem detém o poder na sociedade, de forma praticamente independente do poder político estatal. Na perspectiva da teoria social, a tecnologia é um componente essencial da sociedade, que determina suas origens e trajetórias, ou seja, socialmente determinada.

Sobre o enunciado, Bauman e Lyon (2012, não p.) dissertam:

> Todo desenvolvimento tecnológico certamente é o produto de relações culturais, sociais e políticas. Tudo que chamamos de "tecnologia" é mais propriamente uma característica de relações "tecnossociais" ou "sociotécnicas" (BAUMAN; LYON. 2012). Nesse sentido, todos os dispositivos e sistemas exibem tendências morais; não um comportamento moral em si (em minha visão), mas uma direção moral.

Para Stefano Rodotá (2008), o uso de tais tecnologias exige que "sejam projetadas novas instituições da liberdade, capazes de evitar uma poluição totalitária da sociedade e de garantir a defesa dos direitos fundamentais em um ambiente caracterizado pelo recurso maciço às coletâneas de informações" (RODOTÁ, 2008, p. 147). Para o autor, a suposta alegação de que o "cidadão honesto" não tem nada a temer ou a esconder é uma metáfora totalitária, seja pela pretensão do Estado ou das empresas de saber acerca de todo e qualquer aspecto da vida dos vigiados.

Consoante ensina Bruno Bioni (2016), foi com a automatização dos bancos de dados que houve uma guinada de ordem qualitativa no uso das informações extraídas por este processo:

> [...] cria uma interface para que quem o manipula analisar e descobrir informações para tomada de decisões. Tais decisões vão desde a concepção de um bem de consumo ao direcionamento da mensagem publicitária. Possibilita-se, pois, identificar o perfil do potencial consumidor, seus hábitos e outras "informações necessárias à tomada de decisões táticas e estratégicas". É o que se convencionou a chamar de mineração de dados ou data mining (BIONI, 2016).

Uma das técnicas desenvolvidas se refere à “mineração de dados”, cujo objetivo é extrair informação sobre determinados indivíduos ou populações, conforme ensina o mesmo autor: “A mineração de dados é uma técnica estatística aplicada que consiste num mecanismo automatizado de processamento de grandes volumes de dados cuja função central é a extração de padrões que geram conhecimento” (BRUNO, 2015, p. 158).

Outra tecnologia bastante em voga atualmente diz respeito ao *Big Data* que, de forma didática e com base na abordagem de Doug Laney (2001), está ligado aos três "V’s", quais sejam: volume, velocidade, variedade. Volume e variedade porque excede a capacidade de processamento de uma base de dados comum, em diversos formatos (dados de um texto ou de uma foto) em alta velocidade de processamento. Seu principal escopo são a predição e a inferência da ocorrência de acontecimentos através da correlação estabelecida entre fatos, extraindo um padrão no qual sua recorrência pode permitir prever que eles se repetirão no futuro.

A esse respeito assevera Han (2013) que, por ser uma tecnologia que permite a previsão acerca do comportamento humano, faz com que o futuro se torne previsível e controlável, tornando-se instrumento psicopolítico eficiente, haja vista que permite adquirir um conhecimento propício à dominação e à intervenção na psique.

Outra tecnologia existente é o *profiling*, que são perfis gerados com a identificação de características interpessoais que projetam tendências e padrões aplicáveis a comportamentos, personalidades e competências individuais. Ou seja, características pessoais são inferidas de acordo com os dados passados relacionados à pessoa. A respeito do tema disserta a autora Fernanda Bruno (2015, p. 171):

> De um lado, o *profiling* pode engendrar procedimentos de triagem social que reforcem mecanismos discriminatórios (Gandy, 1993 e 2002) ou desigualdades sociais (Lyon, 2002 e 2003). De outro, pode-se limitar a dinâmica inventiva, aberta e potencialmente múltipla dos desejos e ações que circulam na web a uma taxonomia que privilegia os circuitos do consumo ou a lógica preventiva e securitária (BRUNO, 2015, p. 171).

Assim, essas tecnologias possuem o caráter performativo-preditivas de controle e instrumentalização das escolhas individuais,

tornando possível conhecer de antemão a propensão de cada pessoa e permitindo interferir em suas escolhas diante de opções delimitadas.

Com isso, verifica-se que a vigilância não mais se limita às fronteiras nacionais nem aos Estados: empresas com interesses econômicos fazem parte da ramificação e da expansão quantitativa e qualitativa da vigilância. A exploração comercial, por sua vez, pode ser realizada desde o uso próprio ou da venda de resultados para aplicação de serviços de marketing e publicidade, bem como para a discriminação dos consumidores: é possível selecionar os consumidores que se enquadram no padrão delineado e, dentre estes, classificar seu "valor" para a empresa, seu patrimônio, seu poder aquisitivo, seu histórico de pagamento de dívidas e até mesmo sua predisposição ao consumo de determinados produtos com base em seus gostos pretéritos.

1.6 DIFERENCIAÇÃO, MONITORAÇÃO E DIRECIONAMENTO DO CONSUMO: A SOCIEDADE DE CLASSIFICAÇÃO

Aduz David Harvey que o pós-modernismo e a sua flexibilidade são dominados "pela ficção, pela fantasia, pelo imaterial (particularmente do dinheiro), pelo capital fictício, pelas imagens, pela efemeridade, pelo acaso e pela flexibilidade em técnicas de produção, mercados de trabalho e nichos de consumo" (HARVEY, 2008, p. 304).

De outra ponta, de acordo com Han (2014), o neoliberalismo converte o cidadão em consumidor: a liberdade do cidadão cede ante a passividade do consumidor. O votante, enquanto consumidor, não está disposto nem capacitado para a ação política comum, apenas se relaciona de forma passiva com a política: queixa-se desta como se fosse os produtos que o desagradam. Em paralelo, os partidos também entram na lógica do consumo; é necessário satisfazer os votantes enquanto seus clientes.

Mesmo Canclini (1999, p. 38) já anunciava essa convergência:

> Num tempo em que as campanhas eleitorais dos comícios para a televisão, das polêmicas doutrinárias para o confronto de imagens e da persuasão ideológica para as pesquisas de marketing, é coerente nos sentirmos convocados como consumidores ainda quando se nos interpela como cidadãos.

Stefano Rodotá (2008) chama a atenção para a incapacidade dos indivíduos em perceber o sentido e a consequência que a coleta de dados pode assumir. Ainda, pontua a assimetria de poder (e saber) existente entre os cidadãos-consumidores e as organizações complexas dotadas de meios sofisticados para o tratamento de dados. Desta forma, o controle exclusivamente individual se torna ineficaz para a proteção do indivíduo, visto que o real poder deste é ilusório: "encarregado da gestão de um jogo do qual somente poderá sair como perdedor" (RODOTÁ, 2008, p. 37).

Para Bauman e Lyon (2012), as novas práticas de vigilância forçam uma transparência que ocorre numa direção única: de cima para baixo. Tudo o que é desempenhado por um indivíduo em sua vida cotidiana, seja na esfera pública ou privada, é passível de ser monitorado, checado, testado, avaliado, apreciado e até mesmo classificado, "mas, claramente, o inverso não é verdadeiro" (BAUMAN; LYON. 2012, não p.).

Marx (2016) alerta sobre a desproporção existente entre aquilo que os indivíduos sabem sobre si mesmos e o que as companhias podem saber sobre eles, que pode envolver memória infinita acerca de datas, locais, compras, meios de transporte, algoritmos etc. Basicamente, uma empresa é capaz de saber mais sobre o indivíduo do que ele próprio, que não possui a menor noção acerca da extensão deste conhecimento. [11]

É neste contexto que a expressão "*glass consumers*" ou "consumidores de vidro", criada por Susanne Lace (2005), "cai como uma luva", porquanto representa justamente a condição dos indivíduos nessa dinâmica mercadológica: vulneráveis, frágeis, transparentes e capazes de distorcer o olhar do espectador – sabe-se tanto sobre eles que seria possível ver através deles.

---

11 Bruno Bioni narra o exemplo do "sucesso" do Big Data com a seguinte história aqui sintetizada: a empresa americana Target desenvolveu algoritmo com o intuito de identificar consumidoras grávidas, dado seu potencial de compra. Com fulcro na lista de produtos comumente comprados por estas, foi possível traçar seu perfil. Transcreve-se: "A eficiência de tal ferramental foi comprovada quando um pai furioso entrou no estabelecimento comercial de tal empresa, esbravejando com o gerente por conta do envio de cupons de produtos de bebês endereçados a sua filha e acusando a empresa de incentivá-la a engravidar. Passados alguns dias, o gerente, preocupado em perder o cliente, ligou para o furioso pai, quando o mesmo informou, acanhado do outro lado da linha, que tinha tomado conhecimentos de fatos até então desconhecidos: a sua filha estava grávida, desculpando-se pelo ocorrido" (BIONI, 2016, p. 60).

Susanne Lace assevera que, desde a escrita, a humanidade vive em uma "sociedade da informação". No entanto, a centralidade dos dados enquanto combustível básico de economias é fenômeno recente. A autora faz uma comparação entre o poder de países produtores de petróleo na década de 1980 e o poder de companhias com vastos bancos de dados contendo perfis de consumidores e cidadãos que não estão mais relacionados apenas com marketing direto ou *cre rating*, mas também com decisões de estratégia, produtos e promoções, com base em análise do comportamento do consumidor e da forma de exercício do voto[1213].

De acordo com Pasquale (2015), as empresas de finanças e Internet de hoje classificam, ranqueiam e avaliam. Quando são indagadas acerca de seus algoritmos, porém, a resposta é utilizada é a de que mantêm técnicas estritamente secretas para "preservar a propriedade intelectual". Além disso, embora sustentem que seus algoritmos são

12 Recentemente houve um "escândalo" amplamente noticiado pela mídia envolvendo a empresa *Cambridge Analytica*, o *Facebook* e sufrágios, tal como a eleição presidencial americana e o chamado "Brexit". Conforme escreveu Paulo Flores em notícia jornalística: A *Cambridge Analytica* é uma empresa de publicidade que analisa dados de eleitores e consumidores para executar planos de "comunicação estratégica". Na política, utiliza técnicas de análise de personalidade para elaborar propagandas que estimulem eleitores de diferentes perfis a votarem em um mesmo candidato ou proposta política […]. O trabalho da *Cambridge Analytica* em uma eleição é utilizar informações dos usuários de Internet para impulsionar comportamentos e atitudes – o voto – a favor de determinado candidato. O trabalho da empresa é realizado em três etapas, que vão desde a concepção de como mapear os tipos de personalidade que existem na sociedade até conseguir fazer a propaganda chegar aos eleitores certos. O modelo '*ocean'* A *Cambridge Analytica* utiliza conhecimentos teóricos das ciências comportamentais (em inglês, *behavioral sciences*) para estabelecer parâmetros de personalidade que ela pretende medir. […] A empresa começou a nascer em 2013, quando pesquisadores da Universidade de Cambridge coletaram informações de 50 mil voluntários no *Facebook*. Disponível em: <https://www.nexojornal.com.br/expresso/2017/12/08/O-que-a-Cambridge-Analytica-que-ajudou-a-eleger-Trump-quer-fazer-no-Brasil>. Acesso em: 02/04/2018.

13 A autora alerta para o fato de que tais sistemas exibem erros e distorções: o Relatório *US Public Interest Research Group* (PIRG) apontou que, em junho de 2004, a cada quatro registros de pessoas em banco de dados de *bureaus* de crédito, pelo menos um deles continha sérios erros que por si só seriam suficientes para denegar empréstimos, financiamentos e até mesmo influenciar na hora de conseguir um emprego.

ferramentas neutras e científicas, isso é muito difícil de verificar, justamente por conta de sua opacidade.

Se a interrupção do fluxo de dados é impossível, então é imprescindível construir conhecimento acerca dessas entidades e empresas, a fim de compreender como elas utilizam os dados. Schneier (2015) defende a relevante abertura e transparência de empresas e governos no mesmo *standard* que estes impõem aos indivíduos, por meio de técnicas de *accountability* e de leis que definam os usos considerados razoáveis para cada tipo de informação. Para ele, o que é chamado de "competição" para usuários e "consentimento" para coleta de dados aparenta cada vez mais ser um monopólio e uma coerção, respectivamente.

O indivíduo está nu: o neoliberalismo e a vigilância massificada atuam de maneira tão sutil e sagaz que levantam a bandeira de um consentimento viciado do indivíduo, que precisa aceitar termos de uso extensos, confusos e prolixos para poder participar da vida econômica e social, para sua legitimação e para se cobrir com um véu de legalidade. Ocorre que o indivíduo se encontra totalmente despido sem que realmente o saiba, sem qualquer vexame, sem qualquer sentimento:

> [...] o desnível de poder entre os cidadãos e os que recolhem informações pode ser muito forte, fazendo pressões e condicionamentos que tornam vãs as possibilidades efetivas de controle por parte dos cidadãos, cujo consentimento reduz a um mero requisito formal. Além disso, o controle ligado ao consentimento e ao acesso não tem caráter geral e sistemático, dizendo respeito apenas a particulares situações de interesse que estimulam um cidadão a intervir. Pode então acontecer que áreas inteiras, mesmo onde as coletas de dados podem ser socialmente mais perigosas, permaneçam sem um controle efetivo (RODOTÁ, 2008, p. 149).

Com fulcro no que declara Rodotá (2008), por meio do fluxo informacional é que se delineiam as relações de poder que se manifestam concretamente. Os "pequenos irmãos" não são tão pequenos assim, e com poder de multiplicação e estruturas complexas atingem o porte de grandes irmãos em multiplicidade:

> [...] a propagação de coletas de informações pessoais cada vez mais amplas e especializadas, por iniciativa dos mais variados tipos de sujeitos, põe em discussão a própria identidade da pessoa, que se encontra fragmentada e localizada em diversos lugares, às vezes indeterminados, ou mesmo inatingíveis. A unidade da pessoa está fragmentada. Em seu lugar, encontramos tantas "pessoas eletrônicas", tantas pessoas criadas pelo mercado, quantos são os interesses que induzem à coleta das informações (RODOTÁ, 2008, p. 156).

A questão acerca da criação da identidade e da sua individualização é tratada por Dardot e Laval (2016, p. 326) como um produto consumível, combinado com o aparato econômico e em constante remodelação:

> As identificações com cargos, funções, competências próprias da empresa, assim como a identificação com grupos de consumo, sinais e marcas da moda e da publicidade, funcionam como submissões substitutivas em relação aos lugares ocupados na família ou ao status na cidade.

Já para Canclini (1999), a construção da identidade acontece no consumo. Hoje se leva em conta aquilo que cada um possui ou aquilo que pode vir a possuir, e não necessariamente aquilo que o indivíduo é ou pretender ser.

Neste mesmo entendimento, Ulrich Beck (2011, p. 195) sustenta que a individualização:

> [...] significa dependência do mercado em todas as dimensões da conduta na vida [...] as individualizações conduzem as pessoas a uma padronização e um direcionamento controlados de fora, para os quais os nichos das subculturas estamentais e familiares sempre foram estranhos.

Para o autor alemão, a esfera privada não é uma esfera que se contrapõe ao mundo, mas sim a internalização do exterior, que se crê privada. Nesta sociedade de indivíduos, o indivíduo está sozinho, reconhecendo como "foco da ação, como agência de planejamento no que diz respeito à sua própria carreira, às suas capacidades, orientações,

parcerias, etc." (BECK, 2011, p. 199). Em outras palavras, é o indivíduo quem deve arcar com os riscos da vida; é ele o único responsável por seu sucesso ou fracasso, devendo manter o autocontrole e aplicar a si mesmo as punições, em conformidade com a lógica pós-moderna e com o êxito da sociedade de controle.

Han (2013) expõe que a técnica do poder do regime neoliberal adota uma forma sutil: não se apodera do indivíduo diretamente. Ao contrário, cuida para que este atue de tal maneira que reproduza para si a estrutura de dominação que interpreta como liberdade. A otimização em si bem como a submissão, a liberdade e a exploração aqui coincidem por completo. A técnica de poder do regime neoliberal não é proibitória, protetora ou repressiva, mas sim prospectiva. O consumo não se reprime, mas se maximiza; não gera escassez, mas abundância. Nesta senda, as emoções são tidas como recursos para aumentar a produtividade e o desempenho, e são modeladas com a intenção de maximizar o consumo. As coisas não podem ser consumidas infinitamente, já as emoções sim. Desta forma, abre-se um campo de consumo com caráter infinito.

Na relação entre consumo e sociedade de massa, que identifica a cultura e o lazer, e a exploração das emoções, o consumo dos produtos como o autoconsumo da vida individual, Edgar Morin (1997, 175) sustenta que:

> [...] o indivíduo, desde o momento em que pode ser aliviado da preocupação de sua proteção, de sua velhice e do futuro de seus filhos, desde o momento em que se acha automatizado em seu trabalho e fraco diante dos grandes poderes, desde o momento em que se abrem as possibilidades de consumo e de lazer, procurará consumir mais sua própria vida. O indivíduo privado que quer consumir sua própria vida tende a valorizar o presente. Fica, além disso, cada vez mais privado de passado; este não lhe fornece mais sabedoria e norma de vida; os antigos valores, as grandes transcendências são esmagadas por um devir acelerado. Esse homem cada vez mais privado de passado está cada vez mais privado de futuro. Aliviado das preocupações acumulativas, não ousa encarar um futuro incrível. […] E assim, enquanto o Estado estabelece as relações com o passado e o futuro, o indivíduo agarra-se à grande

> justificação da vida presente: desfrutar e realizar-se (MORIN, 1997, p. 175).

Han (2015) explica que, sendo o indivíduo empresa de si mesmo, a sociedade estaria caracterizada pelo desempenho, com a crença no poder ilimitado e na positividade. Em detrimento da proibição, do mandamento ou da lei, entram em cena o projeto, a iniciativa e a motivação. “A positividade do poder é mais eficiente que a negatividade do dever, assim, o sujeito do desempenho é mais rápido e mais produtivo que o sujeito da obediência” (HAN, 2015, p. 25).

Dardot e Laval identificam no ideal social “uma sociedade de pequenos empreendedores dos quais nenhum tem condições de exercer um poder exclusivo e arbitrário sobre o mercado e a democracia de consumidores que exercem diariamente seu poder individual de escolha” (DARDOT; LAVAL, 2016, p. 116). Prosseguem os autores dizendo que:

> O mercado é concebido, portanto, como um processo de autoformação do sujeito econômico, um processo subjetivo autoeducador e autodisciplinador, pelo qual o indivíduo aprende a se conduzir. O processo de mercado constrói seu próprio sujeito. Ele é autoconstrutivo. [...] a escolha é mais dinâmica, implica criatividade e indeterminação. É o elemento propriamente humano da conduta econômica. Como diz Kirzner, uma máquina pode calcular, mas não pode escolher. A economia é a teoria da escolha. E, em primeiro lugar, a dos consumidores, novos soberanos ativos que procuram o melhor negócio, o melhor produto que corresponderá a sua própria construção de fins e meios, isto é, seu plano. A contribuição do subjetivismo para a qual apelam Von Mises e Kirzner é ter “transformado a teoria dos preços de mercado em uma teoria geral da escolha humana” (DARDOT; LAVAL, 2016, p. 140 - 141).

O mercado precisa da liberdade individual configurada como escolha para obter oportunidade de lucro. A liberdade por si só não possui valor. Se a normatividade das Sociedades Disciplinares tinha por intuito a padronização dos indivíduos, a Sociedade do Controle, em sua face neoliberal, visa ao controle social, à manutenção dos indivíduos

enquanto empresa e consumidores, mantendo a vigilância precisa do espaço público e privado, os sistemas conjuntos de informação, de publicidade e formas de autocontrole dos próprios sujeitos (DARDOT; LAVAL, 2016).

Corroborando esta visão, o sociólogo Lyon (2013) assevera que a construção de identidade e a integração social são articuladas com o mercado e não mais com o trabalho. Identifica o paradoxo: o mundo da liberdade dos consumidores também é o mundo do controle social.

Conforme Marx (2016), modelos estatísticos baseados em probabilidades podem determinar quem está mais propenso a realizar determinada compra ou, em uma situação de interesse, agir de determinada maneira - seja empregado, cidadão, paciente ou consumidor. Deste modo, a liberdade é restringida por opções predeterminadas pelo próprio mercado considerando o perfil do consumidor: as ofertas são direcionadas de acordo com o que determinado indivíduo está propenso a comprar e com base em seu poder aquisitivo[14]. Outra questão importante é a própria formação da vontade e do desejo, uma função do marketing, que se torna cada vez mais específico e assertivo. Ser social e integrado é provar sua capacidade de consumir.

Os ensinamentos de Dardot e Laval (2016, p. 216) acerca do sistema neoliberal concluem o já esposado até o momento acerca da Sociedade de Controle, cujo poder deixa de ser exercido por coerção pura, devendo inculcar o desejo individual e, então, influenciá-lo:

> O que pressupõe que ele penetre no cálculo individual - e até participe dele - para agir sobre as antecipações imaginárias dos indivíduos: para

14 Quanto a esta questão, a prática do chamado "*Persolnalized pricing*" vem se tornando cada vez mais comum e mais precisa e tem o intuito de diferenciar o preço das ofertas para consumidores com poder aquisitivo díspares, visando à maximização do lucro, explorando a margem de disposição ao pagamento do consumidor. Conforme Andrew Odlyzko (2003), "*The logic of price discrimination suggests a future drastically different from the anonymous shopping agents of [4]. Instead, it leads to an Orwellian economy in which a package of aspirin at a drugstore might cost the purchaser $1 if he could prove he was indigent, but $1,000 if he was Bill Gates or simply wanted to preserve his privacy. Such a future would justify the efforts that enterprises are putting into destroying privacy*. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=429762. Acesso em: 02 de abril de 2018.

> reforçar o desejo (pela recompensa), para enfraquecê-lo (pela punição), para desviá-lo (pela substituição de objeto). Essa lógica que consiste em dirigir indiretamente a conduta é o horizonte das estratégias neoliberais de promoção da "liberdade de escolher". Nem sempre distinguimos a dimensão normativa necessariamente lhes pertence: a "liberdade de escolher" identifica-se com a obrigação de obedecer a uma conduta maximizadora dentro de um quadro legal, institucional, regulamentar, arquitetural, que deve ser construído para que o indivíduo escolha "com toda a liberdade" o que deve obrigatoriamente escolher para seu próprio interesse. O segredo da arte do poder, dizia Bentham, é agir de modo que o indivíduo busque seu interesse como se fosse seu dever, e vice-versa. [...] A estratégia neoliberal consistirá, então, em criar o maior número possível de situações de mercado, isto é, organizar por diversos meios a "obrigação de escolher" para que os indivíduos aceitem a situação de mercado tal como lhes é imposta como "realidade" isto é, como única regra do jogo [...].

Os autores, então, reconhecem que os dispositivos sancionadores são substituídos por sistemas de estímulos e desestímulos, por recompensas e punições, de forma a guiar as escolhas do indivíduo, que já se comporta como consumidor não apenas no âmbito do mercado, mas em todas as esferas da sua vida. Por conta disso:

> Serão construídos sistemas de controle e avaliação de conduta cuja pontuação condicionará a obtenção das recompensas e a evitação das punições. A expansão da tecnologia avaliativa como modo disciplinar repousa sobre o fato de que quanto mais livre pra escolher é supostamente o indivíduo calculador, mais ele deve ser vigiado e avaliado para obstar seu oportunismo intrínseco e forçá-lo a conjuntar seu interesse ao da organização que o emprega (DARDOT; LAVAL, 2016, p. 217).

Em suma, o indivíduo somente goza sua condição de cidadão caso exerça a função considerada primordial: a de ser consumidor. Ele acredita controlar sua própria criação de necessidades e desejos, enquanto na realidade vive inserido em um ambiente permeado por mecanismos de marketing e publicidade tão sutis que sequer percebe que é um alvo. Esses mecanismos são otimizados pelo uso de tecnologias de tratamento de dados, cuja base é abastecida a partir de dispositivos de vigilância de organizações. Trata-se de um ciclo de retroalimentação entre vigilância e consumo que se torna cada vez mais inchado, tanto pelo desenvolvimento de tecnologias de informação e comunicação, quanto pelos modelos de negócio e pela cultura de consumo, que se torna natural e banal.

A análise e vigilância de consumidores é um recurso antigo e sempre esteve relacionado ao marketing: armazenamento de registros sobre clientes e suas compras; direcionamento de correspondência via mala direta; e uso de informações sobre compras e pagamentos coletadas por agências de crédito. Ocorre que, com o avanço da tecnologia e seu barateamento, tornou-se possível conhecer com precisão quem compra o que, quando, onde, quantos e com qual frequência. Desta maneira, é possível construir perfis cada vez mais precisos e detalhados, com o desígnio de direcionar marketing direto, despertando desejos, controlando os impulsos e estimulando o consumo.

Outrossim, houve o avanço e a ampliação dos *bureaus* de crédito, que agora não detêm apenas informações sobre quem deixou de pagar determinado débito, como também criam rankings sobre o bom comprador. Aduz Schneier (2015) que quando os detalhes sobre o cliente potencial são conhecidos (se de fato ele é um bom consumidor, por exemplo), é possível saber quais argumentos são persuasivos para esse cliente e que tipo de imagens ele considera mais atraente, tornando a publicidade ainda mais eficaz.

Schneier (2015, não p.) faz uma crítica que vale ser transcrita:

> Somos produtos que essas empresas vendem aos seus clientes reais. A relação é mais feudal do que comercial. As empresas são análogas aos senhores feudais, e nós somos seus vassalos, camponeses e - em um mau dia, servos. Somos agricultores inquilinos para essas empresas, trabalhando em

> suas terras, produzindo dados que, por sua vez, se vendem com lucro. [tradução nossa][15]

Neste cenário, além das questões envolvendo privacidade, outras práticas desafiam a sociologia, a justiça social e o próprio direito devido à possibilidade de categorização social, que permite aplicar parâmetros escolhidos e delineados pelas próprias empresas; devido à quantidade e à densidade de dados coletados, construindo um cenário social de "desvantagens cumulativas".

Atualmente, com base nos perfis pessoais construídos, é possível oferecer determinados serviços a uma pessoa bem como realizar variação de preços: os consumidores estão constantemente submetidos à triagem, seja quando telefonam para uma companhia de telefonia, quando vai ao banco ou mesmo quando pesquisa uma passagem na Internet.

De acordo com Lyon (2013), a vigilância do consumidor exibe traços panópticos, tais como a observação não verificável e a classificação comportamental. O atual mecanismo de integração social e os critérios de participação social se relacionam com as "escolhas livres" feitas no mercado. A disciplina, que antes era carceral e coercitiva se manifesta pela sedução da oferta. Para o autor, este é o meio indireto de controle social. Em uma esfera dominada pelo discurso da "livre escolha", a discussão de "capacidades de vigilância", com suas conotações negativas, parece "inadequada", visto que atrapalha este sistema simbiótico de vigilância e consumo.

Lyon (2013) enuncia que este tipo de monitoramento bem como a intervenção sistemática nos gostos, modas e símbolos de pessoal por meio dos tipos de processos indicados exigem uma recalibração geral das teorias sociais de vigilância. O consumo, na pós-modernidade, teria duas faces: a falsa promessa da felicidade universal na liberdade de escolha e a problemática da liberdade pessoal que se resolveria uma vez que a liberdade do consumidor é oferecida.

Diante desse cenário, Stefano Rodotá (2008, p. 157) trata da possibilidade de discriminação social por conta da exclusão de consumidores que não se enquadrem em seus próprios interesses

---

15 No original: *We're products those companies sell to their real customers. The relationship is more feudal than commercial. The companies are analogous to feudal lords, and we are their vassals, peasants, and—on a bad day—serfs. We are tenant farmers for these companies, working on their land by producing data that they in turn sell for profit.* (SCHNEIER, 2015, não p.)

comerciais, ou seja, no perfil desejado. Fator que está em evidente expansão progressiva em uma sociedade do controle, da vigilância e da classificação.

> A sociedade da vigilância não desaparece; ao contrário, aproveita as novas oportunidades para se fortalecer. Ao mesmo tempo, emerge, e consolida-se, a sociedade da classificação, na qual está ínsita a possibilidade de produção de perfis individuais, familiares, de grupo. Desta forma, a pessoa, a cada momento, pode se tornar o usuário privilegiado de um serviço, o destinatário de uma particular atenção política, o alvo de uma campanha publicitária, ou o excluído da possibilidade de aproveitar determinadas oportunidades sociais.

Neste sistema de catalogação, de forma cada vez mais frequente, decisões são tomadas com a ajuda de bancos de dados, de acordo com a posição do perfil automatizado de um indivíduo inserido em grupos ou categorias. No entanto, ao se impingir a responsabilidade às empresas, estas argumentam que "a mera classificação de um indivíduo dentro de um desses grupos ou categorias não pode ser considerada tecnicamente uma decisão" (RODOTÁ, 2008, p. 116), ainda que seja um fator relevante ou decisivo para a tomada de decisão, dificultando cada vez mais a transparência organizacional.

Dessa forma, conforme Deleuze: "os confinamentos são moldes, distintas moldagens, mas os controles são uma modulação, como uma moldagem auto-deformante que mudasse continuamente" (1992, p. 221)

O referido jurista italiano, de forma otimista, defende a implementação de instrumentos adequados para a tutela dos direitos, e a desconsideração desta dinâmica de dados como apenas espaço comercial, vista a necessidade de se reconhecer um espaço que vai além da troca de bens e serviços: "É preciso impedir o 'novo doce totalitarismo do consumismo', evitar a redução do cidadão a consumidor, ainda que seja um consumidor bem provido de instrumentos de tutela. É necessário impedir que a esfera pública e a privada sejam absorvidas na esfera da produção e da troca" (RODOTÁ, 2008, p. 158).

Por sua vez, Bauman e Lyon observam que "embora o consumo exija a prazerosa sedução dos consumidores, essa sedução é também resultado de vigilância sistemática numa enorme escala" (2012, não p).

A parte mais cara da estratégia de marketing, qual seja, a função de despertar desejos, foi transferida para os ombros dos próprios consumidores: seus próprios gostos e interesses servem de filtro à propaganda ou de resultados para motores de pesquisa que lhe serão exibidos. Por consequência, o desejo do consumidor é ampliado e fomentado de acordo com algo que ele já tinha predisposição para comprar:

> Em vez de perguntarmos por que a pessoa atrás do balcão nos pede número de telefone, identidade e código postal, ou questionarmos a exigência, pela máquina, de novos dados para que a transação se complete, presumimos que deve haver alguma razão que nos beneficiará. Por exemplo, quando se trata do uso, agora generalizado, de "cartões de fidelidade" de cadeias de lojas, linhas aéreas, um recente estudo internacional mostra que as pessoas "não conhecem ou não se importam" com as conexões entre esses cartões e a elaboração de perfis. [...] No marketing de banco de dados, a ideia é induzir os alvos potenciais a pensar que eles contam, quando tudo que se quer é contá-los e, claro, atraí-los para novas compras. Aqui, a individuação está claramente co-modificada; se há um poder pan-óptico, ele está a serviço dos marqueteiros (BAUMAN; LYON, 2012, não p).

Consoante Schneier (2015), as empresas também correlacionam o comportamento *on-line* com ações *off-line*. Os registros de cartões de crédito e os cartões de fidelidade dos supermercados revelam a comida e a bebida que cada consumidor compra, os restaurantes onde come, se está ou não matriculado numa academia e quais os itens que compra em uma farmácia, questão que será objeto de estudo no último capítulo deste trabalho.

Vê-se assim que atualmente a vigilância e o consumo são indissociáveis: atuam de maneira conjunta para criação e renovação de desejos, a fim de que a roda nunca pare de girar. Para o consumidor, a liberdade se resume ao ato de escolha, que sequer tem ciência de que o que lhe fora inculcado e as opções ofertadas são manipuladas de acordo com seu comportamento e consumo anterior.

Quem não está de acordo com o padrão de consumo, está excluído da dinâmica de mercado e, consequentemente, da oportunidade

de aceder a bens e a serviços considerados básicos na vida contemporânea. As atuais arquiteturas, dinâmicas e tecnologias de vigilância oferecem tratamento desigual, garantindo a segurança e a mobilidade de uns em detrimento do controle e da punição de outros, reforçando a reprodução de desigualdades, preconceitos e discriminações já conhecidas.

2. PRIVACIDADE, AUTODETERMINAÇÃO INFORMACIONAL E PROTEÇÃO DE DADOS PESSOAIS: PANORAMA NORMATIVO DA UNIÃO EUROPEIA E DO BRASIL

O estudo do direito à privacidade, à autodeterminação informativa e à proteção de dados pessoais não pode ser dissociado das mudanças urbano-geográficas, político-econômicas, bem como da propagação dos meios de comunicação e do desenvolvimento tecnológico.

A informação que estava até então dispersa se tornou organizada, centralizada e armazenada. Devido ao grande número de companhias e governos que passaram a ter acesso a conhecimento extremamente detalhado e preciso sobre a vida de cidadãos e consumidores, sem a contrapartida da via inversa, novas relações de poder foram instauradas ou reformuladas, aumentando de forma abissal a assimetria de poder em detrimento do exercício do direito à liberdade e à igualdade.

Inicialmente, o direito à privacidade foi considerado o *locus* da proteção do sujeito frente às intromissões de outrem em sua vida privada, em dicotomia à sua esfera pública. Percebeu-se, contudo, que não era mais somente a ingerência e o monitoramento físico e de comunicações que eram capazes de ensejar a violação da personalidade do sujeito, mas o uso indiscriminado da informação que lhe dizia respeito. A demanda por transparência e por ferramentas para que indivíduos e grupos pudessem exercer seus direitos e compreender os processos de decisão e de controle de poder aos quais estavam submetidos fez com que a teoria da privacidade sofresse modificações sensíveis, requerendo ênfase e atenção a uma tutela específica. Delineou-se, o direito à autodeterminação informacional e sucessivamente o direito à proteção de dados pessoais, que apresentava maiores especificidades em relação àquele.

Atualmente, não há consenso doutrinário sobre a natureza jurídica da proteção de dados, existindo as seguintes correntes, consoante Linkesey (2015) que serão vistas neste capítulo: (i) a proteção de dados e à privacidade como direitos separados, mas complementares, fundados na proteção à dignidade da pessoa humana; (ii) a proteção aos dados pessoais como uma faceta própria da privacidade; e (iii) a proteção aos dados pessoais como um direito fundamental independente e autônomo.

Nesse cenário, o presente capítulo tem como intuito traçar o panorama normativo do direito à privacidade, perpassando pela autodeterminação informativa e culminando na proteção de dados

pessoais, com auxílio da classificação geracional das leis de proteção de dados proposta por Mayer-Schonberger (1997), bem como analisar a *General Data Protection Regulation*, da União Europeia e a Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, com as alterações promovidas pela Medida Provisória nº 869/2018.

2.1 MERCADO E CONSUMO NO MUNDO DIGITAL: DADOS, INFORMAÇÃO E CONHECIMENTO

"Os dados pessoais são o novo petróleo da internet e a nova moeda do mundo digital". Essa frase, exarada pela Comissária Europeia para a Defesa dos Consumidores, Meglena Kuneva, apesar de ter se tornado um clichê entre os que estudam o tema, demonstra a guinada da economia industrial para a economia informacional. Seguindo este mesmo entendimento, Frank Pasquale (2015) assevera que os dados são o combustível da economia da informação, pois quanto maior for o volume de dados em posse de uma empresa - seja sobre sua própria produção, estoque, fornecedores e consumidores - mais ela poderá obter conhecimento sobre suas práticas organizacionais e sobre o mercado em que se insere, podendo tanto monetizá-lo quanto reduzir seus custos, auxiliando no processo de tomadas de decisões.

Em síntese, o capitalismo informacional assume uma centralidade em detrimento do capitalismo industrial, sendo que os dados e as informações passam a ser o novo motor das transações econômicas. Neste compasso, Shoshana Zuboff (2015) apresenta sua construção teórica acerca do "*surveillance capitalism*" ou "capitalismo da vigilância", cuja nova lógica de acumulação produz conjuntos em hiperescala de dados objetivos e subjetivos, com o propósito de conhecer indivíduos e suas formas de vida e, consequentemente, controlar e modificar seus comportamentos a fim de produzir novas variedades de mercantilização, monetização e até mesmo de controle social.

Conforme a autora, não apenas as relações políticas, econômicas e sociais são remodeladas; as relações jurídicas, por seu turno, também são objeto de ressignificação: erigiram-se questões relacionadas ao consentimento, à extraterritorialidade, à jurisdição internacional e a contratos, por exemplo. O direito à privacidade, por sua vez, também sofreu transformações, tendo em vista sua redistribuição e, ato contínuo, concentração, uma vez que são as pessoas jurídicas, e não mais as pessoas naturais, que efetivamente exercitam esse direito.

Desta forma, cada vez mais as empresas se tornam opacas e se protegem sob o manto do segredo industrial e da propriedade intelectual. Traçando uma metáfora, pode-se dizer que, tal qual um espelho falso no qual é possível enxergar o outro em apenas uma via, os indivíduos agora se encontram "nus", enquanto as empresas, como o Google e o *Facebook*[16], por exemplo, que exploram os dados e a sociedade como força motriz do seu modelo de negócio, protegem-se e mantêm-se intransponíveis.

Sobre essa nova estrutura de poder, Shoshana Zuboff (2015) sustenta que, de maneira semelhante à lógica do capitalismo industrial, que moldou o caráter da civilização, a nova lógica do capitalismo informacional igualmente irá modificá-la[17]. Assim, torna-se imprescindível compreender a dinâmica global dos fluxos de dados, a atuação dos atores privados e governamentais envolvidos, as negociações e as tomadas de decisões, bem como os riscos latentes, a imputação de responsabilização em caso de falhas etc., haja vista que os indivíduos estão perdendo este "cabo de guerra" informacional.

De acordo com Sergio Amadeu da Silveira (2017), com a possibilidade de desenvolver conhecimento sobre o mercado e o consumidor, é possível criar e oferecer produtos que tenham a capacidade de se adequar especificamente aos seus interesses, uma vez que eles deixam sua condição de cidadão para se aperfeiçoarem em sua experiência como um ser comprador.

Mas, afinal, o que se entende por dado, informação e conhecimento - termos estes utilizados de maneira cada vez mais frequente, tanto na seara científica quanto coloquial? Este subtópico não

---

16 5 *years after rocky IPO, Facebook is stronger than ever* https://money.cnn.com/2017/05/18/technology/facebook-ipo-anniversary/index.html

17 Existem exemplos recentes de utilização de base de dados e informações para influenciar potenciais eleitores por meio de redes sociais e de mensagem, tanto no Brasil quanto nos Estados Unidos: Como funciona a máquina que pode eleger Bolsonaro: https://epoca.globo.com/como-funciona-maquina-de-whatsapp-que-pode-eleger-bolsonaro-23180627 ; *Whatsapp* é vetor de *fake news* no Brasil; nos EUA, papel é do Facebook; https://www1.folha.uol.com.br/poder/2018/10/whatsapp-e-vetor-de-fake-news-no-brasil-nos-eua-papel-e-do-facebook.shtml ; Seu número de telefone vale 9 centavos no zap dos políticos: https://theintercept.com/2018/10/22/whatsapp-politicos/ ; Como o *Facebook* pode ter ajudado Trump a ganhar a eleição https://www.bbc.com/portuguese/geral-37961917 Acesso em 14 de outubro de 2019.

se pretende exaustivo, mas tão somente ilustrativo, a fim de oferecer subsídios para posterior análise da extensão de conceitos presentes nos diplomas legais que abordam o tema.

Robert Logan (2012) observa que, apesar de a palavra "informação" desempenhar papel central na vida econômica, social e cultural, ela não possui um conceito único, tendo em vista que assume noções diferentes dependendo do contexto e da área de estudo e aplicação em que se encontra. O autor ensina que o marco inicial da teoria da informação foi proposto por Claude Shannon, em 1948, para quem informação é "uma mensagem enviada por um emissor para um receptor" (1948 *apud* 2012), que pode ser codificada pela sequência de 0s e 1s ou códigos alfanuméricos, ou seja, por um valor numérico ou matemático, cujo padrão ou sinal não está ligado ao seu significado: "Esses aspectos semânticos da comunicação são irrelevantes para o problema de engenharia. O aspecto significativo é que a mensagem real é selecionada de um conjunto de mensagens possíveis (1948 *apud* 2012)". Assim, ao se despir de qualquer carga semântica, essa teoria se tornou o "padrão pela qual quase todas as formas de informação foram aferidas" (2012, p. 35).

Logan ainda explana acerca do desenvolvimento teórico de David MacKay, que tomou como ponto de partida a subjetividade, defendendo que esta pode estar envolvida na troca de informação e sugerindo sua definição como "a mudança mental em um receptor, portanto, com significado" (1969 apud 2012) e não apenas o sinal do remetente. Enquanto Claude Shannon definiu informação em termos do que ela é, David MacKay a define em termos do que ela faz, ou seja, a partir de seu significado como produto do processo de interpretação da informação dentro de um determinado contexto no qual está inserida.

Robert Logan (2012), por seu turno, desenvolve as suas definições de dados, informação, conhecimento e sabedoria. Para ele, dados são representações de algum fato de maneira bruta, são puros e simples, sem qualquer estrutura ou organização, sendo o átomo da informação. A informação, para o autor, é constituída pela estruturação e pela lapidação dos dados: dentro de um contexto adiciona-lhe significados e significâncias. Por fim, Logon entende que o conhecimento se traduz na possibilidade e na capacidade de se utilizar de tais informações para atingir objetivos pré-determinados.

Por seu turno, de acordo com Mayer-Schonberger (2017), os dados atualmente se referem à descrição de algo que permite que seja registrado, analisado e reorganizado. Ressalta ainda que, para documentar um fenômeno no mundo digital, é necessário colocá-lo em

um formato quantificável, a fim de que possa ser tabulado e analisado: trata-se do processo de conversão de informações analógicas em códigos para que os computadores possam manipulá-las.

Embora existam inúmeras construções teóricas divergentes sobre o tema, há o consenso de que com a transformação de átomos em bits, ou seja, da passagem do analógico para o digital, incrementou-se a capacidade de coleta, armazenamento, tratamento e transferência de dados e informações. Em outras palavras, tanto a esfera qualitativa[18] (utilização de novos métodos, técnicas e algoritmos) quanto a quantitativa dos dados[19] (capacidade de armazenamento e tratamento de dados de maneira maior e muito mais barata) sofreram uma expansão devido ao desenvolvimento tecnológico.

De forma semelhante, a definição de dado pessoal também não é pacífica. Conforme assevera Sergio Amadeu da Silveira (2017), existe uma disputa travada pelas forças do mercado de dados a fim de

---

18 *There is no rigorous definition of big data. Initially the idea was that the volume of information had grown so large that the quantity being examined no longer fit into the memory that computers use for processing, so engineers needed to revamp the tools they used for analyzing it all. That is the origin of new processing technologies like Google's MapReduce and its open- source equivalent, Hadoop, which came out of Yahoo. These let one manage far larger quantities of data than before, and the data — importantly — need not be placed in tidy rows or classic database tables. Other data-crunching technologies that dispense with the rigid hierarchies and homogeneity of yore are also on the horizon. At the same time, because Internet companies could collect vast troves of data and had a burning financial incentive to make sense of them, they became the leading users of the latest processing technologies, superseding offline companies that had, in some cases, decades more experience*. SCHONBERGER-MAYER, Viktor. CUKIER, Kenneth. ***Big Data:*** *The Essential Guide to Work, Life and Learning in the Age of Insight. John Murray Publishers***:** Londres, 2017.

19 *Internet companies have been particularly swamped. Google processes more than 24 petabytes of data per day, a volume that is thousands of times the quantity of all printed material in the U.S. Library of Congress. Facebook, a company that didn't exist a decade ago, gets more than 10 million new photos uploaded every hour. Facebook members click a "like" button or leave a comment nearly three billion times per day, creating a digital trail that the company can mine to learn about users' preferences. Meanwhile, the 800 million monthly users of Google's YouTube service upload over an hour of video every second. The number of messages on Twitter grows at around 200 percent a year and by 2012 had exceeded 400 million tweets a day. (*SCHONBERGER-MAYER; CUKIER, 2017).

determinar a extensão de seu conceito, afinal, implica diretamente no fluxo de dados o que uma lei engloba ou não:

> Representantes de agências de análise de crédito, por exemplo, defendem que dados cadastrais e biométricos não devem ser considerados dados pessoais, não devem requerer autorização para o seu tratamento, uma vez que são de interesse dos agentes econômicos, da polícia e, por conseguinte, seriam de interesse de toda a sociedade. Para alguns segmentos da economia informacional, quase nada deveria ser considerado um dado pessoal. Como mencionado anteriormente, o discurso da morte ou da inadequação da privacidade tem relação direta com a polêmica sobre a definição de dados pessoais.

De acordo com Bruno Bioni (2014), considerar que dado pessoal é a vinculação direta entre dado e uma determinada pessoa é uma lógica restritiva e reducionista, uma vez que essa definição não leva em consideração a capacidade de cruzamento de dados: a multiplicidade de dados pode precisar a identidade do sujeito. Aliás, os pesquisadores Arvind Narayanan e Vitaly Shmatikov (2006), no estudo *How To Break Anonymity of the Netflix Prize Dataset*, demonstraram como é possível fazê-lo a partir da aplicação de metodologia estatística de "desanonimização"[20]: dados de GPS e endereços de IP podem ser cruzados com registros de outros bancos de dados e, a partir do uso de algoritmos de reidentificação, permitir a descoberta da identidade civil de uma pessoa.

Assim, o conceito expansionista dos dados pessoais merece guarida e atualmente é adotado por inúmeros diplomas legais: tanto a pessoa identificada como a identificável (com potencialidade de

20 *We apply our de-anonymization methodology to the Netflix Prize dataset, which contains anonymous movie ratings of 500,000 subscribers of Netflix, the world's largest online movie rental service. We demonstrate that an adversary who knows only a little bit about an individual subscriber can easily identify this subscriber's record in the dataset. Using the Internet Movie Database as the source of background knowledge, we successfully identified the Netflix records of known users, uncovering their apparent political preferences and other potentially sensitive information.* SHMATIKOV, Vitaly; NARAYANAN, Arvind. **How To Break Anonymity of the Netflix Prize Dataset.** Disponível em: https://arxiv.org/abs/cs/0610105

identificação) devem ser tutelada. Essa corrente amplia o escopo do que é considerado dado pessoal, com reflexão direta na proteção do indivíduo. Fernanda Bruno ainda problematiza em relação à vinculação de indivíduos que se enquadrem em perfis gerados por dados supostamente anonimizados:

> Sabe-se que uma imensa parcela do tratamento e uso de dados pessoais coletados de forma automatizada na Internet constituem bancos de dados que são anonimizados e agregados, submetidos a técnicas de "profiling" para categorizar e agir sobre o campo de escolhas, decisões e ações de indivíduos ou grupos específicos. Dados transacionais e comportamentais de usuários, por exemplo, são coletados, anonimizados e tratados de modo orientar ofertas diferenciadas de produtos, concessão ou veto de acesso a serviços, investimentos diferenciados sobre grupos ou indivíduos classificados segundo poder de compra, interesses, preferências políticas, padrões comportamentais etc. A questão é: devem ter os indivíduos o direito de escolher se desejam ou não que seus dados pessoais sejam coletados, ainda que sejam em seguida anonimizados, a depender do tipo de utilização declarado? [...] Se considerarmos que uma política de dados pessoais deva implicar também o controle dos indivíduos sobre as informações que ele gera, caberia o direito de negar a coleta automatizada dos seus dados por sites e corporações cujos propósitos não lhe pareçam interessantes ou desejáveis (BRUNO, p. 153 - 154).

Nessa mesma linha, Sérgio Amadeu da Silveira entende que: "No século XXI, os discursos contra a privacidade vêm principalmente do grande capital informacional e dos aparatos de repressão estatais" (2017), os quais produziram esse arcabouço visando à remoção de um dos entraves ao mercado de dados pessoais, o direito à privacidade. Na narrativa construída[21], a privacidade faz parte de um mundo analógico e

21 Indagar sobre um uso linguístico ou modo de significar é realizar uma análise das alterações significativas que as palavras sofrem no processo de

anacrônico, no qual não são mais apenas os produtos e serviços que obedecem ao método da obsolescência, o direito também passa a fazê-lo, sendo este o entrave para o desenvolvimento tecnológico[22]. "Quem não deve, não teme" é o slogan repetidamente perpetrado[23]:

---

comunicação. Os significados socialmente padronizados possuem sentidos incompletos; são expressões em aberto, que apenas se tornam relativamente plenas em um contexto determinado. Assim, é impossível analisar o significado de um termo sem considerar o contexto no qual se insere, ou seja, seu significado contextual. Desta forma, um termo possui dois níveis básicos de significação: o significado de base e o significado contextual. O primeiro é aquele que conhecemos no plano teórico quando abstraímos a significação contextual e consideramos o sentido congelado, a partir dos elementos de significação unificados por seus vínculos denotativos. O segundo pode ser entendido como o efeito de sentido derivados dos processos efetivos da comunicação social. WARAT, Luis Alberto. **O Direito e a Sua Linguagem**. 2a ed. Porto Alegre: Sergio Antonio Fabris Editor, 1995.

22 *A group of industry executives with members including IBM, Procter & Gamble, Ford, Compaq and AT&T established the Privacy Leadership Initiative (PLI) in June 2000. PLI promptly began an ad campaign in national publications to promote industry self-regulation of online consumer privacy. According to a contemporary news account, the PLI initiative "follows a recent Federal Trade Commission recommendation that Congress establish legislation to protect online consumer privacy". A description of the PLI from its website in 2001 stated that the "purpose of the PLI is to create a climate of trustwhich will accelerate acceptance of the Internet and the emerging Information Economy, both online and off-line, as a safe and secure [...] The Obama Administration supported privacy legislation in its 2012 White Paper, but an actual draft bill was not released by the White House until February 2015. Overcoming the institutional and legislative barriers to privacy legislation or to other forms of privacy regulation may take more public pressure combined with industry recognition that the American status quo for privacy is worse than other alternatives. Whether there is a genuine prospect that the US will seriously address privacy regulation any time soon remains to be seen.* GELLMAN, Robert; DIXON, Pam. Failures of Privacy Self-Regulation in the United States. In: WRIGHT, David; HERT, Paul de. ***Enforcing Privacy****: regulatory, legal and technological approaches.* Londres: Springer, 2016. p. 53-78.

23 *When Google CEO Eric Schmidt was asked in a 2009 CNBC interview about concerns over hiscompany's retention of user data, he infamously replied: "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place." With equal dismissiveness, Facebook founder and CEO Mark Zuckerberg said in a 2010 inter- view that "people have really gotten comfortable not only sharing more information and different kinds, but*

> Com esse regime discursivo, opera-se a tentativa de uma profunda inversão no contexto das democracias que emergiram no capitalismo industrial. A transparência para os poderes de Estado e para as grandes corporações vai sendo substituída pela ideia de que a vida das pessoas deve ser completamente translúcida para as empresas e para o mercado. Que tipo de sociedade estamos forjando com a completa transparência das pessoas para empresas que vendem e adquirem dados sobre preferências, comportamentos, mas também sobre intenções, sonhos e desejos? A privacidade, alardeada pelos consultores de tecnologia, como algo subjetivo e ultrapassado deve ceder lugar a melhores experiências que as empresas podem proporcionar (SILVEIRA, 2017, não p.).

Percebe-se a existência de uma complexa teia de múltiplos interesses que ora se contrapõem e ora atuam cooperativamente, quais sejam: atores da sociedade civil e academia que pleiteiam a máxima tutela do indivíduo; atuação das Autoridades de Supervisão, cuja independência funcional é garantia de seu funcionamento; interesse governamental e privado no controle social privado de fluxo de dados, conhecimento e controle, perpassando neste último caso também à ampliação de margem de lucro.

Nesse cenário, dois diferentes modelos ocidentais foram delineados: o Europeu, geral, que se aplica aos entes públicos e privados com principal preocupação na tutela do sujeito titular dos dados, regulamentação ostensiva a nível nacional e comunitário; e o dos Estados Unidos, com leis setoriais, baseado no movimento de

---

more openly and with more people."Privacy in the digital age is no longer a "social norm," he claimed, a notion that handily serves the interests of a tech company trading on personal information. those who are "doing something wrong," and only they have anything to fear from the invasion of their privacy. This is an old tactic. In a 1969 Time magazine article about Americans' growing concerns over the US government's surveillance powers, Nixon's attorney general, John Mitchell, assured readers that "any citizen of the United States who is not involved in some illegal activity has nothing to fear whatsoever." GREENWALD, Glenn. ***No Place to Hide****: Edward Snowden, the NSA, and the U.S. Surveillance State.* Nova Iorque: Metropolitan, 2014.

derregulation, com pouca intervenção da lei no campo privado. Predominando neste último o modelo de autorregulação, que prima pelo livre mercado e pelo fluxo indiscriminado de informações, perfilhando sua histórica tradição liberal.

Não se olvida o pioneirismo dos Estados Unidos na construção teórica e jurisprudencial sobre o direito à privacidade, sua participação no primeiro documento internacional sobre o conteúdo, as Diretrizes sobre a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais da OCDE (Organização para o Comércio e Desenvolvimento Econômico), e que ainda apresentam importante papel na dinâmica internacional, contudo, foi o modelo europeu que se tornou predominante quando relativo à proteção do indivíduo, razão pela qual se decidiu se debruçar mais detidamente.

2.2 PRIVACIDADE: HISTÓRIA, CONCEITOS E EVOLUÇÃO

Consoante o primeiro capítulo, é possível afirmar que a expansão da vigilância inevitavelmente impacta nos padrões de comportamento dos cidadãos. Destarte, este tópico tem como objetivo analisar como o Direito regula o controle e o uso de dados e informações. Para tanto, será traçado um retrospecto do direito à privacidade, perpassando pelo desenvolvimento do direito à autodeterminação informacional enquanto vertente da privacidade e que culminou na reivindicação de autonomia do direito à proteção de dados pessoais.

Até meados do Século XX, a dicotomia entre a vida pública e a vida privada foi central na noção da privacidade, por consequência, o tratamento impingido pelo direito a essas duas esferas eram diferentes. Segundo discorre Daniel Solove (2008), os primeiros direitos concernentes à privacidade se relacionavam com um direito eminentemente negativo, referente ao poder de exclusão de terceiros na esfera privada: a proibição de escutas, a inviolabilidade de domicílio e do corpo, exemplificadamente.[24]

---

24 *Another important Supreme Court privacy case of the 19th century established protection against physical bodily intrusions. In 1891, the Court held in Union Pacific Railway Co. v. Botsford, that a court could not compel a female plaintiff in a civil action to submit to a surgical examination: The inviolability of the person is as much invaded by a compulsory stripping and exposure as by a blow. To compel any one, and especially a woman, to lay bare the body, or to submit it to the touch of a stranger, without lawful authority, is an indignity, an assault, and a trespass. This case is one of the earliest*

A teoria da privacidade, baseada nessa oposição público-privado, tangencia temas sensíveis, tais como o acesso ao corpo, à sexualidade, à família, à casa e às comunicações, e suscitam debates relevantes até o presente. No entanto, por ser um modelo demasiadamente simplista, não mais deu conta de amparar os sujeitos que passaram a ter uma condição cada vez mais vulnerável. Se antigamente era possível se manter na obscuridade com o fito de preservar sua privacidade, atualmente, qualquer movimento pode ser rastreado ou captado, seja por câmeras espalhadas pela cidade (inclusive com tecnologias já desenvolvidas para reconhecimento facial[25]), pelo rastreamento de conexão da *internet wi-fi* doméstica[26], pelo uso de cartão de crédito[27], exemplificadamente.

---

recognitions of what would later come to be called "substantive due process privacy." The sanctity of the body was also recognized in the common law, even prior to the birth of the privacy torts following Samuel Warren and Louis Brandeis's article. In De May v. Roberts 54 an 1881 case, a physician allowed a "young unmarried man" not schooled in medicine to be present while the plaintiff qave birth. SOLOVE, Daniel. ***A Brief History of Information Privacy Law.*** Washington: *GW Law Faculty Publications*, 2006.

25 *China has been building what it calls "the world's biggest camera surveillance network". Across the country, 170 million CCTV cameras are already in place and an estimated 400 million new ones will be installed in the next three years. Many of the cameras are fitted with artificial intelligence, including facial recognition technology.* Disponível em: *ht*tps://www.bbc.com/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-*state* Acesso em: 20 de agosto de 2018.

26 Google *has been 'accidentally' gathering extracts of personal web activity from domestic wifi networks through the Street View cars it has used since 2007, it said last night. It was discovered as a result of a data audit demanded by Germany's data protection authority, and is likely to inflame critics of Google concerned about the web giant's use of private data. As well as systematically photographing streets and gathering 3D images of cities and towns around the world, Google's Street View cars are fitted with antennas that scan local wifi networks and use the data for its location services.* Disponível em: https://www.theguardian.com/technology/2010/may/15/google-admits-storing-private-data. Acesso em: 2 de setembro de 2018

27 *Whether you're making a phone call, sending a text, or just buying a cup of coffee with your credit card, you're creating a constant stream of electronic data. It turns out this data could be used to track you—even if it doesn't have your name on it. According to Yves-Alexandre de Montjoye, an MIT computer scientist, even totally private metadata—that is, data completely stripped of all person information like names and phone numbers—may not be as anonymous as we'd like to believe. In a new study, he and his colleagues took an anonymized credit card record of 1.1 million people. The researchers found that*

Ademais, o uso de tecnologias de informação e comunicação, bem como o consequente crescimento de burocracias estatais e do poder econômico e político de empresas privadas aumentaram os riscos aos quais os indivíduos estão submetidos. As exigências para a proteção da esfera pessoal passaram a ser cada vez mais específicas e urgentes devido à crescente assimetria de poder.

Conforme ensina Danilo Doneda (2006), na Idade Média, por conta da dinâmica social e do modo de vida eminentemente rural, não era possível verificar o anseio de isolamento ou privacidade, afinal, eram poucas pessoas - senhores feudais e nobres - quem poderiam de fato se isolar do mundo externo.

Posteriormente, contudo, as pessoas passaram a conviver com distâncias cada vez menores: devido à urbanização, por exemplo, ocorreu o início da aglomeração populacional, em evidente contraposição à vida no campo. A nova arquitetura da cidade privilegiava a separação e a segregação, seja por classes ou categorias, conforme explica o autor: “Começa então a se delinear a atual noção de privacidade, que só poderia se desenvolver com esta nova posição do homem diante da sociedade. Esse enriquecimento da esfera privada ocorre como consequência do individualismo” (2006, p. 127).

Ocorre que, consoante ensina Stefano Rodotà, este novo direito correspondia à demanda da burguesia, afinal, era esta quem poderia se dar ao luxo de se recolher a um ambiente de exclusão e de reivindicar a proteção privada. Em contraposição, a classe operária suportava o agrupamento de seus membros em cortiços ou dividia sua casa com outras famílias (questões geográficas e urbanas que persistem até hoje,

---

more than 90 percent of the time, comparing just 4 simple pieces of outside information (for example, if someone shopped at a specific store on a given day) was enough to identify someone. This means that the researchers could connect real people's identities (for example, William Herkewitz) to their anonymous avatar in the "private" data set (say, shopper#2232_8) for every single interaction that was recorded. Having even more specific information, like the exact price someone paid at restaurant, made re-identification 22 percent more likely. "The takeaway is that we really need to rethink what it means when something is 'anonymized'. With regard to this data, anonymous is not a binary term; it's not black and white. And when we run the risk of reconnecting personal information, we should take that into account when we release and share data," de Montjoye says. Disponível em: https://www.popularmechanics.com/technology/security/how-to/a4189/even-anonymous-credit-card-data-can-be-used-to-track-you/ Acesso em: 2 de setembro de 2018.

inclusive). O mencionado autor italiano assevera que a construção da privacidade não proveio de uma exigência natural individual, mas da expressão de um privilégio por parte de um grupo: "Não é por acaso que seus instrumentos jurídicos de tutela foram predominantemente modelados com base naquele característico direito burguês por excelência, a propriedade" (2008, p. 27).

Contudo, não foi o crescente acesso à moradia o principal catalisador da demanda de tutela à privacidade, mas sim o desenvolvimento tecnológico, em conjunto com o crescimento burocrático estatal e mercadológico, combinado com algumas mudanças nas dinâmicas do tecido social, conformaram o ambiente para o clamor e posterior reconhecimento do direito à privacidade.

Uma das grandes contribuições para o desenvolvimento dos estudos sobre privacidade na *common law*, e considerado seu marco inicial, conforme defende Anderson Schreiber (2014), foi um famoso artigo publicado em 1890 na *Harvard Law Review*, de coautoria de Samuel Warren e Louis Brandeis, ambos à época advogados, denominado "*The Right to Privacy*".[28] Conta Schreiber que a motivação teria sido "o destaque exagerado, embora não difamatório, que os jornais de Boston reservavam à vida social da mulher de Samuel" (2014, p. 139).

À época, as máquinas fotográficas se popularizaram por sua redução de preço e por sua redução de tamanho, ou seja, eram portáteis. A empresa que desenvolveu essa tecnologia foi a Kodak Co.: as capturas de momentos e retratos do cotidiano, que até então eram

28 *This article was more than just influential. It has become starting out of of personality: by which Coleridge meant not just the age of asserting an individual's personality, but also attacking the gates and throughout more than a century of legal change, one of the most cited law review articles in history – and very likely the most important, game-changing piece of legal scholarship ever. It invented a whole field of law. [...] It has even influenced the constitutional law applied in U.S. courts today, although the article was never about constitutional limits on privacy as such. Yet even in its more modest realm of the common law (well, modest on hindsight, as it may have been quite radical at the time), in recognizing within the law of states a civil and non-contractual right of protection against invasions of privacy, the article was nothing short of momentous.* CHILDRESS, Steven Alan. **Prefácio** In: BRANDEIS, Louis; WARREN. Samuel. ***The Right to Privacy*.** Nova Orleans: Quid Pro LLC, 2010.

realizados em raros eventos e em reuniões de família, passaram a acontecer a todo instante[2930].

Aliado a isso, novas técnicas de impressão e de distribuição de jornais diminuíram seus custos e ampliaram a sua circulação, sendo as fotografias ali introduzidas. As manchetes sensacionalistas, com a exploração da vida de outrem para satisfação de curiosidades do público já permeavam o cotidiano editorial.

Até aquele momento, somente o direito contratual obrigava à privacidade entre as partes. Warren e Brandeis reclamaram um direito a ser observado por todos, qual seja, o direito à privacidade, o qual estaria subsumido a um direito mais amplo de "inviolabilidade da personalidade", de acordo com Megan Richardson (2017), cuja construção teórica ficou conhecida até a atualidade como *the right to be let alone*, ou "direito a ser deixado só".

Conforme Schreiber (2014), este direito assumia um sentido individualista e proprietário. Identificava-se a proteção à vida íntima, familiar e pessoal, sob a influência do modelo de propriedade, em que se assume um dever geral de abstenção: "não se entra na propriedade, não se entra na vida privada. Do mesmo modo que o direito à propriedade permitia repelir o esbulho dos bens materiais, a privacidade permitia afastar a interferência alheia sobre a vida de cada um" (2014, p. 141).

Schneier (2015) pontua que o referido artigo inaugura os debates modernos sobre direito à privacidade, o qual, apesar de não estar disposto expressamente na Constituição dos Estados Unidos, pode ser deduzido com fulcro na Quarta, na Quinta e na Nona Emendas,

---

29 *Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of the private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whis- pered in the closet shall be proclaimed from the house-tops*. BRANDEIS, Louis; WARREN. Samuel. ***The Right to Privacy.*** Nova Orleans: Quid Pro LLC, 2010.

30 *The release of the first Kodak 'instantenous camera' in America and England, advertised under the slogan 'you push the button, we do the rest', meant that the power to place individuals on public records and cicrulate these to the world was not just limited to professional engravers, caricaturists, portrait photographers and waxwork artists, but could now be extended to the most unskilled ordinary members of the public, encouraged by the Eastman Photographic Company to record every detail of daily life that came within their view*. RICHARDSON, Megan. ***The Right to Privacy*****:** *Origins and Influence of a Nineteenth-Century Idea. Cambridge*: Cambridge University Press, 2017.

consonante reconhecimento e construção jurisprudencial em casos paradigmáticos como *Roe vs. Wade* e *Katz vs. United States*[31].

Explica Daniel Solove que o objeto de proteção da privacidade diante do desenvolvimento da jurisprudência e da doutrina no âmbito da *Common Law* abarca o seguinte: (i) o direito de estar só, conforme formulado por Samuel Warren e Louis Brandeis; (ii) o poder de barrar o acesso de outros a si mesmo; (iii) o segredo, a ocultação de informações e de assuntos próprios a terceiros; (iv) o controle da informação pessoal; (v) a proteção à sua personalidade, individualidade *(personhood)*; (vi) a intimidade, o controle e o acesso limitado de aspectos íntimos e de relacionamentos em aspectos da vida.[32]

---

31 *The Court declared in Roe v Wade that the "right of privacy, whether it be founded in the Fourteenth Amendment's concept of personal liberty and restrictions upon state action, as we feel it is, or, as the district court determined, in the Ninth Amendment's reservation of rights to the people, is broad enough to encompass a woman's decision whether or not to terminate her pregnancy."[...]. The Fourth Amendment protects certain elements of the private sphere of individuals against unreasonable intrusion by government, in particular against unreasonable searches and seizures, but, as confirmed in the landmark case Katz v United States (1967), "The Fourth Amendment cannot be translated into a general constitutional 'right to privacy'. […] [This] right to privacy – his right to be let alone by other people – […] [is] left largely to the law of the individual States." The US Supreme Court created in Katz v United States the notion of a constitutionally protected reasonable expectation of privacy, a notion that is used in a large number of contexts, also within the European Union* (VOIGT; BUSSCHE, 2017).

32 *In 1960, renowned tort scholar William Prosser surveyed the over 300 privacy cases that were spawned by the Warren and Brandeis article. Prosser concluded that the cases recognized four distinct torts: (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) false light or "publicity"; and (4) appropriation. (1) Intrusion upon seclusion protects against electronic eavesdropping into conversations in the home, as well as the deceitful entry and clandestine photographing of activities in the home. The tort is not limited to intrusions into the home. In a case involving well-known consumer advocate Ralph Nader, the court held that an attempt by General Motors to hire people to "shadow" him and "keep him under surveillance" could be tortious if the surveillance was "overzealous." (2) One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public. (3). One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if (a) the false light in which the other was*

Com base em Voigt e Bussche (2017), o direito constitucional à proteção de dados pessoais não é reconhecido nos Estados Unidos, sendo que os termos *data privacy* ou *informational privacy* são mais recorrentes que o uso de *data protection*, ou seja, para eles ainda há uma noção legal da inseparabilidade com o direito à privacidade, considerado este um direito geral de personalidade.

No âmbito internacional, o direito à privacidade foi reconhecido em 1948 pela Declaração Universal dos Direitos do Homem[33]. Posteriormente, outros diplomas internacionais também o fizeram, tais como: o Pacto Internacional de Direitos Civis e Políticos, em 1966; a Convenção Americana de Direitos Humanos, ou Pacto de São José da Costa Rica, em 1969; e a Convenção Europeia para a Proteção dos Direitos do Homem, em 1953.

Entretanto, consigna Megan Richardson (2017) que a ideia de um direito humano universal à privacidade deve ser reconsiderada a fim de contemplar contribuições práticas e teóricas aos problemas e às demandas individuais e sociais identificadas acerca do assunto. Nesse contexto, a Carta de Direitos Fundamentais da União Europeia, em 2000, reconheceu a existência tanto de um direito à privacidade quanto a existência de um direito à proteção de dados pessoais, conforme será estudado a seguir.

Percebe-se, assim, que a privacidade é um termo plurissignificativo. Tal como um poliedro, contêm várias faces que apresentam diferentes nuances e características, as quais se enquadram dentro do termo, por exemplo: o sigilo das comunicações; o controle sobre o próprio corpo; a não intromissão no lar; o controle sobre a informação pessoal; o direito à ausência de vigilância; a proteção contra buscas e interrogatórios.

Bruce Schneier (2015) aponta que as definições de privacidade são culturais e situacionais. Para o autor, existem diferenças entre os

---

placed would be highly offensive to a reasonable person, and (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed. (4). a man has a right in the publicity value of his photograph, i.e., the right to grant the exclusive privilege of publishing his picture, and that such a grant may validly be made 'in gross,' that is, without an accompanying transfer of a business or of anything else (2006, p. 14 - 22).

33 Art. 12: "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".

seus limites atuais e aqueles do passado, e certamente existirão outras diferenças em 100 anos. Além disso, em um mesmo período temporal, há divergências considerando o espaço, como aquelas verificadas, por exemplo, as diferentes percepções culturais sobre o tema nos Estados Unidos, na Europa e no Japão.

Corroborando o esposado, assevera Danilo Doneda que "É provável que nos encontremos em um dos momentos em que se observa certa defasagem entre a carga semântica de um conceito e a ideia que propomos que ele porte" (2006, p. 10). Daniel Solove (2006b), por sua vez, entende que privacidade é um termo guarda-chuva que designa uma pluralidade de casos, devendo haver uma generalidade que permita transcender as particularidades de contextos específicos e, por conseguinte, conferir-lhe uma ampla aplicabilidade, reconhecendo a importância do contexto na compreensão da privacidade: não é possível determinar com base no conteúdo, por si só, se se trata de informação privada, sendo necessária uma análise das circunstâncias que cercam sua revelação.

Em outra obra, Daniel Solove (2008) reconhece que esta concepção moderna e liberal - tal como intrusões de natureza física, revelações de segredos ou distorção de fatos – é uma construção analógica do direito e não consegue abarcar a problemática ligada à coleta de dados, sua manutenção, manipulação, seus usos e à capacidade do sujeito intervir em todo esse processo, bem como à sua suscetibilidade em questões referentes ao direito à liberdade e à igualdade.

2.3 DA AUTODETERMINAÇÃO INFORMATIVA À PROTEÇÃO DE DADOS PESSOAIS

Conforme já explanado, originariamente, a privacidade estava calcada em uma dicotomia - entre a esfera pública e a privada – cujo dever a ser observado era o de abstenção, não intromissão na vida de outrem, seja pelo Estado ou por terceiros. No entanto, devido aos avanços tecnológicos, seja no que se refere a dispositivos audiovisuais ou de informação e comunicação, e o consequente aumento exponencial do fluxo de dados, a regular omissão deixou de ser o único meio para a proteção individual. Passam a ser os dados pessoais e a demanda pelo seu controle o elemento chave acerca da nova estrutura da tutela do indivíduo.

Vance Packard (1964) já advertia que, antes da Segunda Guerra Mundial, o uso de aparelhos de escuta, espionagem e gravação era

bastante raro devido ao seu alto custo e à eficiência reduzida. No entanto, por conta do desenvolvimento tecnológico verificado no decorrer da Segunda Guerra Mundial, tais dispositivos passaram a ser utilizados de maneira cada vez mais vulgarizada. Ademais, naquele mesmo ano o autor já denunciava as *giant memory machines*, ou seja, os "super-computadores" que despontavam à época e que poderiam armazenar uma quantidade de dados até então sem precedentes.[34]

Ratificando o exposto, Anderson Schreiber (2014) explana que o cenário em relação à privacidade começou a mudar a partir da década de 1960, quando se demandou uma tutela abrangente, que se estendesse por todas as fases do processamento de dados, desde a coleta até sua eliminação, perpassando pela possibilidade de acesso para conhecimento ou correção.

Acerca deste novo paradigma em relação à privacidade, Alan Westin, em 1970, trouxe contribuições que são vistas como pioneiras na construção de uma "nova privacidade", ou na autodeterminação informacional. Para ele, trata-se da reivindicação de indivíduos, grupos ou instituições para determinar por eles mesmos quando, como e com qual extensão a informação sobre si pode ser comunicada a outros. Em outras palavras, diz respeito à possibilidade de se exercer o controle sobre o uso de suas informações, tornando-se tal ideia basilar na construção teórica da autodeterminação informacional.

Para tanto, visando à proteção individual e coletiva, iniciou-se um esforço – que perdura até hoje – para construção e implementação prática de um novo feixe de direitos, com ferramentas específicas. Por conta das peculiaridades envolvidas, tiveram início os movimentos para reivindicar sua fragmentação em relação à privacidade, com algumas

---

34 Conforme Martin Hilbert e Priscila Lopez: "*In 2007, humankind was able to store 2.9 × 1020 optimally compressed bytes, communicate almost 2 × 1021 bytes, and carry out 6.4 × 1018 instructions per second on general-purpose computers. General-purpose computing capacity grew at an annual rate of 58%. The world's capacity for bidirectional telecommunication grew at 28% per year, closely followed by the increase in globally stored information (23%). Humankind's capacity for unidirectional information diffusion through broadcasting channels has experienced comparatively modest annual growth (6%). Telecommunication has been dominated by digital technologies since 1990 (99.9% in digital format in 2007), and the majority of our technological memory has been in digital format since the early 2000s (94% digital in 2007)*." HILBERT, Martin; LOPEZ, Priscila. ***The World's Technological Capacity to Store, Communicate, and Compute Information***. Science. Disponível em: http://www.martinhilbert.net/WorldInfoCapacity.html/

dissonâncias entre si. Conforme Orla Linksey (2015) a este respeito, é possível elencar: (i) a proteção de dados e à privacidade como direitos separados, mas complementares como instrumentos de proteção à dignidade da pessoa humana; (ii) a proteção aos dados pessoais como uma faceta da privacidade; e (iii) a proteção aos dados pessoais como um direito fundamenta independente, o qual não se limita à proteção da privacidade.

Cediço que, apesar das tentativas de categorização, ainda existem limites cujo traçado não está claramente delineado, existindo pontos de interseção e matizes de cinza entre as diferentes concepções. Mesmo assim, é possível identificar características principais e relevantes de cada um dos modelos estabelecidos.

Em relação ao primeiro modelo, Peter Hustinx (2014) defende que o direito à privacidade e o direito à proteção de dados estão intimamente ligados, sendo expressão de uma ideia universal com dimensões éticas bastante fortes, quais sejam: dignidade, autonomia e valor único de todo ser humano. Nesse mesmo sentido, Voigt e Bussche (2017) entendem que ambos os direitos fundamentais fazem parte de um só sistema, uma vez que o processamento de dados afeta a privacidade, sendo este o valor que requer proteção.

Segundo Orla Linksey (2015), este primeiro modelo tem como fundamento normativo a proteção da dignidade da pessoa humana, nos termos da construção da autodeterminação informacional na qual se baseiam os direitos da personalidade, de acordo com a construção realizada pelo Tribunal Federal Alemão, a ser adequadamente descrita posteriormente. Sua principal vantagem seria a exaltação da dignidade humana como um interesse a ser observado, mormente em relação às possíveis ameaças e prejuízos concernentes à igualdade e à liberdade que são acentuados pelo tratamento e utilização de dados pessoais.

Os argumentos contrários a essa concepção se relacionam com a existência de divergências e com a falta de clareza acerca da extensão e do conteúdo da dignidade da pessoa humana, bem como sua ampliação e vulgarização, tal como sua utilização para subsidiar diferentes diretrizes filosóficas. Ademais, em relação à União Europeia, há quem defenda a limitação ao poder dos indivíduos haja vista a tensão existente entre este e o livre comércio, uma vez que o mercado de fluxo de dados detém parcela significativa da atividade econômica comunitária.

Em relação à proteção aos dados pessoais como uma faceta da privacidade, Orla Linksey (2015) observa que se trata de uma visão ainda proeminente na percepção pública e na academia. A proteção de dados é vista como um último estágio da evolução do direito à

privacidade, com o incremento de elementos de controle informacional, sendo que todos os elementos da proteção de dados pessoais decorrem e são justificados pela estrutura do direito à privacidade.

Neste sentido, importante foi o desenvolvimento teórico feito por Helen Nissenbaum (2010) da "privacidade como integridade contextual", visando à garantia do fluxo apropriado de informações e não simplesmente à restrição no fluxo de informações. Para a autora, a privacidade exige o controle de informações e deve ser entendida como uma norma contextual que regula a informação, ou seja, deve-se considerar nas relações entre as partes, em circunstância política ou econômica, o contexto no qual ocorre a coleta da informação e sua própria natureza; quem está analisando; quem está divulgando e para quem.

Da mesma forma, Stefano Rodotà entende que a proteção de dados é resultado de um longo processo de evolução do conceito de privacidade, o qual define como: "o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada" (p. 92).

Segundo Orla Linksey (2015), a crítica realizada concerne à impossibilidade de encontrar um denominador comum entre as possibilidades que passam a ser englobadas por esse superdireito. Por exemplo, o direito à não invasão de domicílio, ao sigilo das comunicações, característicos do direito à seclusão que decorre da privacidade e o direito subjetivo de não se submeter a decisões baseadas em processos estritamente automáticos, que decorre da proteção de dados pessoais.

Quanto ao terceiro modelo – o da proteção de dados como um direito autônomo –, a autora pontua que foi este o entendimento adotado recentemente pela Corte de Justiça da União Europeia, bem como por maior parte da doutrina que trata do tema. Por essa razão, a análise dessa corrente será realizada de maneira pormenorizada ulteriormente.

O presente tópico visa resgatar as concausas que culminaram na estruturação teórica e prática da privacidade como autodeterminação informacional e, ato contínuo, na proteção de dados pessoais, levando em consideração o desenvolvimento de tecnologias de informação e comunicação como principal propulsor da demanda pelo controle informacional.

Para auxiliar no objetivo descritivo, será utilizada a classificação geracional das normas de proteção de dados no contexto normativo europeu, desenvolvida pelo pesquisador Viktor Mayer-Schonberger (1997) com fulcro nas similaridades e convergências identificadas no

direito comparado e comunitário. O motivo da adoção dessa classificação foi a sua especificidade e clareza considerando as leis europeias, que foram fonte de influência de modelo regulativo para outros ordenamentos jurídicos, inclusive o brasileiro.

De maneira geral, é possível depreender entre as gerações a existência de um ciclo intrageracional: constatados os problemas no plano fático, arquiteta-se uma norma visando solucioná-los; após curto período de vigência da norma, logo são detectados novos impasses advindos de sua aplicação; ato contínuo, esta é alvo de avaliação e revisão, a fim de superar seus gargalos e lacunas.

2.3.1 Primeira geração de leis de proteção de dados: a centralidade da técnica

Narra Viktor Mayer-Schonberger (1997) que a primeira geração das leis de proteção de dados foi delineada na década de 1970, em resposta às "obscuras visões" de um "Admirável Mundo Novo" que se aproximava inevitavelmente pelo desiderato, tanto do setor privado, quanto da administração pública, de centralização de todos os arquivos de dados pessoais em gigantescos bancos de dados nacionais. Foi uma reação às possíveis violações à individualidade que a informatização poderia determinar.

Mayer-Schonberger (1997) explica que o Estado de bem-estar social requer um sofisticado planejamento e, por corolário, conhecimento acerca da população. Como este modelo governamental passou a ser implementado em diversos países da Europa após a Segunda Guerra Mundial, os governos centrais passaram a coletar e a processar, de maneira crescente, maiores quantidades de informações sobre cidadãos, o que apenas foi possível pelo desenvolvimento do computador, cuja capacidade de armazenamento e processamento foram aumentando exponencialmente.

Cita como exemplos de normas da primeira geração: as leis do Estado alemão de Hesse (1970)[35], a Lei de Dados da Suécia (1973)[36], o

35 *The Hesse Data Protection Act applied exclusively to the public sector; more concretely, to the authorities of the Land and the organisations depending of the Land when using records prepared for the purpose of automatic data processing, storing data, or obtaining results from such data.6 The Act defined Datenschutz as the obligation for records, data and results to be obtained, transmitted and stored in such a way that they cannot be consulted, altered, extracted or destroyed by an unauthorised person.7 It also laid down norms of*

Estatuto de Proteção de Dados do Estado alemão de Rheinland-Pfalz (1974), a Lei Federal de Proteção de Dados da Alemanha (1977)[37], e o *Privacy Act* norte-americano (1974).

---

*data confidentiality in the form of rules of conduct to be observed by the authorities in charge, and by the computer personnel (Hondius 1975, p. 5). The Hesse Data Protection Act additionally contained provisions on the rights of individuals concerned by the information stored, who may notably demand the rectification of incorrect data.8 Moreover, institutional controls were introduced in the form of a Datenschutzbeauftragter (Data Protection Commissioner), charged with supervising compliance with the law, and, generally, with the mission of observing the effects of computerisation on the balance of power between the various public organs of the Land. (*GONZALEZ FUSTER, 2016, p. 57).

36 *The first national law regulating automated data processing ever to see the light in Europe was the Swedish Datalag (Data Act) of 11 May 1973,14 which entered into force on 1 July 1973. The Datalag was the direct outcome of the public concern generated by the public census of 1969, and the subsequent publication in 1972 of the report titled Data och integritet by the Swedish Parliamentary Commission on Publicity and Secrecy of Official Documents. In the 1972 report, the Swedish Parliamentary Commission highlighted the importance of integritet as a problem of trust and confidence between the State and citizens, while emphasising the benefits of the use of computer technology in public administration* (Söderlind 2009, p. 272). *It proposed the adoption of a special statute, as well as the establishment of a new authority, the Datainspektionen or Data Inspection Board, to be responsible for the implementation of the legislation, and for the protection of individuals* (Söderlind 2009, p. 272). *The pioneering role played by Sweden in this field can be explained by a number of reasons. Since the 1940s, it had been developing a system of identification through personal identification numbers, which, in the light of increasingly rapid computerisation public administration, caused concern due to its capacity to rapidly integrate information a priori decentralised (Burkert 1999, p. 48). Perhaps more importantly, Sweden has traditionally granted an extraordinary relevance to openness, and, concretely, to the principle of public access (offentlighetsprincip)* (Steele 2002, p. 19). (GONZALEZ FUSTER, 2016, p. 58).

37 *In January 1977, Germany finally enacted its first Federal Data Protection Law, under the heading Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz, BDSG), or Act on Protection Against the Misuse of Personal Data in Data Processing (Federal Data Protection Act). The Act complemented existing legislation at the State level by focusing on data processing in the private sector, not yet covered. The Act's stated purpose was to protect personal data against misuse during their storage, transmission, modification or deletion (thus, in general, during data*

De acordo com Danilo Doneda (2006), os termos predominantemente empregados nesses textos eram *data, data bank, data record, data base, data file;* sendo raro o uso de palavras como *privacy*, *information* e *protection of intimate, personal data,* ou seja, o foco e a preocupação das normas não era a tutela do indivíduo, mas sim a pretensão de controlar a própria tecnologia. O meio de tornar possível esse controle prévio baseava-se na concessão de autorizações para a criação de bancos de dados.

Para Bruno Bioni (2015): "A racionalidade da primeira geração era praticamente de 'domesticar' a tecnologia, de modo que as primeiras leis buscaram prescrever taxativamente quais seriam os usos lícitos e ilícitos com dados pessoais dos cidadãos". Esse regime, rígido e detalhado, demandava um minucioso acompanhamento, o que dificultava a sua efetivação por conta da multiplicação de bancos de dados descentralizados.

Nesse sentido, o *Big Brother*, representado pelo risco de centralização único de informação, deu lugar aos *Little Brothers*, ou seja, não se tratava mais de um risco singular, mas de sua pulverização, com novos, diversos e potenciais invasores. Por conta do estado da tecnologia, as normas vigentes até então se tornaram ineficazes, o regime de proteção instaurado, que demandava grande empenho e recurso por parte das autoridades de controle, não condizia com a realidade superveniente, uma vez que não poderia acompanhar a expansão do número de bancos de dados.

2.3.2 Segunda geração de leis de proteção de dados: a centralidade do indivíduo

O marco da segunda geração é a Lei Francesa *Informatique et libertees*, de 1978, e as Constituições da Áustria (1978), da Espanha (1978) e de Portugal (1976). Se na primeira geração o enfoque das normas se referia a um regime de controle, com procedimentos regulatórios *ex ante* de registros e licenças, nesta geração subsequente se entendeu que o objeto de tutela não deveria ser o dado em si, mas o sujeito titular de direitos.

---

processing operations) for the safeguarding of the interests worthy of protection of the persons concerned. The basic principle of the 1977 BDSG23 is that the processing of personal data is forbidden, unless it falls under one of the two conditions (GONZALEZ FUSTER, 2016, p. 61).

Como o perigo passou a estar dissipado em milhares de computadores, pensou-se que a melhor resposta a isso seria tornando os próprios cidadãos responsáveis por sua proteção. É neste momento, portanto, que é delineada a figura do consentimento como pré-condição para o processamento de dados: o indivíduo é quem toma a decisão de fornecer ou não seus dados. As bases da privacidade como autodeterminação informativa e como uma extensão das liberdades individuais podem ser identificadas na estrutura desta geração.

Conforme Danilo Doneda (2006), o antigo mecanismo de autorização para o funcionamento de bancos de dados foi diluído e as autoridades de controle, que anteriormente eram centrais, transformaram-se em um intermediário: assumiram outras incumbências, auxiliando a administração pública e atuando também como órgão parajurisdicional. Todos os atores deste ecossistema passaram a cumprir com deveres e possuir direitos, de acordo com sua atuação.

Segundo Bruno Bioni (2018, p. 66) as normas de segunda geração não mais dizem "de antemão quais são os tratamentos lícitos e ilícitos com dados pessoais, deixando espaço para que floresçam novos modelos de negócio e formação de políticas públicas, desde que observem os direitos e deveres previstos na legislação".

Com isso, o ato de fornecimento de dados pessoais já tinha se tornado central e até indispensável para a efetiva participação social e de mercado no acesso a serviços e a produtos de consumo. Já no final da década de 1970 e no início da década de 1980, o controle de informações e o exercício puramente individual da privacidade e da proteção de dados estavam ligados ao custo de exclusão social e/ou econômica. Desse jeito, as consequências sofridas e sentidas eram bem maiores quando comparadas com a concessão de informações pessoais. A disparidade de poder econômico, técnico e jurídico induzia ao consentimento.

Em seguida, compreendeu-se que, diante da complexificação do uso de dados, a dicotomia de consentir ou não consentir, fornecer ou não fornecer, deveria ser superada, levando-se em consideração todo o contexto no qual os dados são solicitados, armazenados e tratados. Deste modo, a fim de equilibrar interesses, verificou-se a necessidade de integrar o controle individual com o coletivo. Segundo Stefano Rodotà, "a proteção de dados não pode mais se referir a algum aspecto especial, mesmo que este seja em si muito relevante, porém requer que sejam postas em operações estratégias integradas, capazes de regular a circulação de informações em seu conjunto" (2008, p. 50).

Nessa mesma época, os primeiros documentos internacionais foram assinados, quais sejam: a Convenção 108 ou Convenção de Estrasburgo, de 1981, do Conselho da Europa, e as Diretrizes sobre a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais da OCDE (Organização para o Comércio e Desenvolvimento Econômico).

2.3.3 Terceira geração de leis de proteção de dados: o desenvolvimento da autodeterminação informativa

O marco da terceira geração de normas de proteção de dados, conforme Mayer Schonberger, ocorreu com a decisão do Tribunal Constitucional Alemão acerca da constitucionalidade e da aplicação da Lei do Recenseamento de 1983, proferida em dezembro deste mesmo ano. Segundo contextualiza Leonardo Martins, além da grande quantidade de respostas a serem coletadas, a norma previa "a possibilidade de uma comparação dos dados levantados com os registros públicos e também a transmissão de dados tornados anônimos a repartições públicas federais, estaduais e municipais para determinados fins de execução administrativa" (2005, p. 234).

Observa Danilo Doneda (2006) que o contexto social alemão à época era de bipolarização do poder e de divisão territorial, logo, prevaleciam a insegurança e a desconfiança de vários setores sociais em relação ao governo, que poderia se valer dos dados obtidos não somente para fins estatísticos, mas também para realizar um controle capilar da condição pessoal dos cidadãos. Em suma, havia um receio de excessiva vigilância e a sensação de que um censo provocaria uma invasão injusta à privacidade.

Por conta disso, houve o ajuizamento de diversas Reclamações Constitucionais em face da mencionada Lei, sob o fundamento de violação direta a direitos fundamentais, precipuamente o direito ao livre desenvolvimento da personalidade. O Tribunal entendeu que os pressupostos processuais dos remédios constitucionais estavam presentes, haja vista que "os reclamantes seriam, em grande parte, própria, direta e atualmente atingidos" (2005, p. 234).

Para melhor elucidar a questão, cabe aqui a transcrição de alguns excertos das razões expostas na referida decisão. Primeiramente o Tribunal inaugura os parâmetros de análise em relação ao intuito da norma e os direitos supostamente violados:

> O parâmetro do exame é em primeira linha o direito geral da personalidade protegido pelo Art. 2 I c. c. Art. 1 I GG. 1. a) No centro da ordem constitucional estão o valor e a dignidade da pessoa que age com livre autodeterminação enquanto membro de uma sociedade livre. À sua proteção serve – além de garantias especiais de liberdade – o direito geral da personalidade protegido pelo Art. 2 I c. c. Art. 1 I GG, que ganha importância principalmente em vista do desenvolvimento moderno e das novas ameaças à personalidade humana, associadas àquele desenvolvimento (BVerfGE 54, 148 [153]). [...] No levantamento de dados para propósitos estatísticos não se pode exigir uma vinculação estrita e concreta de propósito dos dados. Mas dentro do sistema de informação devem existir barreiras respectivas para compensação, em contraposição ao levantamento e manipulação da informação (2006, p. 234 - 235).

Ato contínuo, expõe que o obscurantismo e o não conhecimento sobre o que os bancos de dados de entidades governamentais reservam e guardam a respeito dos cidadãos são ameaças ao livre e pleno desenvolvimento da personalidade. Assim, o Tribunal introduziu a concepção da autodeterminação informacional, com a ressalva de que não se refere a um direito absoluto, mas limitado:

> Quem não consegue determinar com suficiente segurança quais informações sobre sua pessoa são conhecidas em certas áreas de seu meio social, e quem não consegue avaliar mais ou menos o conhecimento de possíveis parceiros na comunicação, pode ser inibido substancialmente em sua liberdade de planejar ou decidir com autodeterminação. Uma ordem social e uma ordem jurídica que a sustente, nas quais cidadãos não sabem mais quem, o que, quando, e em que ocasião se sabe sobre eles, não seriam mais compatíveis com o direito de autodeterminação na informação. Quem estiver inseguro sobre se formas de comportamento divergentes são registradas o tempo todo e definitivamente armazenadas, utilizadas ou transmitidas, tentará

> não chamar a atenção através de tais comportamentos. Esse direito à "autodeterminação sobre a informação" não é garantido ilimitadamente. O indivíduo não tem um direito no sentido de um domínio absoluto, ilimitado, sobre "seus" dados; ele é muito mais uma personalidade em desenvolvimento, dependente da comunicação, dentro da comunidade social. A informação, também quando ela é relativa à pessoa, representa um recorte da realidade social que não pode ser associado exclusivamente ao indivíduo atingido [por causa da demanda de informações do Estado ou de terceiros]. Decisivos são sua utilidade e possibilidade de uso. Estas dependem, por um lado, da finalidade a que serve a estatística e, por outro lado, das possibilidades de ligação e processamento próprias da tecnologia de informação (2005, p. 236 - 237).

Desta forma, à luz da Lei Fundamental de Bonn, o Tribunal Constitucional Alemão declarou a parcial inconstitucionalidade da Lei do Recenseamento e suspendeu provisoriamente o censo, impelindo exigências ao legislador, que deveria elaborar regulamentação complementar sobre a organização e procedimento do recenseamento[38]. Em suma, entendeu que a utilização de dados e informações, tanto para fins administrativos quanto para fins estatísticos, caracterizaria a diversidade de finalidades, as quais eram "inconciliáveis, dado que o rigor estatístico não poderia coexistir com a necessidade dos órgãos administrativos de identificar os titulares destes dados". Deste modo, a impossibilidade de os cidadãos conhecerem o uso efetivo que seria feito de suas informações caracterizaria afronta à dignidade humana e à liberdade.

A tese então fixada, que reverbera até hoje, é a de que esta coleta não pode ser indeterminada, devendo observar ao princípio da finalidade

38 A resposta do Parlamento não tardou a vir. Mesmo que o resultado da decisão possa ser considerado uma grande vitória para os opositores, o censo não foi interrompido, somente retardado. Uma nova lei foi aprovada em 1985 no *Bundestag*, levada agora em conta a decisão do *Bundesverfassungsgericht*, - e o censo populacional efetivamente ocorreu em maio de 1987. Essa nova lei foi igualmente contestada perante o tribunal, mas os juízes a consideraram constitucional. (ASSMAN, 2014, p. 34)

da coleta de dados pessoais. Além disso, os cidadãos possuem o direito à autodeterminação informativa em todas as fases do fluxo de dados, refinando a ideia do mero consentimento do indivíduo na coleta de seus dados.

Segundo Gloria Gonzalez Fuster (2014), levando em conta que os indivíduos podem ser limitados em seu desenvolvimento pessoal e afetados em sua dignidade sempre que não agem com total liberdade, e argumentando que os indivíduos não agiriam com total liberdade se não soubessem quais dados sobre eles estavam sendo processados, o Tribunal Constitucional introduziu a possibilidade de os indivíduos determinarem quais dados sobre eles são processados .

Mayer-Schonberger (1997) explana que, ao formular um direito à autodeterminação informativa, o Tribunal reconheceu uma carga participativa muito maior que a reconhecida pelas normas de proteção de dados pessoais em períodos anteriores, uma vez que a Corte declarou que todas as fases do processamento da informação (coleta, armazenamento, tratamento e transmissão) são passíveis de limitações constitucionais, ou seja, o direito de participação do indivíduo deverá ser estendido a todas essas fases.

Assevera Gloria Gonzalez Fuster (2016) que, com essa decisão, o Tribunal Alemão optou pela aplicação do direito à privacidade enquanto autodeterminação informacional e abandonou outra teoria por ele desenvolvida na década de 1950, qual seja, a "teoria das esferas concêntricas", a qual delineava diferentes áreas com base em graus distintos do privado: a esfera social, a esfera privada e a esfera da intimidade, obedecendo-se à lógica dual público-privado.

Jhonata Assman (2014) relata que, no âmbito dessa teoria, aplicava-se o princípio da proporcionalidade com o intuito de verificar quais restrições foram impostas e qual das esferas atingida - sendo a social aquela mais tolerada, pois presumido interesse público e coletivo (desde que não houvesse agressão à esfera íntima). A teoria apresentava fragilidades: a possibilidade de armazenamento e de cruzamento de quantidades cada vez maiores de dados, que, em tese, eram aparentemente inofensivos e pertencentes tão somente à esfera do social, demonstraram sua potencialidade de violação à personalidade. Por corolário, independentemente do conteúdo da informação e de a qual esfera pertenceria, todos os dados deveriam ser igualmente tutelados.

Consigna Marcel Leonardi (2012): "por meio da agregação e dados isolados e fragmentados de informação aparentemente irrelevantes, é possível montar perfis completos de sua personalidade,

sem que se tenha coletado quaisqer informações íntimas de seu exclusivo conhecimento".

Vê-se que a construção alemã do direito à autodeterminação informativa enquanto direito fundamental, com base no próprio texto constitucional, estabelece a limitação de órgãos estatais e a observância por particulares, estando intimamente ligado ao desenvolvimento da livre personalidade e à proteção de dados pessoais, garantindo igualmente a comunicação e a pluralidade social.

Nesse sentido, de acordo com Stefano Rodotà, a privacidade "além do tradicional poder de exclusão, atribui relevância cada vez mais ampla e clara ao poder de controle. Por outro lado, o objeto do direito à privacidade amplia-se, como efeito do enriquecimento da noção técnica da esfera privada" (2008, p. 93). Por corolário, o direito à privacidade deixa de se estruturar em torno do eixo "pessoa-informação-segredo" para surgir em um eixo "pessoa-informação-circulação-controle", prevalecendo a ideia de controle do indivíduo sobre as suas informações, em detrimento da concepção de seu isolamento social.

Essa mudança estaria ligada à nova arquitetura informacional e de organização de poder, a qual representa riscos conexos ao uso de informações coletadas. Não se trata mais, como nas leis de segunda geração, de decisão "tudo ou nada", mas de um envolvimento contínuo: conforme consignado na decisão, o indivíduo possui o direito de saber quem, por quem, quando, e o que se sabe sobre ele, bem como a sua finalidade. No caso de tomadas de decisão, o que foi levado em consideração e quais as consequências específicas da negativa.

Para Stefano Rodotà, o reconhecimento ao direito à autodeterminação informativa possui importância enquanto o "direito a determinar as modalidades de construção de esfera privada na sua totalidade; apresenta-se, por fim, como precondição da cidadania na era eletrônica e, como tal, não pode ser confiada unicamente à lógica da autorregulamentação ou das relações contratuais" (2008, p. 129).

Mayer-Schonberger aduz que, após a mencionada decisão do Tribunal Alemão, os diplomas normativos daquele país sofreram alterações a fim de incorporar os avanços teóricos alcançados: os estatutos de proteção de dados dos Estados alemães; a Lei Federal de Proteção de Dados da Alemanha (1990); e até de outros países, como a Lei de Proteção de Dados Austríaca e a Norueguesa.

Verifica-se, diante disso, que a referida decisão influenciou na elaboração da teoria da privacidade como autodeterminação informativa e lançou as bases para a construção do direito à proteção de dados

pessoais como um direito fundamental autônomo, inserindo-o como um direito de personalidade.

Nessa toada, Danilo Doneda (2006) entende que é justamente a partir da funcionalização da proteção da privacidade que surge a disciplina de proteção de dados pessoais:

> [...] que compreende pressupostos ontológicos idênticos aos da própria proteção da privacidade: pode-se dizer que é a sua "continuação por outros meios". Ao realizar esta continuidade, porém, assume a tarefa de conduzir uma série de interesses cuja magnitude aumenta consideravelmente na sociedade pós industrial e acaba, por isso, assumindo uma série de características próprias, especialmente na forma de atuar os interesses que protege, mas também em referências a outros valores e direitos fundamentais. Daí a necessidade de superar a ordem de conceitos pela qual o direito à privacidade era limitado por uma tutela de índole patrimonialista, e de estabelecer novos mecanismos e mesmo institutos para possibilidade a efetiva tutela dos interesses da pessoa (2006, p. 26).

No entanto, não tardou para que as leis de terceira geração fossem objeto de crítica e de revisão. A participação do cidadão era um importante pilar de sua estrutura, e este, em tese, teria poderes para acompanhar o fluxo informacional com ferramentas e instrumentos específicos para tanto. Todavia, percebeu-se que a autodeterminação informativa continuava sendo privilégio de um grupo minoritário que tinha condições e decidia enfrentar tais custos e exercer seus direitos.

A validade do consentimento para formação do negócio jurídico e a efetividade para proteção do sujeito começaram a ser alvo de críticas reiteradas. Questões como a liberdade o conhecimento prévio e o direito à informação começaram a ser suscitadas. Paul Schwartz e Karl-Nikolaus Peifer (2017) objetam a suposição de que os indivíduos são capazes de exercer escolhas significativas com relação a suas informações, dada a disparidades no conhecimento e o poder de barganha sobre a transferência de suas informações: a privacidade não envolve apenas controle individual, mas também a regulação social da informação.

Em outras palavras, a privacidade é um aspecto da estrutura social, uma arquitetura de regulação da informação, e não apenas uma alternativa para o exercício do controle individual. Tornou-se imperioso, então, pensar em uma nova estratégia de tutela.

2.3.4 Quarta geração de leis de proteção de dados: autonomia, cooperação e internacionalização

Neste cenário, as leis de quarta geração visam suprir as desvantagens do enfoque individual, outorgando instrumentos que elevam o padrão coletivo e supranacional de proteção, com a previsão de sanções adequadas aos infratores e devida fiscalização por um órgão independente de supervisão. Ademais, devido à característica transfronteiriça e de ubiquidade dos dados, a tutela meramente nacional com algumas aproximações e similaridades era insuficiente para a tutela do indivíduo.

Consoante Bruno Bioni (2018), finalmente se reconhece "a assimetria de poder e de informação entre o cidadão e quem processa seus dados, constituindo-se, então, um modelo de fiscalização e aplicação das leis cuja sua vértebra são autoridades estatais com expertise e missão institucional voltadas a fazer valer o conjunto de normas previsto em tais leis."

Os exemplos por excelência dessa geração são a Diretiva 46/95/CE da União Europeia; a Convenção 108 do Conselho da Europa e as Diretrizes da Organização para o Comércio e Desenvolvimento Econômico, sendo imperioso fazer um recorte temporal para retroceder novamente à década de 1980, quando as primeiras negociações e diplomas normativos internacionais começaram a ser assinados, com a convergência normativa.

Conforme Voigt e Bussche (2017), o primeiro instrumento internacional proposto foi elaborado no âmbito da OCDE (Organização para o Comércio e Desenvolvimento Econômico), sem força vinculativa, com grande influência dos Estados Unidos, expoente do neoliberalismo e do movimento de *deregulation*. Constituiu-se um grupo de trabalho no âmbito da organização em 1978, cuja finalização ocorreu em 1980 com a produção do documento *"Guidelines on the protection of privacy and transborder flows of personal data"*. Seu foco principal era: (i) alcançar um estandarte mínimo de proteção de dados pessoais e privacidade; (ii) reduzir diferenças entre normas e práticas dos Estados nacionais; (iii) evitar interferência indevida no fluxo de dados entre os Estados nacionais; e (iv) eliminar restrições de fluxos de dados transfronteiriços.

Por seu turno, o primeiro instrumento internacional vinculante foi a Convenção 108 ou Convenção de Estrasburgo, de 1981, do Conselho da Europa, cujo foco principal era a proteção de dados e a aproximação das Leis nacionais sobre a matéria. A antiga Comissão das Comunidades Europeias também identificou os riscos e as potencialidades dessas tecnologias, bem como a expansão do domínio de empresas dos Estados Unidos sobre o crescente mercado europeu de computadores e processamento de dados.

A partir disso, foi reconhecida a necessidade de se adotar medidas comuns de proteção dos cidadãos que deveriam ser adotadas pelos Estados-membros, a fim de obter uma harmonização legislativa e evitar divergências e contradições, visando à criação de um ambiente favorável à indústria europeia de processamento de dados.

A partir de ambos os documentos supramencionados, é possível deduzir diversos princípios, os quais ficaram conhecidos como os *Fair Information Principles*, considerados o núcleo comum "das questões com as quais todo ordenamento deve se deparar ao procurar fornecer sua própria solução ao problema da proteção dos dados pessoais" (DONEDA, 2006, p. 217). Por essa razão, acabaram por influenciar na elaboração de diversas normas nacionais, quais sejam:

> (i) Princípio da publicidade (ou da transparência) pelo qual a existência de um banco de dados com dados de pessoas deve ser de conhecimento público, seja através da exigência de autorização prévia para seu funcionamento, pela notificação de sua criação a uma autoridade; ou pela divulgação de relatórios periódicos; (ii) Princípio da exatidão: os dados armazenados devem ser fiéis à realidade, o que compreende a necessidade que sua coleta e seu tratamento sejam feitos com cuidado e correção, e que sejam realizadas atualizações periódicas destes dados conforme a necessidade; (iii) Princípio da finalidade: pelo qual toda utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da sua coleta. Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que é possível a estipulação de um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade (fora da qual haveria abusividade); (iv)

> Princípio do livre acesso: pelo qual o indivíduo tem acesso ao banco de dados no qual suas informações estão armazenadas, podendo obter cópias desses registros com a consequente possibilidade do controle destes dados; após este acesso e de acordo com o princípio da exatidão, as informações incorretas poderão ser corrigidas e aquelas obsoletas ou impertinentes poderão ser suprimidas, u ainda pode-se proceder a eventuais acréscimos; (v) Princípio da segurança física e lógica: pelo qual os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado (2006, p. 216 - 217).

Em que pese a relevância, a Convenção 108 não conseguiu garantir a proteção dos indivíduos e a uniformidade legal a que se propunha, sendo então sobreposta pela Diretiva 95/46/CE[39]. Gloria Gonzalez Fuster (2014) narra que os esforços para adoção de uma nova legislação supranacional e comunitária foram iniciados em 1990, tendo sido o texto final aprovado em 1995.

Segundo sintetiza Bruno Bioni, esses três diplomas normativos foram "todos eles estruturados em arquitetar os direitos e deveres de todos os agentes de governança de dados, especialmente no que diz respeito à perspectiva de se franquear aos cidadãos controle sobre seus dados e a introjeção de autoridades para a efetiva aplicação desse conjunto de regras". (2018, não p.)

Foi nesse cenário e com o intuito de garantir a harmonização normativa entre os países que se lançou mão da Diretiva, instrumento normativo que determina os objetivos e o padrão mínimo a ser observado pelos países da União Europeia, os quais devem adequar seu ordenamento jurídico interno de acordo com as diretrizes da norma comunitária. Neste contexto, Rebecca Wong (2012) comenta que as Cortes Nacionais exerceram um papel importante ao determinar a

39 Foram editadas posteriormente três diretivas complementares: a relativa ao tratamento de dados pessoais e a proteção da privacidade no setor das telecomunicações (97/66/CE); a relativa à regulamentação da proteção de dados pessoais no âmbito da comunicação eletrônica (2002/58/CE); e a relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrônicas publicamente disponíveis ou de redes públicas de comunicações (2006/24/CE);

extensão e a interpretação dos conceitos legais concebidos pela Diretiva[40].

Importante consignar que os objetivos traçados foram os seguintes: aumentar o nível de proteção do indivíduo, seus direitos e liberdades concernentes ao direito à privacidade e ao processamento de dados pessoais; e promover o livre fluxo de dados entre os Estados-membros. Percebe-se a tensão e a dualidade de tais desígnios, quais sejam: interesses econômicos versus direitos humanos, apresentando na prática dificuldades em sua conciliação.

Outro aspecto importante introduzido pela Diretiva em questão concerne ao dever imposto aos Estados-membros de estabelecer uma ou mais autoridades independentes de supervisão responsável pela proteção

---

40 *Whilst most of the EU Member States have managed to implement the DPD by introducing new laws or amending their data protection laws, the application of the DPD and interpretation of legal concepts has resurfaced before the national courts, beginning with the well-known case of Lindqvist that was brought by the Swedish courts before the European Court of Justice, a case that was about to test the extent in which the DPD can be applied online. Whilst the ECJ has clarified the scope of the Data Protection Directive, its decision was not a popular one. It led to changes made to the existing data protection laws within Sweden by using the existing exceptions provided under the Swedish Personal Data Act to amend their laws and adopt the misuse-orientated approach. The next landmark case was Productores de Musica de Espaha (Promusicae) v Telefonica' 2 whereby Promusicae, a non-profit-making organisation of producers and publishers of musical recordings asked the Spanish Court to order Telefonica to disclose the identities and physical addresses of certain individuals who were using P2P applications such as Kazaa. The Court of Justice considered several Directives in relation to the preliminary reference ruling, including Directive 2002/58/EC for deciding the case. It held that the Directive did not preclude the possibility for the Member State to lay down an obligation to disclose the personal data in the context of civil proceedings. The Court of Justice was able to conclude that the Directives in question did not require Member States to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings. A fair balance needed to be drawn between the various fundamental rights that are protected by the Community legal order. The implications of this case are that it reinforces the need to protect the privacy of its users and that this should not be compromised at the expense of other rights. The key to this is whether there are other means without having to disclose information of other users by looking at the proportionality test*. WONG, Rebecca. The Data Protection Directive 95/46/EC: Idealisms and Realisms. ***International Review Oflaw, Computers & Technology***: Routledge, Nova Iorque, v. 26, n. 2-3, p.229-244, nov. 2012.

de dados. Não obstante a preexistência dessa instituição em alguns países (tal qual a França com a *Commission Nationale de l'Informatique et des Libertés - CNIL*, estatuída pela Lei *Informatique et Libertes*), foi a primeira vez que houve a determinação de sua criação em uma norma de abrangência supranacional.

Posteriormente, inclusive, no âmbito da Regulação 45/2001/CE, foi erigida a Autoridade Europeia para a proteção de dados, "encarregada de assegurar que os direitos e liberdades fundamentais das pessoas singulares, especialmente o direito à vida privada, sejam respeitados pelas instituições e órgãos comunitários"[41].

41 Conforme art. 46 do Regulamento nº 45/2001: "Autoridade Europeia para a protecção de dados deve: a) Ouvir e investigar as reclamações e informar do resultado as pessoas em causa num prazo razoável; b) Realizar inquéritos por sua iniciativa ou com base numa reclamação e informar do resultado as pessoas em causa num prazo razoável; c) Controlar e garantir a aplicação do presente regulamento e de qualquer outro acto comunitário relativo à protecção de pessoas singulares no que se refere ao tratamento de dados pessoais por qualquer instituição ou órgão comunitário, com excepção do Tribunal de Justiça das Comunidades Europeias no exercício das suas funções judiciais; d) Aconselhar, por sua própria iniciativa ou em resposta a uma consulta, todas as instituições e órgãos comunitários, sobre o conjunto das matérias relativas ao tratamento de dados pessoais, nomeadamente antes de estas instituições e órgãos elaborarem regras internas sobre a protecção dos direitos e liberdades fundamentais em relação ao tratamento de dados pessoais; e) Acompanhar factos novos com interesse, na medida em que incidam na protecção de dados pessoais, nomeadamente, a evolução das tecnologias da informação e das comunicações; f) i) Cooperar com as autoridades nacionais de controlo referidas no artigo 28.o da Directiva 95/46/CE dos países a que esta é aplicável, na medida do necessário ao cumprimento das suas obrigações respectivas, nomeadamente procedendo ao intercâmbio de todas as informações úteis, solicitando a essas autoridades ou órgãos que exerçam as suas competências ou respondendo a um pedido dessas autoridades ou órgãos; ii) Cooperar igualmente com órgãos de controlo da protecção de dados por força do título VI do Tratado da União Europeia, nomeadamente para melhorar a coerência na aplicação das normas e processos cujo respeito devam assegurar; g) Participar nas actividades do «grupo de protecção das pessoas no que diz respeito ao Tratamento de dados pessoais», criado pelo artigo 29.o da Directiva 95/46/CE; h) Determinar, fundamentar e publicar as excepções, garantias, autorizações e condições referidas nos n.os 2.b), 4, 5 e 6 do artigo 10.o, no n.o 2 do artigo 12.o, no artigo 19.o e no n.o 2 do artigo 37. i) Manter um registo das operações de tratamento de dados que lhe sejam notificadas nos termos do n.o 2 do artigo 27.o e registadas nos termos do n.o 5 do mesmo artigo, e fornecer os meios de acesso aos registos mantidos pelos encarregados da protecção de dados nos termos do

Desta forma, a proteção coletiva e a individual se aproximaram de maneira definitiva e significativa, sendo essa uma das principais características das Leis de Quarta Geração, que reconhecem que a mera outorga de poderes ao indivíduo é insuficiente para sua tutela, uma vez que este se encontra em uma posição de maior vulnerabilidade por conta da assimetria de poder.

Paralelamente, delineou-se uma estrutura institucional a fim de garantir o cumprimento geral das regras de proteção de dados, conferindo às autoridades de supervisão poder para tutela ampla e coletiva, cuja relevância se torna crescente devido ao papel exercido. Combinam-se, assim, duas diferentes posições com a função de reforçar, suportar e suplementar da proteção do indivíduo. Outro ponto importante se refere às figuras dos controladores e processadores de dados, com delimitação de suas incumbências e responsabilidades.

Conforme Mayer-Schonberger (1997), um importante fator inserido na proteção do sujeito diz respeito à vedação prévia do tratamento de dados pessoais considerados sensíveis, tais como os dados relativos à etnia, à opção sexual, à opinião política e à religião[42], que podem acarretar em grave discriminação social.

---

artigo 26.o; j) Efectuar controlos prévios das operações de tratamento que lhe sejam notificadas; k) Elaborar o seu regulamento interno."

42 *Credit raters, search engines, major banks, and the TSA take in data about us and convert it into scores, rankings, risk calculations, and watch lists with vitally important consequences. But the proprietary algorithms by which they do so are immune from scrutiny, except on the rare occasions when a whistleblower litigates or leaks. Most of us don't know that we're being profiled, or, if we do, how the profiling works. We can't anticipate, for instance, when an apparently innocuous action—like joining the wrong group on Facebook—will trigger a red flag on some background checker that renders us effectively unemployable. Another world of consumer profiling—ranging from ad networks to consumer scores—is barely touched by law. They revive some of the worst aspects of unregulated credit reporting, but well out of the public eye. University of Pennsylvania law professor Oscar Gandy presciently described all this in 1993 as the "panoptic sort": "The collection, processing, and sharing of information about individuals and groups that is generated through their daily lives as citizens, employees, and consumers and is used to coordinate and control their access to the goods and services that define life in the modern capitalist economy." Those who have this power have enormous power indeed. It's the power to use discriminatory criteria to dole out different opportunities, access, eligibility, prices (mostly in terms of special offers and discounts), attention (both positive and negative), and exposure*. PASQUALE, Frank. ***The***

Foi no âmbito da quarta geração que o direito à proteção de dados pessoais como direito autônomo ganhou impulso e força. Com a crescente aplicação de tecnologias de predição e ranqueamento, que podem acarretar na seleção e na classificação de indivíduos, percebeu-se que a isonomia era outro direito fundamental que poderia ser diretamente afetado, afinal, os dados constantes em um banco de dados podem determinar, de maneira direta e significativa, as oportunidades de acesso a bens, serviços e até a empregos.

Stefano Rodotà (2008, p. 105) faz a seguinte crítica:

> A difusão do recurso aos perfis pode ocasionar a discriminação das pessoas que não correspondem ao modelo geral, acentuando a estigmatização dos comportamentos desviantes e a penalização das minorias. Pode-se identificar aqui um obstáculo ao pleno desenvolvimento da personalidade individual, cercada em meio a perfis historicamente determinados. Ao se privilegiar os comportamentos "conformes" aos perfis predominantes, torna-se mais difícil a criação de novas identidades coletivas, com riscos para a própria dinâmica social e para a organização democrática. Diante disso, deve ser vigorosamente assegurado o "direito de deixar rastros" sem receber por isso nenhuma penalidade.

Bruno Bioni (2014, p. 126) sustenta a insuficiência do modelo de privacidade para se pensar a proteção de dados pessoais, haja vista que aquele se enquadra na dicotomia público e privado, ao passo que neste, tal lógica não é aplicável quando se pensa no fluxo informacional:

> O eixo da privacidade está ligado ao controle de informações pessoais que seja algo íntimo e/ou privado do sujeito. A proteção dos dados pessoais não se satisfaz com tal técnica normativa, uma vez que a informação pode estar sob uma esfera permitida (pública), discutindo-se, apenas, a sua exatidão pelo seu titular. Tal direito de retificação (princípio da qualidade dos dados) é uma

---

***Black Box Society**: The Secret Algorithms That Control Money and Information*. Cambridge: *Harvard University Press*, 2015.

> construção que deriva da própria perspectiva da identidade do sujeito representado por seus dados e não, propriamente, do direito à privacidade. É o primeiro direito de personalidade que conforma a necessidade de haver uma correspondência fidedigna entre a pessoa e seus dados pessoais. O direito à proteção de dados pessoais angaria autonomia própria. A tutela jurídica dos dados pessoais é um novo direito da personalidade que não pode ser amarrada a uma categoria específica, em particular ao direito à privacidade. Demanda-se uma correspondente *ampliação normativa* por meio de uma construção dogmática própria que clareie e não empole a dinâmica de proteção desse novo direito da personalidade.

Dessa maneira, para além da ideia de privacidade, a proteção de dados pessoais possui como função precípua evitar a manutenção ou o surgimento de discriminações em razão de informações extraídas de bancos de dados, deve-se tutelar igualmente outras esferas, como a igualdade e a liberdade do sujeito.

Finalmente, em relação à emancipação do direito à proteção de dados pessoais, Laura Schertel Mendes entende que este deu origem: (i) a um setor de políticas públicas autônomo; (ii) à existência de instrumentos legais próprios e organismos regulatórios específicos; (iii) à existência de jornalistas e ativistas que atuam em âmbito local e internacional, visando demonstrar abusos e violações; (iv) e à crescente comunidade acadêmica que se debruça sobre o tema.

Gloria Gonzalez Fuster (2016) enuncia que, até os anos 2000, predominava a concepção de que o direito à privacidade de maneira ampla incluía a proteção de dados, sendo esta uma faceta relacionada à "dimensão informacional" do direito ao respeito pela privacidade, com fulcro enquadramento sustentado pela Convenção 108 e pela Diretiva 95/46/CE.

Um dos principais fatores para o reconhecimento de sua independência foi a proclamação da Carta de Direitos Fundamentais da União Europeia, em 2000, que foi o primeiro catálogo de direitos pactuados pelas três maiores e mais importantes instituições da União Europeia: o Parlamento, o Conselho e a Comissão. Posteriormente, com a entrada em vigor do Tratado de Lisboa em 2009, foi conferida força juridicamente vinculativa à Carta, consolidando tal rol de direitos

fundamentais e elevando-a a mesma categoria de Tratados da União Europeia.

De acordo com Gloria Gonzalez Fuster (2016), esse documento é considerado relevante para a autonomia da disciplina de proteção de dados pessoais porque foi o primeiro que reconheceu de maneira específica e separadas o direito ao respeito pela vida privada e familiar (artigo 7[43]) e o direito à proteção de dados pessoais (artigo 8º[44]), ambos inseridos no capítulo sobre as liberdades. Para a autora (2016), a incorporação de ambas as disposições de maneira apartada facilitou o desacoplamento jurídico das duas noções, fomentando a teoria de que se trata de direitos fundamentais diversos, e não superpostos ou mesmo do próprio direito à privacidade.

Ademais, destaca-se o papel da Corte de Justiça da União Europeia no que se refere à aplicação e à interpretação do mencionado diploma normativo internacional, que impulsionou o reconhecimento da proteção de dados pessoais como um direito autônomo.

Explica Gonzalez (2012) que, inicialmente, o posicionamento da Corte era de que as disposições da Diretiva 46/95/CE deveriam ser interpretadas à luz do direito fundamental à privacidade, conforme estabelecido no artigo 8º da Convenção Europeia dos Direitos do Homem (CEDH). Posteriormente, em 2008, no acórdão referente ao caso "Promusicae" (C-275/06, Promusicae v. Telefônica de Espanha)[45],

---

43 Artigo 7: Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicaçıes.

44 Artigo 8: 1. Todas as pessoas têm direito à proteção dos dados pessoais que lhe digam respeito. 2. Esses dados devem ser tratados de forma justa para fins específicos e com base no consentimento da pessoa em causa ou em qualquer outra base legítima estabelecida por lei. Todos têm o direito de acessar os dados coletados sobre ele e o direito de retificá-los. 3. O cumprimento destas regras está sujeito ao controlo de uma autoridade independente.

45 *Promusicae, an association of music producers and publishers, lodged an application before a Spanish court against he ISP Telefóinica, requesting that Telefónica disclose the names and addresses of a number of its clients. Promusicae had data to indicate that acts of copyrights infringement had been committed from certain IP addresses; however, it needed the names and addresses of IP holders in order to commence civil proceedings. [...] The court consequently held that Article 15 (1) 'must be interpreted as expressing the Community legislature's intention not to exclude from its scope the protection of the right to property, or situations in which authors seek to obtain that protection in civil proceedings". The conclusion was, therefore, reached that the E-privacy Directive neither precludes Member States from laying down an*

embora não tenha aplicado diretamente, a Corte fez referência direta ao artigo 8º da Carta de Direitos Fundamentais, sendo consignado que a tal enunciado normativo "expressamente proclama o direito à proteção dos dados pessoais".

Finalmente, em 2014, no seio do julgamento do caso 131/12, *Google Spain and Google Inc*. versus *Agencia Española de Protección de Datos and Mario Costeja Gonzalez*[46], com base em um requerimento explícito para que a Diretiva 46/95/CE fosse interpretada à luz da Carta de Direitos Fundamentais, a Corte reconheceu a proteção de dados pessoais como um direito fundamental autônomo, revendo seu entendimento anterior. Para Linksey (2015), esse julgamento enfatizou a necessidade da obtenção de efetividade da proteção de dados pessoais, sendo que no caso de desindexação de informação em um sistema de buscas no qual a criação de perfis pessoais e sua disseminação pode ser ampla e facilitada, a pessoa deve ser protegida. Ainda, fez a diferenciação entre a liberdade de expressão que deve predominar em face de informações de interesse público e as informações nas quais o público possa a vir ter algum interesse.

Narra a autora que alguns Estados-membros ofereceram resistência a essa interpretação do documento, tendo em vista divergências e ambiguidades entre a Carta e as normas internas. Um deles foi a Alemanha, que demonstrou dificuldade para desenhar uma linha divisória entre ambos os direitos, uma vez que o entendimento alemão é o de que o direito à proteção de dados deriva do direito à privacidade – autodeterminação informativa - conforme já delineado.

---

obligation to disclose personal data in the context of civil proceedings, nor does it compel Member States to impose such an obligation.

46 *Mr Costeja Gonzalez was involved in insolvency proceedings were reported in a regional newspaper the late 1990s. These proceedings were reported in a regional newspaper in Spain in 1998 and the article was later made available online. Mr Costeja Gonzalez, who was named in the report, asked the newspaper to delete the piece arguing that the insolvency proceedings were concluded and i was no longer of relevance.The newspaper refused to erase the data on the basis that the Ministry of Labour and Social Affairs had ordered its publication. Mr Costeja then redirected his request for erasure to Google Spain asking it to no longer show links to the newspaper in its search results when his name was entered as a search term in the search engine. [...] The Spanish Data Protection Authority upheld the complaint against Google Spain and Google Inc, requesting that the contested links be removed from Google's index of search results.*

Da mesma forma, a literatura científica começou a reconhecer de maneira progressiva o direito à proteção de dados pessoais como autônomo, ou seja, passou a reconhecer a coexistência de duas noções distintas: de um lado, a privacidade ou o respeito pela vida privada; e, de outro, a proteção dos dados pessoais.

Embora não seja possível afirmar que haja consenso doutrinário ou legislativo, Gloria Gonzalez Fuster (2016) defende que a visão da autodeterminação informacional enquanto parte integrante do conceito de privacidade está perdendo força em detrimento do direito à proteção de dados emancipada. Para ela, apesar da histórica conexão, a proteção de dados pessoais não se trata de um direito cuja natureza seja homóloga à do direito à privacidade, pelo contrário, possuem essência e natureza jurídica divergentes. Por conta disso, advoga que a intercambialidade dos termos enfraquece justamente o direito à proteção de dados pessoais, o qual deve ser reconhecido autonomamente, juntamente com seu impacto disruptivo.

2.3.5 O papel dos Estados Unidos no contexto internacional

Apesar do pioneirismo despontado pelos Estados Unidos quanto à matéria no âmbito da OCDE, posteriormente o país perdeu grande parte de seu espaço no debate bem como sua influência. Enquanto a União Europeia se baseou em um sistema geral de proteção de dados, com participação de uma Autoridade Supervisora, os Estados Unidos se basearam em um setorial. Conforme Linksey (2015), no início dos anos 1970 até foi proposto no Senado dos EUA um projeto de lei geral, destinado e aplicável a todas as esferas da federação e ao setor privado, contudo, este foi denegado pelo Congresso.

Consoante Voigt e Bussche (2017), o movimento de *deregulation*, as demandas de livre mercado e a cultura de resistência americana à intervenção regulatória foram cruciais para sua rejeição. Neste mesmo sentido, Orla Linksey indica que, pelos mesmos motivos, foi igualmente rechaçada a criação de uma Autoridade de Supervisão, considerada uma nova camada de burocrática. Explica Stefano Rodotà (2008, p. 150-153):

> A recusa ao paternalismo legislativo e a reafirmação obstinada de uma liberdade na rede, identificada com a ausência de qualquer regra, convertem-se em um ulterior crescimento das possibilidades de influência da pura lógica do

> mercado sobre toda a dinâmica da rede, com efeitos negativos muito graves, que podem ser facilmente evitados por uma disciplina legislativa sóbria e objetiva. Essa orientação, contudo, não exclui uma política que valorize os códigos deontológicos e a ética profissional, ainda que tais instrumentos não tenham até agora gerado resultados satisfatórios. Mas as novas formas de auto-regulamentação, e sua integração no sistema jurídico, podem ser consideradas como instrumentos aptos a favorecer soluções mais eficazes socialmente, a serem experimentadas até mesmo como ponto de partida para posteriores e eventuais intervenções legislativas. [...] Já foi dito que estamos diante de um conflito mais amplo entre um modelo liberal, hostil à regulação legislativa e favorável à auto-regulamentação (modelo norte-americano), e um modelo europeu baseado na lei e, logo, no proibicionismo.

Nesse mesmo enleio, afirma que nos Estados Unidos predomina a concepção de que o setor privado deve se autorregulamentar, a interferência estatal deve ser mínima. Diante do livre mercado, o tema da privacidade seria um diferencial competitivo e um requisito para se obter a confiança do consumidor, adotaram as empresas o modelo de observância de códigos de boas práticas (BENNETT, apud MENDES 2014).

Adotou-se assim um modelo tão somente setorial, atendendo questões específicas, sendo a primeira lei o *US Privacy Act of 1974*, que limita sua tutela aos indivíduos em face tão somente ao governo federal, sem se aplicar ao setor privado ou aos Governos Estaduais, tendo sua aprovação impulsionada pelo escândalo Watergate[47]. Ademais, outras

47 *The Watergate scandal, revelations of White House bugging, and Congressional investigations of domestic spying by the Central Intelligence Agency have served to underscore the developing paranoid theme of American life: Big Brother may be watching you! Proposals for national data banks, uses of surveillance helicopters by urban police forces, the presence of observation cameras in banks and supermarkets, and airport security searches of person and property are but some of the signs that our private lives are under such increasing scrutiny*. GREENWALD, Glenn. ***No Place to Hide****: Edward Snowden, the NSA, and the U.S. Surveillance State***.** Nova Iorque: Metropolitan, 2014.

leis posteriores criaram diversas exceções à proteção outorgada, tal qual o *US Foreign Intelligence Surveillance* e o escândalo Snowden, que demonstraram a sua não observância. A aplicação também é limitada, uma vez que apenas é aplicável a cidadãos estado-unidenses ou estrangeiros que estejam residindo de maneira permanente e legal nesse país.

Com o decorrer dos anos, criou-se um quebra-cabeça legislativo: observada a urgência de regulação de matérias sensíveis, foram promulgadas leis com a regulação específica, exemplificadamente: o *Fair Credit Reporting Act (FCRA),* em 1970, que protege contra práticas injustas e imprecisas de empresas que coletam informações para subsidiar análise de crédito; e o *Health Insurance Portability and Accountability Act* (HIPAA), de 1996, que regula o uso e a divulgação de Informações Protegidas de Saúde. Ademais, os próprios Estados Federados também promulgaram suas normativas sobre o tema.

Esse sistema setorial pode gerar distorções por conta de sua especificidade, tal qual o *Video Privacy Protection Act*, que tem por intuito a regulação do (antigo) mercado de aluguel de fitas de vídeo. Essa lei veio como resposta aos protestos populares decorrentes da publicação por um veículo de comunicação americano da lista de filmes que Robert Bork, à época indicado para a Suprema Corte de Justiça, havia previamente alugado. Isso sem mencionar as incoerências sistemáticas, como, por exemplo, sua não aplicação quando se trata de compra de filmes ou consumo no cinema ou mesmo em novos modelos atuais de consumo desse tipo de entretenimento, como o rol de filmes visualizados em plataformas de *streaming*.

De acordo com Gloria Gonzalez Fuster (2016), por conta da ausência de uma normativa horizontal, o sistema setorial dos Estados Unidos vem ficando cada vez mais isolado. Por seu turno, a influência do europeu está em evidente crescimento, mormente após a recente entrada em vigência do *General Data Protection Regulation*, que será analisada a seguir.

2.4 *GENERAL DATA PROTECTION REGULATION*

O desenvolvimento teórico e normativo europeu esteve na vanguarda da disciplina nas últimas décadas. Embora sejam documentos circunscritos aos países da Europa, a Convenção de Estrasburgo e a Diretiva 46/CE exerceram grande influência em países estrangeiros, não apenas pela estrutura normativa a ser seguida, mas também pelas suas previsões de fluxo internacional de dados, cujos países destinatários

devem possuir um "adequado nível de proteção de dados pessoais". Devido à recente promulgação e entrada em vigência do *General Data Protection Regulation*, com suas previsões de aplicações extraterritoriais, a tendência é a de que este influxo seja ainda crescente.[48]

Ademais, recentemente, em maio de 2018, consumidores de diversas nacionalidades, inclusive do Brasil, receberam notificações acerca da atualização de políticas de privacidade e requerimentos de consentimento para o tratamento de dados pessoais de empresas com quem mantinham relações: o *General Data Protection Regulation* entrou em vigor, sendo aplicada para além das fronteiras e sujeitos da União Europeia.

Em janeiro de 2012, os Estados-membros da União Europeia iniciaram o processo de revisão, compilação, uniformização e atualização das normativas até então vigentes. Decorreram-se quatro anos até se chegar ao texto consolidado, fruto de um processo de negociação com inúmeras emendas ao texto legal, com entraves às concepções nacionais preexistentes e às disparidades econômicas e competitivas. Finalmente, o *General Data Protection Regulation*, GDPR, com força vinculativa aos seus membros, foi promulgada em 2016, com *vacatio legis* de vinte e quatro meses, substituindo a Diretiva de Proteção de Dados Pessoais de 1995.

Prosseguindo-se à lógica proposta pela classificação geracional proposta por Viktor Mayer Schonberger, seria possível consignar que o GDPR inaugura uma quinta geração de normas. Além de sua relevância e abrangência, dispõe de uma arquitetura de controle que combina dois mecanismos: um deles centralizado no indivíduo e no consentimento; e

[48] A partir de uma análise da estrutura das leis de 39 países não europeus, identificou-se que 33 deles seguiam os estandartes Europeus estabelecidos, incluindo países da América Latina (GREENLEAF, 2012 apud LINKSEY, 2015). Sobre a implementação do modelo europeu e a criação ou atualização de leis gerais de proteção de dados, Nougrères (2017) entende que, apesar dos esforços impingidos para seguir o modelo do sistema europeu, ainda há muito a ser feito para que os níveis de proteção existentes na Europa sejam atingidos. Os principais pontos críticos seriam: a falta de harmonização normativa e de integração política e a ausência de uma estrutura supranacional latino-americana, tais fatores dificultariam a transferência de dados por conta da insegurança jurídica dos interessados; e a pouca independência e autonomia das autoridades de supervisão alocadas nos setores públicos, que também enfrentam limitados orçamentos.

outro ramificado e difuso, em que os diversos atores envolvidos no ecossistema de tratamento de dados devem observar os parâmetros estabelecidos e agir cooperativamente - controladores, processadores, autoridades de supervisão, certificadores - com o fito de se atingir à consecução dos objetivos da norma.

Para Bruno Bioni (2018), trata-se de um meio termo entre o Estado regulador e a autorregulação, que seria a meta-regulação ou regulação responsiva: o Estado, com a indicação das diretrizes e objetivos, delega aos atores participantes desse ecossistema a execução de tarefas regulatórias, cujos meios para se chegar lá ficarão a cargo destes.

Assumem relevância instrumentos como relatórios de impacto à proteção de dados pessoais, códigos de boas condutas, selos de certificação, ou seja, os próprios agentes econômicos, entidades de classe, entidades certificadoras de cada setor, tal como, saúde, aviação, varejista, deverão se articular para identificar os riscos específicos aos quais estão submetidos, cumprir os comandos legais e comprovarem que observaram as metas da regulação, incorporando a *accountability* nessa nova racionalidade regulatória, que possui a cooperação como ponto chave.

Existem discussões acerca dos pesos de cada um desses mecanismos, por exemplo, se o indivíduo no controle de dados pessoais é um protagonista ou atua de forma subsidiária às obrigações impostas aos controladores; ou se estes, conjuntamente com as autoridades de supervisão, são os novos personagens principais e, portanto, são predominantes.

Cediço que além da questão mencionada, existem diversos pontos de discussão e desacordo acerca da interpretação e aplicação do diploma legal, mormente por conta dos diferentes interesses dos atores envolvidos. Ademais, pelo curto período de vigência, muitos desafios teóricos e práticos ainda irão se apresentar[49]. Por exemplo, apesar de a

49 *At the time of the adoption of the Commission proposal for the General Data Protection Regulation, judge Masing, a member of the German constitutional court, wrote a newspaper article in which he criticised the fact that the entry into force of a directly applicable EU regulation dealing with a fundamental right could mean that certain fundamental rights in the German constitution could no longer be applied. Hence, to a certain extent Member States would be deprived of the power to protect the fundamental rights of their nationals.* VOIGT, Paul; Bussche, Axel von dem. ***The EU General Data Protection Regulation (GDPR).*** Londres: Springer, 2017.

norma estabelecer a ausência de distinções entre o setor público e o setor privado e dizer que ambos estão sujeitos às mesmas obrigações na condição de controladores, mantendo a diretriz já delineada desde a Convenção de Estrasburgo, na prática, por conta das diversas exceções inseridas sob o manto do interesse público (por exemplo, segurança nacional, segurança pública, investigações, acusações criminais), o caráter supostamente neutro da estrutura normativa é alterado, nos termos de Orla Linksey (2015).

Ocorre que, por conta do escopo deste trabalho, não é possível fazer uma análise aprofundada destes aspectos, cuja relevância deve ser reconhecida. Contudo, considera-se imprescindível trazer um panorama acerca dos principais pontos abordados pelo Regulamento.

Retomando ao GDPR, explicam Voigt e Bussche (2017) que seus principais objetivos são: (i) garantir um elevado nível de proteção dos dados pessoais à escala europeia, a fim de garantir a livre circulação de dados pessoais e estimular as empresas no mercado (semelhante ao intuito das primeiras regulações nacionais e supranacionais da década de 1980); (ii) harmonizar os estandartes de regulação, por conta das divergências de direitos e tratamentos na tutela da pessoa, oriundas da aplicação da Diretiva de Proteção de Dados em diferentes estados nacionais, o intuito foi trazer unificação das legislações; e (iii) criar mecanismos consistentes entre as autoridades de proteção de dados pessoais.

Consonante consigna Orla Linksey (2015), a regulamentação retirou quase todas as referências ao direito à privacidade que existiam na antiga diretiva, para tão somente dizer respeito à proteção de dados pessoais, corroborando, assim, com a corrente que defende a emancipação deste último.

A norma está dividida em onze diferentes capítulos, quais sejam: condições gerais; princípios; direitos do sujeito; controlador e processador; transferência de dados pessoais para outros países ou organizações internacionais; autoridades de supervisão independentes; cooperação; responsabilidades e penalidades; provisões relativas a situações específicas de processamento; atos de implementação e delegação; e provisões finais.

Em termos gerais, o GDPR se aplica tão somente aos dados de pessoas naturais vivas identificadas ou identificáveis, que são aquelas que podem ser identificadas direta ou indiretamente por uma referência que as identifica, seja nome, número de identificação (CPF, por exemplo), dados de localização ou até mesmo o conjunto de outras informações e fatores específicos concernentes à condição física,

psicológica, genética, econômica, cultural e de identidade social que permeiam qualquer pessoa natural.

Foi mantida a vedação prévia concernente aos dados sensíveis, ou seja, dados que revelam a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação a sindicatos, bem como aos dados relativos à vida sexual ou à orientação sexual de uma pessoa natural, relativos à saúde, à genética e a biometria (por exemplo, impressões digitais e imagens faciais), se processados com a finalidade de identificar exclusivamente uma pessoa.

Explicam Voigt e Bussche (2017) que a diferenciação da figura do controlador e do processador, já existente na Diretiva anterior, foi conservada. O controlador diz respeito à pessoa jurídica ou natural, autoridade pública ou agência que, sozinha ou em conjunto com outros, possui o domínio de todas as fases do tratamento de dados: planeja a estratégia de coleta, determina os propósitos e a forma do processamento de dados pessoais. Em outras palavras, o controlador deve assegurar a implementação de medidas técnicas e organizacionais para garantir que o processamento seja realizado de acordo com o GDPR. É ele quem decide quais dados serão coletados e processados, por quanto tempo estes dados serão armazenados e quem pode ter acesso a eles, devendo primar pela segurança dos dados transferidos, sendo que tudo deve estar documentado e monitorado para fins de fiscalização pela autoridade de supervisão.

Cabe ao controlador ainda se certificar de que os processadores observem as regras, uma vez que mantém com estes relação jurídica, sendo responsável seja pelo eventual dano que o processador venha a causar no caso de infração do Regulamento ou mesmo pela obrigação de informar a autoridade de supervisão no caso de falha interna ou de vazamento de dados, sempre dentro da maior brevidade possível.

Já o processador é aquele que processa a informação aos comandos do controlador, ou seja, é o responsável pela coleta, pelo armazenamento, pela estruturação, pela alteração, pela recuperação, pelo uso, pela divulgação por transmissão, pelo apagamento ou eliminação. São contratados pelos controladores e agem sob a coordenação destes para cumprir algumas funções do processamento de dados pessoais. Questões técnicas e menos cruciais, como a escolha do *hardware* ou *software*, também podem ser delegadas ao processador.

Segundo Voigt e Bussche (2017), uma diferença primordial existente entre controladores e processadores concerne à possibilidade de exploração comercial dos dados: enquanto a prática é permitida ao controlador, é vedada ao processador, que apenas pode utilizar os dados

de acordo com o propósito da coleta. Em que pese as maiores responsabilidades designadas à figura do controlador, este fato motiva a concentração de ambos em uma única pessoa, bem como a caracterização de *joint controller*, processador ou terceiro com poder de ingerência e decisão quanto à forma de coleta e as categorias de processamento.

Ademais, confidencialidade, integridade e disponibilidade do sistema devem ser garantidas por ambos, os quais ficam sujeitos a multas de até 20 milhões de euros ou 4 % do seu faturamento, podendo responder solidariamente com o controlador.

Pontua-se: ainda que somente um dos parceiros esteja instalado na União Europeia, o GDPR se aplica a ambos, ou seja, caso o controlador ou o processador estejam fixados em outro país, também devem observar as normas. A consequência disso é que não apenas os cidadãos e residentes na União Europeia que são protegidos pelo guarda-chuva normativo, mas todo e qualquer sujeito, independentemente de sua nacionalidade ou território também pode ser tutelado indiretamente, uma vez que as empresas que lhe prestam serviços estão submetidas à regulação.

Além do mais, o tema da jurisdição e da aplicação do GDPR é um dos pontos nevrálgicos da Regulação, não apenas porque se trata de um documento supranacional, mas porque, além da hipótese mencionada, também se aplica ao prestador de bem ou serviço, gratuito ou oneroso, que atue dentro da União Europeia, independentemente de onde estejam fixados o controlador ou o processador. Ademais, é vedada a transferência internacional de dados a países que não se adequem aos parâmetros mínimos de proteção da norma. Em suma, qualquer empresa do mundo pode se sujeitar ao GDPR caso ofereça seus serviços na União Europeia, estendendo as hipóteses de extraterritorialidade da norma.

Outra figura essencial do GDPR são as autoridades de supervisão que possuem poderes de investigação e sanção (tal qual a imposição de multas) prescritos pelo Regulamento e visando à tutela coletiva. Os procedimentos administrativos internos e a natureza jurídica, no entanto, não são pormenorizados no texto, ficando a cargo de cada membro nacional fazê-lo de acordo com seu ordenamento interno.

O consentimento aparece como instrumento legal individual para a permissão do tratamento dos dados pessoais, devendo conter indicação livre, específica, informada e inequívoca dos desejos do titular de dados, de maneira clara.

Além da possibilidade de tratamento de dados coletados com consentimento pessoal, a norma traz outras hipóteses: (i) se o tratamento for necessário para cumprir um contrato no qual titular dos dados faz parte ou esteja em fase de policitação, a fim de obter dados estritamente sobre o atendimento às exigências do contrato, não se estendendo à coleta e ao processamento de dados que não possuam correlação com os objetivos do contrato; (ii) se o processamento for necessário para o controlador cumprir uma obrigação legal; (iii) se o processamento for necessário para proteger os interesses vitais de alguém, como por razões de segurança ou proteção de interesses econômicos, por exemplo; (iv) se o processamento for necessário para uma tarefa realizada no interesse público ou no exercício da autoridade oficial investida no controlador; (v) e se o processamento for necessário para fins de interesses legítimos do responsável pelo tratamento ou de um terceiro, entendido este como pesquisa científica ou histórica, ressalvado quando esses interesses forem sobrepostos pelos interesses, direitos ou liberdades do titular dos dados.

Todos os dados devem ser processados dentro da legalidade, de maneira transparente, e somente serão coletados para fins específicos, explícitos e legítimos, sendo vedado o processamento se houver alteração de finalidade, salvo se: (i) o controlador obtiver novo consentimento do titular dos dados; (ii) a alteração estiver baseada em uma lei da União Europeia ou de Estado-Membro que constitua medida para salvaguardar segurança nacional, defesa, segurança pública; ou (iii) for compatível com a finalidade para a qual os dados pessoais são inicialmente coletados.

Igualmente, algumas categorias de processamento consideradas especiais, como aquelas que lidam, por exemplo, com dados sensíveis, são em regra proibidas pelo GDPR. Contudo, existem exceções, sendo elas: (i) preexistência de uma base para processamento de informação pessoal; (ii) consentimento explícito e documentado; (iii) proteção do bem público, do próprio sujeito dos dados ou da coletividade, sendo esta última invocada principalmente por instituições e autoridades públicas.

Todo o exposto até o momento são amostras de mecanismos apostos na norma com o fito de efetivar os seus princípios e a incorporação de padrões mínimos de proteção. De acordo com Calder (2018), em relação às restrições e à observância de requisitos para coleta e tratamento de dados quando ausente o prévio consentimento, por exemplo, executam-se os princípios da limitação de finalidade, de respeito à legalidade e minimização e precisão de dados (os dados processados devem ser precisos e atualizados, bem como relevantes e

limitados ao que é necessário em relação aos fins para os quais são processados).

Outro exemplo de padrões a serem seguidos são as políticas a serem aplicadas pela iniciativa privada em relação a estandartes mínimos de proteção. Conforme pontuado por David Wright e Paul de Hert (2016), um deles se refere ao *Privacy by Design*, baseado no planejamento de estratégias e no estabelecimento prévio de ferramentas preventivas para o processamento de dados, tanto de *softwares* quanto de *hardwares*, visando a um processamento o menos invasivo possível, em observância ao princípio de minimização de dados. Por seu turno, relacionado principalmente ao princípio da finalidade, o *Privacy by Default* limita a coleta de dados para aqueles que sejam necessários tão somente para o propósito específico do tratamento de dados, abarcando a quantidade de dados pessoais coletados, a extensão de seu processamento, o período de armazenamento e sua acessibilidade.

Outros importantes princípios elencados são: limitação de armazenamento (os dados pessoais podem ser armazenados pelo período em que ainda estejam vigentes os propósitos especificados); integridade e confidencialidade; transparência, que se correlaciona ao binômio dever de informar e direito de ser informado, por exemplo, acerca da identidade do controlador, dos propósitos do processamento; obtenção de confirmação e comunicação das atividades de processamento efetuadas com base nos seus dados pessoais; e *accountability*, inexistente termo fungível no português para sua justa tradução, no entanto, seus elementos auxiliam a compreender a extensão do seu significado: imputar-se ao responsável pelo tratamento de dados, no caso, o controlador, a garantia da conformidade com o GDPR; e sua capacidade de comprová-la junto às Autoridades de Supervisão.

Nesse sentido, ensinam David Wright e Paul de Hert (2016) que a norma introduz o *privacy through accountability* enquanto um novo modelo de regulação e de governança de dados, cujos atores privados e públicos atuam conjuntamente, de maneira até mesmo simbiótica, tanto na esfera nacional quanto na comunitária.

Com efeito, é notável a aproximação entre a esfera pública e a esfera privada, que devem atuar cooperativamente a fim de que seja alcançada a máxima conformidade ou *compliance a*os ditames legais, imprescindível para a interação entre ambos os campos. Por exemplo, não basta ao controlador demonstrar que está de acordo com as normas, deve também facilitar o acesso e a fiscalização pelas autoridades supervisoras; e deve notificar, o mais brevemente possível, as

autoridades centrais acerca de vulnerabilidades de segurança ou vazamento de dados.

Explicam Voigt e Bussche (2017) que um dos instrumentos práticos concernentes à aplicação do GDPR diz respeito à adoção e à aplicação de Códigos de Conduta. Embora estes não possuam diretamente reconhecimento legal, auxiliam na prova de cumprimento da conformidade ou *compliance* dos controladores e processadores junto às autoridades supervisoras. Da mesma forma atuam as Certificações, auxiliando na verificação de *accountabilty* e *compliance* das operações de controle e processamento com o GDPR por parte das autoridades supervisoras. Por corolário, ao alcançá-la elevam o nível de segurança e proteção dos seus consumidores em relação aos produtos e serviços prestados. O procedimento de certificação pode ser procedido tanto pelas autoridades de supervisão, como por organismos independentes, os quais devem preencher uma série de condições e critérios a fim de se credenciar como entidade de certificação, obedecendo ao GDPR e às exigências locais de cada autoridade para sua constituição.

Diante do que foi exposto, é possível depreender que, visando à tutela do titular de dados pessoais, o rol de princípios assentado, se comparado ao da Convenção de Estrasburgo, foi expandido e detalhado, sendo estes implementados por instrumentos e ferramentas, como aquelas mencionadas anteriormente. Ademais, correlacionam-se aos direitos ali garantidos, por exemplo, o direito à informação, que está intimamente ligado ao princípio da legalidade e ao da transparência, instituindo o dever de informar do controlador e do processador. Assim, as informações sobre o processamento de dados, bem como sobre os direitos do detentor e como exercê-los devem estar colocadas num documento chamado *Privacy Notice*, o qual deve ser conciso, transparente e inteligível, além de ser acessível, com linguagem clara e simples.

Devido à disparidade técnica, econômica e jurídica existente nas relações de tratamento de dados, o direito à informação (desde a concepção da privacidade como autodeterminação informativa) foi tido como basilar e fundante, uma vez que somente a partir de seu exercício o titular de dados pôde obter conhecimento de ferramentas para exercer todos os seus direitos específicos relacionados à gestão de seus dados.

Logo, o sujeito possui o direito de saber, por exemplo, se o processamento é realizado na própria pessoa do controlador ou por um terceiro processador; qual a finalidade do processamento; as categorias de dados pessoais em causa; o período de armazenamento previsto ou, se não for possível, os critérios para determinar esse período; para quem

os dados foram transferidos - principalmente se a outros países ou a organizações internacionais.

Intimamente ligado ao direito à informação está o direito ao acesso, que igualmente se constitui como um dos pilares da proteção de dados, uma vez que instrumentaliza o direito à informação e é a fonte a partir da qual se desdobram outros direitos, tais como o direito à retificação, à objeção e à justa decisão.

De acordo com Calder (2018), a ferramenta prática é chamada *data subject access request* (DSAR), e o prazo para a resposta do controlador é de até um mês, sendo que a negativa injustificada ou uma resposta inadequada pode, no futuro, desencadear reclamação para uma autoridade de supervisão, uma ação judicial ou mesmo ambos.

Verificada a existência de algum equívoco, o sujeito possui o direito de ter seus dados corrigidos e removidos ou ainda o direito de que seu processamento seja restrito pelo controlador. Ou seja, relacionado à ideia inicial da autodeterminação informacional – o que demonstra a relevância da decisão do Tribunal Constitucional Alemão –, o titular de dados tem o direito de interferir nas fases de seu processamento, podendo solicitar a retificação de dados incorretos, a eliminação de dados imprecisos ou desnecessários, bem como manifestar a oposição e solicitar ainda a restrição no processamento quando houver extrapolação das finalidades do controlador.

Quando existe alguma requisição de retificação por parte do sujeito, a organização não é automaticamente obrigada a atendê-la caso esteja em exercício regular de direito; se a manutenção for necessária para proteger o direito à liberdade de expressão e à informação; para cumprir outra obrigação nacional ou da União Europeia; para cumprir interesse público ou exercício de autoridade oficial, sendo responsável pelos riscos de sua decisão de manutenção.

Por seu turno, o direito à objeção se refere aos casos quando ausente o consentimento do titular de dados, que pode então questionar e refutar a justificativa na qual o controlador se baseia, seja no interesse legítimo, no interesse público ou no processamento para fins estatísticos ou de pesquisa e até de marketing direto (nesses casos, os controladores devem desenvolver um método simples de remover os dados pessoais). O ônus da prova neste caso é do próprio controlador, o qual deve demonstrar que está resguardado sob uma dessas três hipóteses.

Além disso, o GDPR estabelece o direito à apropriada decisão, ou seja, veda que decisões que possam acarretar consequências na esfera de liberdades e direitos do titular de dados estejam baseadas tão somente em um processo automatizado de dados. Destarte, possui o direito de

conhecer os motivos considerados primordiais para a decisão que lhe foi dada e solicitar a intervenção humana. Contudo, há exceção: se houver previsão contratual de que esta decisão seja necessária para a celebração do negócio jurídico, desde que amparado pelos objetivos contratuais que as partes acordaram.

Consonante Voigt e Bussche (2017), o GDPR introduziu dois outros direitos que ainda não estavam no catálogo: o direito à portabilidade e o *right to be forgotten*. O direito à portabilidade se refere à possibilidade do consumidor de solicitar que suas informações constantes em base de dados sejam transferidas de um controlador para outro, independentemente de sua motivação.

O *right to be forgotten* ou direito ao esquecimento se apresenta como um derivado e uma consequência do *right to erasure* ou direito à exclusão ou direito ao apagamento. Neste, o titular pode demandar a exclusão de seus dados pessoais caso tenham sido coletados de maneira ilegal, tenha havido a perda superveniente do legítimo interesse ou a retirada do consentimento. Por corolário, caso os dados estejam *online*, ou seja, tenham sido publicados para um número indefinido de pessoas, é possível exercer o *right to be forgotten* a fim de se providenciar a retirada de links, cópias ou replicações desses dados pessoais.

Por fim, a norma ressalva os casos de colisão e de conciliação com outros direitos, tal qual o direito à liberdade de expressão e informação, incluindo o processamento de dados por propósitos jornalísticos, acadêmicos, artísticos ou literários. Aos controladores e processadores que estão sujeitos à obrigação profissional de sigilo (advogados ou médicos, por exemplo), está estipulada a exceção da obrigação de fornecer informações ou acesso a dados pessoais às autoridades de supervisão.

2.5 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LEI n. 13.709/2018

Apesar da efervescência do tema e do início da regulação da proteção de dados pessoais na Europa desde a década de 1970, conforme levantamento feito por Nelson Angarita Remolina, citado por Zanatta (2015), na América Latina o avanço da matéria se iniciou nos anos 2000[50], com a proliferação de normas específicas em que se verifica

50 Conforme se extrai de tabela ilustrativa, foram promulgadas as Leis nos seguintes países seguintes: Argentina, Lei 25.326/2000; Chile, Lei 19.628/1999, Lei 19.812/2002 e Lei 20.575/2012; Colômbia, Lei 1.581/2012; Costa Rica, Lei

forte influência europeia, identificando-se três tendências: "(i) a positivação de direitos de proteção de dados pessoais, (ii) a criação de autoridades administrativas independentes ou semi-independentes para proteção de dados pessoais, e (iii) a criação de instrumentos jurídicos específicos para proteção de tais direitos" (ZANATTA, 2015, p. 454).

No Brasil, por seu turno, a matéria apenas foi estritamente regulada em agosto de 2018, quando promulgada a Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, conhecida pelo acrônimo LGPD. Não é possível afirmar, todavia, que havia até então um vácuo normativo a ponto de inviabilizar qualquer proteção coletiva ou individual, conforme breve retrospecto.

No que se refere à privacidade em sentido amplo, além das previsões da Constituição Federal, consubstanciadas no art. 5º, X a XII, que estabelecem como direito fundamental a inviolabilidade da vida privada, inviolabilidade de domicílio e sigilo das comunicações, respectivamente, no plano infraconstitucional, foram reconhecidos o sigilo fiscal e bancário (Lei Complementar n. 104/2001), bem como a privacidade como direito da personalidade no Código Civil.

Concernente à proteção de dados pessoais, a Constituição Federal instituiu o *Habeas Data* como remédio constitucional e, no plano infraconstitucional, normas que tangenciam o tema, tais como: o Código de Defesa do Consumidor; a Lei Geral de Telecomunicações (Lei n. 9472/1997); o Marco Civil da Internet (Lei n. 12.965/2014); a Lei do Cadastro Positivo (Lei n. 12.414/2011); a Lei de Acesso à Informação (Lei n. 12.527/2011); e o Marco Civil da Internet (Lei n. 12.965/2014).

Essa multiplicidade formou um mosaico normativo em relação à proteção de dados que dificultava sua instrumentalização, mesmo com recursos como interpretação e integração tendo em vista a ausência uma regulação explícita e ampla que pudesse concatená-las.

Segundo Jhonatan Assman (2014), um dos motivos para o atraso no Brasil (e na América Latina), atine à falta de estabilidade político-institucional, afinal, o país viveu sob regime militar por mais de duas décadas, ausente o interesse de fortalecer a posição jurídica dos cidadãos enquanto detentor do direito de acessar as informações obtidas e armazenadas sobre ele. Inclusive, a previsão do remédio constitucional

---

8.968/2011; México, Lei Federal 05-07-2010; Nicarágua, Lei 787/202; Paraguai, Lei 1.682/2012 e Lei 1.691/2002; Peru, Lei 29733/2011; e Uruguai, Lei 18.311/2008). (Zanatta, 2015, p. 453)

Habeas Data[51] *(*artigo 5º, LXXII, da Constituição Federal) é tida como uma resposta ao passado, uma motivação imediata à ditadura militar.

Conforme aduz Luís Roberto Barroso (2001), não apenas a violência física era utilizada como ferramenta de opressão, mas também o uso indevido de informações sobre a vida dos cidadãos: "Inicialmente, tais dados, muitas vezes obtidos de forma ilegal, forneciam a matéria-prima que alimentava a perseguição política, mesmo quando não havia qualquer imputação formal de violação da ordem jurídica" (p. 199).

José Carlos Barbosa Moreira (1998, p 49) comenta a atuação discricionária nesse regime de exceção:

> Informações aleatoriamente colhidas, em fontes de discutível idoneidade e por meios escusos, não raro manipuladas sem escrúpulos, ou mesmo fabricadas pela paranóia de órgãos repressivos, viram-se incorporadas a registros oficiais ou paraoficiais e passaram a fornecer critérios de avaliação para a imposição de medidas punitivas ou discriminatórias. Tais critérios eram insuscetíveis de objeção e discussão, até pelo

51 Relata José Afonso da Silva: "A partir dessas constatações, propusemos perante a Comissão Provisória de Estudos Constitucionais (Comissão Afonso Arinos) um Anteprojeto de Constituição cujo art. 17 reconhecia o direito nos termos seguintes: "1. Toda pessoa tem direito de acesso aos informes a seu respeito registrados por entidades públicas ou particulares, podendo exigir a retificação de dados, e a sua atualização. 2. É vedado o acesso de terceiros a esse registro. 3. Os informes não poderão ser utilizados para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa ou vida privada, salvo quando se tratar do processamento de dados estatísticos não individualmente identificáveis. 4. Lei federal definirá quem pode manter registros informáticos, os respectivos fins e conteúdo". No art. 31 instituímos o remédio constitucional específico: "conceder-se-á habeas data para proteger o direito à intimidade contra abusos de registros informáticos públicos e privados", curto e seco como se vê. O Anteprojeto da Comissão acolheu a declaração do direito em seu art. 17 com aperfeiçoamentos e o remédio no art. 48: "Dar-se-á *habeas data* ao legítimo interessado para assegurar os direitos tutelados no art. 17". Daí saiu para o debate constituinte, andando o deito e sua garantia específica em dispositivos separados até que no Projeto da Comissão de Sistematização fosse aprovado num único dispositivo, ou seja: reconhecia-se o direito mediante sua garantia específica (art. 6º §52). Daí sofreu modificações para pior até o texto do atual, art 5º, LXXII, objeto de nossas considerações no texto". SILVA, José Afonso da. Curso de Direito Constitucional Positivo. 36 ed. São Paulo: Malheiros, 2012, p. 457.

> simples e óbvio motivo de que os interessados não tinham acesso aos dados constantes dos registros. Ninguém pode sequer tentar demonstrar a falsidade ou incorreção de algo que ignora em que consiste... Situação desse gênero foi literariamente imortalizada pela pena de Kafka.

Para o autor, o *Habeas Data* vem como instrumento a concretizar o direito que qualquer cidadão possui de ter conhecimento do que outros "sabem ou supõem saber a seu respeito, nem a possibilidade de contestar a exatidão de tais noções e, sendo o caso, retificar o respectivo teor, principalmente quando a utilização dos elementos coligidos seja capaz de causar dano material ou moral (1998, p. 49-50)". Apesar da aplicabilidade imediata da norma, o remédio foi regulamentado pela Lei n. 9.507/1997, chancelando soluções propostas em sede doutrinária e jurisprudencial existentes até aquele momento.

Porém, para Gilmar Ferreira Mendes (2013, p. 634) atualmente o remédio não traduz de forma integral a preocupação que circunda a proteção de dados pessoais, porquanto a utilização prática do instrumento tenha ficado restrita ao conhecimento e à retificação de dados existentes somente em bancos de dados de caráter público: "o *habeas data* acabou por se constituir em instrumento de utilidade relativa na Constituição de 1988. Talvez isso se deva, fundamentalmente, à falta de definição de um âmbito específico de utilização não marcado por contingências políticas".[52]

Destacam-se possíveis razões pela qual o instrumento é pouco utilizado: (i) a necessidade de estar representado por advogado em juízo, o que, consequentemente, demanda despesas (apesar de ser isento de custas processuais); (ii) a impossibilidade de em um mesmo *writ* obter o acesso à informação e sua retificação, sendo necessária a propositura de duas diferentes ações[53]; e (iii) a necessidade de "esgotamento das vias administrativas" e sua comprovação.

---

[52] Em fevereiro de 2019, o autor, que também ocupa o cargo de Ministro do Supremo Tribunal Federal, foi alvo de vazamento de dados, de maneira alegadamente ilegal, pela Receita Federal. Veja-se: Vazamento de dados do ministro Gilmar Mendes preocupa comunidade jurídica. Disponível em: https://www.conjur.com.br/2019-fev-08/vazamento-dados-gilmar-mendes-preocupa-comunidade-juridica?utm_source=dlvr.it&utm_medium=twitter Acesso em: 11 de fevereiro de 2019

53 Veja-se entendimento do Superior Tribunal de Justiça: 1" Em razão da necessidade de comprovação de plano do direito do demandante, mostra-se

Para Andres Guadamuz (2001), conquanto seja um instrumento importante de inovação institucional latino-americano[54], apresenta limitações no que tange à efetiva proteção de dados pessoais. Observa ainda o autor que, apesar do berço do *habeas data* ter sido no Brasil, a legislação que a regulamenta, comparativamente à de outros países da mencionada divisão geopolítica, é a menos desenvolvida, cujos pontos negativos seriam: (i) a ausência de previsão para exclusão de dados falsos; (ii) a impossibilidade de aceder a dados de empresas privados; e (iii) a dificuldade de juristas e dos Tribunais compreenderem temas técnicos relacionados à informática e à base de dados.

Outrossim, a Constituição Federal prevê a defesa do consumidor como direito fundamental, nos termos do art. 5º, XXXII; e como princípio da ordem econômica, nos termos do art. 170, IV; assim, há de se destacar o Código de Defesa do Consumidor (Lei n. 8.078/90), uma lei principiológica que se destina a efetivar e a instrumentalizar tais mandamentos constitucionais a fim de sistematizar e ordenar a tutela ao consumidor, que se irradia a todos os ramos do Direito onde se verifica a existência de relações de consumo.

Igualmente, Laura Schertel Mendes (2014, p. 200) comenta que os princípios e conceitos abertos constantes no Código de Defesa do Consumidor demonstram a capacidade da norma "de se adaptar a novas

---

inviável a pretensão de que, em um mesmo habeas data, se assegure o conhecimento de informações e se determine a sua retificação. É logicamente impossível que o impetrante tenha, no momento da propositura da ação, demonstrado a incorreção desses dados se nem ao menos sabia o seu teor. Por isso, não há como conhecer do habeas data no tocante ao pedido de retificação de eventual incorreção existente na base de dados". 2. "O fornecimento de informações insuficientes ou incompletas é o mesmo que o seu não fornecimento, legitimando a impetração da ação de *habeas data*." Conforme exposto, a recusa do acesso às informações, bem como da retificação das informações inexatas, ensejam a interposição do habeas data. BRASIL. Superior Tribunal de Justiça. Acórdão nº HD 160. Relator: Ministra Denise Arruda. **Diário Oficial da União**. Brasília. Julgado em: 22/09/2008.

54 O autor assevera o seguinte: *Following the Brazilian example, Paraguay incorporated the Habeas Data right to its new Constitution in 1992. After that, many countries followed suit and adopted the new legal tool in their respective constitutions: Peru in 1993, Argentina in 1994, Ecuador in 1996, and Colombia in 1997. Habeas Data is gaining momentum and moving northwards. There are projects to incorporate the new right in Guatemala, Uruguay, Venezuela and Costa Rica, and several important writers and political groups support the implementation of the figure both in Panama and in Mexico*. (GUADAMUZ, 2001)

demandas e de oferecer novas respostas foi fundamental para o desenvolvimento continuo de mecanismos de proteção da personalidade do consumidor, inclusive contra os riscos advindos do processamento de dados pessoais".

A desigualdade existente na relação jurídica entre fornecedor e consumidor é fundamento da presumível vulnerabilidade deste último. Por conseguinte, visando ao equilíbrio contratual das partes, justifica-se tanto a existência de normas protetivas aos consumidores, quanto seu reconhecimento como princípio autônomo, uma vez que o fornecedor é quem detém o conhecimento técnico, jurídico e econômico do bem ou serviço ofertado, ou seja, de toda a cadeia de produção e do ciclo de consumo.

Na seara consumerista, para tutela do consumidor, destacam-se: (i) o binômio direito-dever à informação clara, suficiente e adequada como alicerce nas relações de consumo, nos termos do art. 6º[55] e art. 8º[56] do Código de Defesa do Consumidor, os quais mantêm paralelo com o direito à informação medular à proteção de dados; (ii) a vedação às práticas abusivas, que impõem barreiras à atividade econômico-comercial do fornecedor, e, especificamente, ao uso indiscriminado de informações acerca do consumidor[57]; e (iii) a existência de um Sistema Nacional de Defesa do Consumidor e de mecanismos para a realização da Política Nacional de Relações de Consumo.

O Código de Defesa do Consumidor possui uma seção específica denominada "Dos Bancos de Dados e Cadastros de Consumidores". Originariamente, possuía estes três enunciados normativos, contudo, o que estipulava multa civil por infrações[58], fora vetado sob o argumento

55 Art. 6º São direitos básicos do consumidor: [...] III - a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem;

56 Art. 8° Os produtos e serviços colocados no mercado de consumo não acarretarão riscos à saúde ou segurança dos consumidores, exceto os considerados normais e previsíveis em decorrência de sua natureza e fruição, obrigando-se os fornecedores, em qualquer hipótese, a dar as informações necessárias e adequadas a seu respeito.

57 Art. 39. É vedado ao fornecedor de produtos ou serviços, dentre outras práticas abusivas: V - exigir do consumidor vantagem manifestamente excessiva;

58 A redação do enunciado normativo era a seguinte: "Art. 45 - As infrações ao disposto neste Capítulo, além de perdas e danos, indenização por danos morais, perda dos juros e outras sanções cabíveis, ficam sujeitas à multa de natureza

de que "O art. 12 e outras normas já dispõem de modo cabal sobre a reparação do dano sofrido pelo consumidor". A supressão deste retirou mecanismos específicos de *enforcement*, que poderia coibir a prática de condutas abusivas.

Remanesceram então o art. 43 e o art. 44. Este último estabelece, em síntese, a obrigação de órgãos públicos de defesa do consumidor de registrarem reclamações feitas por consumidores em face de fornecedores, sendo tal banco de dados de livre acesso e consulta. Por seu turno, o art. 43 disciplina o seguinte: (i) princípio da qualidade dos dados, consubstanciado na linguagem clara, verdadeira e de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos (art. 43, §1º); (ii) princípio da transparência, consubstanciada na obrigação de comunicação de abertura de cadastro ou registro de dados pessoais (art. 43, §2º); (iii) o direito de acesso e retificação (art. 43, § 3º); (iv) direito à exclusão quando consumada a prescrição relativa à cobrança de débitos do consumidor pelos respectivos sistemas de proteção ao crédito (art. 43, §5º).

Ocorre, no entanto, que esses dois únicos artigos não regulam suficientemente a proteção de dados pessoais. Por exemplo: a despeito de o parágrafo terceiro assentar a possibilidade de correção de dados inexatos, não há estipulação clara e detalhada acerca da forma de aceder à base a fim de saber, afinal, quais os dados estão ali armazenados e, identificada imprecisão, solicitar a retificação. A ausência do princípio da finalidade também contribui para sua erosão.

Mesmo com os esforços da sociedade civil organizada e do Ministério Público, a vagueza e as lacunas existentes dificultaram o reconhecimento, pelo judiciário e por órgãos administrativos do governo, de diversas práticas como abusivas, e, consequentemente, os avanços na matéria. Na realidade, o seu exercício e a sua aplicabilidade, com efetivo reconhecimento de violação à direito da personalidade do consumidor, principalmente no âmbito judicial, ficaram restritos ao sistema de proteção ao crédito, de acordo com as delimitações redacionais existentes tanto no parágrafo primeiro, quanto no parágrafo quinto.

Tamanha importância do setor de concessão de crédito que foi editado um diploma específico: a Lei do Cadastro Positivo, Lei n.

---

civil, proporcional à gravidade da infração e à condição econômica do infrator, cominada pelo juiz na ação proposta por qualquer dos legitimados à defesa do consumidor em juízo".

12.414/2011, cuja função, consoante Cláudia Lima Marques, Antônio Herman Benjamin e Bruno Miragem é "a manutenção e acesso dos fornecedores em banco de dados de informações positivas diz respeito a uma redução dos riscos do inadimplemento". (2010, p. 291)

Na realidade, trata-se de dois interesses contrapostos: a busca pelo crédito pelo consumidor e a diminuição dos riscos para os mutuantes. Os autores alertam sobre a prática:

> [...] ao mesmo tempo em que é legítimo aos fornecedores organizar e explorar as informações pessoais e econômicas dos consumidores, por outro lado há a necessidade de proteger o consumidor em relação ao mau uso destas informações, o que ocorre quanto isto se dá em prejuízo aos direitos da personalidade, como o direito à honra ou direito à privacidade, assim como a divulgação de informações incorretas e inverídicas termina por causar danos aos consumidores. (2010, p. 294)

No final do ano de 2010, após aprovação das duas Casas Legislativas, foi para sanção presidencial o Projeto de Lei n. 263/04, que incluía ao art. 43 do Código de Defesa do Consumidor um novo parágrafo referente à coleta de dados referente ao adimplemento e informações positivas do consumidor.

Este, todavia, fora vetado integralmente pelo Presidente à época, Luís Inácio Lula da Silva, sob a motivação da falta de clareza quanto às definições das categorias básicas relacionadas ao novo instituto, conforme entendimento emanado pelo Ministério da Justiça:

> O texto que trata de formação de cadastro positivo, tal como apresentado, pode redundar em prejuízos aos cidadãos, posto que traz conceitos que não parecem suficientemente claros, o que é indispensável à proteção e defesa do consumidor, ao incremento da oferta de crédito, à promoção de relações de consumo cada vez mais equilibradas e à proteção da intimidade e da privacidade das pessoas.

Em seguida, com o desiderato de instituir e disciplinar a matéria do Cadastro Positivo com maior detalhamento e garantias ao

consumidor, o mencionado Presidente promulgou a Medida Provisória n. 518/2010, convertida em Lei, cujo objetivo é disciplinar 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.

Em comparação ao Código de Defesa do Consumidor, pode-se dizer que a Lei trouxe avanços à matéria, estabelecendo: o direito ao cancelamento do cadastro (art. 5º, I); direito ao acesso, à objeção e à retificação de dados (art. 5º, II e III); a vedação ao armazenamento de informações sensíveis e excessivas (art. 3º, §3º); o consentimento informado em instrumento específico (art. 4º); a possibilidade de solicitar revisão de decisão realizada exclusivamente por meios automatizados (art. 5º, VI).

O princípio da finalidade da coleta de dados aparece diversas vezes no diploma (arts. 2º, I; 5º, VII, e 7º), e determina que as informações armazenadas nos bancos de dados somente poderão ser utilizadas somente de acordo com a finalidade para a qual foram coletados, ou seja, para a "realização de análise de risco de crédito do cadastrado" ou para "subsidiar a concessão ou extensão de crédito e a realização de venda a prazo ou outras transações comerciais". Nesses casos, a "informação" recebe diversos adjetivos, a fim de minudenciar a extensão de sua utilização, explicam Tartuce e Neves (2017, não p.):

> Informações objetivas: aquelas descritivas dos fatos e que não envolvam juízo de valor; Informações claras: aquelas que possibilitem o imediato entendimento do cadastrado independentemente de remissão a anexos, fórmulas, siglas, símbolos, termos técnicos ou nomenclatura específica; Informações verdadeiras: aquelas exatas, completas e sujeitas à comprovação; Informações 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.

Relacionado ao tema, o Superior Tribunal de Justiça julgou em sede de demanda repetitiva o Recurso Especial nº 1.419.697-RS que versava acerca da controvérsia do *credit scoring*: sistemas de ranqueamento de consumidores, utilizando matemática avançada, modelagem estatística e algoritmos para prever o comportamento futuro, avaliar os riscos e essencialmente determinar como tratar diferentes

consumidores. No caso de mutuantes, avalia-se o risco de crédito para cada tomador, com base em fatores predeterminados que influenciam o nível de risco no empréstimo.

O ponto nevrálgico da demanda consistia na análise acerca da necessidade, ou não, do consentimento do consumidor acerca do emprego deste método: se fosse considerado um "banco de dados", este seria imprescindível. Neste caso, haveria violação legal, cabendo indenização por dano moral aos consumidores; se fosse considerado apenas uma ferramenta matemática de análise de risco, não haveria infração, e, portanto, não haveria o que se falar em dano.

O Ministro Relator, Paulo de Tarso Sanseverino, seguido do voto dos outros Ministros, entendeu que o *credit scoring* seria mero instrumento matemático aplicável, sendo despicienda qualquer anuência do consumidor e, sucessivamente, fixou teses acerca de parâmetros mínimos para o funcionamento desses sistemas, em que se definiu:

> a) é um método desenvolvido para avaliação do risco de concessão de crédito, a partir de modelos estatísticos, considerando diversas variáveis, com atribuição de uma pontuação ao consumidor avaliado (nota do risco de crédito); b) essa prática comercial é lícita, estando autorizada pelo art. 5º, IV, e pelo art. 7º, I, da Lei 12.414/2011 (Lei do Cadastro Positivo); c) na avaliação do risco de crédito, devem ser respeitados os limites estabelecidos pelo sistema de proteção do consumidor no sentido da tutela da privacidade e da máxima transparência nas relações negociais, conforme previsão do CDC e da Lei 12.414/2011; d) apesar de desnecessário o consentimento do consumidor consultado, devem ser a ele fornecidos esclarecimentos, caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem como as informações pessoais valoradas; e) o desrespeito aos limites legais na utilização do sistema credit scoring, configurando abuso no exercício desse direito (art. 187 do CC), pode ensejar a responsabilidade objetiva e solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente (art. 16 da Lei 12.414/2011) pela ocorrência de danos morais nas hipóteses de utilização de informações excessivas ou sensíveis

> (art. 3º, § 3º, I e II, da Lei 12.414/2011), bem como nos casos de comprovada recusa indevida de crédito pelo uso de dados incorretos ou desatualizados" (STJ – REsp 1.419.697/RS – Rel. Min. Paulo de Tarso Sanseverino – j. 12.11.2014).

Em seguida, o acórdão foi objeto de verbete da Súmula 550: "A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo".

Tal decisão foi recebida de maneira dúbia por entidades de defesa do consumidor e pela academia: conquanto se tenha reconhecido avanços, diversas críticas foram despendidas. Com efeito, qualquer *score* é um algoritmo, porém, sua eficácia e acurácia de aplicação dependem de enorme volume de dados, ou seja, indispensável um banco de dados para que atinja sua finalidade. Dessa forma, percebe-se que mesmo com a vigência do Código de Defesa do Consumidor e da Lei do Cadastro Positivo, que possuem previsões expressas, o consentimento foi considerado despiciendo, sendo o consumidor preterido neste caso.

Por outro lado, também ficou reconhecido o progresso da jurisprudência acerca da matéria, porque fixou expressamente o princípio da transparência e condicionou a licitude do funcionamento dos sistemas às balizas e diretrizes legais reconhecendo a tutela dos dados pessoais, tais como o direito de acesso, direito à retificação e à objeção.

A configuração da responsabilização civil restou condicionada ao descumprimento dos parâmetros fixados, sendo esta objetiva e solidária entre o fornecedor de serviços, do responsável pelo banco de dados, da fonte e do consulente, nos termos da Lei do Cadastro Positivo e em consonância com o Código de Defesa do Consumidor.

Por fim, o Marco Civil da Internet, Lei nº 12.965 de 2014, tem por escopo determinar princípios, garantias, direitos e deveres para o uso da internet no Brasil, tanto para usuários como para provedores que participam da cadeia de serviços. Consoante Marcel Leonardi (2014, p. 622), a norma trouxe "sólidos princípios reconhecidos globalmente como o arcabouço mínimo necessário para fomentar uma internet livre e equilibrada, preocupada tanto com a inovação quanto com direitos fundamentais".

A privacidade e a proteção de dados pessoais foram abordadas expressamente pelo Marco Civil da Internet no seu rol de princípios (artigo 3º, II e III, respectivamente). Por seu turno, o Decreto nº 8771/2016 traz as definições legais relativas a "dado pessoal", de acordo com vertente expansionista, bem como a "tratamento de dados pessoais", de acordo com seu art. 14.

Questões relacionadas ao consentimento, à transparência, à finalidade também são abordadas na norma. No rol dos direitos assegurados aos usuários (artigo 7º, I), elencam-se os direitos: (i) informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, de acordo com as finalidades que justifiquem sua coleta e especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; (ii) o consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais (ii) não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado, ou nas hipóteses previstas em lei; e (iv) exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros

Esses dois últimos itens listados se relacionam com um dos pontos de maiores controvérsias dentro do Marco Civil da Internet: a obrigatoriedade imposta aos provedores de conexão e de aplicação para a guarda de dados de conexão e de acesso à aplicação dos usuários, (endereços IP utilizados durante o acesso à internet, datas e horários de *login* e *logout*, nome de usuário utilizado) de maneira indistinta. Marcel Leonardi (2015, p. 624) entende que a guarda obrigatória foi um retrocesso normativo e comenta o seguinte:

> Em sua versão original o Marco Civil da Internet privilegiava o modelo de preservação de dados, impondo a provedores de conexão e de aplicações que recebem uma ordem judicial o dever de preservar, a partir daquele momento, dados específicos de usuários determinados, suspeitos de terem praticado crimes ou atos ilícitos por meio da Internet. Todos os demais usuários do provedor não seriam afetados. Insista-se, portanto, que para a proteção da privacidade do usuário o modelo de preservação de dados é mais adequado. Isso

> porque, nesse modelo, a guarda de registros apenas é realizada a partir do momento em que há uma denúncia ou se constata uma suspeita da ocorrência de crime ou de prática de ato ilícito, iniciando-se então o processo de investigação somente contra os possíveis usuários envolvidos, sem implicações para os direitos dos demais usuários de um determinado serviço.

Não obstante o diploma faça ressalvas sobre a proteção dos dados pessoais e da privacidade, bem como imponha deveres de segurança e sigilo, a compulsoriedade delineada favorece a instituição de mecanismos de vigilância, afinal, generaliza a guarda dos registros de conexão e de acesso de qualquer usuário que possua acesso à rede, independentemente de ordem judicial de investigações de suspeitos, com formalização em inquérito criminal devidamente instaurado.

José Luiz Bolzan de Morais e Elias Jacob de Menezes Neto (2015) entendem que a norma trata da privacidade de maneira reducionista, como sinônimo de vida particular, com poucos avanços no que tange à construção sobre o tema de proteção de dados. Com efeito, o Marco Civil da Internet, apesar dos seus esforços, não regulamentou de forma satisfatória o tema da proteção de dados pessoais.

Avalia-se que a evolução para a matéria de proteção de dados pessoais foi tímida, principalmente porque o Marco Civil da Internet apenas se circunscreve ao ambiente da internet. Os destinatários da norma são os usuários, os provedores de conexão e os de aplicação, não estando no âmbito de aplicação qualquer controlador que esteja fora desse ecossistema ou indivíduo cuja coleta de dados fora feito por outro meio.

Em relação à aparente antinomia do Marco Civil da Internet com a Lei Geral de Proteção de Dados, Ricardo Alexandre de Oliveira (2018) defende a especialidade desta em relação àquela sob o argumento de que a LGPD versa tão somente acerca de um tema, ao passo que o Marco Civil possui uma abrangência panorâmica, regulando diversos assuntos sobre internet no Brasil.

De acordo com este breve retrospecto, depreende-se que por conta da fragmentação normativa, persistiu nas últimas décadas a demanda por uma lei que estabelecesse uma tutela abrangente, completa e estruturada e uma "arquitetura institucional adequada para a proteção da personalidade do cidadão contra os riscos decorrentes do

processamento de dados pessoais pelo setor público e privado" (MENDES, 2014, p. 181).

Finalmente, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) vem complementar e trazer modernização e harmonia ao tratamento da informação pessoal dentro do ordenamento jurídico brasileiro. É fruto da reunião de dois Projetos de Lei que tramitavam juntos na Câmara dos Deputados – o PL 4060/2012, com origem na própria Câmara, e o PL 5276/2016, de autoria do Executivo. Nesta Casa Legislativa foi a criada a Comissão Especial de Proteção de Dados Pessoais, cujo relator, Deputado Orlando Silva, após diversas audiências públicas, reuniões setoriais e seminários, conduziu o Projeto para votação no Plenário, que o aprovou por unanimidade. Remetido ao Senado Federal para revisão, designada a relatoria ao Senador Ricardo Ferraço, foi renumerado como PLC (Projeto de Lei da Câmara) nº 53/2018, bem como lhe foi apensado o PL 330/2013, que ali corria. No dia 10 de julho de 2018, o Projeto de Lei foi aprovado por unanimidade na Casa Legislativa Revisora.

Sucessivamente, foi à sanção do Presidente, à época Michel Temer, que vetou os enunciados normativos destinados à criação da Autoridade Nacional de Proteção de Dados. Posteriormente, este promulgou a Medida Provisória nº 869/2018, que além de promover alterações profundas na Lei, instituiu a Autoridade Nacional de Proteção de Dados de maneira diversa à prevista originariamente.

Conforme explicam Laura Schertel Mendes e Danilo Doneda (2018a, p. 470), o objetivo da norma "é proporcionar garantias aos direitos do cidadão, ao mesmo tempo em que fornece as bases para o desenvolvimento da economia da informação, baseada nos vetores da confiança, segurança e valor". Para os autores, sua maior inovação consiste na instituição de um modelo *ex ante* de proteção de dados, baseado no conceito alemão de que não existem mais dados irrelevantes diante do processamento digital de dados.

Pretende-se a partir de então apresentar os principais aspectos constantes na Lei de Proteção de Dados. O curto lapso temporal entre a promulgação da norma e a redação desta pesquisa foram empecilhos para encontrar bibliografia aprofundada especificamente sobre a norma, porquanto muitos trabalhos ainda não foram publicados. Não se olvida ainda que, diante de qualquer mudança legislativa, demanda-se tempo para o amadurecimento doutrinário, bem como para criação de uma jurisprudência consolidada, ou, como neste caso, para atuação sólida e coerente da Autoridade Nacional de Produção de Dados. Segue o desafio de analisar a norma com base no arcabouço que se tem até então.

Durante a tramitação legislativa, a Comissão de Assuntos Econômicos citou, em seu parecer, como motivação o escândalo da *Cambridge Analytica* e *Facebook*[59], e a investigação referente à suposta de venda de dados pela empresa pública Serviço Federal de Processamento de Dados - SERPRO[60], demonstrando-se a urgência e a relevância do tema; e, o GDPR como modelo normativo a se espelhar[61].

Consoante Mendes e Doneda (2018a), são claras as influências europeias advindas tanto do GDPR quanto da Convenção 108 da Comissão da Europa o seguinte: exigência de base legal para o tratamento de dados; regras especiais para os dados sensíveis; a instituição de uma Autoridade para a aplicação da lei; responsabilidade dos agentes de tratamento; e a existência de princípios gerais;

Contém dez capítulos: disposições preliminares; do tratamento de dados pessoais; dos direitos do titular; do tratamento de dados pessoais pelo poder público; dos agentes de tratamento de dados pessoais; da segurança e das boas práticas; da fiscalização; da Autoridade Nacional de Proteção de Dados e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; e disposições finais e transitórias, sendo seus os principais aspectos objeto de descrição e análise.

2.5.1 Jurisdição e Aplicação

Uma das principais características da norma se refere à sua unidade e à sua generalidade, ou seja, dirige-se tanto às pessoas naturais, quanto jurídicas, de direito público ou privado, quando: (i) a operação de tratamento ou de coleta de dados seja realizada no território nacional;

---

59 O uso ilegal de dados do *Facebook* pela *Cambridge Analytica*. Disponível em:.https://www.nexojornal.com.br/expresso/2018/03/19/O-uso-ilegal-de-dados-do-Facebook-pela-Cambridge-Analytica.-E-o-que-h%C3%A1-de-novo

60 MP do DF aponta suposto esquema de venda de dados pessoais de brasileiros pelo Serpro. Disponível em: https://g1.globo.com/df/distrito-federal/noticia/mp-do-df-aponta-suposto-esquema-de-venda-de-dados-pessoais-de-brasileiros-pelo-serpro.ghtml Acesso em: 29 de novembro de 2018

61 “O texto, tal como nossa proposta de Substitutivo ao PLS 330, de 2018, foi inspirado fortemente em linhas específicas da regulação europeia, por reconhecimento expressivo de sua relevância para o mundo. A RGPD entrou em vigor no dia 25 de maio do corrente ano e tem provocado mudanças substanciais em todo o globo, em razão de sua característica de extraterritorialidade. Adotar, portanto, essa influência normativa constitui um ganho expressivo para o País, quando da construção de nosso próprio marco regulatório”.

(ii) fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; e, (iii) a coleta de dados tenha sido feita no território nacional.

Consoante Mendes e Doneda (2018a), apesar da regra geral ser a proteção de dados, a lei estabelece exceções de sua aplicação, moldadas para não comprometer a integridade normativa, quais sejam: (i) quando realizado por pessoa natural sem fim econômico e meramente particular (art. 4º, I); (ii) para fins jornalísticos, artísticos ou acadêmicos (art. 4º, II); (iii) defesa nacional, segurança de Estado, atividade de investigação e repressão de infrações penais (art. 4º, III); e (iv) referente a transferência internacional de dados, quando não houver agentes de tratamento brasileiros ou o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na LGPD.

A primeira circunstância concerne à pessoa natural, quando sua finalidade for particular e não econômica. A desoneração destes é medida que se impõe quando se busca a razoabilidade da aplicação da norma, afinal, seria desacertado exigir de uma pessoa natural, que, por exemplo, gerencia seus contatos ao longo da vida, todos os deveres impingidos aos controladores e operadores.

No que tange aos fins jornalísticos, acadêmicos e artísticos, entende-se que a norma andou bem, uma vez que poderia ser utilizada como subterfúgio para promover censuras. A liberdade de expressão e de imprensa foram privilegiadas, afinal, são dois direitos fundamentais expressos (Art. 5, IX, XIV, e Art. 220 da Constituição Federal).

Certo que tal previsão não autoriza a violação à privacidade ou divulgação de dados pessoais indiscriminadamente. Além das previsões predispostas pela própria norma, como nos casos de pesquisa com dados sensíveis, existe um interesse público ao acesso à informação, que devem ser equilibrados aos interesses privados. Esta questão suscita diversos debates, e, apesar da existência de balizas delineadas pelo ordenamento jurídico, deve ser analisado o caso concreto pelo judiciário, a fim de saber qual direito deve prevalecer.

Outra isenção colacionada pela norma diz respeito aos dados concernentes à segurança pública, defesa nacional, segurança do Estado; ou atividades de investigação e repressão de infrações penais.

Neste caso, em um Estado Democrático de Direito, as garantias constitucionais devem ser observadas, logo, principalmente no que se refere à coleta de dados, imprescindível à ordem judicial, bem como parâmetros e balizas legais, como consigna o parágrafo primeiro, que prevê que tal inciso “será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento

do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.". Importante que esta prime pela proteção do indivíduo, caso contrário, tal previsão pode abrir brechas no sentido de legalizar abusos cometidos pelo Poder Público, com ações de vigilância estatal indiscriminadamente.

Como, por exemplo, o caso divulgado pela Folha de São Paulo, no ano de 2015, que revelou que a Polícia Federal planejou instalar *softwares* espiões a serem infiltrados clandestinamente em dispositivos, permitindo àquele quem controla o *software* o acesso remoto a todas as informações armazenadas nos aparelhos celulares cuja interceptação telefônica já foi autorizada.

Sobre o tema, Laura Schertel Mendes (2015, não p.), comenta decisão do Tribunal Constitucional Alemão em sede de controle de constitucionalidade da Lei do Estado de Nordrhein-Westfalen, "que permitia às autoridades locais de inteligência fazerem a busca remota de informações e o monitoramento online de computadores de suspeitos de cometerem práticas criminosas", tendo ao final delineado parâmetros a serem observados para legalidade das investigações e reconhecido um novo direito fundamental relacionado à privacidade: o direito à confidencialidade e à integridade dos sistemas informáticos.

> O julgamento esclareceu que a infiltração dos sistemas informáticos não estaria completamente vedada pela Lei fundamental alemã, mas somente poderia ser realizada se presentes determinadas condições: a existência de uma base legal específica, a emissão de autorização judicial e a identificação de um perigo concreto a um bem jurídico fundamental, como a vida e a liberdade individuais ou a segurança da coletividade. De toda forma, ainda que atendidos esses requisitos, em nenhuma hipótese poderia tal monitoramento violar o núcleo da intimidade e das formas de vida privada do indivíduo. Isso significa que medidas adicionais de segurança devem ser adotadas para que informações íntimas e excessivas não sejam coletadas durante a infiltração ou – caso isso não seja possível – que tais informações sejam descartadas ou desconsideradas no processo de avaliação dos dados. (2015, não p.)

Tais medidas não podem ser banalizadas[62] considerando o histórico brasileiro de não respeito a garantias individuais de inviolabilidade de comunicações.[63]

Ainda sobre dados de segurança, originariamente, previa-se a vedação do tratamento desses dados por qualquer pessoa jurídica de direito privado. Com as modificações implementadas pela Medida Provisória n. 869/1018, permitiu-se que os dados pessoais constantes de bancos de dados constituídos para o fim de segurança pública sejam tratados por pessoa jurídica de direito privado, desde que não seja em sua totalidade e com tutela de pessoa jurídica de direito público.

Não obstante haja previsão de tratamento parcial e de supervisão, estas viabilizam o acesso de empresas a dados que, em tese, são de segurança pública, defesa nacional e de segurança de Estado. Em outras palavras, abrem-se exceções levantando a bandeira do interesse público ou estatal para, em seguida, permitir o tratamento destes dados pela iniciativa privada.

Ponto nevrálgico se refere ao conceito de dado pessoal, dado pessoal sensível e dado anonimizado, isso porque determinam se haverá aplicação da norma e, caso sim, o seu alcance. Em suma, tais conceitos irradiam seus efeitos sobre praticamente todos os meandros normativos. Conforme explicam Machado e Doneda (2019, não p.) "A delimitação do conceito de dado pessoal é hoje imprescindível na interpretação do alcance normativo de leis de proteção de dados. [...] O direito brasileiro seguiu a orientação Europeia e adotou o conceito amplo".

Dessa forma, dado pessoal abarca tanto a identificação imediata ou mediata da pessoa: "informação relacionada a pessoa natural identificada ou identificável"; e, dado pessoal sensível: "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política,

62 Moro pretende ampliar banco de DNA de criminosos para facilitar investigações. Disponível em: https://oglobo.globo.com/brasil/moro-pretende-ampliar-banco-de-dna-de-criminosos-para-facilitar-investigacoes-23215001 Acesso em: 4 de fevereiro de 2019

63 Um exemplo é a condenação do Brasil pela Corte Interamericana de Direitos Humanos no Caso Escher, o qual condenou o Brasil pelo uso de interceptações telefônicas, pela divulgação ilegal das gravações e pela impunidade dos responsáveis ilegais, no ano de 1999, em desfavor de trabalhadores rurais ligados ao Movimento dos Trabalhadores Rurais Sem Terra (MST) no Paraná. Disponível em: http://emporiododireito.com.br/leitura/lembre-o-caso-escher-e-a-condenacao-do-brasil-pela-cidh-por-interceptacoes-telefonicas-ilegais Acesso em 30 de janeiro de 2019

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", reconhecendo-se a exigência de maior amparo, tendo em vista os maiores riscos que os envolvem.

Se os dados não são relativos nem a pessoa identificada ou identificável, desde a origem após ulterior tratamento, são dados ditos anônimos ou que foram anonimizados, sendo este o "dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento". Ciente da possibilidade do avanço da técnica, condiciona a classificação do dado como pessoal ou anonimizado de acordo com a possibilidade de correlação ou associação, direta ou indireta, ao seu titular diante do estado da técnica em que ocorre o seu tratamento.

Pontua-se que tal diferenciação a dados de categorias diferentes leva a um maior equilíbrio entre os direitos à privacidade e à proteção dos dados pessoais e o direito à inovação e ao desenvolvimento de empresas.

Quanto às possibilidades de tratamento de dados pessoais, é indispensável que seja realizado com fulcro em uma das hipóteses autorizativas, ou seja, exige-se o enquadramento em uma das bases legais para que a atuação fique dentro da legalidade.

A primeira hipótese se refere ao consentimento pelo titular (art. 7º, I). O consentimento é considerado pela lei a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (art. 5º, XII). A ampliação ou modificação da finalidade pelo controlador deve ser comunicada ao indivíduo, a fim de que este ratifique seu consentimento. A qualquer tempo, o consentimento poderá ser revogado pelo titular, sendo que a mesma facilidade encontrada para ofertá-lo, deve ser tida retirá-lo, logo, o procedimento deve ser simplificado e gratuito.

A falta de transparência e de informação pode macular a validade do consentimento, sendo este considerado nulo quando: informação genérica, ou seja, as finalidades não estão determinadas e especificadas; e as informações fornecidas ao titular terem conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência. Nesses casos o tratamento de dados é vedado.

Nas outras hipóteses, o consentimento é dispensável, ou seja, caso o controlador esteja sustentado por uma dessas possibilidades, ele não precisa solicitar o consentimento ao titular de dados, são as bases legais alternativas que respaldam o tratamento de dados pelos

controladores nos seguintes casos: (i) para cumprimento de obrigação legal ou regulatória, para o tratamento e uso compartilhado de dados necessários à execução (art. 7º, II); (ii) de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres (art. 7º, III) (desta forma, tenta-se limitar a atuação do governo sem respaldo legal, evitando-se excessos na coleta e tratamento de dados); (iii) 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 (art. 7º, IV); (iv) para o exercício regular de direitos em processo judicial, administrativo ou arbitral (art. 7º, V); (v) para a proteção da vida ou da incolumidade física do titular ou de terceiro (art. 7º, VI); e (vi) para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais (art. 7º, VII); (vii) para atender aos interesses legítimos do controlador; (viii) para a proteção ao crédito (art. 7º, X); (ix) quando os dados do titular forem tornados manifestamente públicos (art. 7º, §4º).

Quanto a essa última, entra-se em uma área cinzenta, afinal, o que pode ser considerado dado público, ou não. Recorde-se a decisão proferida pelo Tribunal Alemão que construiu a autodeterminação informacional, motivado pela crescente capacidade técnica e de armazenamento de dados, entendeu que qualquer tratamento de dados, por influenciar na representação dos indivíduos na sociedade, possui o condão de afetar a sua personalidade.

Um exemplo recente foi o caso da empresa Serasa Experian e o Tribunal Superior Eleitoral[64], que assinaram Convênio para compartilhamento de dados sob a justificativa de que os dados cadastrais de eleitores, como situação da inscrição eleitoral, nome, CPF e dados relativos à óbito e a quitação eleitoral, seriam dados públicos e, portanto, poderiam ser objeto de livre transação. O interesse do órgão de proteção de crédito era obter informações sobre o óbito de inadimplentes, em contrapartida, ao Tribunal seriam fornecidos certificados digitais pela empresa. O Convênio foi suspenso por

64 Entendendo o acordo entre Serasa e Justiça Eleitoral, que repassa dados de 141 milhões de brasileiros. Disponível em: https://gizmodo.uol.com.br/acordo-tse-serasa/ Acesso em: 3 de janeiro de 2019.

Decisão[65] proferida pela Corregedora-Geral Eleitoral, Ministra Laurita Vaz, que entendeu que a prática violaria o sigilo de informações.

No que se refere à proteção ao crédito, o dispositivo acena a uma leitura sistemática da LGPD conjuntamente com a Lei de Cadastro Positivo e o Código de Defesa do Consumidor. Para Mendes e Doneda (2018ª, p. 474), espera-se o fortalecimento da "unidade sistêmica e ampliando as garantias do titular dos dados nessas situações para além das previsões setoriais". Mister pontuar, porém, que tal exceção abre brecha para a aprovação de Projeto de Lei Complementar n. 441/2017, que tramita atualmente em regime de urgência e aguarda votação do Plenário do Senado Federal e visa suprimir a necessidade do prévio consentimento no Cadastro Positivo.

Finalmente, hipótese importante concerne ao interesse legítimo do controlador (art. 7º, IX). Para Bruno Bioni, (2018, p. 63) trata-se de uma carta coringa regulatória que poderá ser utilizada pelos agentes de tratamento em situações que a autorização do titular dos dados é dispensada porque o agente está respaldado por seu legítimo interesse: "diante desse conceito jurídico indeterminado, nada mais lógico do que prever testes em que se realize um balanço e um equilíbrio de quem trata esses dados, dos modelos de negócio, e das legítimas expectativas do cidadão".

Conforme Mendes e Doneda (2018, p. 474):

> A previsão da hipótese para a realização de interesses legítimos do controlador ou de terceiro se afigura como uma espécie de cláusula geral, na qual opera-se um teste de proporcionalidade entre os interesses na utilização dos dados pessoais, que são do controlador ou de terceiro, e os direitos do titular. Nesse caso, verifica-se se a realização de uma determinada finalidade com o tratamento de dados pessoais à qual corresponde o interesse legítimo, possui efeitos potenciais para os direitos e liberdades fundamentais do titular. Se estes restarem concreta e potencialmente afetados, há de se concluir que o legítimo interesse não deve

65 A íntegra da decisão está disponível em: http://www.tse.jus.br/noticias-tse/2013/Agosto/corregedoria-geral-eleitoral-suspende-acordo-entre-tse-e-serasa Acesso em: 3 de janeiro de 2019

> ser considerado como uma hipótese que autorize o tratamento.

A própria norma traz parâmetros a serem considerados, como o apoio e promoção de atividades do controlador, as legítimas expectativas do titular de dados e os direitos e garantias fundamentais que lhe são assegurados (art. 10, I e II), respeitando-se os princípios da finalidade, da minimização dos dados e da transparência (art. 10, §1º e §2º).

Nesses casos, poderá a Autoridade Nacional de Proteção de Dados solicitar a elaboração de relatório de impacto à proteção de dados pessoais "que é uma descrição de uma operação de tratamento de dados pessoais que execute conjuntamente as medidas que tenha adotado para aumentar a segurança e mitigar o risco presente no tratamento" (MENDES; DONEDA, p. 475) Consoante consigna Bruno Bioni (2018, p. 65 -66), a Autoridade não vai conseguir atender às especificidades que cada setor possui, por exemplo, o setor de planos de saúde oferece riscos diversos em relação ao de aviação:

> É, nesse contexto, que faz ainda mais sentido essa nova racionalidade regulatória cujo resultado final é convidar quem está desenvolvendo, quem está com a mão na massa, projetando seus produtos e serviços, dizer quais são os riscos envolvidos na sua atividade. Nesse sentido, a nossa lei e a GDPR têm disposições sobre relatórios de impacto à proteção de dados pessoais. De forma bem franca, esse movimento acena para o seguinte: eu, regulador, não consigo de antemão dizer quais são os riscos, você, agente econômico, tem mais informação e conhecimento do que eu, então você será convidado a fazer isso. Por isso, há emergência de diversas normas relacionados a esse dever de emissão de relatórios de impacto a proteção de dados pessoais.

Destarte se denota que a aplicação das normas por cada setor, e a análise de casos concretos, serão essenciais para o desenvolvimento dos limites possíveis do legítimo interesse, a serem utilizados de parâmetro de acordo com cada especificidade e realidade dos controladores.

Imagine-se uma academia de ginástica que armazena os dados de identificação, de frequência, de peso e de bioimpedância dos seus

alunos. É factível afirmar que o estabelecimento possui legítimo interesse em identificá-los para fins de cobrança no caso de inadimplemento contratual, por exemplo, bem como de acompanhar a evolução de seus clientes, a fim de auxiliá-los em seus treinos e, consequentemente, nos resultados perquiridos. Contudo, se houver o desiderato de compartilhar esses dados com lojas de suplemento, a justificativa do legítimo interesse se fragiliza. Outro ponto seria o término do tratamento de dados: enquanto o aluno estiver matriculado, há amparo, porém, com o desligamento do aluno, apenas devem ser mantidos por período razoável de tempo.

Veja-se que, neste momento, apenas é admissível especulações: um ano parece ser plausível, porque existe a possibilidade de rematrícula; dez anos, por outro lado, parece demasiadamente exagerado. São os casos concretos que irão subsidiar tais parâmetros, por isso a importância da articulação privada com a Autoridade de Proteção de Dados Pessoais.

Por seu turno, atinente ao tratamento de dados pessoais sensíveis, opera-se a mesma estrutura de bases legais, porém, estas são mais restritas. Exige-se que o consentimento, além de livre, informado e inequívoco, deva ser exarado de forma específica e destacada (art. 11, I), ou seja, no contexto de uma declaração escrita, deve ser apresentado de forma que o distinga de outros assuntos ali apostos.

Pertinente às outras bases legais, a maioria das previsões já elencadas aos dados não sensíveis é repetida, excetuadas as que concernem ao interesse legítimo; à proteção ao crédito; e à execução de contrato. Chama a atenção o fato de que na hipótese do tratamento compartilhado de dados pessoais sensíveis para execução de políticas públicas, esteja mais ampla que de dado pessoal, uma vez que foi suprimido o trecho final (art. 11, II, b), que as qualifica na previsão de dado pessoal "previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres" (art. 7º, III).

Foi inserida a garantia da prevenção à fraude e à segurança do titular nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, legalizando, assim, a utilização de dados biométrico[66] para implementação de projetos como Documento

66 Identidade única: como funcionará o novo sistema de identificação no país. Disponível em: https://www1.folha.uol.com.br/cotidiano/2017/04/1877918-identidade-unica-como-funcionara-o-novo-sistema-de-identificacao-no-pais.shtml Acesso em: 15 de janeiro de 2019.

Nacional de Identificação[67], pelo Governo Federal e o cadastramento biométrico do Tribunal Superior Eleitoral.

Por fim, quanto ao término do tratamento dos dados, este deverá ocorrer a depender da base legal que o respalda: (i) quando esgotada a sua finalidade (art. 15, I); (ii) pelo fim do período de tratamento (art. 15, II); (iii) pela revogação do consentimento pelo titular (art. 15, III); ou (iv) por determinação da autoridade nacional, quando verificada infração às normas da lei.

Nesses casos, o dado deverá ser eliminado, autorizada a conservação para cumprimento de obrigação legal pelo controlador; estudo por órgão de pesquisa; transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; e uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

2.5.2 Agentes de Tratamento

Conforme observa Oliveira (2018, p. 255), a criação e a definição das figuras de controlador e de operador, agentes de tratamento, na Lei Geral de Proteção de Dados têm por função "delimitar direitos e obrigações, aclarando a posição de cada personagem que participa do tratamento de dados [...] para a responsabilização dos agentes, o que fará com que as empresas em geral delimitem muito bem o papel que desejam assumir no tratamento de dados.".

O autor traça um interessante paralelo com a relevância das definições de consumidor e fornecedor constantes no Código de Defesa do Consumidor, que auxiliaram na delimitação da aplicação da norma: "Mesmo que hoje em dia ainda existam discussões sobre a condição de Consumidor e de Fornecedor de certas pessoas em alguns casos concretos (como comércio entre pessoas jurídicas), a dificuldade seria redobrada se as definições não existissem". (2018, p. 254).

A Lei Geral de Proteção de Dados, tal qual o GDPR, instituiu a figura do controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (art. 5º, VI), ou seja, quem delibera estrategicamente

67 Os desafios da nova identidade. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/dni-os-desafios-da-nova-identidade-02042018 Acesso em: 15 de janeiro de 2019.

acerca dos dados que serão coletados e em qual base legal se respaldará, sua finalidade, o tempo de armazenamento, etc.

Por seu turno, a incumbência da figura do processador nos moldes da norma europeia é realizada pelo operador, pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, ou seja, age de acordo com os comandos deste último (art. 5º VII).

O encarregado faz as vezes do *Data Protection Officer* (DPO) europeu, sendo a pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (art. 5º, VIII), uma espécie de ouvidor. Ressalta-se quanto a este que, originariamente, constava expressamente a necessidade de ser "pessoa natural". A Medida Provisória nº 869/2018, porém, suprimiu a expressão "natural", abrindo margem a incumbência tanto à pessoa natural, quanto à pessoa jurídica, comitês, grupos de trabalho e até mesmo terceirizando o serviço, beneficiando principalmente pequenas empresas, uma vez que não precisa mais despender um colaborador especificamente para tais funções, podendo encontrar outros meios considerados adequados, de acordo com a sua realidade.

Controlador e operador devem manter os registros de operações, especialmente quando o tratamento ocorrer com base no legítimo interesse. Conforme já visto, o controlador está sujeito à elaboração de relatório de impacto à proteção de dados pessoais, a requerimento da Autoridade Nacional de Proteção de Dados, em que deve descrever os tipos de dados coletados, a metodologia e estatística de segurança e mecanismos mitigação dos riscos.

Conforme Mendes e Doneda (2018, p. 476), a Lei Geral de Proteção de Dados, "exige a adoção por todos que tratam dados de medidas que garantam a integridade, a confidencialidade e a disponibilidade dos dados sob tratamento.".

Nesse sentido, o art. 46 e seguintes estipulam obrigações a serem observadas quanto à segurança, sigilos dos dados, boas práticas e governança dos dados, que deverão ser observados desde a concepção do produto, até a sua execução, aproximando-se da ideia do *privacy by design* a fim de garantir a segurança e os direitos dos titulares.

Em relação à responsabilidade civil, o art. 45 expressamente estabelece que quando se tratar de relação de consumo, sujeita-se às regras previstas na legislação pertinente, qual seja, o Código de Defesa do Consumidor, que estabelece a responsabilidade objetiva do fornecedor/controlador.

Em outras conjunturas, há certa nebulosidade acerca do regime dispensado à responsabilização nos casos em que não há relação de consumo. Importante consignar que a norma estabelece o princípio da responsabilização e prestação de contas (art. 42), o qual se relaciona ao da *accountability* constante no GDPR, em que se imputa ao controlador a observância e a conformidade com a norma; e sua capacidade de comprová-la junto às Autoridades de Supervisão.

Para Laura Schertel Mendes e Danilo Doneda (2018a), aos agentes de tratamento se imputa responsabilidade objetiva, haja vista que se trata de risco intrínseco à atividade, sendo que a própria regulação tem como um de seus fundamentos principais a mitigação das ameaças advindas das atividades de tratamento de dados.

O artigo 43 da LGPD, além da hipótese de culpa exclusiva da vítima ou de terceiros, estipula que os agentes de tratamento só não serão responsabilizados quando provarem que não realizaram o tratamento de dados pessoais que lhes é atribuído e que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados.

O regime prevê especificações quanto à responsabilidade de determinados agentes. O operador, por exemplo, somente será responsabilizado quando não observar suas obrigações legais ou tiver atuado para além das instruções do controlador, responsabilizando-se neste caso solidariamente. Ao controlador cabe a responsabilidade nos demais eventos, caso haja controladores atuando conjuntamente (*joint controller)*, todos se responsabilizam solidariamente perante o titular.

Na União Europeia, conforme relatório da Autoridade Europeia para a Proteção de Dados[68], desde a entrada em vigência do GDPR, em maio de 2018, até janeiro de 2019, foram computadas pelas *Data Protection Autorities* dos países da União Europeia: 41.502 notificações sobre ameaças ou incidentes de vazamento de dados, conhecidos como "data breach"; e 95.180 de reclamações realizadas pela própria população. Em comparação com outros períodos, tais dados denotam que houve uma crescente participação da população na denúncia de possíveis atos lesivos, demonstrando a disseminação de uma cultura de privacidade e de proteção de dados pessoais.

[68] GDPR in numbers. Disponível em: https://www.jota.info/wpcontent/uploads/2019/02/4edbba8aaa08b68ee3b09d48441df5ed.pdf?x48657 Acesso em: 9 de fevereiro de 2019

2.5.3 Direitos e Princípios

Vale destacar que a partir de alguns enunciados contidos ao longo da norma, aparentemente, diversamente das últimas normativas da União Europeia e do movimento doutrinário vanguardista que reconhecem o direito à proteção de dados como direito fundamental autônomo, a opção legislativa foi de se filiar à corrente que sustenta seu pertencimento a uma faceta da privacidade.

Isso porque o art. 1º dispõe que o escopo da norma é "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural", tendo a disciplina de dados pessoais como fundamento o respeito à privacidade, à autodeterminação informativa e à inviolabilidade da intimidade, da honra e da imagem (art. 2º).

Outro indicativo concerne ao artigo 17, que não equipara a proteção de dados pessoal aos outros direitos fundamentais ali elencados, apenas assegura a titularidade dos dados, veja-se: "Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei".

Conforme Mendes e Doneda (2018, p. 474) os princípios de proteção de dados e os direitos do titular dos dados estipulados pela Lei procuram garantir, por um lado, "um arcabouço de instrumentos que proporcionem ao cidadão meios para o efetivo controle do uso de seus dados por terceiros, por outro, confere unidade sistêmica à própria disciplina de proteção de dados pessoais".

Ressalta-se a presença de uma série de princípios que são comuns à enorme maioria das legislações de proteção de dados atuais, as quais decorrem, em geral, de um tronco comum: os *Fair Information Practice Principles*, presentes em documentos como a Convenção 108 do Conselho da Europa, repisem-se: finalidade, livre acesso, segurança, transparência e qualidade. Somam-se a estes outros princípios que foram construídos contemporaneamente: não discriminação; adequação; necessidade; prevenção e responsabilização e prestação de contas. Outrossim, o enunciado traz em seu *caput* o princípio da boa-fé.

Esta boa-fé concerne à boa-fé objetiva, que a partir de sua função integrativa, estabelece deveres anexos ou laterais implícitos a todas as relações jurídicas, que estão além do dever jurídico obrigacional principal, por exemplo: deveres de lealdade, respeito, probidade, garantia e informação (FARIAS; ROSENVALD, 2018).

De modo igual ao microssistema consumerista, o dever de informar assume importante papel no ecossistema de proteção de dados. Trata-se de uma coluna vertebral de onde decorrem diversos direitos em todas as fases do tratamento de dados: desde a policitação, em que o indivíduo possui o direito à informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa (art. 18, VIII); o direito de obter a confirmação da existência de tratamento de dados (art. 18, I); o direito de saber o procedimento específico a ser seguido com a finalidade de ter acesso aos dados (art. 18, II); e o direito de ter conhecimento sobre o compartilhamento de dados com terceiros realizado pelo controlador (art. 18, VII).

Guilherme Goulart (2018) afirma que o uso e aplicação de categorias já conhecidas no Direito Civil e no Direito do Consumidor (a boa-fé objetiva e o dever de informar) irão auxiliar no processo de internalização, adequação e harmonização com o ordenamento jurídico brasileiro, bem como na compreensão das inovações trazidas pela Lei Geral de Proteção de Dados.

Os princípios se correlacionam com mecanismos aqui já mencionados, por exemplo, o legítimo interesse do controlador, que tanto na ponderação prévia, quanto no trato dos dados, deverá observar os princípios da finalidade, adequação, necessidade e qualidade: devem ser coletados apenas os dados estritamente necessários para a consecução de uma determinada finalidade, adequando-se a extensão de tratamento e o período de armazenamento, por exemplo.

Com fulcro em Mulholland (2019), dois princípios assumem relevância no que toca ao tratamento de dados sensíveis, quais sejam, o princípio da finalidade, uma vez que os dados devem ser tratados em conformidade com o intuito pelo qual foram coletados, e o da não discriminação. Esgotando-se a finalidade, encerra-se igualmente a legalidade do tratamento daqueles dados, sendo imperioso o seu término, portanto, sendo importante limitador a ser observado.

A coleta de dados não pode ser feita indiscriminadamente. Segundo metáfora feita por Maria Celina Bodin de Moraes (2008, p. 9), em apresentação à obra de Stefano Rodotà (2008), "não pode ser tomada como uma 'rede jogada ao mar para pescar qualquer peixe'. Ao contrário, as razões de coleta, principalmente quando se tratarem de 'dados sensíveis', devem ser objetivas e limitadas".

Em relação ao princípio da não discriminação, fica vedada a utilização dos dados pessoais para fins discriminatórios ilícitos ou abusivos. Nas palavras de Mulholland (2019, p. 164-165):

> O legislador, ao relacionar o uso discriminatório às qualidades de ilicitude e abusividade, parece reconhecer a possibilidade de tratamento distintivo, desde que lícito e não abusivo. Isto é, aparentemente, seria legítimo ao operador de dados realizar tratamentos de segregação, no sentido de diferenciação, sem que, com isso leve a consequências excludentes que poderiam ser consideradas ilícitas. Assim, por exemplo, seria legítimo a um operador de dados que esteja realizando a precificação de um serviço de seguros de automóveis, tratar de maneira diferenciada os dados de mulheres entre 35 e 45 anos e mães, com a finalidade de oferecimento de um valor que reflita os riscos de danos usualmente ocasionados ou sofridos por esse grupo determinado de pessoas. Ou seja, há a possibilidade de tratamentos discriminatórios de dados, desde que não se caracterizem pela ilicitude ou abusividade, o que será determinado segundo critérios definidos tanto pelas regras expressas de direito civil e penal, quanto por princípios como o da boa-fé objetiva. O que se questiona é se esse tratamento segregado - desde que lícito e não abusivo - pode ser realizado também quando considerados os dados pessoais sensíveis, na medida em que eles possuem características personalíssimas, que devem ser tuteladas prioritariamente.

O uso de dados pessoais sensíveis aumenta a possibilidade de discriminação e de segregação abusiva no âmbito das relações de consumo. Defende a autora que a assimetria de poder e de conhecimento entre titulares e controladores é ainda maior no que tange aos dados pessoais sensíveis, gerando um desequilíbrio social e sustenta que a proteção é pressuposto para a efetivação dos direitos à igualdade e à liberdade.

Por seu turno, também possuem associação o livre acesso com a transparência, afinal, este garante aos titulares o direito de receber informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, (como está sendo realizado, por quem, com quem está sendo compartilhado, por exemplo) e, inclusive sobre os instrumentos de requisição de acesso.

A redação em princípios gerais permite ao intérprete a adequação às novas realidades técnicas e sociais. Com isso, tenta-se garantir o acompanhamento da norma à velocidade das inovações ao longo do tempo. Diretrizes e posicionamentos claros trazem segurança jurídica às atividades econômicas e estatais, bem como asseguram a necessária proteção dos direitos dos titulares de dados pessoais.

Por fim, vale pontuar que o princípio da transparência é muito caro, mormente quando o controlador é uma entidade pública. Apesar de não ser objeto específico da presente pesquisa a atuação do Público, a advertência parece oportuna. A Lei de Acesso à Informação (Lei n. 12.527/2011) representou avanços democráticos no acesso à informação, sendo importante instrumento utilizado pela sociedade civil, jornalistas e pesquisadores para obtenção de dados concernente à atuação governamental. A referida norma instituiu expressamente a transparência como princípio básico da administração pública, bem como dever do Estado de garantir o acesso à informação, que será franqueada, mediante procedimentos objetivos e ágeis, de forma transparente, clara e em linguagem de fácil compreensão.

Entretanto, recente Decreto emanado pelo Governo Federal pode ter esvaziado em parte a Lei de Acesso à Informação. Isso porque permite que Servidores comissionados, dirigentes de autarquias, fundações, empresas públicas e sociedades de economia mista classifiquem os documentos e informações como dados ultrassecretos (antes restrito aos altos cargos da República)[69] ou secretos, ou seja, passam a ser sigilosos, inclusive a própria justificativa de classificação. A mudança foi recebida com críticas pela sociedade civil e por jornalistas[70].

A medida poder acarretar na limitação de acesso às informações coletadas e armazenadas pelo Poder Público. Somando-se as inúmeras exceções ao Poder Público apostas na Lei de Proteção de Dados Pessoais e as modificações concernentes ao regime jurídico e a estrutura

69 Originariamente, apenas o Presidente da República, o Vice-Presidente, os Ministros de Estado, os comandantes das Forças Armadas e os chefes de missões diplomáticas e consulares permanentes no exterior podiam classificar dados como ultrassecretos. A decisão das últimas duas categorias ainda precisava ainda ser ratificada por Ministros, num prazo de 30 dias.

70 **O sigilo deveria ser exceção. O decreto do Governo prejudica a transparência**
https://brasil.elpais.com/brasil/2019/01/24/politica/1548360497_872168.html. Acesso em: 30 de janeiro de 2019.

da Autoridade Nacional de Proteção de Dados colocam o alerta sobre a criação de bases jurídicas que permitam a opacidade governamental e impeça o cidadão o controle de suas próprias informações.

Os direitos assegurados ao titular pela Lei Geral de Proteção de Dados assumem papel de suma importância. Conforme indica Laura Schertel Mendes (2014, p. 65), o direito geral de informação:

> [...] consiste no direito que as pessoas têm de conhecer sobre a existência dos bancos de dados, bem como dos seus objetivos e de seu conteúdo. Para que o individuo possa proteger a sua personalidade, é preciso que todo o processo de tratamento de dados pessoais seja transparente. Assim, o direito à informação consiste no direito do individuo cujos dados são coletados de conhecer a identidade do responsável pelo tratamento, o objetivo do tratamento e os destinatários dos dados em caso de transferência. Ademais, o individuo deve ser informado a respeito de quais são os seus direitos e como ele pode exercê-los em cada fase do tratamento de dados pessoais.

O direito à confirmação de existência e ao acesso a dados pessoais (art. 19), por exemplo, denotam justamente a possibilidade do receber ampla informação se há algum registro sobre si e, caso afirmativo, poder aceder a tais dados. A norma estipula ao controlador que tais informações deverão ser disponibilizadas em formato simplificado ou por meio de declaração clara e completa, fornecida no prazo de até quinze dias, contado da data do requerimento do titular, sendo que a Autoridade Nacional de Proteção de Dados poderá regular de forma diferente tais questões, a depender do setor envolvido.

No caso em que não for possível cumprir com a requisição, deverá o controlador: (i) se não houver relação jurídica prévia, comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente (art. 18, §4º, I); ou, (ii) indicar as razões de fato ou de direito que impedem a adoção imediata da providência (art. 18, §4º, II).

Segundo Laura Schertel Mendes (2014, p. 66):

> A frequência desse acesso varia de acordo com as diversas legislações, assim como a sua gratuidade

> ou onerosidade. Entende-se que, para a garantia da efetividade do referido direito, seria fundamental garantir a gratuidade do acesso a essas informações, conforme estabelece, por exemplo, a Lei Federal de Proteção de Dados alemã (BDSG), em seu § 19, (7). O direito de acesso compreende também o direito do individuo de conhecer, na hipótese da existência de uma rede de bancos de dados, em qual banco de dados estão armazenadas as suas informações. Nesse caso, pode o cidadão procurar qualquer um desses bancos, que terá a obrigação de encaminhar a sua solicitação ao organismo responsável pelo armazenamento, bem como de comunicar tal informação ao cidadão.[71]

O acesso aos dados é pressuposto para o exercício de outros direitos, tais como o de correção de dados incompletos, inexatos ou desatualizados (art. 18, III); de eliminação dos dados pessoais tratados com o consentimento do titular (art. 18,VI); e de anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade (art. 18, IV).

Por seu turno, o direito à portabilidade de dados (art. 18, V), conforme Cravo (2018), correlaciona-se tanto com o direito de escolha do consumidor, quanto com o direito concorrencial. Este direito suscita controvérsias, tais como: a quem cabe o custo da transação da portabilidade; como ocorrerá a adequação para a interoperabilidade dos sistemas; quais os parâmetros devem ser adotados na regulamentação própria do controlador, que não estão detalhados na norma. Assim

[71] Interessante o relato feito pela autora sobre o exercício do direito de acesso na Alemanha: A esse respeito, vale mencionar a polêmica na Alemanha, envolvendo a SCHUFA (empresa alemã que presta serviços de proteção ao crédito), que, no âmbito da avaliação de risco do consumidor, classificava como critério negativo o pedido de acesso do consumidor a seus próprios dados. A empresa sofreu severas criticas tanto da opinião pública como das autoridades de proteção de dados, em face dessa prática, que penalizava o consumidor com um *scoring* pior, unicamente, em razão do exercício de um direito. Diante dessa prática claramente abusiva, o legislador alemão reagiu na reforma da lei federal de 2009 e estabeleceu que os dados relativos ao exercício de direitos somente podem ser utilizados pelo responsável pelo processamento para o cumprimento das obrigações legais, não podendo acarretar prejuízos ao titular dos dados (BDSG,§6, Abs. 3). (MENDES, 2018, p. 67)

sendo, trata-se de direito cuja sua extensão e desenvolvimento dependerá do posicionamento dos agentes de tratamento, da atuação da Autoridade de Proteção de Dados e do entendimento jurisprudencial futuro.

Finalmente, o artigo 20 trata do direito à adequada e apropriada decisão, estabelecendo a viabilidade de revisão da decisão quando tomadas exclusivamente com base em tratamento de dados. Na versão aprovada pelo Poder Legislativo, essa deveria necessariamente ser revista "por pessoa natural", contudo, tal expressão foi suprimida do texto legal pela Medida Provisória nº 869/2018, em suma, ainda que o titular recorra de uma decisão tomada por uma base de dados, esta poderá ser decidida pelo mesmo sistema que já deliberou anteriormente.

A sujeição a uma deliberação individual automatizada, sem uma norma que garanta a possibilidade de revisão desta por um humano, esvazia o direito à adequada e apropriada decisão, porque seu núcleo consiste na não submissão a decisões que influenciem significativamente a sua posição jurídica tomadas exclusivamente com base no tratamento automatizado de dados.

Este direito se relaciona principalmente ao princípio da não discriminação, isso porque os algoritmos de decisão estão sujeitos a vieses. Conforme Cathy O'neil (2018), tais algoritmos são formulados por especialistas, que carregam seus preconceitos e traduzem sua forma de pensar a números. Por conseguinte, podem produzir propositadamente, ou não, resultados desiguais; ou ainda replicar desigualdades já conhecidas[72].

---

72 Transcreve-se excertos de entrevista dada pela a diretora de inovação do Google ao El Pais: "Nossos usuários são muito diferentes e temos de cuidar para que essas diferenças não sejam mal interpretadas por tecnologias novas baseadas na coleta de dados do mundo real, como *machine-learning* e inteligência artificial", resume. Por exemplo, evitar que, no caso do desenvolvimento de uma plataforma de emprego, apenas homens sejam identificados como possíveis candidatos a cargos de direção – uma vez que são os que tradicionalmente ocuparam esses cargos – ou que seus sistemas de reconhecimento de voz identifiquem sotaques diferentes ou inclusive pessoas com distúrbios da fala, como a gagueira. "Na comunidade tecnológica, pecamos pela ingenuidade. Agíamos convencidos de que tudo o que fazíamos seria fantástico para todos, e isso nem sempre foi verdade. Devemos assumir a responsabilidade pelo que criamos", argumenta. Disponível em: https://brasil.elpais.com/brasil/2019/01/28/eps/1548684447_982945.html. Acesso em: 28 de janeiro de 2019

Com fulcro em Raquel Saraiva (2018), um algoritmo de decisão, ao ser confrontado, deveria responder pelo menos uma dessas perguntas: (i) quais foram os principais fatores levados em conta para a decisão; (ii) mudar um desses fatores mudaria a decisão; e (iii) por que dois casos que parecem similares podem ter duas decisões diferentes.

Segundo ambas as autoras, a falta de transparência visa à isenção de responsabilidades. A manutenção de um sistema opaco sob o argumento de estarem acobertados por direitos de segredo industrial ou de propriedade intelectual protege o algoritmo, os resultados e, consequentemente, os agentes de tratamento que utilizam acordo exclusivamente com seus interesses.

Por fim, a norma estabelece que o titular dos dados pessoais possui o direito de peticionar contra o controlador perante a Autoridade Nacional de Proteção de Dados(art. 18, §1º). A despeito de a norma prever a tutela coletiva tão somente nos casos em juízo, considerando-se a racionalidade regulatória delineada pena norma, defende-se a possibilidade de exercício da tutela coletiva perante a Autoridade Nacional de Proteção de Dados. Logo, entende-se que a previsão do art. 22 e do art. 42 também se estendem à esfera administrativa da Autoridade Nacional de Proteção de Dados.

2.5.4 Autoridade Nacional de Proteção de Dados e a Medida Provisória nº 869/2018

O Presidente Michel Temer, vetou os artigos 55 a 59, que versavam acerca da criação e competências da Autoridade Nacional de Proteção de Dados (Autoridade Nacional de Proteção de Dados), sob o argumento de existência de vício de iniciativa: "Os dispositivos incorrem em inconstitucionalidade do processo legislativo, por afronta ao artigo 61, § 1º, II, 'e', cumulado com o artigo 37, XIX da Constituição[73]".

73 Constituição Federal, Art. 61. A iniciativa das leis complementares e ordinárias cabe a qualquer membro ou Comissão da Câmara dos Deputados, do Senado Federal ou do Congresso Nacional, ao Presidente da República, ao Supremo Tribunal Federal, aos Tribunais Superiores, ao Procurador-Geral da República e aos cidadãos, na forma e nos casos previstos nesta Constituição. § 1º São de iniciativa privativa do Presidente da República as leis que:II - disponham sobre: e) criação e extinção de Ministérios e órgãos da administração pública, observado o disposto no art. 84, VI.

Embora houvesse argumentos a favor da constitucionalidade da Autoridade, visto que o Projeto de Lei nº 5276/2015 era de autoria do o Executivo, proposto pelo Ministério da Justiça do governo Dilma Rousseff (e fora apensado ao Projeto de Lei nº 4060/2012) e previa a instituição da Autoridade nos moldes do texto aprovado por ambas as Casas Legislativas, prevaleceu a tese no sentido da inconstitucionalidade de sua criação por vício de iniciativa.

Surgiram, então, movimentos organizados pela sociedade civil para a derrubada dos vetos pelo Congresso, o qual não foi analisado pela interrupção das atividades parlamentares pelo recesso. Eis que, no dia 28 de dezembro de 2018, foi promulgada pelo Presidente Michel Temer, nos últimos dias do exercício de seu mandato, a Medida Provisória nº 869/2018, acarretando inúmeras alterações no texto da Lei e instituiu a Autoridade Nacional de Proteção de Dados, com regime jurídico e estrutura bastante diversa do que fora inicialmente desenhado.

Originariamente, o regime jurídico a que estaria submetida a Autoridade de Proteção de Dados Pessoais seria de autarquia especial, membro da administração pública indireta, dotada de personalidade jurídica própria, vinculada ao Ministério da Justiça tão somente por tutela. Neste modelo, a Autoridade brasileira estaria alinhada tanto à experiência brasileira de agências reguladoras, quanto às Autoridades do modelo europeu, que lhe serviram de inspiração.

Ocorre, contudo, que a Medida Provisória nº 869/2018 promoveu modificações profundas à arquitetura anteriormente delineada: instituiu a Autoridade como órgão integrante da Presidência da República (art. 55 -A), ou seja, deixa de ser uma instituição com personalidade jurídica própria para compor a administração pública direta, submetida hierárquica e diretamente ao Chefe do Executivo.

Esta mudança estrutural provoca preocupações diversas, tanto relativas ao funcionamento eficiente de suas funções, quanto à abertura de possibilidade para ingerência política. Isso porque estão asseguradas às autarquias as seguintes prerrogativas, conforme José dos Santos Carvalho Filho (2018): (i) sua independência administrativa; (ii) sua autonomia técnica; (iii) autonomia decisória; e (iv) poder normativo técnico ou poder regulador; (v) autonomia administrativa; e (vi) autonomia econômico-financeira, com recursos próprios e dotação orçamentária.

Para Maria Sylvia Zanella Di Pietro (2012, p. 564), a independência deve ser entendida de forma compatível com a ordem constitucional, no caso, suas decisões podem ser revistas pelo Poder Judiciário e devem respeitar as normas aprovadas pelo Poder

Legislativo. Dessa forma a independência se refere ao Poder Executivo, estando sujeitas à tutela do Ministério a que estão vinculadas, "porém, como autarquias de regime especial, os seus atos não podem ser revistos ou alterados pelo Poder Executivo".

Neste caso, a partir do momento que deixa de ser autarquia especial equiparada às agências reguladoras, para ser um órgão subordinado, abre-se a possibilidade para interferência política na Autoridade. Sobre o tema, aduz José dos Santos Carvalho Filho (2018, p. 523):

> [...] o sistema verdadeiro das agências reguladoras implica lhes seja outorgada certa independência em relação ao governo no que tange a vários aspectos de sua atuação. Se há interferência política do governo, o sistema perde a sua pureza e vocação. Aqui e ali, no entanto, têm surgido investidas e escaramuças de órgãos governamentais, com o propósito de reduzir o poder daquelas entidades, e esse tipo de ingerência denota flagrante distorção no processo de desestatização.

Alexandre Santos de Aragão (2013, p. 333) ressalta igualmente a importância da independência de agências reguladoras:

> O grande risco da fluidez dos objetivos fixados na legislação é a possibilidade de, em razão da sua inevitável generalidade, serem instrumentalizados politicamente pelas forças políticas momentaneamente dominantes. Estabilizar as decisões políticas adotadas pelo Legislador em determinado setor objeto da regulação estatal, fazendo com que os objetivos fluidos fixados pela lei, aptos, portanto, a se adaptarem à realidade socioeconômica, sejam perseguidos de forma estável por estas entidades, dotadas de autonomia frente aos agentes políticos do Estado.

O novo arranjo institucional delineado, porém, não garante a independência em relação ao Poder Público, o qual é pressuposto para o adequado funcionamento da Autoridade de Proteção de Dados. Consoante indica Barroso, as agências reguladoras "precisam ver preservado seu espaço de legítima discricionariedade, imune a injunções

de qualquer natureza, sob pena de falharem em sua missão (2002, p. 111)*”.* Além de possíveis ingerências políticas diretas, o Poder Público também é destinatário da norma, fica patente sua suspeição, uma vez que desta forma possui ingerência sobre as regras do jogo ao qual se submete, pelos seus poderes de fiscalização e de dar interpretação às normas, podendo desequilibrar todo o ecossistema, com autofavorecimentos e abrindo brechas para instauração de mecanismos estatais de vigilância.

Inclusive, dispõe o art. 55 - G que a estrutura regimental da Autoridade Nacional de Proteção de Dados será feita por ato da Presidência da República, estando neste ínterim apoiado técnica e administrativamente pela Casa Civil no exercício de suas atividades.

Em relação à autonomia técnica, ainda que a Medida Provisória a tenha assegurado expressamente (art. 55 - B), esta pode restar prejudicada justamente porque seu espaço de legítima discricionariedade deixa de estar imune de interferências políticas, comprometendo sua missão. Veja-se que sequer possuía correspondente anterior à previsão da autonomia técnica, afinal, é pressuposto da própria natureza jurídica autárquica.

A autonomia decisória, por seu turno, decorre da independência: os conflitos administrativos são instruídos e decididos internamente. Por conta da ausência de qualquer subordinação, inexiste recurso próprio para alteração ou revisão de seus atos e decisões pelo Poder Executivo. Entretanto, na estrutura delineada pela Medida Provisória, sendo um órgão hierarquicamente inferior, seus atos e decisões passam a ser passíveis de revisão pelo próprio Executivo.

Relativo ao poder de fiscalização, retirou-se do texto a previsão expressa da possibilidade de realização de auditorias sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, inclusive do poder público (antigo artigo 56 XVI), mantido tão somente a possibilidade de “requisitar informações, a qualquer momento, aos controladores e operadores de dados pessoais que realizem operações de tratamento de dados pessoais” (artigo 55 - IV). Certamente essa supressão prejudica a atuação da Autoridade, uma vez que suas ferramentas de fiscalização ficaram restritas ao poder de requisitar informações, competência que outras instituições já possuem, como, por exemplo, o Ministério Público.

Foi mantido na íntegra o antigo inciso IV, agora inciso VI: “fiscalizar e aplicar sanções na hipótese de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito

de recurso", porém, na prática, devido à ausência de independência, esta competência pode ser esvaziada, afinal, se a Autoridade não dispuser de recursos ou se houver ingerência sobre sua atuação, a atuação fiscalizatória, por conseguinte, pode sofrer interferências.

Foi inserido um novo inciso, que prevê o seguinte: verificado o descumprimento legal por órgãos e entidades da administração pública federal, há o dever comunicar aos órgãos de controle interno. O enunciado traz inconsistências: primeiramente, apenas consigna em relação à administração pública federal, ao passo que incumbe à Autoridade Nacional de Proteção de Dados supervisionar as atividades de tratamento de dados pessoais realizadas por Estados, Municípios e órgãos públicos de diferentes classes.

Quanto à aplicação de sanção, o art. 55 - K determina que a competência da Autoridade Nacional de Proteção de Dados prevalecerá sobre as competências correlatas de outras entidades ou órgãos da administração pública. Consequentemente, a atuação de tais órgãos de controle, no que tange ao poder sancionatório, será subsidiária.

No que atine ao poder normativo ou regulatório, Edmir Netto de Araújo (2002) explica que não pode ser confundido com o poder regulamentar de competência do Chefe do Executivo, que se vincula à norma legal para esclarecê-la, minudenciá-la e facilitar sua execução. Seu escopo, portanto, refere-se à possibilidade de edição de normas gerais de caráter técnico formalizada por atos administrativos normativos sobre matéria de ordem técnica, que, por ser extremamente particularizada, não estão contidas na lei.

Tais transformações implicaram diretamente no rol de competências da Autoridade. Ao passo que na versão aprovada pelas Casas Legislativas previa a incumbência de "editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, assim como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco para a garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; " (antigo art. 56, XIII), em referência clara ao poder regulador, e à atuação prévia e conjunta com empresas referentes aos relatórios de riscos; o atual suprimiu a segunda parte, e apenas prevê de maneira genérica "editar normas e procedimentos sobre a proteção de dados pessoais" (art. 55 - J, II), como forma de esvaziamento de seu esvaziamento.

O poder regulador junto ao poder fiscalizatório da Autoridade é inerente à sua própria razão de ser, uma vez que deve emanar regulamentos e diretrizes a serem observados a todos os segmentos de mercado e, ato contínuo, realizar controle do cumprimento das suas

disposições e da própria LGPD. O bom funcionamento imprescinde de independência funcional, livre de vinculações políticas ou de *lobby* de setores específicos.

Relativo à autonomia financeira, foi eliminada a competência para arrecadar e aplicar receitas, dependendo seu funcionamento tão somente do orçamento do executivo (antigo art. 55, XV), restringindo sua capacidade em empreender medidas destinadas à consecução de seus objetivos institucionais. Ademais, a norma dispõe que não haverá a previsão de novos gastos, sendo "os cargos em comissão e as funções de confiança da Autoridade Nacional de Proteção de Dados serão remanejados de outros órgãos e entidades do Poder Executivo Federal" (art. 55 - H). Por sua vez, "Os ocupantes dos cargos em comissão e das funções de confiança da Autoridade Nacional de Proteção de Dados serão indicados pelo Conselho Diretor, nomeados ou designados pelo Diretor-Presidente" (art. 55 - I).

Ocorre, no entanto, que quem indica o Conselho Diretor e o Diretor-Presidente é o Presidente da República, ou seja, este possui ingerência indireta em relação a todo o quadro de pessoal da Autoridade. É prejudicial ainda a falta de servidores de carreira, aprovados em concurso público com prova que ateste os conhecimentos técnicos e jurídicos específicos que se exige, isento de pressões advindas de questões políticas.

Conforme Bruno Bioni (2018), a Autoridade precisa ter capacidade institucional com recursos humanos especializados para atingir a missão regulatória e fiscalizatória atribuída. Cita, por exemplo, a autoridade francesa de proteção de dados (CNIL), em que além do advogado e de cientistas políticos, existem engenheiros e cientistas da computação que analisam e fazem as auditorias de códigos e de *sites* para analisar os mecanismos e a atuação dos agentes de tratamento, com o fim de auferir possível responsabilidade[74].

A estrutura interna delineada é a seguinte: Conselho Diretor; Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, com previsão de composição multissetorial; Corregedoria; Ouvidoria; órgão de assessoramento jurídico próprio; unidades administrativas e unidades especializadas. A estrutura regimental será disposta por ato do Presidente da República (Art.55-G).

---

74 *EU Privacy Law Snares Its First Tech Giant*: Google https://www.wired.com/story/eu-privacy-law-snares-first-tech-giant-google/ Acesso em: 6 de fevereiro de 2019.

Foram mantidas algumas prerrogativas existentes no exercício da investidura no Conselho Diretor característicos de agência reguladora. Desta forma, a nomeação deve ser por prazo determinado, com relativa estabilidade em seus cargos, ausente a possibilidade de exoneração *ad nutum* pelo Chefe do Executivo, cujos membros somente podem deixar o cargo voluntariamente, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar. Com a saída, ainda é preciso respeitar o período de quarentena (art. 55 - F).

Em que pese tal previsão, vê se que o Conselho Diretor está frente a um órgão sujeito à subordinação e à hierarquia da Presidência da República, logo, sua independência funcional é reduzida, ainda mais quando o crivo sobre a instauração e julgamento de processo administrativo disciplinar fica a cargo deste (art. 55 - E).

Quanto às competências, foram mantidas as previsões destinadas à promoção de estudos e de medidas para difundir conhecimento sobre as normas e as políticas públicas de proteção de dados pessoais e sobre medidas de segurança, bem como realizar consultas públicas sobre temas de sua área de atuação; o respeito ao segredo industrial e comercial; a existência de consultas públicas; e o estímulo à adoção de padrões.

Ressaltam Moncau *et al* que a independência é fator de extrema importância para o funcionamento das Autoridades de Proteção de Dados. Cita o caso decidido em 2014 pelo Tribunal de Justiça da União Europeia, que entendeu que a Autoridade húngara teve sua esfera de independência não respeitada porquanto o supervisor da autoridade foi substituído antes do fim de seu mandato de seis anos: “O Tribunal considerou que as autoridades não podem estar sujeitas a nenhum tipo de influência externa, e que a alteração da liderança da autoridade seria uma ofensa à independência da instituição” (2015, não p.).

Sobre os processos de nomeação aos cargos decisórios das Autoridades, detalha o documento:

> Em diferentes países, a nomeação dos cargos da autoridade de proteção de dados é feita envolvendo o executivo, o legislativo, o judiciário e por vezes grupos da sociedade civil. Há casos em que se questiona a independência das autoridades tendo em vista que a indicação ou nomeação dos agentes é feita somente pelo Governo, sem que seja recebida a opinião, o

> consentimento ou a revisão do poder legislativo. Este é o caso da Lituânia, da Letônia, da Estônia, da Irlanda e do Reino Unido (2015, não p.).

Em comentários sobre a mudança legislativa, Ronaldo Lemos *et. al.* (2018) entendem que:

> Ressaltamos, todavia, que entre as principais razões para a necessidade de criação da própria Autoridade está justamente sua atuação como instância regulatória capaz de apresentar opiniões técnicas específicas à proteção da privacidade nos diferentes segmentos de mercado, e de realizar controle unificado e homogêneo do cumprimento das disposições da LGPD, independentemente de quaisquer vinculações políticas ou ideológicas ou pressões de setores específicos. Além disso, a sofisticação e a rápida mudança das questões relacionadas à privacidade e proteção de dados (sobretudo em ambiente virtual) requerem a atuação de profissionais capacitados para lidar com os novos e cada vez mais complexos cenários referentes ao tema, diante da sua aplicação em diferentes setores de mercado.

A independência faz parte essencial das Autoridades, a fim de que estejam protegidas contra influências político-partidárias, bem como para a aplicação devida da norma à administração direta e indireta. Também como proteção dos próprios cidadãos, isso porque a própria Medida Provisória também promoveu mudanças às regras sobre tratamento de dados pelo Poder Público, ampliando possibilidades de transferência de dados pessoais a entidades privadas: existência de previsão legal ou a transferência respaldada em contratos, convênios ou instrumentos congêneres; casos em que a transferência dos dados objetivar a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados; e casos em que os dados forem acessíveis publicamente.

Sobre o tema, Ronaldo Lemos *et. al*. (2018) asseveram:

> Embora o texto original da LGPD apresentasse problemas de técnica legislativa que tornavam de difícil compreensão o capítulo sobre tratamento de dados pessoais pelo Poder Público, de modo a

> permitir o surgimento de interpretações contrárias ao interesse público e aos princípios constantes da referida lei, a alternativa instituída pela Medida Provisória apresenta hipóteses demasiadamente amplas e desacompanhadas de obrigações de transparência sobre o uso de dados de cidadãos pelo governo. Mais que isso, a dispensa de obrigação de comunicação da Autoridade Nacional de Proteção de Dados sobre referidas práticas, reduz drasticamente a capacidade de fiscalização dessas práticas pela autoridade ou outros interessados. Similar flexibilização das regras de tratamento de dados pelo Poder Público é bastante prejudicial porque gerar riscos à preservação de direitos e garantias individuais, em virtude da ausência de protocolos rígidos, procedimentos claros e limites legais. Entendemos que o envio e recebimento de dados pessoais por órgãos públicos em razão de parceria com entidades públicas ou privadas poderá gerar benefícios sociais.

Além das reformas mencionadas, outras foram inseridas pela Medida Provisória n. 869/2018: a exclusão do direito à revisão por pessoa natural às decisões automatizada, agravando a condição do consumidor sujeito a critérios de discriminação, diminuindo as possibilidades de entendê-la e contestá-la; aumentou o período de *vacatio legis* de 18 para 24 meses; e permitiu o compartilhamento de dados de saúde por agentes de saúde suplementar.

De acordo com Mendes e Doneda (2018a, p. 477-478), a Autoridade de Proteção é um dos pilares de sustentação do regime de proteção de dados pessoais sustentando o arcabouço normativo e principiológico delineado:

> Sem uma autoridade central, independente e com credibilidade técnica, dificilmente será possível a aplicação consistente e harmônica da Lei em setores tão diversos como os que compõem o seu âmbito de aplicação. Somente por meio de uma autoridade nesses moldes, com competência inclusive para atuar e incentivar a cooperação institucional, é que será possível superar o risco da atomização de decisões múltiplas e conflitantes entre os diversos atores legitimados para atuar na

> proteção de dados, considerando o arranjo institucional brasileiro como o de fiscalizar o tratamento de dados e sancionar o descumprimento à legislação, regulamentar hipóteses não especificadas na legislação.

A subordinação da Autoridade Nacional de Proteção de Dados à Presidência da República cria instabilidade política e insegurança jurídica, afinal, proporciona bases legais para a opacidade governamental, com respaldo de uma norma que, em tese, possui o intuito de proteger o indivíduo. Igualmente, esvazia o espaço de autonomia da Autoridade, mormente no que tange ao poder fiscalizatório e sancionatório, ou seja, no que se refere ao *enforcement* da norma, com instrumentos eficazes de verificação, coação, e aplicação de sanções em relação a todos os atores que se submetem à norma.

Ademais, conforme lembram Mendes e Doneda (2018b, p. 586) a Autoridade é uma peça indispensável para que o Brasil obtenha as vantagens econômicas e políticas derivadas da LGPD, como o ingresso facilitado na Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e a adequação prevista no GDPR para o fluxo e o comércio internacional de dados, os quais têm exigido "requisitos mais concretos quanto à proteção de dados, sendo um deles a existência de uma autoridade independente como condição para que empresas ou órgãos brasileiros possam participar livremente de fluxos internacionais de dados, tão caros à nova economia da informação".

Segundo o exposto até o momento, nessa nova racionalidade regulatória, privilegia-se tanto a tutela coletiva, quanto a individual. A cooperação entre os atores desse ecossistema – órgão regulador, agentes econômicos, terceiros certificadores, poder público, sociedade civil – faz-se imprescindível para atingir e manter os níveis de conformidade (*accountability)* exigidos pela norma.

A função a ser exercida pela Autoridade Nacional de Proteção de Dados com vistas a integrar todos os atores, é a supervisional e interpretativa, por exemplo, validar códigos de boa conduta, de certificar a atuação dos agentes de tratamento, de avaliar e construir os parâmetros de legítimo interesse. Não se olvida ainda as outras funções fiscalizatória e sancionatória que lhe foram designadas.

Nesse enleio, verificou-se: "A existência de autoridades supervisoras robustas tem sido considerada como condição sine qua non para a adequada proteção à privacidade, pois as leis não são autoimplementáveis e a cultura da privacidade não pode se estabelecer

sem uma autoridade que a patrocine" (BENNET; RAAB, apud MENDES, 2014, p. 48)."

Finalmente, já está no Congresso Nacional a análise da Medida Provisória n. 869/2018 que ainda precisa ser votada pelo Congresso Nacional para sua conversão em Lei. No âmbito de sua tramitação, no dia 4 de fevereiro de 2019, foi criada uma Comissão Mista para análise e avaliação. Em apenas uma semana após sua formação, foram propostas oitenta e oito emendas à redação da Medida Provisória[75].

Propostas realizadas pelo Senador Humberto Costa, pelo Deputado Alessandro Molon e pelo Deputado Ivan Valente preconizam a retomada da estrutura inicial da Autoridade Nacional de Proteção de Dados, qual seja, instituição da administração pública federal indireta, submetida a regime autárquico especial, vinculada ao Ministério da Justiça. Leia-se a justificação constante na Emenda dos parlamentares:

> A independência da ANDP é de extrema importância para o exercício de suas funções. A garantia é fundamental para o exercício isonômico e imparcial de sua função precípua, a fiscalização do poder público e das empresas. Subordinada diretamente ao governo, o acompanhamento do tratamento de dados realizado pelo poder público fica significativamente comprometido, sujeito a influências políticas dos governantes de plantão. Garantir a autonomia e independência técnica e política da Autoridade é garantir a eficácia da Lei de Dados Pessoais, justamente porque é a ANPD que tem a capacidade de monitorar e impor penalidades às condutas que venham a contradizer a Lei. Tanto é que tais características figuram, na avaliação da OCDE (Organização para Cooperação e Desenvolvimento Econômico), como essenciais para a proteção de dados pessoais nos países que pretendem ingressar no bloco. O reconhecimento internacional do Brasil como um país que confere um nível de adequado de proteção de dados pessoais também depende, necessariamente, da existência de uma Autoridade independente e autônoma.[...]Estar vinculada ao Ministério da Justiça, ao invés da Casa Civil, é

[75] Disponível em: https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/135062 Acesso em: 11 de fevereiro de 2019

> também uma necessidade importante. A autoridade, como prevista na Lei, terá diálogo direto com os órgãos administrativos integrantes do Sistema Nacional de Defesa do Consumidor, tal como a Secretaria Nacional do Consumidor (Senacon/MJ) e os Procons. Vinculadas ao mesmo ente administrativo - o Ministério da Justiça - o diálogo institucional e as possibilidades de colaboração e atuação complementar são evidentemente incrementadas. Além disso, a Autoridade Nacional de Proteção de Dados é também requisito importante para o combate à corrupção e para a investigação de crimes em escala internacional, uma vez que é também considerada necessária pela Interpol (Organização Internacional das Polícias) para a colaboração em investigações.1 Assim, não faz sentido manter a autoridade vinculada à Casa Civil, diretamente ligada ao Executivo Federal, o que compromete o exercício de suas competências.[76][77][78]

Nesse compasso, o Deputado Orlando Silva também aventou Emenda Modificativa, a fim de mudar a natureza jurídica da autoridade para autárquica, contudo, nos termos da redação deste parlamentar, sua vinculação seria à Casa Civil, e não ao Ministério da Justiça.

Devido à falta de tempo hábil para análise de todas as propostas de Emendas à Medida Provisória citam-se algumas outras propostas: inclusão de arguição pública pelo Senado Federal na escolha de membro do Conselho Diretor; reinclusão da revisão de decisão automatizada por pessoa natural; diminuição do período de *vacatio legis;* inclusão da incumbência do operador também indicar encarregado, equiparando-se no ponto a controlador; exclusão da necessidade de minimização dos dados quando o tratamento for baseado no legítimo interesse, etc.

---

[76] Disponível em: https://legis.senado.leg.br/sdleg getter/documento?dm=7912637&ts=1549895776602&disposition=inline Acesso em: 11 de fevereiro de 2019.

[77] Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7911686&ts=1549895775576&disposition=inline: Acesso em: 11 de fevereiro de 2019.

[78] Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7910927&ts=1549895774988&disposition=inline. Acesso em: 11 de fevereiro 2019.

Em 27 de março de 2019 foi instalada uma Comissão Mista para tratar do assunto, em que foi eleito como Presidente o Senador Eduardo Gomes e designado Relator o Deputado Orlando Silva.

Em suma, algumas Emendas possuem o desiderato de que prevaleça a redação original aprovada pelas Casas Legislativas, em detrimento das reformas forjadas pelo Executivo, ao passo que outras tendem a prejudicar o regime de proteção destinado ao titular dos dados. O ponto nevrálgico versa sobre a natureza jurídica da Autoridade Nacional de Proteção de Dados, porquanto refletirá diretamente em sua estrutura, suas competências e na sua futura atuação. Fatores como especialidade e autonomia técnica, independência política e funcional, independência administrativa e financeira são cruciais tanto para o sucesso da Autoridade, e, por corolário, da Lei Geral de Proteção de Dados: certificações, ações de fiscalização e aplicações de sanção, por exemplo, são essenciais para coagir as mudanças perquiridas nas práticas empresariais e do poder público, bem como proporcionar transformações para criação de uma cultura de privacidade e de proteção de dados pessoais.

A despeito da existência da urgência existente na criação da Autoridade de Proteção de Dados Pessoais, a forma em que está delineada não atende aos anseios e preocupações para a maior proteção e tutela coletiva do indivíduo, sendo essencial a reversão pelo Legislador, a fim de que a redação e a proposta original sejam retomadas.

3. A PROTEÇÃO DE DADOS REFERENTES À SAÚDE DE PROGRAMAS DE FIDELIZAÇÃO EM REDES DE FARMÁCIA

O mercado de varejo farmacêutico no Brasil gera cifras bilionárias de receita. Segundo pesquisa realizada pela QuintilesIMS[79], empresa especializada no mercado de dados farmacêuticos, em 2017, o setor faturou aproximadamente 57 bilhões de reais. Comparativamente, em 2013, o faturamento havia sido de 36 bilhões de reais. O país figura como o sexto maior mercado de medicamentos do mundo.

Outra pesquisa foi realizada pelo grupo[80], em 2017, com o fito de entender o perfil geral de consumo dos brasileiros em farmácias. Na amostra, foram analisados dados de homens e mulheres, com idades entre 18 e 55 anos, com padrão econômico médio e alto (classes A, B e C), que fizeram compras em 850 farmácias em todo o Brasil, durante o período de 30 dias.

O estudo demonstrou, em síntese, que medicamentos e produtos de higiene pessoal estão entre os itens recorrentemente comprados e que os consumidores brasileiros estão consumindo com maior regularidade em lojas pertencentes a grandes cadeias e redes de farmácia, do que em estabelecimentos independentes, como farmácias de bairro, por exemplo. Além disso, a frequência e o número de viagens para realização de transações aumentaram mais de um terço em comparação ao mesmo estudo realizado no ano anterior.

Com fulcro nesses dados, na conclusão do estudo, o conselho destinado às *health care companies* para o aumento de suas vendas foi o seguinte*: "*para que aproveitem ao máximo essas oportunidades de varejo, elas precisarão refletir sobre suas estratégias de preços e usar promoções criativas e ofertas de cupons para atrair esses compradores a maximizar seus gastos.".

A estratégia utilizada pelas redes de farmácia para promover "promoções criativas" e "ofertas de cupons" é a de fidelizar os consumidores com programas que, supostamente, promovem descontos e benefícios. Por trás, está a massiva coleta de dados referentes à saúde dos clientes.

---

[79] https://www.interfarma.org.br/guia/guia2018/dados_do_setor#varejo_brasileiro

[80] Where Brazilians go to shop Disponível em: https://www.iqvia.com/en/blogs/2017/11/where-brazilians-go-to-shop. Acesso em: 11 de fevereiro de 2019.

Essas práticas colocam o consumidor em uma posição que a concessão dos dados é praticamente compulsória, não apenas pela forma impositiva que eles são solicitados, mas porque os supostos descontos levam, inevitavelmente, a pessoa a aceitar. Amanda Yumi Ambriola comentou sobre tal prática em entrevista realizada por Sergio Amadeu da Silveira: "Um medicamento que você vai comprar sem cartão da farmácia é R$ 150,00 e com o cartão é R$ 60,00. Isso é obrigar o usuário a fazer o cadastro. Ele fala que é uma vantagem, mas sabemos que nossos dados não valem R$ 90,00. A gente tá sendo punido por não conceder os dados.".[81]

É possível perceber a compulsoriedade quando se avalia a realidade social, cujo valor do salário mínimo é de apenas R$ 998,00 mensais, e o custo médio com medicamentos *per capita* anual atinge o valor de US$ 200,00[82].

Ademais, nesse contexto, o consumidor, além da vulnerabilidade que lhe é inerente, encontra-se em uma situação cuja assimetria informacional é abissal, sequer possui conhecimento dos possíveis usos de seus dados, quem terá acesso, por quanto tempo, e as possíveis futuras repercussões negativas em sua vida.

À vista disso, este capítulo, cerne do trabalho, tem por intenção examinar as disposições relacionadas à proteção de dados referentes à saúde constantes na recente Lei Geral de Proteção de Dados e outras normativas esparsas, bem como os instrumentos contratuais que respaldam os programas de fidelidade de redes de farmácia da Grande Florianópolis.

3.1 DADOS DE SAÚDE

Com a evolução das tecnologias de informação, o registro de dados de saúde que era realizado em meio físico, gradativamente passou a ser realizado no meio digital. De acordo com Bologna *et al*. (2016), o que era tido simplesmente como *health data* ganhou nova qualificação e passou a ser chamado de *e-Health*, em menção à *electronic health*

[81] SILVEIRA, Sérgio Amadeu. AMBRIOLA, Amanda Yumi; **As implicações políticas dos algoritmos.** Tecnopolítica. 7min 28s. Disponível em: https://www.youtube.com/watch?v=aRkqfx_XTVY. Acesso em: 30 de dezembro de 2018.

[82] https://www.interfarma.org.br/guia/guiam2018/dados_do_setor#varejo_brasileiro

record (EHR). Neste caso, alude-se tanto ao armazenamento digital dos dados diretamente neste meio, ou digitalização do que fora coletado em meio físico, quanto ao compartilhamento dos dados aos atores do sistema, com o intuito de processamento e de comunicação.

A Lei Geral de Proteção de Dados Pessoais utiliza a expressão "dado relacionado à saúde" ao longo do seu texto, contudo, não traz sua definição. Conforme será visto de maneira detida posteriormente, a ausência da limitação semântica do termo poderá causar insegurança jurídica e ser prejudicial à proteção dos titulares, de acordo com a extensão da interpretação empregada.

Assim, com a finalidade de auxiliar na compreensão do termo, reproduz-se a definição contida no GDPR, qual seja, "dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde". Ainda consta na exposição de motivos contida no preâmbulo o seguinte:

> Deverão ser considerados dados pessoais relativos à saúde todos os dados relativos ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro [...] qualquer número, símbolo ou sinal particular atribuído a uma pessoa singular para a identificar de forma inequívoca para fins de cuidados de saúde; as informações obtidas a partir de análises ou exames de uma parte do corpo ou de uma substância corporal, incluindo a partir de dados genéticos e amostras biológicas; e quaisquer informações sobre, por exemplo, uma doença, deficiência, um risco de doença, historial clínico, tratamento clínico ou estado fisiológico ou biomédico do titular de dados, independentemente da sua fonte, por exemplo, um médico ou outro profissional de saúde, um hospital, um dispositivo médico ou um teste de diagnóstico in vitro.

No GDPR, os dados relacionados à saúde também são considerados sensíveis, sendo vedado seu tratamento, salvo para as seguintes finalidades: medicina preventiva ou do trabalho para a avaliação da capacidade laboral; gestão de sistemas e serviços de saúde; por força de um contrato com um profissional de saúde, em todos os

casos devem ser tratados sob a responsabilidade de pessoa sujeita à obrigação de sigilo profissional ou outra igualmente sujeita a uma obrigação de confidencialidade.

Elenca ainda a possibilidade de derrogação da proibição por motivos de interesse público como questões sanitárias, saúde pública ou gestão de serviços de saúde quando houver alerta em matéria de saúde, prevenção ou controle de doenças transmissíveis; a fim de regularizar a prestação governamental, de serviços no quadro do regime de seguro de saúde, ou para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos. Nesses casos, o tratamento independe de consentimento e é vedado o compartilhamento de dados a terceiros com outros fins, como os empregadores ou as companhias de seguros e entidades bancárias.

O Regulamento em sua exposição de motivos número 64 dispõe ainda o seguinte acerca do acesso a dados de saúde pelo titular:

> [...] os dados dos registos médicos com informações como diagnósticos, resultados de exames, avaliações dos médicos e quaisquer intervenções ou tratamentos realizados. 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.

O direito de acesso no caso de dados de saúde assume relevância ainda maior, uma vez que são dados que respeitam ao estado do indivíduo, devendo ter seu controle e os compartilhando apenas com quem preferir: membros da família, pesquisadores e médicos de sua confiança.

Nos Estados Unidos, por exemplo, onde não há regulamentação geral sobre o tema, os controladores assumem uma posição proprietária

dos dados coletados. Conforme Schneier (2016) não se trata da figura dos médicos que fazem o armazenamento, mas sim de empresas terceiras que centralizam essas informações.

Lá existem movimentos de pacientes e famílias de pacientes que clamam pelo direito de acessar seus dados de saúde, protestando-se pelo direito de poder escolher com quem compartilhá-los, um deles, inclusive é liderado pelo cripógrafo Bruce Schneier.[83]

Outro tema que causa preocupação no país norte-americano concerne justamente à segurança destes dados. Conforme Deborah Lupton, no ano de 2017, em apenas duas empresas de seguro de saúde - Anthem e Premera Blue - foram reportadas centenas de invasões em bases de dados envolvendo milhões de registros de saúde apenas de duas empresas, afetando mais de 90 milhões de americanos[84]. As invasões são frutos de tentativas de extorsão baseadas no sequestro de dados; e a facilidade para falsificações ideológicas, a fim de conseguir remédios para revender posteriormente e também para fraudar as empresas de seguro.

Um caso que chamou a atenção foi a falha de segurança no banco de dados da *Red Cross Blood Service*, prestadora de serviços de coleta e doação de sangue na Austrália. Em 2016 ocorreu o vazamento e publicação de dados referentes a coletas de sangue realizadas entre os anos de 2010 e 2016,[85] afetando aproximadamente 550.000 doadores. Além dos dados de identificação, ainda constavam categorizações relativas a "pessoa com comportamento sexual de risco", ilação obtida de acordo com as respostas a um questionário disponibilizado ao doador no momento da coleta de sangue.

Veja-se que o tema envolve diversas áreas do conhecimento, setores econômicos, interesses governamentais, e, até mesmo éticos ligados ao exercício da medicina. Neste capítulo, primeiramente, será abordado, de maneira bastante breve, a relação entre o controle desses dados e o exercício do biopoder tanto pelo governo quanto por entidades

---

83 Who controls your medical data? Disponível em: https://www.youtube.com/watch?v=l7Y8sKYL--c. e Let's pool our medical data https://www.ted.com/talks/john_wilbanks_let_s_pool_our_medical_data Acesso em: 10 de dezembro de 2018.

84 Disponível em: https://simplysociology.wordpress.com/category/digital-health/. Acesso em: 19 de dezembro de 2018

85 *Red Cross Blood Service admits to personal data breach affecting half a million donors.* Disponível em https://www.abc.net.au/news/2016-10-28/red-cross-blood-service-admits-to-data-breach/7974036 Acesso em: 22 de janeiro de 2019.

privadas; e, em seguida, as disposições específicas constantes na LGPD sobre o assunto.

3.1.1 Saúde e Medicina

Devido ao processo de urbanização e ao início da conformação das cidades modernas, a gestão de questões relacionadas à saúde, à sexualidade e à natalidade passaram a ser objeto de preocupações políticas. Consoante Foucault, em Microfísica do Poder (1998), a medicina foi erigida, no Século XVIII, como um dos campos de poder sobre o corpo do indivíduo[86]: enquanto mecanismo de controle passou a fazer parte da noção de biopolítica, exercido pelo Estado sobre a "população [que] passa a ser modulada por mecanismos de regulação perante uma prática de governo e norteada pela formação de um conjunto de saberes estatísticos e demográficos" (Hur, 2013).

Foucault (1998) aduz que nessa época também se iniciaram as estratégias de políticas públicas: os Estados buscavam informações dos indivíduos com o fito analisar estatisticamente sua população, a fim de desenvolver estratégias de atuação visando ao aumento da natalidade e controle de doenças infecciosas e epidêmicas. Neste contexto, os planos de ação eram definidos, quais doenças seriam observadas e combatidas, e, consequentemente, quais doenças seriam negligenciadas.

Nesse diapasão, constatam-se as duas faces do biopoder: ao mesmo tempo em que o indivíduo passa a ser cuidado pelo Estado, também é dominado por este, ou seja, a promoção da vida e da saúde têm um custo, qual seja, o controle da vida e dos corpos.

No caso relativo aos dados de saúde, as informações eram captadas, principalmente, por profissionais da saúde, tais como médicos, enfermeiros e técnicos, que atendiam os sujeitos que demandavam sua

86 Roberto Machado, na apresentação do livro Microfísica do Poder: "Muitas vezes, esses saberes desenvolvidos, que fazem parte dos repertórios da Medicina, Psiquiatria, Psicologia, etc., entram em conflito com o próprio Estado. Foucault (1982), por exemplo, trabalha essa tensão entre Estado e mecanismos disciplinares em sua obra 'Eu, Pierre Rivière, que degolei minha mãe, minha irmã e meu irmão'. Trata-se do caso de uma pessoa que matou sua família e que se tornou disputa entre Direito e Medicina. Dessa forma, deveria ser preso ou internado no manicômio? Era um criminoso ou louco? Ou seja, qual instância tinha poder sobre Pierre Rivière? A base jurídica do Estado ou o mecanismo disciplinar Medicina? Portanto, gerou-se um conflito entre poder de Estado e mecanismo disciplinar, em que Foucault trabalhou esse caso como analisador dessa tensão" (1998, p. XVIII).

atenção, seja na residência dos pacientes ou em locais centralizados como clínicas e hospitais. Quem está na ponta, em contato com os indivíduos, coleta e transfere as informações para os pontos mais altos de hierarquia, de modo que no cume dessa pirâmide disciplinar haja uma onisciência do que ocorre abaixo dela, sendo latente a relação entre o saber e o poder: quem vigia tem a possibilidade do registro contínuo de fatos e a construção de conhecimento, intimamente ligado ao exercício das relações de poder, segundo observa Foucault (1998, p. 110):

> Em primeiro lugar, técnicas de identificação dos doentes. Amarra-se no punho do doente uma pequena etiqueta que permitirá distingui-lo mesmo se vier a morrer. Aparece em cima do leito a ficha com o nome e a doença do paciente. Aparece, também uma série de registros que acumulam e transmitem informações: registro geral das entradas e saídas em que se anota o nome do doente, o diagnóstico do médico que o recebeu e a sala em que se encontra, e depois, se morreu ou saiu curado; registro de cada sala feito pela enfermeira-chefe; registro da farmácia em que se fiz que receitas e para que doentes foram despachadas; registro do médico que manda anotar, durante a visita, as receitas e o tratamento prescritos, o diagnóstico, etc. [...] constitui-se, assim, um campo documental no interior do hospital que não é somente um lugar de cura, mas também de registro, acúmulo e formação do saber.

Han (2018, p. 74) faz a seguinte síntese: "O biopoder exerce funções de incitamento, de reforço, de controle, de vigilância de potenciação e de organização das ofertas que submete. Destina-se a produzir forças, a fazê-las crescer e a ordená-las, mais do que contê-las, ou destruí-las".

Sem embargo o papel exercido pelo Estado para manutenção da articulação de saberes com a estrutura social[87], a partir do século XIX, esse não deve mais ser considerado um aparelho único e exclusivo de poder, que passa a ser também exercido por instituições privadas. Em

87 O autor descreve três diferentes modelos principais de intervenção médica que foram desenvolvidos na Europa, a Medicina de Estado (prioritariamente na Prússia/Alemanha), a Medicina Urbana (prioritariamente na França) e a Medicina da Força de Trabalho (prioritariamente na Inglaterra).

outras palavras, o poder se manifesta em outros locais, específicos, circunscritos a uma pequena área de ação, que atinge o cotidiano e a realidade mais concreta dos sujeitos. Roberto Machado, na apresentação do livro supramencionado, assevera: "a razão é que o aparelho de Estado é um instrumento específico de um sistema de poderes que não se encontra unicamente nele localizado, mas o ultrapassa e complementa" (1998, p. XIX).

Atualmente, verifica-se que tanto entidades governamentais, quanto privadas, atuam na coleta de dados de saúde dos indivíduos, cujo sistema não mais se restringe a profissionais que possuem contato direto com o paciente: além da expansão do número de atores, a quantidade e a acurácia referente ao armazenamento e processamento de tais dados cresceu significativamente, por conta do contexto tecnológico informacional já assinalado.

Está desenhado um sistema capilar que penetra em todos os cantos da vida e coleta dados a partir de diferentes fontes, tais como: compras em farmácias; buscas em mecanismos de pesquisas[88]; utilização de cartões de benefícios e de planos de saúde; cadastros dos próprios laboratórios da indústria farmacêutica; laboratório de exames; aplicativos destinados a controles e informações de saúde, como período fértil, perda de peso, rendimento físico em esportes ou academia; compra e consumo de comidas; redes sociais e de apoio para pessoas enfermas ou portadoras de alguma situação patogênica. Em suma, dados de medicamentos, dados de aplicativos, dados de dispositivos, dados clínicos, de comportamento e até de sentimento podem ser coletados e permitem o conhecimento cada vez mais preciso acerca de um indivíduo.

Sabido que tais programas, aplicativos e dispositivos, bem como sistemas de armazenamento de dados de saúde cativam também os pacientes, afinal, lhe são convenientes; bem como redes de contato com

88 *Google Flu mines search engine queries to track real-time flu trends, yielding results much faster than the CDC's traditional epidemiological surveillance methods. It is possible that such tactics could deter people from using the tool and render it useless. The efficacy of the tool has already been called into question: while Google's tool had been accurate in the past, in early 2013 Google grossly overestimated the actual flu patterns in the U.S. due to increased public interest caused by extensive media coverage. However, early detection allows for early public health intervention, which may reduce the spread of disease and potentially save lives*. Disponível em: http://www.theatlanticwire.com/technology/2013/02/google-flu-trends-wildlyoverestimated-years-flu-outbreak/62113/

outras pessoas enfermas que lhe dão apoio psicológico. Veja-se a exposição de motivos da recente Resolução do Conselho Federal de Medicina n. 2.227/208, que disciplina a telemedicina como forma de prestação de serviços médicos mediados por tecnologias:

> O impacto da ascensão da telemedicina como crescente e variável número de aplicativos e dispositivos móveis amigáveis permite que os pacientes usem a tecnologia para monitorar sua saúde. Dispositivos de uso doméstico simples, que podem monitorar sinais vitais, permitem a coleta de informações necessárias para diagnóstico por um médico.

Quando se fala em avanços tecnológicos na área de medicina, são ressaltados apenas suas externalidades positivas, pouca atenção é dada às negativas, como, por exemplo, a instauração de um ambiente de vigilância, catalogação, ranqueamento e classificação. Os dados proporcionam um regime que vai além da biopolítica, chegando à psicopolítica, afinal, quem possui o acesso a eles, tem condições de ler e controlar pensamentos (HAN, 2018).

Ademais, conforme Frank Pasquale (2015) e Pam Dixon e Robert Gellman (2014), já foram desenvolvidos e são utilizados os *health scores*[89] que possuem amparo em um *body score*, tal qual os sistemas de crédito conhecidos como *credit score*.

Em linhas gerais, nos termos de Schmitz (2014), o *consumer scoring* tem por base a coleta de dados usando matemática avançada, modelagem estatística e algoritmos para cristalizar muitos fatores em números. São utilizados para se poder prever algum comportamento

89 O Fórum Mundial da Privacidade assim define *score* de consumo: *A consumer score that describes an individual or sometimes a group of individuals (like a household), and predicts a consumer's behavior, habit, or predilection. Consumer scores use information about consumer characteristics, past behaviors, and other attributes in statistical models that produce a numeric score, a range of scores, or a yes/no. Consumer scores rate, rank, or segment consumers. Businesses and governments use scores to make decisions about individual consumers and groups of consumers. The consequences can range from innocuous to important. Businesses and others use consumer scores for everything from predicting fraud to predicting the health care costs of an individual to eligibility decisions to almost anything.* Disponível em: https://www.ftc.gov/system/files/documents/public_comments/2014/08/00014-92369.pdf

futuro, avaliar os riscos, e, essencialmente, auxiliar no processo de tomada de decisão. As empresas de pontuação do consumidor empregam cálculos atuariais e matemáticos para prever o valor provável de um consumidor individual como cliente.

Pam Dixon e Robert Gellman (2014), afirmam que tanto o setor privado[90], quanto o setor governamental se utilizam de *scores.* Seu risco está no potencial de ameaçar a privacidade, a igualdade e até mesmo a garantia de devido processo, uma vez que os fatores, pesos e informações que alimentam os algoritmos são desconhecidos dentro de um sistema opaco e complexo ao consumidor, que se revela uma verdadeira caixa preta, conforme cunhou Frank Pasquale (2015).

Especificamente quanto ao *health score,* observa-se sua utilização para subsidiar a tomada de decisão para propósitos diferentes, tal como marketing, avaliação de plano de saúde e até mesmo para avaliação de crédito (*credit score),* por exemplo: um indivíduo que possui uma doença crônica oferece mais riscos de inadimplir um empréstimo, por conta da probabilidade de convalescer ou vir a falecer, em relação a um indivíduo saudável.

Indústria farmacêutica, redes de farmácia, clínicas, empresas de recrutamento de pessoal, seguradoras de saúde e de vida são exemplos de setores que podem se valer das informações extraídas com arrimo no histórico de uso de medicamentos ou no *health score*. No caso destas últimas, podem ser subsídios não apenas para regulação de preço, mas também para denegação da contratação, ou invocar como uma excludente de cobertura, por exemplo, a utilização de um medicamento

90 Conforme consta no Relatório do Fórum Mundial da Privacidade: *Launched on June 23, 2011 by analytics firm Fair Isaac Corp., this score identifies a patient's propensity to adhere to a medication prescription plan during the next 12 months. It is a predictive score designed to let pharmacies and insurers know when or if a patient is at risk and needs a medication reminder. The score pulls from public data and from patients' prescription histories when available. The score ranges from 1-500, with a score above 400 indicating that a patient is likely to take medications as prescribed. Patients who score 200 or below may get a reminder, as a low score predicts nonadherence. [...] If the manufacturer can identify those patients who are likely to refill prescriptions anyway, it can tell the intermediaries to send reminders only to those who have a low adherence score. The effect is to pay less to FICO and avoid paying a larger amount for a notice.* Disponível em: https://www.ftc.gov/system/files/documents/public_comments/2014/08/00014-92369.pdf

autoadministrado, cujos efeitos colaterais estão ligados ao desenvolvimento da doença que acomete o indivíduo.

No caso de empresas de recrutamento de empregados, podem ser verificadas quais doenças afligem uma pessoa, a probabilidade de ela vir a adoecer e, no caso das mulheres, se esta possui filhos, com base em compras de teste de gravidez de maneira periódica, que está tentando engravidar; se compra pílulas anticoncepcionais ou outros métodos contraceptivos.

Ocorre, contudo, que no âmbito desse ecossistema, conforme pesquisa realizada por Dixon e Gellman (2014), a maioria dos consumidores sequer possui conhecimento básicos sobre a coleta e o uso de dados. No caso específico de farmácias, que é uma importante ponta de contato direto com consumidores, e que coleta dados importantes acerca da venda de medicamentos, e até de outros artigos ligados à higiene pessoal e à contracepção, ainda se utilizam de técnicas de fidelização consumidor, como será visto a seguir.

O jornalista Chad Ternuhe revelou como nos Estados Unidos os dados de prescrição médica utilizados na compra de medicamentos nas farmácias estavam baseando denegações de cobertura no mercado de seguros de saúde individuais e, consequentemente, aumentar seus lucros[91]. Em um dos casos estudados, em que houve rejeição de contratação a um indivíduo que havia tomado medicamentos para pressão arterial e antidepressivos - os quais foram devidamente prescritos pelos médicos - tornaram-se uma barreira para contratação do seguro saúde. Os medicamentos antidepressivos e para saúde mental, aliás, são costumeiramente considerados uma bandeira vermelha. Em contato com uma das seguradoras, um representante afirmou que o histórico de compras em farmácias faz parte do processo de avaliação de assegurados.

De acordo com Ternuhe, a maioria dos consumidores não possui conhecimento que os agentes de seguro utilizam o histórico de prescrição e compras para tais análises. O jornalista ainda comenta que uma investigação feita pela *Federal Trade Commission*, no ano de 2007,

---

91 *They know what is in your medicine cabinet: An untold number of people have been rejected for medical coverage for a reason they never could have guessed: Insurance companies are using huge, commercially available prescription databases to screen out applicants based on their drug purchases.* Disponível em: https://www.bloomberg.com/news/articles/2008-07-22/they-know-whats-in-your-medicine-cabinet

encontrou irregularidades em duas empresas, MedPoint e IntelliScript[92], com esteio na opacidade em relação aos consumidores[93]. Entretanto, nenhuma sanção foi imposta, apenas se requereu esclarecimentos sobre se as informações de prescrição causaram negação de cobertura ou alguma outra ação adversa.

Ternuhe relata a existência de um ambiente de empresas com papel intermediário, conhecidas como *pharmacy-benefit managers*, tal qual a Medco Health Solutions, ou outras redes de varejo de farmácia, em que se possui amplo acesso a informações de compra de medicamentos. O que fora inicialmente coletado para ajudar os médicos acerca da condição dos pacientes, como forma de acompanhamento no

92 A apresentação institucional da empresa é a seguinte: *The Milliman IntelliScript system is a proven method for insurance companies to quickly gather and review their applicants' prescription histories. Milliman IntelliScript delivers complete and current prescription histories that allow insurers to make instant underwriting decisions with confidence. Insurers use Milliman IntelliScript to gather prescription information in real time and then review an easy-to-read online report. This cost-saving approach to obtaining health histories results in fast and effective risk assessment.* Disponível em: http://www.milliman.com/Solutions/Products/IntelliScript/ Acesso em: 28 de novembro de 2018.

93 Em relatório final referente à reclamação aberta em face da Milliman, a *Federal Trade Commission* não impôs sanção alguma, apenas determinou as seguintes recomendações: *Since at least 2005, respondent has marketed IntelliScript, a data aggregation service that provides individual medical profiles, including, but not limited to, prescription drug purchase histories of insurance applicants, to health and life insurance companies. 3. Respondent has contractual relationships with insurance companies that use IntelliScript for underwriting or claims review purposes. These insurance companies require applicants to sign a consent form, which authorizes the insurance company or its agents to access the consumer's health and medical records, including prescription drug records. The medical profile generated by IntelliScript includes, but is not limited to: all prescription drugs, including dosage and number of refills filled by the insurance applicant for the previous five years. It also includes, for each drug, the name and address of the dispensing pharmacy, as well as the name and address of the prescribing doctor, including medical specialty. The medical profile generated by IntelliScript analyzes the individual's prescription drug history and provides a "map" of the risk levels associated with each drug, based on information provided by the insurer.* Disponível em: https://www.ftc.gov/sites/default/files/documents/cases/2008/02/080212complaint_0.pdf Acesso em 12 de janeiro de 2019.

tratamento, passaram a ser fornecidos a terceiros, como seguradoras e a empregadores.

Na investigação realizada, dois terços das companhias de seguro estavam utilizando dados de prescrição médica para seus cálculos atuariais. O custo para o acesso a um perfil específico contendo informações sobre medicamentos, dosagens e relatórios de possíveis condições médicas, é de apenas 15 centavos de dólar.

Não é à toa que tais questões erigiram em um país como os Estados Unidos, que possui alto grau de desenvolvimento tecnológico aliado a uma cultura privatista, inclusive na área da saúde[94]. No entanto, questões como essa ganham cada vez mais relevância também no nosso país, cuja saúde pública está sendo alvo de tentativas de sucateamento e de privatização.

Em pesquisa específica sobre o tema de mercado de dados pessoais na saúde Joyce Ariana de Souza (2018, p. 64) explica que:

> O mercado de dados pessoais na saúde ainda é pouco analisado e explorado em pesquisas. Por ser um setor que agrega normativas específicas sobre vazamento de informações referentes aos pacientes e ética de conduta destinada aos profissionais da área, é como se o mercado estivesse se desenvolvendo quase que de forma invisível, sem alardes que possam criar barreiras. Por meio de levantamentos bibliográficos é possível detectar que alguns estudos abordam a questão dos dados pessoais na saúde, porém poucos apresentam cartografias e mapeamentos com situações concretas de como os dados são coletados, armazenados, classificados e vendidos nos mais variados setores da saúde.

Questões como exatidão das informações, possibilidade de retificação ou objeção[95], intrinsecamente ligadas aos direitos de proteção

94 *Amazon Makes Inroads Selling Medical Supplies to the Sick*. Disponível em:https://www.wsj.com/articles/amazon-makes-inroads-selling-medical-supplies-to-the-sick-1543487401. Acesso em: 26 de novembro de 2018.

95 Caso de uma enfermeira que trabalha como enfermeira e pelo histórico de medicamentos comprados, inferiu-se que consumia drogas e teve seu pedido de contratação de seguro saúde denegado: a *Bloodwork was supposed to be the last step in Isela's application for life insurance. But when she arrived at the lab, her appointment had been canceled. "That was my first warning," Isela said.*

de dados pessoais são evidentemente relevantes neste ambiente. Todavia, ainda é possível perceber como o consumidor se encontra vulnerável, exemplificadamente, se o uso de determinado medicamento, prescrito pelo médico da pessoa, foi determinante para uma decisão, como o próprio consumidor pode formular uma objeção se não foi uma escolha sua, mas sim do médico? E se este estiver incorrido em erro ou inexatidão? A hipossuficiência técnica do consumidor nesses casos é bastante acentuada: não se sabe o que está por trás dos algoritmos, o que de fato compõe o número do *score*, ou seja, um processo que não pode ser totalmente compreendido, contestado[96] ou auditado.

Neste ambiente, percebe-se que pessoas que não podem pagar por serviços que tenham a segurança e a privacidade, ou que podem pagar para reivindicações fundamentadas ou objeções substanciais, são as principais vítimas do sistema, que não possuem condições para "limpar" sua reputação.

Pasquale (2015) advoga para que tais dados sejam considerados sensíveis e sua utilização proibida no processo de tomada de decisão. Além disso, sugere que o foco das políticas de proteção de dados não deve estar no indivíduo, mas sim de um esforço conjunto para redução dos perigos que envolvem o uso de tais dados.

Em artigo sobre proteção de dados, Emilie Debaets (2018) afirma que, para pesquisa e análise de tumores, as amostras biológicas coletadas, registradas e armazenadas em *biobanks* implicam necessariamente na coleta e uso de dados pessoais, isso porque para a

---

She contacted her insurance agent and was told her application was denied because something on her medication list indicated that Isela uses drugs. Isela, a registered nurse who works in an addiction treatment program at Boston Medical Center, scanned her med list. It showed a prescription for the opioid-reversal drug naloxone — brand name Narcan. "But I'm a nurse, I use it to help people," Isela told her agent. "If there is an overdose, I could save their life." Disponível em: https://khn.org/news/nurse-denied-life-insurance-because-she-carries-naloxone/ Acesso em 30 de dezembro de 2018.

96 Conforme indica Pasquale (2015): *Where exactly is the line to be drawn between characterizing a potential employee as 1) diabetic, 2) in a "diabetic-focused household" (to use a category publicly disclosed by a data broker), 3) concerned about diabetes, 4) having a demanding home life (a determination that may in part be based on proprietary formulas extrapolating the effect of the data that would lead to attributions 1, 2, and 3)? Any effort to expand the protected zone beyond 1 is likely to draw resistance from businesses enamored with "big data" methods of increasing productivity, particularly because it would likely require extensive auditing of business records.*

pesquisa médica na área devem ser analisados dois conjuntos de dados de maneira correlacional.

O primeiro deles se refere à pessoa: informação demográfica (nome, endereço, data e local de nascimento, etc.); informação biológica (sexo, origem étnica, dados genéticos, etc.); informação médica (diagnóstico, testes, terapia, antecedentes pessoais ou familiares, doenças ou eventos relacionados, etc.); e, informações ambientais (situação familiar, vida profissional, sexualidade, estilo de vida e comportamento, etc.). O segundo se refere à própria amostra (natureza da lesão, extensão da lesão, etc.) e às condições de conservação (tipo de amostra, método de preparação, recursos biológicos associados, etc.) de análise. Por consequência, as amostras de tumores são indissociáveis dos dados da pessoa em que foi coletado e, por isso, importantes para a distinção de casos, correlações ou checagem.

Sustenta Debaets (2018) a importância do compartilhamento de tais dados com outros pesquisadores visando a estudos de casos e a estudos de correlação, por conta disso, a anonimização total é inviável. Alerta que mesmo respeitados os princípios de confidencialidade e com técnicas de pseudonimização, a probabilidade e os riscos de identificação são reduzidos, porém, não extintos.

Jane Yakowitz Bambauer (2011) defende que estes riscos devem ser suportados pelos pacientes e pela sociedade, em favor da acurácia científica e da qualidade de decisões de políticas públicas de saúde realizadas com pesquisas. Para o autor, é importante encontrar um equilíbrio entre riscos de vazamentos e a qualidade da saúde ofertada, uma vez que a tutela exacerbada pode prejudicar o desenvolvimento e a transparência científica.

Não se olvida que tais tecnologias trazem diversos avanços à medicina, às estratégias de políticas públicas e à saúde dos indivíduos. Em regra, quando se fala sobre o tema, apenas são ressaltados os pontos positivos, no entanto, é necessário avaliar os prós e os contras, e o custo social a ser suportado, bem como estar ciente dos possíveis riscos existentes.

Veja-se que o tema suscita debates e questões científicas, jurídicas e até éticas. Pretendeu-se apresentar a complexidade e a relevância assumida nesta seara. Estes últimos dois relatos demonstram que a adoção de padrões de segurança, códigos de conduta e de *compliance*, e sua observância, assumem importância para fins de responsabilização e demonstração de que a Lei fora obedecida e impingidos todos os esforços técnicos e jurídicos viáveis à época para

salvaguarda da integridade dos dados, pseudoanonimização dos pacientes e da confidencialidade imputada aos profissionais de saúde.

3.1.2 Dados de Saúde no Brasil: Panorama Normativo

No Brasil, até a promulgação da Lei de Proteção de Dados Pessoais, as normas sobre o tema se circunscreviam a regulamentos administrativos de Conselhos de Profissão, Pastas Ministeriais ou de Agências Reguladoras, pautado pela Política Nacional de Informação e Informática em Saúde - PNIIS, destacando-se a Resolução nº 2073 do Ministério da Saúde, que regula os padrões de uso de dados do Sistema Único de Saúde e a Resolução nº 305 de 2012 da Agência Nacional de Saúde Suplementar - ANS, sobre o padrão obrigatório para troca dos dados de atenção à saúde dos beneficiários de Plano Privado de Assistência à Saúde, e ainda os Códigos de Ética de profissionais da saúde que preveem o sigilo funcional.

Recentemente, o Conselho Federal de Medina editou a Resolução nº 2.227/2018[97], que disciplinou a telemedicina como forma de prestação de serviços médicos mediados por tecnologias para fins de assistência, educação, pesquisa, prevenção de doenças e lesões e promoção de saúde.

Ressaltam-se alguns pontos importantes da norma. O texto abrange questões relacionadas à segurança da informação, a padrões mínimos de interoperabilidade de dados, a infraestrutura de *internet* com o fim de assegurar o registro digital apropriado e seguro, pertinentes à guarda manuseio, integridade, veracidade, confidencialidade, privacidade e garantia do sigilo profissional das informações, uma vez que há obrigatoriedade de preservação de todos os dados trocados por imagem, texto e/ou áudio entre médicos, entre médico e paciente e entre médico e profissional de saúde.

Em seu artigo 18, a Resolução versa acerca do consentimento exarado pelo paciente:

> O paciente ou seu representante legal deverá autorizar a transmissão das suas imagens e dados por meio de consentimento informado, livre e esclarecido, por escrito e assinado, ou de

[97]Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2018/2227#search=%22telemedicina%22

> gravação da leitura do texto e concordância, devendo fazer parte do Sistema de Registro Eletrônico/Digital do teleatendimento ao paciente. Parágrafo único. É preciso assegurar consentimento explícito, no qual o paciente deve estar consciente de que suas informações pessoais podem ser compartilhadas e sobre o seu direito de negar permissão para isso

Houve preocupação com questões básicas, tais como segurança, interoperabilidade e infraestrutura de rede. Tratou-se do consentimento informado, livre e esclarecido a ser oferecido pelo paciente, garantindo-lhe o conhecimento de compartilhamento de suas informações pessoais.

A norma apresenta algumas inconsistências e lacunas, como, por exemplo, a falta de indicação do término do armazenamento dos dados e o direito de acesso do paciente aos dados. Com a entrada em vigor da Lei Geral de Dados Pessoais, tais questões deverão ser harmonizadas e adequadas, garantindo ao paciente um rol mais extenso de direitos.

Quanto às farmácias, a Agência Nacional de Vigilância Sanitária - Anvisa - possui a Resolução da Diretoria Colegiada nº 44 de 17 de agosto de 2009, cujo intuito é a regulação de farmácias para a comercialização de produtos e da prestação de serviços farmacêuticos. Contudo, a única previsão sobre a proteção de dados existente se refere à venda online de medicamentos, basicamente à segurança dos dados e limitação de uso no que concerne ao meio de publicidade de medicamentos.

> Art. 59. É responsabilidade do estabelecimento farmacêutico detentor do sítio eletrônico, ou da respectiva rede de farmácia ou drogaria, quando for o caso, assegurar a confidencialidade dos dados, a privacidade do usuário e a garantia de que acessos indevidos ou não autorizados a estes dados sejam evitados e que seu sigilo seja garantido. Parágrafo único. Os dados dos usuários não podem ser utilizados para qualquer forma de promoção, publicidade, propaganda ou outra forma de indução de consumo de medicamentos.

Outro ponto é a obrigatoriedade da coleta de dados do paciente que faz compra de medicamentos de uso controlado[98], cujo intuito é justamente a contenção de vendas para que tão somente pacientes que realmente demandam o uso de determinadas substâncias tenham acesso a elas, ou de programas sociais, como a Farmácia Popular, do Ministério da Saúde. De acordo com a Resolução nº, 20 de 5 de maio de 2011[99] da ANVISA, sobre a compra e venda de antibióticos, e a Portaria nº 344, de 12 de maio de 1998[100], sobre substâncias e medicamentos sujeitos a

98 As chamadas substâncias controladas ou sujeitas a controle especial são substâncias com ação no sistema nervoso central e capazes de causar dependência física ou psíquica, motivo pelo qual necessitam de um controle mais rígido do que o controle existente para as substâncias comuns. Também se enquadram na classificação de medicamentos controlados, segundo a Portaria SVS / MS nº 344/1998, as substâncias anabolizantes, substâncias abortivas ou que causam má-formação fetal, substâncias que podem originar psicotrópicos, insumos utilizados na fabricação de entorpecentes e psicotrópicos, plantas utilizadas na fabricação de entorpecentes, bem como os entorpecentes, além de substâncias químicas de uso das forças armadas e as substâncias de uso proibido no Brasil. Agência Nacional de Vigilância Sanitária – Anvisa, Disponível em http://portal.anvisa.gov.br/controlados. Acesso em 19 de janeiro de 2019.

99 Art. 5º A prescrição de medicamentos antimicrobianos deverá ser realizada em receituário privativo do prescritor ou do estabelecimento de saúde, não havendo, portanto modelo de receita específico. Parágrafo único. A receita deve ser prescrita de forma legível, sem rasuras, em 2 (duas) vias e contendo os seguintes dados obrigatórios: I - identificação do paciente: nome completo, idade e sexo; II - nome do medicamento ou da substância prescrita sob a forma de Denominação Comum Brasileira (DCB), dose ou concentração, forma farmacêutica, posologia e quantidade (em algarismos arábicos); III - identificação do emitente: nome do profissional com sua inscrição no Conselho Regional ou nome da instituição, endereço completo, telefone, assinatura e marcação gráfica (carimbo); e IV - data da emissão.

100 Art. 55. As receitas que incluam medicamentos a base de substâncias constantes das listas "C1" (outras substâncias sujeitas a controle especial) , "C5" (anabolizantes) e os adendos das listas "A1" (entorpecentes), "A2" e "B1" (psicotrópicos) deste Regulamento Técnico e de suas atualizações, somente poderão ser aviadas quando prescritas por profissionais devidamente habilitados e com os campos descritos abaixo devidamente preenchidos: a) identificação do emitente: impresso em formulário do profissional ou da instituição, contendo o nome e endereço do consultório e/ ou da residência do profissional, n.º da inscrição no Conselho Regional e no caso da instituição, nome e endereço da mesma; b) identificação do usuário: nome e endereço completo do paciente, e no caso de uso veterinário, nome e endereço completo do proprietário e identificação do animal; c) nome do medicamento ou da substância prescrita

controle especial, é imprescindível a identificação do consumidor, com seu nome, endereço completo, idade e sexo, compostos por CPF e/ou RG, bem como o registro de todos os dados do médico emitente do receituário.

A Lei Geral de Proteção de Dados Pessoais estabelece parâmetros a serem observados tanto pelos entes privados e públicos sobre dados de saúde, classificando-os como dados pessoais sensíveis. As hipóteses de tratamento de dados, independentemente de consentimento são as seguintes: (i) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; (ii) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; (iii) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias.

O art. 13 da Lei, em síntese, versa sobre importante hipótese dos dados com o fim de realização de estudos em saúde pública:

> Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas. § 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais. § 2º O órgão de pesquisa

---

sob a forma de Denominação Comum Brasileira (DCB), dosagem ou concentração, forma farmacêutica, quantidade (em algarismos arábicos e por extenso) e posologia; d) data da emissão; e) assinatura do prescritor: quando os dados do profissional estiverem devidamente impressos no cabeçalho da receita, este poderá apenas assiná-la. No caso de o profissional pertencer a uma instituição ou estabelecimento hospitalar, deverá identificar sua assinatura, manualmente de forma legível ou com carimbo, constando a inscrição no Conselho Regional; f) identificação do registro: na receita retida, deverá ser anotado no verso, a quantidade aviada e, quando tratar-se de formulações magistrais, também o número do registro da receita no livro correspondente.

> será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro. § 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências. § 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

O art. 5º, XVIII, da LGPD desse modo conceitua órgão de pesquisa:

> [...] órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

Tal previsão consagra princípios basilares como a finalidade, segurança, controle de acesso e anonimização e minimização dos dados, proibindo o compartilhamento a terceiros não envolvidos na pesquisa, assegurando a continuidade e realização de estudos sobre saúde pública respeitando-se os direitos dos titulares.

Quando o intuito for obter vantagem econômica, o compartilhamento de dados referentes à saúde é defeso, nos termos do art. 11, §4º: "É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica".

Recorde-se que a LGPD não definiu a expressão "dados referentes à saúde". A partir disso, é provável que se iniciem discussões acerca dos critérios a serem adotados para se verificar se determinada informação se trata, ou não, de um dado relacionado à saúde, ou seja, a extensão da sua definição.

Setores como a indústria farmacêutica, o de varejo farmacêutico e de exercício físicos, por exemplo, poderão advogar para que a sua extensão seja restritiva, enquadrando-se como dado relacionado à saúde tão somente os coletados na relação médico-paciente ou hospital-paciente, ou dados coletados no âmbito da telemedicina. De certa forma o cabo de guerra travado para conceituação de "dado pessoal" também se repetirá quanto aos "dados referentes à saúde".

No entanto, constam duas exceções legais à proibição imposta: portabilidade de dados quando consentido pelo titular; ou a necessidade de comunicação para a adequada prestação de serviços de saúde suplementar. .

A primeira isenção já existia na redação originária da Lei Geral de Proteção de Dados Pessoais. Tal enunciado é inconsistente, uma vez que a portabilidade é direito subjetivo do titular, não cabendo a ele consentir, mas tão somente exercer esse direito. Não se sabe se houve inserção proposital ou má técnica na sua redação, porém, evidente que esta imprecisão abre margem para que controladores de bases de dados relacionados à saúde, quando tiverem interesse de compartilhá-las, apenas requeiram o consentimento ao titular, contornando a proibição imposta aos dados referentes à saúde.

Por seu turno, a segunda foi inserida pela Medida Provisória nº 869/2018 e assegura a legalidade da prática de compartilhamento de dados entre "serviços de saúde suplementar", que já era prevista e realizada sob os auspícios da Resolução nº 305 de 2012 da Agência Nacional de Saúde Suplementar - ANS, que estabelece o Padrão obrigatório para Troca de Informações na Saúde Suplementar (Padrão TISS) dos dados de atenção à saúde dos beneficiários de Plano Privado de Assistência à Saúde.

O art. 4º da Resolução trata do compartilhamento de dados de atenção à saúde entre os seguintes agentes da saúde suplementar: operadora de planos privados de assistência à saúde; prestador de serviços de saúde; contratante de plano privado de assistência à saúde familiar/individual, coletivo por adesão e coletivo empresarial; beneficiário de plano privado de assistência à saúde ou seu responsável legal ou ainda terceiros formalmente autorizados por ele; e ANS.

Embora a observância da segurança e da privacidade seja um dos requisitos para atendimento do Padrão para Troca de Informações na Saúde Suplementar, a Resolução versa de maneira bastante genérica sobre o mote, tão somente assegura ao indivíduo o sigilo e a confidencialidade dos seus dados baseados no sigilo profissional.

Já constava na Resolução a previsão de acesso aos dados pelo paciente ou por terceiros formalmente autorizados; e a vedação de compartilhamento de informações com terceiros não participantes da cadeia de agentes de saúde suplementar, quando existente possibilidade de individualização.

Caso não fosse inserida a previsão pela Medida Provisória, este sistema já instaurado pelos agentes de saúde suplementar seria considerado ilegal. Sobre a ação em si, viu-se os riscos aos consumidores causados por práticas predatórias por seguros e planos de saúde, dessa forma, imprescindível o detalhamento das atividades de segurança, o controle no compartilhamento dos dados; e o exercício dos direitos de acesso, retificação objeção e portabilidade pelos pacientes. Vê-se como transações de dados há muito são realizadas. Embora com respaldo infralegal, não havia detalhamento suficiente sobre o tema para o exercício de direitos pelos indivíduos.

Resta saber se, com o permissivo legal, tal prática ficará circunscrita aos agentes de saúde suplementar, interpretação restritiva do termo, ou será expandida para legalizar o fluxo de dados com outros atores da cadeia de saúde.

Essa preocupação, inclusive, respalda a justificação da proposta de Emenda Supressiva, proposta pelo Deputado Alessando Molon, tendente a retirar esta previsão inserida pela Medida Provisória, a fim de que a redação volte à sua originalidade. Veja-se:

> O inciso II passa a permitir a livre comunicação de dados sobre saúde com o objetivo de obtenção de vantagem econômica, quando necessário para a "adequada prestação de serviços de saúde suplementar". A "adequada prestação de serviços" é expressão bastante ampla, que na prática permitiria qualquer tratamento de informações que operadoras de planos de saúde considerassem úteis para a própria prestação de serviços. A "brecha" abriria margem para que, por exemplo, fossem permitidas práticas de compartilhamento de dados coletados em farmácias, que permitissem identificar a frequência e os medicamentos de um consumidor para um plano de saúde determinar preços diferenciados. Trata-se, assim, de dispositivo que está na contramão da lógica protetiva da lei e mesmo do parágrafo em que foi adicionado, ao sequer condicionar a hipótese ao

> consentimento do usuário. Afirmar que não é permitido o uso compartilhado de dados com o objetivo de obter vantagem econômica para, em seguida, afirmar que se excetua a hipótese de "adequada prestação de serviços de saúde suplementar", corresponde a uma negação quase completa da própria regra, já que a saúde suplementar deve ser responsável pelo tratamento de dados de saúde com o objetivo de obter vantagem econômica. Abre-se margem, assim, para que grandes abusos ocorram, na contramão do que vem sendo discutido internacionalmente e negando-se o propósito da própria lei, de proteção do usuário e respeito ao seu consentimento.[101]

Nesse mesmo sentido é a Emenda proposta pelo Deputado Felipe Rigoni e pelo Senador Humberto Costa: "A imprecisão do termo 'adequada prestação do serviço' pode estimular os prestadores a utilizarem essa previsão legal para justificar o processamento e compartilhamento de dados pessoais de forma indiscriminada e, portanto, à margem dos preceitos estabelecidos na Lei nº 13.709/2018."[102]

Caso o setor de varejo farmacêutico não consiga se desvencilhar da consideração de que os dados por ele coletados se trata de "dados referentes à saúde", é provável que o setor de varejo farmacêutico tente se enquadrar em uma dessas exceções. Em ambos os casos ainda é necessário observar as bases legais para sua atuação. Porém, nessa segunda possibilidade, os dados coletados ainda são considerados dados sensíveis, afinal, não perderam a qualificação de dados referentes à saúde, dessa forma, não é possível invocar o interesse legítimo para o tratamento de dados. Remanescendo apenas o consentimento, enquanto manifestação livre, informada, inequívoca, específica e destacada, para finalidades específicas, como base legal, assumindo papel central nessa dinâmica quando os dados coletados forem compartilhados com terceiros.

Mesma lógica se aplica, então, à coleta de dados destinada ao tratamento pelo próprio controlador, ressalte-se, sem o intuito de

---

[101] Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7912643&ts=1549895776695&disposition=inline

[102] Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7912027&ts=1549895776121&disposition=inline

compartilhamento com terceiros: se considerado os seus dados como referentes à saúde, incorrerá como dado sensível, tendo o consentimento como base legal; se não for considerado dado referente à saúde, cairá na regra geral, podendo invocar o legítimo interesse.

Por fim, não se olvida que redes de farmácia comercializam diversos artigos, cuja vinculação aos dados de saúde podem escapar, como, por exemplo, cosméticos, maquiagem e produtos de higiene, ao contrário dos que possuem enquadramento em que se defende ser aqui certo, como itens relacionados à concepção ou à contracepção ou medicamentos.

3.2 PROGRAMAS DE FIDELIZAÇÃO: CONSUMO, VIGILÂNCIA E SEGMENTAÇÃO

Os programas de fidelidade são técnicas de micro marketing e de marketing relacional, desenvolvidos tanto para atender uma estratégia comercial, quanto para obtenção de dados do consumidor, esta é a definição que traz Jason Pridmore (2008). Nesse ambiente, na maioria dos casos os programas de fidelidade são amplamente dependentes (e vistos como sinônimos) de cartões de identificação pessoal ou numericamente indicados no momento de uma transação.

Logo, pode-se consignar que os principais objetivos dos programas de fidelidade são: consumo e faturamento; e coleta de dados com o fim de identificar e monitorar o consumidor, em que ambos se retroalimentam. Em contrapartida, são oferecidos aos consumidores benefícios e vantagens, visando à aproximação com o indivíduo, cuja experiência de compra naquele local ultrapassa o exercício econômico ou de participação de mercado: através da fidelidade, não se trata apenas de uma relação de consumo, mas também social e cultural, segundo consiga Nils Zurakski (2011), corroborando o esposado no capítulo primeiro, ou seja, o ato de consumir envolve o sentimento de pertencimento, de identificação e lealdade a uma marca.

Este autor (2011) realizou uma pesquisa na cidade de Hamburgo, Alemanha, com o intuito de analisar o papel dos programas de fidelidade nas práticas de compras e os modos de vigilância do consumidor. Para tanto, entrevistou quarenta e nove pessoas de diferentes classes sociais, dos quais quarenta possuíam pelo menos um cartão de fidelidade. Ao responderem acerca das suas motivações acerca da fidelização, foram identificadas precipuamente as seguintes: possibilidade de ganhar bônus ou pontos, bem como a aquisição de benefícios; criação e manutenção da confiança com a empresa; hábitos

de compra; sentimento de obrigação ou compulsão advindo daquela relação; e a paixão por acumular pontos, bônus ou milhas. Ou seja, proporcionam ao consumidor sensações positivas de reciprocidade, *status* e pertencimento social.

Nesta mesma pesquisa, Nils Zuraski (2011) constatou que a minoria dos entrevistados possuía conhecimento acerca do sistema de coleta de dados que permeia os programas de fidelização. Os poucos que relataram que sabiam, todavia, declararam não se importar com a questão do uso de dados[103], uma vez que apenas vislumbravam benefícios. Em outro estudo, realizado por Timothy Graeff e Susan Harmon (2012), nos Estados Unidos, com 480 pessoas, demonstrou que desta amostra, mais de 90% estava vinculada a algum programa de fidelidade. Indagadas acerca do intuito primordial dos programas de fidelidade: 49,8% responderam que a competitividade da empresa no mercado; 15,5% responderam que era presenteá-los com promoções e descontos nos preços ofertados; 6,9% que era impingir preços mais altos aos consumidores não fidelizados; e, finalmente, 16,5% que estava associado ao marketing relacional e à coleta de dados para monitorar os hábitos de consumo dos consumidores (6,5% não responderam de acordo com os parâmetros da pesquisa; e 4,8% se recusaram).

Em geral, as pessoas pensam que o objetivo é tão somente para *marketing* segmentado. Ocorre, contudo, que: (i) não se trata apenas de estratégia de publicidade, existem potencialidades, compartilhamentos e usos de seus dados para outras finalidades, cujos consumidores sequer imaginam; (ii) ainda que seu uso seja tão somente para publicidade, que os produtos, os serviços, as expectativas oferecidas moldam o contexto e a realidade em que se vive e, consequentemente, a própria subjetividade.

Esse sistema massivo de coleta de dados que, aparentemente, é *off-line* e local, a partir do momento que é registrado em um banco de

---

103 Perguntou-se ao entrevistado se a coleta e a identificação de dados em programas de fidelidade o incomodava, a resposta dele foi a seguinte: "*Well, not really. Not at all. You need to read the fine print. I don't read it, but I know that they store the data. And I know that they pass them on and trade them for advertisement purposes, I know all that."* [...] Contudo, de maneira contraditória, advertiu sobre os riscos do acesso de terceiros a extratos bancários depois de obtê-los da máquina. *"it is life threatening. You must not leave a bank statement left behind in a bank. The one, who finds that statement can do you great harm and cause a great loss." He then went on to tell a second story [...]: " They stole the data. This came all over during the court case. I is unbelievable what they can do with the data today. But I am not afraid, even if I am telling those stories. But it is dangerous what they do with the data, devastint"*.

dados, passa a ser *on-line* e global, assumindo o dado seu caráter ubíquo devido aos movimentos de fluxos de dados. Além da possibilidade de criação de *digitized biographies*[104] a partir do histórico de consumo, esse

104 Smith e Sparks (2002) obtiveram acesso a um banco de dados, em que a partir do histórico de consumo do cliente obtido a partir de registros de compras por meio de programa de fidelidade, tentou-se fazer uma análise da rotina, relacionamento, eventos da vida, personalidade, cujo pseudônimo foi Brenda, transcreve-se excertos da pesquisa: "*Brenda purchases a lot of broad health and beauty products and appears to take care of her appearance. She wears contact lenses not glasses, but does return to glasses for occasional use (glass cleaning cloths are purchased). She is a regular purchaser of lipstick (often shades of red) and a considerable user of lip salve, possibly in an effort to ward off cold sores (Blisteze). She purchases a lot of nail varnish and handwashes and spends a regular amount on hair care. She probably has long hair, as attested by hair grips, pony tail clasp etc. She could suffer from poor circulation if the hot water bottle purchased in April is symptomatic. From June 1999 onwards (week 42) she has problems with her feet and there are regular purchases of insoles, foot deodorants, corn plasters and other Scholl products. She suffers from hay fever. When she gets a cough or cold (approximately once a year) she takes several weeks to shake it off. She occasionally buys vitamin pills. Brenda also resorts to instant tan products despite (or because of) taking holidays. As a loyal customer and big spender with this retailer, Brenda gains substantial reward points on her loyalty card. She redeems these points on 5 occasions, saving her ,105.72 (an approximate return of 4.5%). The first four points redemptions are effectively special purpose purchases. The first is aftershave, bought in December, presumably as a gift for Christmas. The fourth redemption is another pre-Christmas purchase on a beauty aid, again possibly as a gift. Holidays would seem to be the theme of redemptions two and five. Both occur at the same time of the year and involve suncare products. The third redemption is far more mundane. It is unclear why this redemption is so different to the others. Is it fair to conclude vanity is a trait and that appearance (of herself and others) is very important to Brenda? Brenda however appears to suffer from spots and/or bad complexion, as attested by a high spend on blemish concealer and the occasional purchase of Clearasil. This might be related to her purchase and presumed intake of chocolate and fizzy drinks. She is a large woman judging by the size of the tights purchased. This is consistent with the size of her typical lunch and other clues in the record (she does buy a set of weighing scales during the two-year period). Brenda appears to have a boyfriend or partner/s and occasionally buys him aftershave and deodorant, as well as (men's) razor blades. We can only speculate as to whether Brenda is trying to tidy him up or he has asked her to buy these things. Perhaps it is Brenda's nature to be highly planned and organised and this includes for her partner (in October 1999 she buys an organiser but whether this is for her or is a gift we do*

processo cria um conglomerado de indivíduos que, por algum motivo, estão categorizados junto a outros devido às similaridades ou características em comum, seja por morarem na mesma vizinhança, por padrões anteriores de compra de produtos, idade, sexo, níveis de renda, etc.

Conforme Pridmore (2008), os programas classificam e categorizam os consumidores como entidades digitalizadas que efetivamente estabelecem os parâmetros em torno dos quais os consumidores são compreendidos e, a partir do momento que são conhecidos, podem ser influenciados, gerenciados, controlados.

Assim sendo, em um primeiro momento o consumidor é identificado, em seguida, é objeto de diferenciação, segmentação e categorização, de acordo com o interesse do controlador da base de dados.

Para Anthony Danna e Oscar Gandy Jr. (2002), o controle do consumo em massa envolve o uso de informações sobre os consumidores e da eficácia da intervenção: analisar quanto eles foram expostos a mensagens persuasivas, e, em contrapartida, os índices de sua capacidade de resposta a tais recursos. Ao final, os perfis são criados e os consumidores devem se enquadrar em algum destes estandartes, de acordo com o qual são oferecidos diferentes produtos e serviços.

Rememorando o capítulo primeiro, neste ponto se insere o paradoxo do consumo e da liberdade em que se oferece "todo tipo de oportunidades e experiências", ao mesmo tempo em que direcionam os consumidores "para certas rotas predeterminadas de consumo", ou seja, realizam-se simulações e previsões de nível de superfície do comportamento do consumidor. O espaço da autonomia do consumidor passa a ser plástico, variando o seu enquadramento em *standards* pré-fixados, aumentando o risco de ser discriminado no mercado de consumo caso não faça parte daquela segmentação pré-determinada.

Dessa forma que o direito à proteção de dados, com o direito ao acesso, à retificação e à objeção são imprescindíveis em uma lógica econômica de circulação de informação “pois se o consumidor não consegue determinar quais informações sobre si são conhecidas na sociedade e podem ser utilizadas para a tomada de decisões que influenciem a sua vida, ele terá a sua capacidade de autodeterminação

---

not know). She clearly plans Christmas well in advance (cards for her parents/family in October) and the same is true of holidays. In the latter case she buys after-sun and sun lotion a few weeks in advance (we can tell when she is away because of the two week gap in the record.”

reduzida" (MENDES, 2014, p. 92). Na realidade, o consumidor normalmente sequer possui conhecimento com os potenciais usos de seus dados.

De acordo com Gandy (1989), quem não se enquadra ou, pelo menos não se aproxima deste padrão mínimo, são excluídos das oportunidades econômicas e, por extensão, das possibilidades sociais e políticas que eles acarretam. Em suma, são as bases de dados, que alimentam algoritmos e várias técnicas de análise de dados tais como o *scoring, profiling* ou *predictive modeling* há capacidade de extrair informações e obter conclusões acerca do comportamento de consumidores, suas qualidades e gostos pessoais, hábitos e predileção de compras e até mesmo de predições e que se sujeitam a erros e a imprecisões, regulando a exclusão do consumidor no mercado, com baixa transparência.

Lyon (2003) alerta que a categorização social não é um processo neutro porque constitui uma intervenção social no mundo real daqueles que são classificados: ainda que as externalidades não sejam deliberadas ou intentadas, as consequências são iminentes. A coleta sistemática de dados e o arranjo de dados em categorias afetam tanto a forma como concebemos a sociedade, como descrevemos o outro, além disso, é capaz de transformar o que consumidor, o que escolhemos fazer, quem tentamos ser e até mesmo o que pensamos de nós mesmos.

Para Lawrence Lessig (2005), os perfis começarão a normalizar a população da qual a norma é desenhada, uma vez que a observação afetará o observado. Por seu turno, o sistema contempla o que você faz; encaixando-se em um padrão, em seguida, o padrão é então enviado de volta para você na forma de opções pré-definidas; as opções, por seu turno, reforçam o padrão; o ciclo começa novamente.

Conforme Maria Celina Bodin de Moraes e Chiara Teffè (2017, p. 121): "Uma vez munidas de tais informações, entidades privadas e governamentais tornam-se capazes de 'rotular' e relacionar cada pessoa a um determinado padrão de hábitos e de comportamentos, situação que pode favorecer inclusive graves discriminações".

Vê-se que os programas de fidelidade são peças pertencentes a essa engrenagem de vigilância e de consumo, contribuindo com a coleta de dados e no detalhado conhecimento acerca do comportamento do consumidor, exemplificadamente: onde reside, a frequência com que o consumidor faz compras; qual dia de predileção; se possui crianças ou não; se mora sozinho ou possui família na mesma residência; quais os seus produtos e marcas preferidos. Com base de tais informações, o estabelecimento comercial pode segmentar suas ofertas aos

consumidores que já sabe de antemão que irá despertar o interesse. Sobre o mote, Laura Schertel Mendes:

> Ademais, a partir desses dados de transações comerciais, que são dados comportamentais, a empresa pode avaliar e classificar o consumidor em relação à sua frequência, à última vez que esteve na loja e ao seu valor monetário (*recency, frequency and monetary value – RFMV).* As consequências dessa classificação podem ser indesejáveis, tais como a possibilidade de exclusão do consumidor de menor capacidade financeira. Tanto na coleta de dados a partir de transações comerciais como de cartões de fidelidade, o consentimento do consumidor é essencial para que a obtenção de dados pessoais seja legítima. Assim, não é o consumidor obrigado a fornecer os seus dados pessoais, a menos que a transação econômica escolhida requeira, para a sua efetivação, tais informações. Com relação ao cartão de fidelidade, a questão é mais preocupante, pois nem sempre o consumidor percebe que por trás dessa fidelização estão, na realidade, o monitoramento e o armazenamento dos dados referentes ao seu comportamento de consumo. (2014, p. 97)

Enfim, o episódio *Nosedive* da terceira temporada do seriado britânico *Black Mirror* não retrata uma distopia, mas uma realidade: já está sendo implementado na China um sistema de crédito social (*social scoring)*[105]. O sistema de *scoring*, já mencionado, é expandido para todos os aspectos da vida dos cidadãos chineses, sendo seu comportamento constantemente avaliado de acordo com princípios e valores do Estado, e, sucessivamente, categorizado, indicando ao final uma classificação numérica única e pública daquela pessoa.

Com isso, baseado no *rating* alcançado, determinar-se-á se um cidadão terá direito a certas políticas públicas, por exemplo, a prestação de serviços médico-hospitalares ou a indicação de escolas em que os filhos devem ser matriculados; ou até mesmo benefícios na iniciativa

105 *The odd reality of life under China's social rating system* Disponível em: https://www.wired.co.uk/article/china-blacklist

privada, que atua juntamente ao governo na implementação do projeto.[106]

Por enquanto, a participação neste sistema voluntária, todavia, o projeto de implementação prevê que no ano 2020, ela será obrigatória para todos, inclusive para as pessoas jurídicas que tenham sede na China.

3.3 PROTEÇÃO DE DADOS RELACIONADOS À SAÚDE EM FARMÁCIAS: PANORAMA BRASILEIRO

A estratégia de redes de farmácia acerca da narrativa de proporcionar descontos no âmbito de programas de fidelização, com a identificação do consumidor por meio do CPF, um identificador único, já foi alvo de matérias jornalísticas, pesquisas acadêmicas e até investigações realizadas pelo Ministério Público. Este tópico tem por intuito de relatá-las, a fim de se identificar o estado da arte atual sobre o assunto.

Bruno Marchetti, em matéria realizada para a Vice.[107], narra o cotidiano no caixa de maioria das farmácias que possuem um Programa de Fidelidade:

> Na hora de comprar remédio, você já deve ter ouvido o simpático pedido do outro lado do balcão: “Me fala o CPF para ver se você tem desconto”. Existe boa chance de você ser seduzido pela palavra mágica: desconto. Mas, se você é

106 *Big data meets Big Brother as China moves to rate its citizens*: *If their score reaches 600, they can take out a Just Spend loan of up to 5,000 yuan (around £565) to use to shop online, as long as it's on an Alibaba site. Reach 650 points, they may rent a car without leaving a deposit. They are also entitled to faster check-in at hotels and use of the VIP check-in at Beijing Capital International Airport. Those with more than 666 points can get a cash loan of up to 50,000 yuan (£5,700), obviously from Ant Financial Services. Get above 700 and they can apply for Singapore travel without supporting documents such as an employee letter. And at 750, they get fast-tracked application to a coveted pan-European Schengen visa. "I think the best way to understand the system is as a sort of bastard love child of a loyalty scheme," says Creemers*. Disponível em: https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion

107 A distopia do 'me fala o CPF' nas farmácias do Brasil. Disponível em: https://www.vice.com/pt_br/article/9kzbx5/por-que-farmacias-insistem-para-ter-seu-cpf

> dessas pessoas que não se sente confortável em passar dados a qualquer um, pode ter sido surpreendido com a expressão incrédula dos farmacêuticos. “Como assim você não quer desconto?”, indagam, em tom de condenação.

O jornalista faz a seguinte indagação: “por que, em toda compra nas grandes drogarias, querem tanto assim o número dos nossos CPFs? O que está por trás dessa insistência para que forneçamos nossos cadastros de pessoa física?”. Em busca das respostas, deste jeito redigiu:

> Uma primeira resposta para essa pergunta é a cota de registros que os atendentes devem adicionar ao sistema. Em breve conversa que tive com atendente da Droga Raia na Vila Madalena, em São Paulo, fui informado de que cada funcionário precisa atingir uma meta de 100 novos cadastros no sistema por mês. A pergunta que não é respondida de barriga no balcão é qual é este sistema que está sendo alimentado com nossos dados e para o que estão sendo usados. A dúvida permanece em quem estuda os direitos do consumidor. Para os especialistas que consultei, trata-se de algo obscuro, perigoso e abusivo.

Ramon de Souza, em reportagem realizada para o Canal Tech[108], entrou em contato com Renan Pessim, diretor da unidade de negócios de saúde, da empresa Dunnhumby, multinacional especialista em ciência do consumidor, em que um dos clientes é a Rede de Farmácia Raia, reproduz-se trechos da entrevista com suas respostas:

> “Por meio de dados anonimizados de programas de fidelidade, a dunnhumby entende o comportamento de compra dos consumidores para ajudar os varejistas e indústrias a tomarem decisões centradas nos clientes. Essas decisões estão relacionadas a layout da loja, disposição e tamanho das categorias, sortimento de produtos e serviços, atividades promocionais e preço. É

108 Onde, como e pra que é usado seu CPF nas lojas físicas Disponível em: https://canaltech.com.br/seguranca/privacidade-onde-como-e-para-que-e-usado-seu-cpf-cadastrado-em-lojas-fisicas-112546/. Acesso em 28 de janeiro de 2019.

> importante salientar que não temos acesso a nenhum tipo de dado pessoal. Cada indivíduo é representado por um número no nosso banco de dados", explica. Ao ser questionado se essas informações são compartilhadas com terceiros, Pessim responde que sim, mas de forma anônima e para melhorar a experiência do próprio cliente. "A dunnhumby somente compartilha dados de comportamento de compra anonimizados e agregados com as indústrias parceiras do seu cliente (varejista), para ajudá-las a tomarem melhores decisões em relação ao sortimento de produtos e serviços, atividades promocionais nas lojas dos varejistas e definição dos preços dos seus produtos para o consumidor final", ressalta.

O Internetlab, centro de pesquisa, fez uma experiência com uma câmera escondida para saber o quanto as pessoas estão dispostas a entregar suas informações pessoais sem se perguntar o porquê. Um ator que estava no caixa de uma farmácia requerera o CPF dos consumidores, que respondiam de forma bastante natural. Em seguida, o ator solicitava outras informações, por exemplo, se possuía animal de estimação ou se poderia mostrar a foto do filho, somente a partir de então que as pessoas começavam a titubear e mostrar algum desconforto com o repasse desses dados[109].

Joyce Ariana de Souza realizou sua pesquisa de mestrado sobre o mercado dos dados pessoais de saúde no âmbito do Município de São Caetano do Sul, em que faz uma radiografia panorâmica de todos os atores envolvidos, hospitais, clínicas, postos de saúde, laboratórios e farmácias. Quanto a estes últimos, analisou tanto a coleta de dados obrigatória para compra e fornecimento de medicamentos controlados, conforme normativa do Ministério da Saúde, quanto a realizada via programas de fidelidade.

A autora cita o programa Viva Saúde, desenvolvido e administrado por uma das vertentes do Grupo, a DPSP Publicidade Ltda., voltado exclusivamente aos clientes da Drogaria São Paulo e da Drogaria Pacheco, em que se oferece redução do preço a depender do medicamento ou do produto adquirido (essa rede não possui atuação na

109 E quando te pedem informações pessoais em uma compra? Disponível em: https://www.youtube.com/watch?v=uHZs3ADb6RQ Acesso em: 2 de fevereiro de 2019.

Grande Florianópolis). Na pesquisa realizada pela autora sobre este programa, a adesão depende de cadastro, que pode ser feito em qualquer filial da drogaria ou pelo site, os dados coletados são: CPF, *e-mail*, nome completo, data de nascimento, sexo, número do telefone celular e endereço completo, em que consente com as regras internas vigentes e o CPF passa a ser o indexador utilizado.

A autora comenta que no caso da Drogaria São Paulo existe outros dois tipos de convênios que oferecem mais descontos: um vinculado às seguradoras de planos de saúde e outro às empresas parceiras. Imperiosa a transcrição integral da resposta de uma das entrevistadas, a qual foi anonimizada pela autora, sobre o tema:

> No caso dos convênios com planos de saúde e empresas, a Drogaria São Paulo tem acesso a dois bancos de dados. Um com o número das carteirinhas do convênio médico de todos os segurados de cada administradora e outro com o CPF e a data de nascimento dos funcionários das empresas parcerias. Assim que o cliente informa um desses dados, o nosso sistema, que até onde sei foi desenvolvido internamente, faz uma rápida busca nesses bancos e já verifica se o cliente está atrelado mesmo a uma das parcerias ou não e, em caso positivo, já disponibiliza os descontos. Além disso, uma parte da Central da Drogaria São Paulo atua diretamente nesse setor e envia mensalmente para as seguradoras e para as empresas um relatório detalhado sobre cada cliente que utilizou o serviço de descontos. No relatório vão os dados do cliente. No caso de clientes das seguradoras, é obrigatório registrar o número da carteirinha, quais produtos e medicamentos ele adquiriu, por qual meio, via rede física ou site, e a forma de pagamento (descreve a entrevistada 6). (2017, p. 97)

Joyce Ariana de Souza (2018, p. 94) comenta a existência de obscuridade no setor e a sua experiência com a pesquisa sociológica na área: “dificuldade para a realização de entrevistas e levantamento de informações, foi possível detectar pequenas amostras que podem vir a delinear o que está ocorrendo nestas corporações”; e acrescenta: “As pessoas que atuam nos cadastros e na construção de relatórios não

sabem dizer quais são os softwares empregados pelas farmácias/drogarias" (2018, p. 99).

Há ainda investigações realizadas pelo Ministério Público do Distrito Federal e Territórios, que possui uma Comissão de Proteção de Dados Pessoais[110], coordenada pelo Promotor Frederico Meinberg Ceroy. Com o fito de averiguar a legalidade da prática de coleta de dados por redes de farmácias, foram enviadas perguntas[111] ao Sindicato

[110] Importante destacar a atuação da Comissão no que se refere à proteção de dados pessoais dos consumidores, veja-se, por exemplo: Netshoes paga R$ 500 mil em danos morais após vazamento de dados. Netshoes faz acordo com MPDFT para evitar ação coletiva; empresa sofreu vazamentos de dados em 2017 e 2018. Disponível em: https://tecnoblog.net/277594/netshoes-acordo-mpdft-vazamento-dados/; MPDFT ajuíza ação contra o Banco Inter por vazamento de dados pessoais Disponível em: http://tiinside.com.br/tiinside/31/07/2018/mpdft-ajuiza-acao-contra-o-banco-inter-por-vazamento-de-dados-pessoais; Disponível em: MPDFT investiga suposto vazamento de dados da Fiesp https://www.baguete.com.br/noticias/23/11/2018/mpdft-investiga-suposto-vazamento-de-dados-da-fiesp. Acessos em: 11 de fevereiro de 2019

111 As perguntas realizadas foram as seguintes: 1) A Rede [XXXXXX] é adepta da prática de concessão de descontos nas compras de produtos para os clientes previamente cadastrados em suas bases de dados? Os descontos são concedidos em um mesmo percentual para clientes não cadastrados ou que não desejam se cadastrar? 2) Qual o objetivo primordial da citada prática indicada no item 1: descontos em troca de dados? 3) A empresa armazena informações sobre todas as compras de seus clientes cadastrados (histórico de compras), online e no balcão? 4) Algum software específico é utilizado para coletar, armazenar e tratar estes dados pessoais sensíveis? 5) De que forma os bancos de dados dos clientes são armazenados? Indicar as medidas de segurança utilizadas atualmente para a proteção dos dados pessoais, inclusive procedimentos de criptografia. 6) Os dados pessoais dos clientes (nome, telefone, CPF, endereço, histórico de compras, etc) são compartilhados com outros estabelecimentos farmacêuticos, seja do mesmo grupo econômico da empresa ou de grupos econômicos diversos? 7) Como funcionam os programas de benefícios ou descontos oferecidos pela empresa, em troca de dados pessoais? Explicar de forma detalhada, para além do que é apresentado nos "FAQs" da empresa; 8) Os dados pessoais dos clientes são compartilhados com empresas externas, não ligadas ao setor farmacêutico? Em caso positivo, por quais motivos? 9) Os dados pessoais dos clientes são de alguma forma comercializados? Se sim, quem são os adquirentes desses dados e quais as modalidades de transações e negócios embasando a comercialização. 10) Os dados pessoais dos clientes são compartilhados com o Governo (Federal, Estadual, Municipal)? Em caso

do Comércio Varejista de Produtos Farmacêuticos do DF (Sincofarma) questionando o tratamento que o setor dá para os dados dos clientes e o porquê da exigência do CPF para oferecer descontos. Apesar da tentativa junto à Promotoria que cuida do caso, não se conseguiu acesso à íntegra do Processo Administrativo.

A estratégia adotada pelo Ministério Público do Estado de Minas Gerais foi diferente, ao invés de oficiar as diversas farmácias, uma única foi destacada para se proceder à apuração dos fatos. Em junho de 2018, o Instituto de Referência em Internet e Sociedade ofereceu representação ao Ministério Público de Minas Gerais, cujo objeto se tratava de suposta prática abusiva por estabelecimentos farmacêuticos no Estado de Minas Gerais, baseada na coleta e utilização de dados pessoais, por meio da solicitação de CPF, sem notificação ao consumidor de abertura de cadastro, ou fornecimento de informações adequadas sobre a utilização dos dados, bem como identificada ausência de política de privacidade e de termos de uso, e, consequentemente, seu tratamento sem o consentimento qualificado do consumidor. Transcrevem-se excertos da peça inaugural:

> Desde 2017, tem sido prática comum que farmácias de Belo Horizonte e de outras cidades brasileiras solicitem o número de Cadastro Nacional de Pessoas Físicas - CPF dos clientes para realizar qualquer compra em seus estabelecimentos. O fornecimento desse dado de identificação pessoal tem como alegada contraprestação ao consumidor somente a atribuição de descontos sobre produtos que estejam vinculados a uma promoção. Essa prática está sendo adotada pelas mais diversas redes de farmácias, inclusive algumas cujas redes atuam em todo o território nacional. Nenhuma dessas redes de farmácias demonstra de forma transparente para os consumidores qual seria o propósito efetivo dos estabelecimentos ao coletar e armazenar informações individualizadas sobre o histórico de compras de cada cliente. Como exemplo dessa prática, citamos o programa de descontos da Drogaria Araújo “Tem + Araujo”.

---

positivo, por quais motivos ou obrigações legais? (Processo Administrativo n. MPMG 0024.18.002027-3. Representação - Anexo)

> (Processo Administrativo n. MPMG 0024.18.002027-3. Representação)

Acatada a representação, direcionada em face Drogaria Araújo S.A, foi instaurado o Processo Administrativo n. MPMG, por suposta infringência ao Código de Defesa do Consumidor, em seus artigos 4º,I, 6º, III, 31, 43, §2º e do Decreto Federal nº 2.181/97, artigo 14, por condicionar a concessão de determinadas promoções ao repasse de dados pessoais do consumidor, sem informação clara e adequada sobre a abertura de cadastro e a utilização posterior dos registros de consumo.

A empresa, em suas manifestações, sinteticamente, defendeu que não havia abusividade em sua conduta, haja vista que observara seu dever uma vez que todas as informações são claramente fornecidas por meio de panfleto publicitário, bem como disponíveis no *website* do programa, o qual: "contém todas as regras e informações claras, corretas, precisas e ostensivas, também suprindo todas as exigências da legislação consumerista".

Apesar de extensas, vale conhecer as alegações das peças de defesa, a fim de analisar os argumentos suscitados:

> O denominado "Tem + Araujo" é um programa de vantagens criado para estreitar o relacionamento do cliente com a Drogaria Araujo e que propicia ao interessado a participação em promoções exclusivas, caso seja do seu desejo aderir ao referido programa. Não se questiona, portanto, a legalidade de prática de um programa de vantagens ou fidelização do cliente, o que inclusive se encontra disseminado no comércio de produtos de bens e serviços nacional, o que também já foi exaustivamente consolidado pela jurisprudência pátria. Registe-se, portanto, que não é obrigatória e tão pouco vinculativa a participação no referido programa "Tem + Araujo", sendo esta apenas uma faculdade concedida àqueles que se interessarem em manter um maior vínculo com a Drogaria Araujo e usufruir das respectivas benesses concedidas. (Processo Administrativo n. MPMG 0024.18.002027-3. Defesa prévia).

Ademais, afirma que não há identificação do usuário:

> [...] sobre a política de privacidade da Requerida em relação aos dados informados, é impreterível ressaltar que o próprio cliente digita o seu CPF no *pin pad*, a mesma máquina utilizada nos pagamentos em cartão, contando com o mesmo protocolo de segurança de quando a senha do cartão é informada. Após digitado o CPF, o cliente é transformado em um *token* interno da Drogaria Araujo, tendo seus dados de cadastro e informações de compras reunidas de acordo com o número de seu *token*, desvinculando, desta forma, ao nome a o CPF do titular, para que seja respeitada sua privacidade e confidencialidade. Uma vez transformado em *token*, não há como o cliente ser identificado. Os dados cadastrados ficam armazenados em um banco de dados privado, no mesmo local onde são mantidos os dados da própria Drogaria Araujo, sendo certo que as informações dos clientes não são cruzadas, vendidas ou fornecidas para terceiros.(Processo Administrativo n. MPMG 0024.18.002027-3. Defesa).

Além de confundir o documento com a prática comercial e rotineira, observa-se a aparente contradição, afinal, primeiramente ela fala da anonimização do cliente e, em seguida, fala da possibilidade de identificar os clientes: "Quanto à necessidade da informação do CPF, tem-se que este é o meio mais fácil de identificar os clientes, sendo que o cadastro da pessoa física é apenas a chave de entrada para identificar um cliente ao seu respectivo *token*."

O promotor Fernando Ferreira Abreu, do Ministério Público do Estado de Minas Gerais, entendeu que a prática era abusiva por condicionar os descontos à identificação pessoal do consumidor, sem que houvesse consentimento específico para tanto, uma vez que ausente o oferecimento de informações claras sobre a prática.

Por conseguinte, propôs Transação Administrativa e Termo de Ajustamento de Conduta, mecanismo extrajudicial para resolução de conflitos com as seguintes condições: pagamento de multa no valor aproximado de 635 mil reais; instauração de sistema prévio de cadastro dos consumidores; informar prontamente aos consumidores os termos e condições do programa de fidelidade, inclusive que os descontos ofertados são em troca da identificação do consumidor; vedação à solicitação do CPF de maneira genérica; e possuir os termos e condições

de forma impressa em todos os estabelecimentos para consulta. O agente econômico, contudo, recusou-se a assinar a proposta extrajudicial.

Em decisão final administrativa, o membro do *parquet* mineiro entendeu que a concessão de descontos não pode estar condicionada ao fornecimento de dados pessoais, sendo necessário o cadastro prévio pelo consumidor após conhecer e aceitar todos os termos de condições do programa, de acordo com informação clara, acessível e ostensiva, ou seja, a informação que deveria ser repassada ao consumidor é que a inserção do CPF visa à abertura de cadastro e não à obtenção de desconto. Alerta ainda para a fragilidade do sistema, afinal, uma pessoa poderia digitar CPF de terceiro. Extrai-se o seguinte das suas conclusões e da decisão administrativa:

> Na informação de lançamento do programa de vantagens "Tem + Araujo", o próprio fornecedor informa: "quer ter todas essas vantagens? É só informar sempre o seu CPF no caixa ou se cadastras no nosso site: araujo.com.br/cadastro". Em sequência no verso do mesmo documento, na parte de perguntas e respostas, a pergunta de número 1 é por demais comprobatória da prática abusiva: '1. Como faço para participar do Tem + Araújo? Resposta: Basta informar seu CPF no caixa ao fazer as suas compras na Araujo'.No mesmo sentido, ainda na parte de perguntas e resposta do documento em cotejo, chama atenção o teor da pergunta número 9. Eu não tenho CPF. Vou perder os descontos? Resposta: No caso de estrangeiros, crianças, adolescentes e outras situações especiais de pessoas que não possuem CPF, a compra deve ser validada por meio do CPF padrão 123.456.789-09. Utilize apenas nas exceções, pois com ele não identificamos o cliente e nem conseguimos oferecer vantagens personalizadas.' Verifica-se, portanto, que nitidamente a intenção do fornecedor é simplesmente captar o CPF do consumidor, porquanto existe um CPF padrão que permite que os descontos sejam fornecidos ao consumidor, independente da inserção de seus dados originais. [...] (Processo Administrativo n. MPMG 0024.18.002027-3. Decisão administrativa).

O promotor Fernando Ferreira Abreu ainda considerou que “a abusividade revela-se tão gritante e ofensiva aos direitos básicos do consumidor, que o assunto é abordado de forma expressa em documentos internos da reclamada, denominados de Boletins Gerenciais”, de fato, o teor de tais documentos demonstram como a prática é predatória e como a empresa força os gestores e seus funcionários a agirem de forma a compelir o consumidor a apresentar seu dado de identificação. Traslada-se o conteúdo de alguns destes, para ilustração:

> Estamos captando, xem média, o CPF de apenas 25% dos nossos clientes atendidos. Lojas como Serena Mall e Itapajós estão conseguindo resultados acima de 70%. Por isso é muito importante que você reforce com seu time sobre o procedimento de registro do CPF. (Processo Administrativo n. MPMG 0024.18.002027-3. Relatório Gerencial)
>
> Para o funcionamento efetivo do novo programa de relacionamento da Araujo, o Tem + Araujo, você já sabe que o registro do CPF em todas as compras realizadas em nossas lojas é uma etapa fundamental. Agora você também pode acompanhar a conversão do CPF realizado por cada colaborador no Portal Araújo. (Processo Administrativo n. MPMG 0024.18.002027-3. Relatório Gerencial)
>
> Operador de caixa: ao receber o cliente, o operador deve sempre solicitar o CPF e explicar que o cadastro é para aproveitar as vantagens do Tem + Araujo. Se for questionado a respeito do cadastro, ele deve falar que o registro do CPF permite que o cliente tenha direito às promoções que já estão identificadas nas gôndolas e no tabloide.(Processo Administrativo n. MPMG 0024.18.002027-3. Relatório Gerencial)
>
> Lembre-se: o cadastro e o registro do CPF são importantes para criarmos um histórico de compras dos nossos clientes e criar promoções exclusivas e personalizadas, de acordo com o hábito de compras de cada um. (Processo

> Administrativo n. MPMG 0024.18.002027-3. Relatório Gerencial)

Por fim, com base nas infrações identificadas e no faturamento da empresa, o Ministério Público determinou, em dezembro de 2018, a multa de R$ 7.137.721,55, a ser paga pela Drogaria Araújo, com destinação ao Fundo Estadual de Proteção e Defesa do Consumidor.

Posteriormente, em março de 2019, a empresa reviu seu posicionamento frente ao Termo de Ajustamento de Conduta proposto inicialmente pela promotoria e concordou em assiná-lo. Dessa forma, comprometeu-se a, inicialmente, suspender seu programa de fidelidade, cessar a captação e solicitação de CPF dos consumidores, bem como retirar o material relacionado ao programa fidelidade de suas lojas.

Ademais, garantiu-se à empresa a possibilidade de desenvolver uma plataforma própria para o programa de fidelidade, desde que respeitados os parâmetros mínimos de defesa ao consumidor e à proteção de dados pessoais, ou seja, deverá conter todas as regras e condições do programa de maneira clara e explícita. Neste compasso, poderá consentir de forma específica se autoriza, ou não, o compartilhamento com terceiros de seus dados pessoais, havendo a possibilidade de solicitar o cancelamento a qualquer momento. Em caso de autorização, o consumidor deverá ser informado, pela via eletrônica, sobre a data e a empresa que recebeu seus dados.

Finalmente, o regulamento do programa deverá ficar disponível em site próprio e nas lojas da drogaria, por via impressa ou digital, para consulta dos consumidores. Em caso de descumprimento do acordo, a Drogaria Araujo poderá pagar multa em valor entre R$ 50 mil a R$ 100 mil, além de outras penalidades.

3.4 PROGRAMAS DE FIDELIDADE EM REDES DE FARMÁCIA NA GRANDE FLORIANÓPOLIS: CONSENTIMENTO E POLÍTICAS DE PRIVACIDADE

O consentimento, aliás, é um dos pilares presentes na estrutura das leis de proteção de dados pessoais, tanto no modelo europeu, quanto no norte-americano. Não se pretende aqui fazer uma análise exaustiva sobre o tema, mas tão somente apresentar os principais pontos que darão substrato para as conclusões no âmbito deste trabalho.

O consentimento surgiu na segunda geração de leis de proteção de dados pessoais como uma alternativa ao sistema de autorizações e proibições em torno do fluxo de informações presente na primeira

geração. O Estado, por conseguinte, descentralizou o poder de controle que possuía e outorgou ao sujeito o poder de decisão.

Conforme Bruno Bioni (2016), as políticas de privacidade surgiram como uma resposta a essa demanda autorregulatória, estes são, na realidade, contratos de massa e de adesão. Tais "contratos seriados", como chama Orlando Gomes (1999), criam um regulamento coativo e inalterável, imposto por uma parte, com a preordenação uniforme das cláusulas preestabelecidas. Por meio de tal técnica contratual, basta obter o prescrito e necessário consentimento para legitimar toda e qualquer operação de tratamento dos dados pessoais.

Veja-se: as cláusulas do contrato, das políticas de privacidade, são fixadas unilateralmente pelo controlador. Consoante capítulo segundo, o controlador é a pessoa jurídica ou natural que domina todo o fluxo de dados, ou seja, quem possui conhecimento sobre todo o processo de tratamento de dados e que impõe ao indivíduo um documento contratual, devendo este simplesmente aderir ao pacto, sendo o seu consentimento central nesse modelo decisório.

Ocorre, entretanto, que a imposição dos termos do contrato esvazia a eficácia de um modelo individual de autocontrole informacional baseado no consentimento: adotou-se uma lógica de tudo ou nada, que se demonstrou bastante perversa, afinal, ou o indivíduo aceita o que lhe fora exposto, ou está excluído de determinada seara social ou mercadológica.

Segundo Daniel Solove (2006), um conjunto tão limitado de escolhas não permite que os indivíduos expressem suas preferências com precisão, as pessoas podem concordar com certos usos de suas informações pessoais, mas não com outros, contudo, raramente são encontrados instrumentos de granulação desse consentimento, em que se possa indicar quais são os usos permitidos.

Nesse mesmo enleio, Paul Schwartz critica a abordagem puramente mercadológica no âmbito dessa autorregulação, que culminam na "falácia do consentimento" e na "lacuna de conhecimento". Esta última se refere à ignorância individual generalizada sobre os termos que regulam o tratamento de dados pessoais, para o autor, o desconhecimento das práticas de processamento é uma conseqüência sistemática da estrutura social e institucional do uso de dados pessoais, cuja falta transparência apenas beneficia os próprios agentes de tratamento.

A falácia do consentimento, por seu turno, repousa na impossibilidade de que o indivíduo possa ofertar, realmente, o consentimento informado sob o argumento de que, em geral, não

possuem têm conhecimento do contexto tecnológico do uso de dados; e de que o consentimento seja voluntário, tendo em vista os mecanismos de compulsoriedade que circundam esta autorização.

Constata-se que a vida contemporânea baseada na economia de dados impõe suas forças sobre a parte mais vulnerável da relação, não capacita, efetivamente, o cidadão para exercer um controle sobre as suas informações pessoais. Estes estão impotentes e a aceitação se configura como compulsória, afinal, o não consentimento implica na sua exclusão de âmbito da vida social e econômica. O futuro não é animador, a assimetria de saber técnico e jurídico, e consequentemente, a relação de poder existente entre controladores e titulares apenas tende a aumentar.

Conforme sintetiza Bruno Bioni (2016, p. 189): “Mistifica-se a capacidade dos cidadãos de autoproteção de seus dados pessoais, notadamente por sua pseudoautonomia em controlar as suas informações pessoais. O resultado é a sua contínua exploração por ser o ativo econômico da atual economia.”.

Para Daniel Solove (2006) não se deve imputar ao indivíduo a sua falta de responsabilidade quanto à proteção de seus dados pessoais, isso porque os instrumentos, os custos e as burocracias impedem o exercício de seus direitos. O problema não seria simplesmente a falta de controle individual sobre a informação, mas sim a existência de uma situação em que ninguém está exercendo controle significativo sobre sua própria informação.

Nesse contexto, o Bruno Bioni (2016, p. 201) faz a seguinte crítica:

> a proteção contratual do consumidor que é por excelência, um controle *ex post* mediante a declaração de nulidade das cláusulas contratuais abusivas. No mais das vezes, é em juízo que tal relação assimétrica é, por assim dizer, equalizada. Ao passo que a proteção dos dados pessoais tem sido forjada sob uma racionalidade regulatória *ex ante*. [...] ainda que válida, a proteção contratual do consumidor no âmbito das políticas de privacidade seria frustrante, já que, na melhor das hipóteses, a prometida esfera de controle seria *a posteriori*. Por isso, a proteção contratual do consumidor no âmbito das políticas de privacidade não deve ser vista como o mecanismo ideal para a proteção dos dados pessoais. Deve ser encarada como uma ação paliativa se a causa regulatória primária falhar, qual seja, o

> empoderamento *ex ante* do cidadão para exercer um controle genuíno sobre seus dados pessoais.

Apesar disso, mesmo com tais constatações, o consentimento enquanto pilar central da proteção de dados perdura e atravessa quase todas as gerações de leis de proteção de dados, sendo uma base legal prevista tanto no GDPR, quanto na LGPD, razão pela qual ainda deve ser estudada.

Ademais, conforme visto, se o setor farmacêutico se enquadrar na exceção da vedação de compartilhamento de dados referentes à saúde com finalidade de obter vantagem econômica, o consentimento será sua base legal para o tratamento de dados.

Via de regra, propositalmente, são utilizados na redação de tais documentos, que são bastante extensos, uma linguagem prolixa, paradoxal e extremamente técnica. Dessa forma, o dever de informar e a obtenção do consentimento pelo consumidor são apenas formalmente cumpridos, afinal, este, por sua vulnerabilidade técnica e jurídica raramente se dispõe a ler tais documentos e, quando o faz se mostram de difícil compreensão.

Quantidade não quer dizer qualidade. Segundo Nissenbaum (2011), em alguns cenários, são tantas informações a serem lidas, interpretadas, assimiladas pelo usuário, que este passa a não ter condições de incorporá-las em sua tomada de decisão. Em um modelo de tratamento de dados baseado no consentimento, a informação precisa, adequada e clara passa a ser crucial, contudo, muitas vezes, na prática, por sua complexidade e pelo volume, tais informações sequer são assimiladas. Deve-se indicar ao consumidor, de maneira simplificada e clara, quais atividades de tratamento os seus dados pessoais estão sujeitos e os riscos que lhe podem sobrevir.

Em suma, tratando-se de um modelo de consentimento, a qualidade da informação que deve ser priorizada, a fim de permitir que o consumidor tenha conhecimento do que poderá ser feito com seus dados, por quem e por quanto tempo, parâmetros mínimos quando se considera a tutela do consumidor e de seus dados pessoais.

A doutrina sugere novas formas de apresentação e de disponibilização de tais documentos, com a utilização de linguagem clara, simples, com uso de ferramentas de *design* e apresentação amigáveis, para uma interface funcional e de fácil manejo. Ademais, a própria tecnologia como um fator a ser utilizado para auxiliar nesses processos de decisão e proteção do consumidor, são os chamados *privacy enhancing technologies.*

Contraditoriamente, alguns estudos também demonstram que a mera existência de uma política de privacidade leva confiança ao usuário, muito embora seu conteúdo não seja regularmente acessado (JENSEN, POTTS, JENSEN, 2005).

Nesse ponto, retoma-se a questão das políticas de privacidade dos programas de fidelidade de redes farmácias. É incontestável a relevância que os dados relacionados à saúde possuem e as potencialidades que assumem, tanto para o desenvolvimento de estudos e pesquisas na área da medicina, quanto para serem utilizados de forma discriminar e marginalizar indivíduos que não se enquadram em um padrão preestabelecido. Consoante já exposto, a partir da análise de diversas transações realizadas em farmácias, é possível traçar perfis e inferir informações deveras delicadas de um consumidor, como sua atividade sexual, as doenças e enfermidades que o acomete, se houve automedicação, se possui filho, entre outros[112].

Não é à toa que a própria Lei Geral de Proteção de Dados Pessoais classifica os dados referentes à saúde como dados pessoais sensíveis, ou seja, merecedor de atenção e tutela especial pelo ordenamento jurídico e pelos atores atuantes no ecossistema do fluxo informacional. Aliás, não se olvida que a mencionada norma ainda está em sua *vacatio legis*, no entanto, conforme delineado, existe arcabouço jurídico capaz de conferir proteção ao consumidor.

No mundo dos fatos, contudo, não é o que ocorre. Considerando as redes de farmácia, que utilizam o subterfúgio de programas de fidelidade para coleta de dados, verifica-se uma opacidade generalizada, sendo um impeditivo para que consumidores e pesquisadores saibam,

---

112 Conforme foi visto ao longo do trabalho, pode-se elencar alguns dados que podem ser registrados: valor gasto; forma de pagamento; local da transação; frequência de compras; predileção de marcas e produtos de higiene e cosméticos; compra de medicamentos sem prescrição médica ou com prescrição médica, podendo esta ser obrigatória, ou não; compra de pílulas ou outros métodos de contracepção; testes de gravidez; todo e qualquer medicamento vendido na loja, desde um simples antiácido, até mesmo com influência psicotrópica. Stefan Tataru ainda elenca as possibilidades dos dados a serem coletados especificamente em uma farmácia *online*, quais sejam: (i) dados técnicos, como endereço de IP, informações de login, o tipo e a versão do navegador, bem como as extensões instaladas (*plug-ins)*, sistema operacional, e a marca e modelo do dispositivo utilizado; (ii) dados do visitante, como a sequência de cliques e o caminho percorrido no site, produtos vistos ou procurados no site, dados repassados no momento de criação de conta, como nome, *e-mail*, endereço residencial.

efetivamente, a destinação e o uso dos dados de saúde coletados. Princípios básicos consumeristas e de proteção de dados pessoais sequer são observados. Faltam transparência e boa-fé, restam especulações e hipóteses.

Resta, portanto, a avaliação dos instrumentos contratuais que respaldam os programas de fidelidade de redes de farmácia da Grande Florianópolis, objeto deste tópico, a fim de se atingir o objetivo deste trabalho, qual seja, examinar o nível de proteção ofertado aos consumidores e seus dados relacionados à saúde.

Para compor a amostra da análise documental, foram escolhidas cinco diferentes redes que atuam comercialmente na Grande Florianópolis, variando-se sua participação no mercado, de acordo com seus nomes fantasias/marcas: Sesi e Catarinense, com abrangência estadual; Panvel, com abrangência regional; e Droga Raia e Pague Menos, com abrangência nacional.

Em todas, adotou-se o seguinte procedimento: (i) análise inicial do regulamentos do programa e identificação da presença de políticas de privacidade presentes no *site* institucional ; (ii) contato com o Sistema de Atendimento ao Consumidor, questionando-se acerca do funcionamento do programa e de sua política de privacidade; (iii) visita na loja física, solicitando aos atendentes regulares acesso ao regulamento.

3.4.1 Farmácia SESI

A Rede de Farmácias SESI/SC compõe uma das atividades do Serviço Social da Indústria de Santa Catarina (SESI/SC) e sua atividade varejista se circunscreve ao Estado de Santa Catarina[113]. Possui um Programa de Fidelidade[114] em que o consumidor, após fornecer seus dados pessoais e assinar termo de adesão, recebe uma tarjeta de cartão para ser utilizado nas suas compras na loja, e, em contrapartida receber descontos e benefícios.

No regulamento do programa existem cláusulas concernentes a regras de acúmulo; conversão de pontos; resgate de prêmio; transferência de pontos; e exclusão. Não consta disposição alguma sobre privacidade ou proteção de dados pessoais, nem os coletados para a

113 Disponível em: http://www.sesifarmacias.com.br/institucional/sobre
114 Disponível em:
http://www.sesifarmacias.com.br/fidelizacao/sesi_fidelidade/regulamento

realização do cartão, nem os que registrados nas transações realizadas pelo consumidor.

Em contato com o Serviço de Atendimento ao Consumidor, a resposta obtida foi a seguinte:

> Primeiramente agradecemos o seu contato e informamos que mesmo não estando descrito em nosso regulamento, os dados de contato fornecidos pelos nossos clientes em nosso Programa Fidelidade são utilizados para comunicação de ofertas, produtos, serviços e demais informações relacionadas a saúde.

Perquiriu-se maiores esclarecimentos, transcreve-se a réplica:

> Novamente agradecemos o seu contato e em resposta à sua dúvida, sobre o uso e segurança de informações em nosso programa de fidelidade, informamos que, os dados fornecidos no cadastro e registros de compras são utilizadas em ações de relacionamento com os nossos clientes. Essas informações ficam armazenadas em nossos servidores por tempo indeterminado e estão sob os cuidados e proteção dos protocolos de segurança do Sistema da Informação da FIESC.

Na loja física, no bairro Coqueiros, em Florianópolis, o atendente abordado afirmou que não havia regulamento na loja. Conversou-se posteriormente com o gerente da loja que informou que todas as informações estariam disponíveis no *site.*

3.4.2 Drogaria Catarinense

A Rede de Farmácias Drogaria Catarinense faz parte da Companhia Latino Americana de Medicamentos e possui dois diferentes programas de fidelidade, um deles chamado “Fidelidade” e o outro “Fidelidade e Prazo”, cuja diferença é a concessão de crédito neste último, oferecendo ao consumidor a possibilidade de pagar as compras a prazo.

Em análise ao regulamento do Clube de Relacionamento Drogaria Catarinense[115], extrai-se que o consumidor, após assinar um termo de adesão, fornecendo seus dados pessoais e comprovando o local de sua residência, torna-se um "associado". No caso de Fidelidade & Prazo, o consumidor ainda deve comprovar renda mínima de um salário mínimo, bem como de situação creditícia regularizada. Em seguida, recebe a tarjeta de um cartão para utilizar em suas compras.

No documento não consta disposição alguma sobre privacidade ou proteção de dados pessoais, nem os coletados para a realização do cartão, nem os que são registrados nas transações do consumidor, tão somente cláusulas sobre: regras de acúmulo; conversão de pontos; resgate de prêmio; transferência de pontos; e exclusão do programa.

A primeira tentativa de contato no Sistema de Atendimento ao Consumidor foi realizada via *e-mail* no dia 19 de janeiro de 2019. Sem nenhum retorno, tentou-se novo contato via telefone no dia 25 de janeiro de 2019, cobrando-se a resposta da requisição feita. A atendente informou que conversou com o setor responsável e que a solicitação ainda estava em análise. Finalmente, no dia 30 de janeiro de 2019, recebeu-se o seguinte:

> Primeiramente agradecemos seu contato conosco e em atenção ao seu questionamento, informamos que a Drogaria Catarinense age em conformidade com a legislação vigente e que zela por todos os dados e informações que lhe são apresentados. Destacamos ainda que atuamos em um ramo regulado, e como tal, temos o dever de guarda das informações de nossos clientes. Compras não submetidas a esses procedimentos somente são registradas com autorização dos clientes, no ato da compra. Esclarecemos por fim que trabalhamos diuturnamente na melhoria de nossos processos de segurança e conformidade, de modo que cientes da promulgação da Lei Geral de Proteção de Dados, estamos reavaliando e reorganizando os processos impactados.

Na loja física, no bairro Kobrasol, em São José, o atendente abordado afirmou que não conhecia nenhum regulamento e comentou que, em doze anos que ali trabalhava, ninguém havia solicitado

115 Disponível em: http://www.clubedrogariacatarinense.com.br/regulamento_assinado_2019.pdf

anteriormente. A orientação repassada foi de que poderia conversar com o gerente da loja, entretanto, ele não estava presente naquele dia; ou de que poderia entrar em contato com a loja matriz, em Joinville.

3.4.3 Panvel

A Farmácia Panvel faz parte do grupo Dimed S/A - Distribuidora de Medicamentos e possui lojas no Rio Grande do Sul, Santa Catarina, Paraná e São Paulo. Com base no Regulamento, para aderir ao Programa Fidelidade, basta a apresentação de documento com foto. Sobre o que está sendo perscrutado, existe uma cláusula em disposições finais, a qual se reproduz:

> 5.7 Informações cadastrais necessárias para participação no Programa de Fidelidade: CPF, e-mail, data de nascimento, RG, endereço e telefone. Caso o cliente associado titular não queira manter seus dados cadastrais no banco de dados da Panvel, deverá remeter e-mail informando tal opção. Fica ajustado que os dados não serão cedidos a terceiros. O presente Programa visa criar um canal de comunicação com os clientes, especialmente via *e-mail*, razão pela qual será priorizada tal forma de comunicação.

Em contato, no dia 20 de janeiro de 2019, com o Serviço de Atendimento ao Consumidor por *e-mail*, a resposta foi a seguinte: "No site é possível obter o regulamento do Programa Fidelidade que segue em anexo. A parte interessada está em Disposições Finais 5.7.".

Ocorre, contudo, que tal cláusula fica muito aquém do que pode ser chamado de política privacidade, afinal, tão somente trata de maneira parca sobre as informações cadastrais, sem disciplinar sobre todos os outros dados de compras que estão envolvidos na transação. Em seguida, no dia 24 de janeiro de 2019, foi enviado um novo *e-mail* solicitando informações detalhadas. A réplica foi a seguinte:

> A Panvel já está ciente e de acordo com a nova Lei Geral de Proteção de dados (nº 13709), que entra em vigor em 2020. Mesmo assim, até lá a Panvel garante a proteção das informações de clientes, conforme trecho do regulamento do Programa Fidelidade em anexo [a cláusula já

> transcrita], utilizando-se de um sistema rígido de proteção de dados.

Em visita à loja situada no bairro Kobrasol, em São José, primeiramente, a atendente abordada aduziu que não sabia se havia o documento físico na loja. Ato contínuo foi conversar com o gerente da loja, que afirmou que o regulamento não estava disponível na loja física, no entanto, poderia ser acessado pelo *site* da Farmácia.

3.4.4 Droga Raia

A Droga Raia faz parte do Grupo RD e sua abrangência de mercado é nacional[116]. Nos termos de uso do programa de fidelidade possui diversas cláusulas concernentes à sua política de privacidade. Reproduzem-se disposições relevantes:

> 2.2. Para inscrever-se no Programa Sua Droga Raia, os interessados devem preencher corretamente um cadastro com os seus dados pessoais em qualquer loja física Droga Raia, podendo a Administradora disponibilizar outros canais de cadastramento oportunamente. O aceite no momento do cadastro autoriza automaticamente o envio de comunicação dirigida referente à Administradora, bem, como de empresas parceiras da Administradora, enviadas ao cliente exclusivamente pela própria Administradora.
> 2.3. Concluído o cadastro, o cliente deverá utilizá-lo em todas as suas transações de compra e relacionamento com a rede Droga Raia, devendo identificar-se por seu CPF ou por um Código de Identificação (ou por login no Site ou Aplicativo da Administradora). O cadastro é de uso pessoal e intransferível e sua guarda e correta utilização condicionada aos termos deste Regulamento são de total responsabilidade do participante.

Consta expressamente a prática do uso do CPF como identificador único do indivíduo no momento da compra, bem como de

[116] Disponível em: https://www.drogaraia.com.br/nossa-historia

marketing segmentado e direto pela própria farmácia e empresas parceiras, sem, no entanto, denominá-las.

> 4.1. Ao fazer sua adesão ao Programa Sua Droga Raia o cliente autoriza a Administradora armazenar em seu banco de dados suas informações cadastrais e suas informações transacionais geradas nas lojas Droga Raia.
> 4.2. A Administradora compromete-se a respeitar a privacidade do cliente e manter a confidencialidade das informações, podendo usar as informações de seus clientes pelos seguintes motivos:
> 4.2.1. Para entender sua base consumidora e analisar o comportamento de compra dos clientes em todo o negócio Droga Raia, tanto online como no mundo real, incluindo todas as lojas Droga Raia; 4.2.2. Para entrar em contato com os clientes ao longo do tempo acerca de produtos, conteúdo, campanhas, serviços, ofertas, competições e outros eventos; 4.2.3. Para obter feedback dos clientes acerca dos produtos, conteúdo, sites, comunicações, aplicativos de celular e outros serviços e atividades da Droga Raia; 4.2.4. Para divulgar produtos ou serviços para os clientes, por exemplo, através de empresas de terceiros na internet e em sites de mídia social (por exemplo, Facebook e Twitter), atividade publicitária que pode incluir a elaboração de campanhas publicitárias direcionadas aos clientes com base no seu histórico de compras e/ou perfil; 4.2.5. A Administradora poderá compartilhar informações de qualquer cliente participante do Programa Sua Droga Raia com empresas de pesquisa, tecnologia da informação, mídia e consultoria, fornecedoras de terceiros e outros terceiros, bem como empresas de mídia social como Facebook e Twitter, a fim de fornecer aos clientes uma experiência de alta qualidade e custo-benefício ao comprar com a Droga Raia e/ou para divulgar produtos ou serviços para os clientes em plataformas de mídia social e todos os outros meios de comunicação (incluindo a Internet).

Percebe-se como são usadas expressões demasiadamente vagas “informações cadastrais” e “informações transacionais”, sem delimitar quais dados estão abarcados nessas categorias; e utiliza linguagem paradoxal, primeiramente, afirma que será mantida a confidencialidade das informações e a privacidade do cliente, e, em seguida estabelece os usos possíveis, como o compartilhamento dos dados “com empresas de pesquisa, tecnologia da informação, mídia e consultoria, fornecedoras de terceiros e outros terceiros, bem como empresas de mídia social como Facebook e Twitter”, ou seja, com qualquer pessoa, sendo a finalidade a justificativa a vaga expressão “melhoramento dos serviços oferecidos”.

Formalmente, a política de privacidade institui mecanismos de acesso, retificação e objeção pelo consumidor no que tange às suas informações armazenadas na base de dados da cadeia:

> 4.3. A Administradora oferece instrumentos para que os clientes cessem qualquer comunicação que recebam da Droga Raia, podendo ser realizada em qualquer loja física Droga Raia ou através de link de opt-out nos e-mails marketing ou através do Serviço de Atendimento ao Cliente – telefone 3003 7242, podendo a Administradora disponibilizar outros canais oportunamente. Além disso, os clientes podem optar por não permitirem qualquer utilização de seus dados pela Administradora, conforme especificado nestes termos e condições, incluindo qualquer atividade de elaboração de perfis realizada pela Droga Raia ou por terceiros com os quais as informações dos clientes podem ser compartilhadas, qualquer atividade de rastreamento e o serviço de anúncios direcionados aos clientes através de mídias sociais ou a internet.
> 4.4. Um cliente pode solicitar pelo Serviço de Atendimento ao Cliente – telefone 3003 7242- ou por correio, todas as informações sobre si mesmo, incluindo qualquer informação de marketing em posse da Administradora que esteja associada a esse cliente.
> 4.5. Caso qualquer cliente tenha motivos para acreditar que qualquer informação coletada pela Administradora sobre si é incorreta, e este cliente não consiga corrigir seus dados através de suas contas on-line com Droga Raia, favor entrar em

> contato com o Serviço de Atendimento ao Cliente através do telefone 3003 7242.

Com o intuito de investigar a efetividade destes instrumentos, ligou-se para o telefone ali descrito (protocolo 21505556) e fez-se a solicitação, no entanto, a resposta do atendente foi de que esta não poderia ser feita pelo telefone, apenas com um documento escrito de próprio punho enviado ao *e-mail* "contato@drogaraia.com.br". Confrontado verbalmente, entre o teor da cláusula acima e a orientação, o preposto da empresa afirmou que não conseguiria fazer o procedimento por ali.

Assim sendo, em 25 de janeiro de 2018, procedeu-se ao envio da mencionada correspondência. Diante da ausência de até confirmação de recebimento e de protocolo, entrou-se em contato telefônico novamente com o Serviço de Atendimento ao Consumidor (protocolo 21802219). Na ocasião foi informado que a solicitação fora registrada e estava com o setor competente. O prazo previsto para atendimento do requerimento foi de trinta dias. Até o dia 8 de abril de 2019 nenhum documento fora recebido

Conforme já consignado, as outras duas cláusulas estipulam o direito à objeção e à retificação dos dados, contudo, estes dois últimos dependem diretamente do acesso à informação, afinal, apenas se houver conhecimento prévio do que consta nas bases de dados que poderá haver insurgência ou pedido de correção.

> 4.7. Para melhor adequação dos benefícios, a Administradora se reserva no direito de, mediante informações coletadas no ato do cadastro, realizar consultas a terceiros autorizados para validação dos dados cadastrais.

Trata-se de hipótese de cruzamento de base de dados. Por exemplo, com base no CPF, que se trata de um identificador pessoal único, pode-se acessar outra base de dados a fim de acessar outras informações complementares sobre o indivíduo, a fim de traçar perfil mais preciso sobre o consumidor.

Comparativamente, dentre todos os documentos analisados, a política de privacidade do programa de fidelidade da Droga Raia é o mais detalhado, porém, aparentemente, na prática, não destoa das outras redes, uma vez que a solicitação de acesso aos dados sequer foi atendida. Ademais, na visita em loja situada no bairro Kobrasol, em São

José, a atendente abordada afirmou que não tinha conhecimento sobre o documento, sucessivamente, foi conversar com o gerente da loja, em retorno, disse que esse documento sequer existia.

3.4.5 Pague Menos

A Farmácia Pague Menos, Empreendimentos Pague Menos S/A, é considerada a maior rede do setor no país, sendo a única do varejo farmacêutico presente em todas as unidades da federação[117]. Em pesquisa no site, apesar de constar um link "Política de Privacidade", ao clicar nele, foi-se redirecionado a uma "Central de Atendimento", em que não constava em local algum o documento.

Por corolário, entrou-se em contato telefônico, no dia 24 de janeiro de 2019, com o Serviço de Atendimento ao Consumidor (protocolo 2966102). A primeira orientação foi de que o documento estava disponível justamente no link "Política de Privacidade" localizado no site, ato contínuo, informou-se o erro de redirecionamento, o qual foi reconhecido. Em seguida, solicitou-se a retificação no *site*, bem como o encaminhamento via *e-mail* do documento. O mesmo erro acontecia na utilização do aplicativo de vendas. Tais erros persistiram até o dia 11 de fevereiro de 2019 e o documento não fora recebido.

Em loja situada no bairro Kobrasol, em São José, a atendente afirmou que não dispunha da informação e ainda comentou que "nunca ninguém havia solicitado tal documento". A gerente da loja não estava presente no momento, a atendente tentou entrar em contato via telefone, todavia, não conseguiu. Esta solicitou então para que retornasse em outro momento a fim de conversar com a pessoa encarregada da gerência.

3.4.6 Perspectivas gerais: a falta de congruência entre o formal e a prática

Foram escolhidas para compor a amostra cinco diferentes redes de farmácias, com diferentes participações no mercado farmacêutico varejista: duas de alcance estadual, uma de alcance regional e duas outras de alcance nacional.

É possível depreender que a prática da coleta de dados por meio de programas de fidelidade não está circunscrita às redes nacionais, com

[117] Disponível em: http://portal.paguemenos.com.br/portal/empresa Acesso em: 24 de janeiro de 2019.

maior poder econômico, estando presente igualmente nas estaduais e regionais. Somam-se às matérias jornalísticas, pesquisas e investigações realizadas em diferentes unidades da Federação.

Ademais, com fulcro nas redes de alcance nacional, infere-se que a prática da coleta de dados pessoais por meio de programas de fidelidade não se limita à Grande Florianópolis, mas que se estende por todo o território nacional, corroboradas as pesquisas e as investigações trazidas, que se espalham por outras unidades da federação.

Inicialmente, acreditava-se que a estratégia adotada pelas redes de farmácia seria de adoção de políticas de privacidade com os problemas normalmente encontrados (texto extenso, linguagem prolixa e técnica), porém, o que se viu foi um cenário ainda mais precário, a de ausência praticamente completa de regulação e de opacidade ao consumidor.

Das cinco diferentes redes de farmácias situadas na Grande Florianópolis apenas uma possuía documento formal do regulamento do programa de fidelidade (Droga Raia); três não possuíam políticas de privacidade (Catarinense, Sesi e Panvel); e em uma a situação de abusividade e obscuridade foi ainda mais patente: sequer estava disponível no *site* e, mesmo após a tentativa junto ao Serviço de Atendimento ao Consumidor, não se conseguiu acesso. Ressalte-se que se optou por não continuar reiteradamente as tentativas, a fim de perceber se haveria alguma mudança após a incursão, com o desiderato de retratar o descaso e a dificuldade enfrentada pelo consumidor.

Nenhum dos prepostos abordados sabia informar acerca da existência de um regulamento do programa de fidelidade; alguns dos supervisores por eles consultados, igualmente, não possuíam informação precisa sobre a existência e as formas alternativas de consultar o documento; em nenhuma delas havia *in locus* o regulamento do programa. Depreende-se que inexiste preocupação organizacional tanto na redação de tais documentos, quanto em oportunizar seu acesso aos consumidores.

Tais práticas não são tão recentes, logo, é possível inferir que por período significativo de tempo, e ainda hoje, as redes de farmácia atuam como terra sem lei. Questões básicas sobre quais dados estão sendo coletados; sua finalidade; compartilhamento a terceiros; período de tratamento; e retirada de consentimento, sequer são abordadas na maioria dos regulamentos, indicando a ausência de política de privacidade.

Foi verificado que tão somente a Droga Raia disciplina de maneira minudenciada os termos do Programa de Fidelidade. No

entanto, foram identificadas abusividades nas cláusulas, escritas de maneira genérica, sem indicação precisa de quais dados coletados, do tempo de armazenamento e do compartilhamento com terceiros (que da forma escrita, pode ser qualquer empresa).

No mundo dos fatos, encontraram-se entraves para o exercício de direitos ali expostos: na previsão do direito de acesso aos dados continha previsão de que poderia ser realizado tanto pelo telefone, quanto pelo correio, na tentativa de conhecer o mecanismo, já não foi possível utilizá-lo pelo meio telefônico – primeiro entrave. A informação repassada é de que somente por carta de próprio punho seriam consideradas – segundo entrave – e o prazo para resposta era de trinta dias – terceiro entrave. Há um descompasso da previsão formal e a prática e até mesmo sobre a sua aplicação dentro da organização. Ademais, como a informação acerca da existência desse instrumento chega ao consumidor é deveras relevante, bem como possuir de antemão orientações da forma como utilizá-lo.

Quando a esta última questão, ou seja, como a informação chega ao consumidor, foi analisada também a disponibilidade de acesso ao consumidor às politicas de privacidade e regulamento do programa de fidelidade: nenhum dos propostos abordados sabia informar peremptoriamente acerca da existência de um regulamento do programa de fidelidade e de existência de política de privacidade; em nenhuma delas havia *in locus* o regulamento do programa e/ou política de privacidade. Não havia sequer um mecanismo de publicidade com as informações sintetizadas do programa, mormente no que tange à finalidade do programa de fidelidade e da coleta de dados – ocultada do consumidor.

Veja-se, por exemplo, a atendente e o supervisor da Droga Raia que afirmaram que não existia qualquer regulamento, sendo, na realidade, o único que possui a política de privacidade de maneira minudenciada.

Os Serviços de Atendimento ao Consumidor responderam de maneira bastante vaga e genérica às provocações feitas: tudo está em conformidade com a lei. Ainda que não seja possível averiguar processos internos, a omissão ao consumidor dessas informações e a falta de disciplina em documentos considerados básicos para autorregulação no tratamento de dados, demonstram o contrário. A opacidade atrapalha o conhecimento e a diminuição da assimetria informacional.

Tanto na Drogaria Catarinense, como na Panvel, informaram estarem cientes da LGPD, como se ausente qualquer outro arcabouço

normativo de proteção ao consumidor, à privacidade e de proteção aos dados pessoais. Certamente a LGPD irá de suprir lacunas e disciplinar de maneira detalhada o tema no Brasil e provocará diversas modificações no arranjo e nas bases legais no setor de varejo farmacêutico, seria interessante para a agenda de pesquisa no tema acompanhar os rearranjos internos e a movimentação institucional com vistas à conformidade a lei.

Por fim, destaque-se um trecho de uma das respostas recebidas pelo Serviço de Atendimento do Consumidor da Drogaria Catarinense: "[as informações] somente são registradas com autorização dos clientes, no ato da compra.".

Veja-se que todo o respaldo que existe atualmente é o consentimento, assumindo papel importante nesse setor. Ocorre, no entanto, que diante das circunstâncias de marketing, de preços praticados e de opacidade, não é possível afirmar que o consumidor, ao digitar ou ditar seu CPF, sem qualquer conhecimento prévio, tenha exarado consentimento seja livre, informado e inequívoco, por todo o exposto.

Para a conformidade com a Lei Geral de Proteção de Dados, não basta que o controlador obtenha um consentimento precário, devem ser respeitados todos os meandros e limites legais: como no direito tributário, não basta cumprir com as obrigações principais, devendo também observar todas as normas que lhe impõem obrigações acessórias.

A falta de regulação adequada do tema nos programas de fidelidade demonstra a falta de transparência no fluxo de dados do varejo farmacêutico. Não se tem conhecimento acerca dos usos dos dados, por quem, por quanto tempo, por quem são armazenados, nem com quem são compartilhados.

Consoante já exposto, o conteúdo dos dados coletados em farmácias é delicado por sua própria natureza. A partir da análise de diversas transações realizadas em farmácias, é possível traçar perfis e tirar conclusões sobre o comportamento de compra; sua atividade sexual; se faz uso de psicotrópicos; as doenças e enfermidades que possivelmente o acomete e se são crônicas ou agudas; se houve automedicação; qual médico prescreveu o medicamento, se possui filhos pequenos; se faz uso de psicotrópicos, etc.

Com base em padrões e perfis são tomadas decisões que repercutirão na esfera jurídica do consumidor. Na área do consumo, a publicidade que lhe é exposta, quais produtos serão ofertados, como será realizada a apresentação e o preço praticado, por exemplo; e até mesmo

decisões que impactam de maneira ainda mais direta, evidente e significativa a vida do consumidor: de concessão de crédito; de contratação de plano de seguro saúde, com modulação em condições, coberturas, tempo de carência; contrato de emprego ou demissão.

Os riscos, ameaças e prejuízos devem ser conhecidos, por tal razão se reitera a questão da informação substancial: imperioso construir conhecimentos sobre as dinâmicas desse ecossistema, a fim de diminuir a assimetria de poder e informacional existente entre agentes de tratamento e sociedade civil.

CONCLUSÃO

Embora os programas de fidelização não sejam uma novidade no mercado, esta estratégia de marketing exponencialmente se disseminou nos últimos anos em diversos setores. No varejo farmacêutico, a solicitação de dados de identificação do cliente na boca do caixa já foi normalizada. A prática se demonstrou abusiva e até mesmo predatória.

Conforme verificado, na rede de farmácia investigada pelo Ministério Público de Minas Gerais, existem metas internas institucionalizadas determinando que os prepostos façam um número mínimo de novos cadastros de clientes; e que o maior número possível de vendas sejam realizadas com a identificação do cliente. A coleta de dados dos consumidores é massiva e praticamente compulsória.

Em geral, a publicidade realizada reiteradamente é de que o consumidor informa seu CPF para ganhar descontos—como se esse ecossistema tivesse sido forjado tão somente para beneficiá-lo – induzindo o consumidor a conceder seus dados de identificação sem prévia reflexão. Omitem-se na hora da compra quaisquer informações sobre a criação de cadastros com o armazenamento dos dados, suas possibilidades de uso pela própria rede de farmácias e o compartilhamento com terceiros. Em nenhum momento é alertado ao consumidor os riscos inerentes do uso dessas bases de dados.

Ademais, os supostos descontos praticados são de alíquotas consideráveis: na loja, medicamentos chegam a custar metade do preço mediante a identificação do consumidor. Cediço que nossos dados podem ser monetizados e possuem alto valor econômico, mas um único registro da compra de um determinado produto pode chegar a valer, por exemplo, cento e vinte reais? A provocação feita por Ambriola é precisa: nesse ambiente, estariam os consumidores sendo beneficiados pelos descontos, ou punidos por não se identificarem?

A opacidade é generalizada: não é possível afirmar com exatidão como tais dados fluem, apenas especular com fulcro em esparsas fontes de informações. Trata-se de um artifício para isenção de responsabilidades, impedindo que tanto consumidores, quanto pesquisadores saibam, efetivamente, a destinação e o uso dos dados de saúde coletados.

O tratamento de dados pelas redes de farmácia se assemelha a terra sem lei, princípios básicos consumeristas, de privacidade e de proteção de dados pessoais presentes no ordenamento jurídico sequer

são observados. Os instrumentos contratuais, por seu turno, as ditas políticas de privacidade, que respaldariam sua atuação, deixam a desejar. Das cinco diferentes redes de farmácias analisadas detidamente, três não possuíam cláusulas respeitantes ao tema, uma delas sequer se conseguiu acesso ao regulamento do programa de fidelidade e apenas uma possuía documento detalhado disciplinando o assunto (nesta última, contudo, ainda foi identificado que a prática diverge do que está ali exposto, com entraves para o exercício do acesso aos dados, pelo consumidor).

Foram analisadas as políticas de privacidade e a sua disponibilidade de acesso ao consumidor, de cinco diferentes redes de farmácias situadas na Grande Florianópolis: nenhum dos propostos abordados sabia informar acerca da existência de um regulamento do programa de fidelidade; alguns dos supervisores por eles consultados, igualmente, não possuíam informação precisa sobre a existência e sobre as formas alternativas de consultar o documento; em nenhuma delas havia *in locus* o regulamento do programa; finalmente, apenas em uma há disciplina minudenciada de políticas de privacidade, porém, foram identificadas cláusulas abusivas e práticas desconexas com o que está exposto; uma delas sequer foi possível aceder ao regulamento de dados. Depreende-se que inexiste preocupação organizacional tanto na redação minudenciada de tais documentos, quanto em oportunizar seu acesso aos consumidores.

Por outro lado, os comentários exarados pelos prepostos das farmácias, no sentido de que nunca alguém havia solicitado tal documento, são bastante sintomáticos: falta a cultura e a preocupação pela própria população de proteger seus próprios dados.

Em suma, considera-se, assim, que no Brasil, inclusive na Grande Florianópolis, o nível de proteção despendido aos consumidores e a seus dados pessoais referentes à saúde está aquém de uma tutela adequada. Por todo o exposto, viu-se que, apesar da fragmentação legislativa, existem normas de proteção ao consumidor e à privacidade e princípios básicos de proteção de dados que não são observados. Já as políticas de privacidade, instrumento privado de regulação, são utilizadas por apenas uma das cinco redes de farmácia constantes na amostra – e na única que possuía, cláusulas abusivas e distorção entre o texto e o atendimento ao consumidor foram encontradas. A Lei Geral de Proteção de Dados Pessoais, ainda em sua *vacatio legis*, além de suprir lacunas e disciplinar de maneira minudenciada o tema no Brasil provocará diversas modificações no arranjo e nas bases legais no setor de varejo farmacêutico.

Isso porque a LGPD expressamente proíbe o compartilhamento de dados pessoais sensíveis referentes à saúde quando houver objetivo de obter vantagem econômica. Lembre-se de que "dados relacionados à saúde" foram classificados expressamente como dados pessoais sensíveis, contudo, não houve definição legal da expressão, abrindo-se margem interpretativa e discursiva para o que deve ser enquadrado, ou não, como tal. Setores como o varejo farmacêutico e de rendimento em academia ou em esportes, por exemplo, poderão advogar para que a sua extensão seja restritiva, enquadrando-se como dado relacionado à saúde tão somente os coletados em ambientes que esses dados ficam mais evidentes, como, por exemplo, na relação médico-paciente ou hospital-paciente, ou até mesmo no âmbito da telemedicina.

Outros gargalos identificados concernem às exceções legais a essa vedação: a portabilidade de dados quando consentido pelo titular; ou a necessidade de comunicação para a adequada prestação de serviços de saúde suplementar.

A primeira isenção, como se viu, é deveras inconsistente, uma vez que a portabilidade é direito subjetivo do titular, não cabendo a ele consentir, mas tão somente exercer esse direito. A redação abre margem para que controladores de bases de dados relacionados à saúde, quando tiverem interesse de compartilhá-las, apenas requeiram o consentimento ao titular (com todos os problemas inerentes esposados), contornando a proibição atinente aos dados referentes à saúde.

A segunda igualmente suscita preocupação, e inclusive é objeto de proposta de Emenda Supressiva pelo Congresso Nacional, no bojo da tramitação da Medida Provisória nº 869/2018, quanto à extensão interpretativa que poderá atingir a expressão "adequada prestação de serviços pelos agentes de saúde suplementar", erodindo-se o intuito da norma, qual seja, a proteção do indivíduo.

Além disso, conseguindo o setor de varejo farmacêutico se enquadrar em uma dessas exceções, ainda é necessário observar as bases legais para sua atuação. Tratando-se de dados sensíveis, não há a possibilidade de invocar legítimo interesse, dessa forma, remanesce apenas o consentimento enquanto manifestação livre, informada, inequívoca, específica e destacada, para finalidades específicas. Sobrevindo toda a discussão que envolve o consentimento e do direito à informação substancial.

Mesma lógica se aplica, então, à coleta de dados destinada ao tratamento pelo próprio controlador, ressalte-se, sem o intuito de compartilhamento com terceiros: se considerado os seus dados como referentes à saúde, incorrerá como dado sensível, tendo o consentimento

como base legal; se não for considerado dado referente à saúde, cairá na regra geral, podendo invocar o legítimo interesse.

Deste ponto para o futuro, detecta-se a necessidade de acompanhar as próximas movimentações legislativas no que tange aos mencionados dispositivos, como também na Autoridade Nacional de Proteção de Dados. Cediço que se não houver um órgão forte de fiscalização, a Lei Geral de Proteção de Dados pode virar letra morta, e, práticas como estas poderão ser perpetradas, mesmo que ao arrepio da lei.

Assim, o período de *vacatio legis* porvir será crucial. A agenda de pesquisa na área precisa estar atenta para acompanhar e identificar os esforços, gargalos e dificuldades enfrentadas na implementação de mecanismos para atuação em conformidade com a lei, bem como de boas práticas, visando à modificação da cultura e estrutura organizacionais, tanto no setor público, quanto no setor privado.

Resta, agora, fazer o retrospecto do caminho traçado neste trabalho para se chegar até aqui.

Ao primeiro capítulo, reservou-se a incumbência de contextualizar as circunstâncias sociais em que a vigilância e o consumo se inserem. Inicialmente, abordaram-se as modificações das características da vigilância decorrentes do desenvolvimento de tecnologias de informação e comunicação: no início do Século XX, ainda possuía um caráter analógico, específico e local; a partir da década de 1960 passou a ter caráter ubíquo, transfronteiriço e transtemporal, penetrando-se com capilaridade, de forma inevitável, em todos os campos da vida contemporânea.

O panóptico, como dispositivo e técnica de vigilância, descrito por Foucault, precisou abandonar parcialmente sua antiga arquitetura, especialmente delineada para o exercício do poder na Sociedade Disciplinar, para então se adequar às novas relações de poder presentes na Sociedade do Controle, observada por Deleuze. O exercício do poder deixou de atuar diretamente sobre os corpos dos indivíduos, sucedido pelo poder indireto sobre suas mentes: o controle social passa a ser realizado por técnicas de manipulação e desejo. Se na Sociedade Disciplinar os indivíduos deviam ser moldados como dóceis e úteis para servirem e expandirem o sistema de produção, na Sociedade do Controle o que deve ser amplificado é o consumo, a fim de criar uma demanda que tenha capacidade de absorver a incessante produção de bens e serviços.

Foram identificados os novos dispositivos dessa nova arquitetura de vigilância: *dataveillance*, sinóptico, banóptico, palinóptico, técnicas

que visam à criação, à manutenção e à expansão de bases de dados contendo informações sobre o comportamento, personalidade e hábitos de compra de cada indivíduo. Essa base de dados se transforma em objeto de trabalho para monitoramento, construção de perfis e identificação de "categorias-alvo" de compradores, para o êxito de ações de marketing segmentado. Para o consumidor, a liberdade se resume ao ato de escolha, sem ciência de que suas vontades foram inculcadas e de que as opções ofertadas manipuladas de acordo com seu comportamento e consumo anterior.

Viu-se que a vigilância e o consumo, atualmente, são indissociáveis: necessita-se do consumo para se coletar dados; necessita-se da vigilância para a manutenção do consumo. Quem não está de acordo com o padrão preestabelecido, está excluído da dinâmica de mercado e, consequentemente, da oportunidade de aceder a bens e a serviços considerados básicos. Pontuou-se que as dinâmicas e tecnologias de vigilância, associado às tecnologias de tratamento de dados, podem oferecer tratamento desigual, garantindo a segurança e a mobilidade de uns em detrimento do controle e da punição de outros, reforçando a reprodução de desigualdades, preconceitos e discriminações já conhecidas.

No capítulo seguinte, sintetizou-se a evolução histórica e o desenvolvimento teórico do direito à privacidade, perpassando pela autodeterminação informativa e culminando na proteção de dados pessoais. Ambos deram substrato para a apresentação do prisma normativo europeu e do brasileiro.

Com auxílio da construção feita por Mayer-Schonberger (1997), foram expostas as diferentes gerações de leis de proteção de dados, em que se pôde observar a existência de um ciclo intrageracional, que se repetiu ao longo das gerações: constatados os problemas no plano fático, uma norma nova é arquitetada visando solucioná-los; após curto período de vigência da norma, logo são detectados novos impasses advindos de sua aplicação; ato contínuo, esta é alvo de avaliação e revisão, a fim de superar seus gargalos e lacunas.

Discorreu-se, então, sobre a mais recente norma da União Europeia de proteção de dados pessoais: o *General Data Protection Regulation.* Esta introduziu uma nova racionalidade regulatória no âmbito da proteção de dados: além da proteção centrada no indivíduo e no consentimento, privilegiou-se a tutela coletiva, em que os diversos atores envolvidos no ecossistema—controladores, processadores, autoridades de supervisão, certificadores—devem observar os parâmetros estabelecidos e agir cooperativamente com o fito de se

atingir à consecução das diretrizes e dos objetivos estabelecidos pela norma.

Constatou-se que a estrutura da Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, teve por inspiração o supracitado Regulamento europeu, assemelhando-se à sua lógica de participação dos diversos atores participantes do ecossistema do fluxo de dados para atuação cooperativa e transparente, a fim de que se esteja em conformidade legal, bem como a presença de uma Autoridade Nacional de Proteção de Dados, com funções de supervisão, interpretativa, regulatória, fiscalizatórias e sancionatórias, como garante desse novo arranjo.

Por conta de sua relevância, debruçou-se sobre a Medida Provisória nº 869/2018, que, comparativamente ao texto original aprovado por ambas as Casas Legislativas, modificou drasticamente a natureza jurídica e a estrutura da Autoridade Nacional de Proteção de Dados, subordinando-a à Presidência da República na condição de órgão da administração direta. Apesar daquela ainda não ter sido votada pelo Congresso Nacional, investigaram-se as possíveis consequências e repercussão dessas alterações e da falta de independência para a atuação do órgão e do *enforcement* normativo.

No que atine aos direitos e princípios, além de incorporados os *Fair Information Practice Principles* - finalidade, livre acesso, segurança, transparência e qualidade - também foram positivados outros conquistados contemporaneamente, quais sejam: não discriminação; adequação; necessidade; prevenção e responsabilização e prestação de contas. Perpassando todo o espectro principiológico subsiste ainda a boa-fé objetiva como ditame a ser observado pelos agentes de tratamento.

No terceiro capítulo, inicialmente, tratou-se do exercício da biopolítica: o mesmo poder de Estado que promove a saúde da população, também se utiliza dessa relação de poder para controlar os corpos dos indivíduos. A estrutura de coleta de dados de saúde, antigamente circunscrita tão somente aos profissionais específicos da área da saúde e ao Estado, expandiu-se e ramificou-se, abarcando também a área privada: planos de saúde, mecanismos online de pesquisa, laboratórios de exame, aplicativos de celular referentes a ciclo menstrual, rendimento físico e farmácias agora fazem parte de uma estrutura de vigilância.

Situaram-se, em seguida, os programas de fidelidade como engrenagem da relação vigilância e consumo, retomando-se as ideias esposadas no primeiro capítulo, aprofundando-se as questões relativas às

técnicas de análise de dados visando ao perfilamento, a classificação e ao ranqueamento dos indivíduos, utilizados para processos de tomada de decisões por agentes econômicos e governamentais e os eventuais riscos e custos sociais envolvidos nesse obscuro sistema.

Em seguida, adentrou-se à questão específica da proteção do consumidor e de seus dados referentes à saúde em programas de fidelidade de redes de farmácia. Foram relatadas pesquisas, ações de jornalistas e de grupos de pesquisa, e investigações do Ministério Público, em todo o Brasil, visando à compreensão da prática da coleta de dados no ambiente comercial.

Foram analisadas as políticas de privacidade e a sua disponibilidade de acesso ao consumidor, de cinco diferentes redes de farmácias situadas na Grande Florianópolis: nenhum dos propostos abordados sabia informar acerca da existência de um regulamento do programa de fidelidade; alguns dos supervisores por eles consultados, igualmente, não possuíam informação precisa sobre a existência e sobre as formas alternativas de consultar o documento; em nenhuma delas havia *in locus* o regulamento do programa; finalmente, apenas em uma há disciplina minudenciada de políticas de privacidade, porém, foram identificadas cláusulas abusivas e práticas desconexas com o que está exposto; uma delas sequer foi possível aceder ao regulamento de dados. Por fim, para além do objetivo perquirido, este trabalho pode ajudar a compreender o fluxo de informações que perpassa o setor farmacêutico, demonstrando sua opacidade, demandando-se maior transparência. Conforme consignado, é importante construir conhecimentos sobre as dinâmicas desse ecossistema, a fim de diminuir a assimetria de poder e informacional existente entre sociedade civil e pesquisadores e agentes de tratamento de dados.

De mais a mais, pode ser um veículo de disseminação de informação: chamar a atenção dos titulares de dados, a fim de que se preocupem com seus dados pessoais, principalmente seus dados sensíveis, e conheçam os possíveis riscos e as consequências que envolvem o tratamento indiscriminado de dados. Apenas assim se iniciará a construção de uma cultura popular e coletiva de proteção de dados, reconhecendo-se a importância deste direito em atual construção e da privacidade no mundo digital.

REFERÊNCIAS

ARAGÃO, Alexandre Santos de. **Agências reguladoras e a evolução do direito administrativo econômico.** 3. ed. Rio de Janeiro: Forense, 2013.

ARAÚJO, Edmir Netto de. A aparente autonomia das agências reguladoras. In. MORAES, Alexandre de. **Agências Reguladoras.** São Paulo, Atlas, 2002, p. 39 - 55.

ASSMAN, Jhonata. **O direito à autodeterminação informativa no direito germânico e brasileiro.** 2014. 65 f. TCC - Curso de Direito, Universidade Federal de Santa Catarina, Florianópolis, 2014.

BARBOSA MOREIRA, José Carlos. O Habeas Data brasileiro e sua Lei Regulamentadora. **Revista de Direito Administrativo.**v. 211, 1998 http://dx.doi.org/10.12660/rda.v211.1998.47125

BARROSO, Luis Roberto. Apontamentos sobre as Agências Reguladoras. In: MORAES, Alexandre de. **Agências Reguladoras.** São Paulo: Atlas, 2002, p. 109 - 118.

BAUDRILLARD. **A Sociedade de Consumo.** Lisboa: Edições 70, 1995.

BAUMAN, Zygmunt. **A Vida para Consumo: A Transformação das Pessoas em Mercadoria**. Rio de Janeiro: Zahar, 2008.

BAUMAN, Zygmunt. **Globalização**: As consequências humanas. Rio de Janeiro: Zahar, 2008.

BAUMAN, Zygmunt. **Modernidade Líquida**. Rio de Janeiro: Zahar, 2001.

BAUMAN, Zygmunt. **O Mal-Estar da Pós-Modernidade**. Rio de Janeiro: Zahar, 1998.

BAUMAN, Zygmunt; LYON, David. **Vigilância Líquida.** Rio de Janeiro: Zahar, 2012.

BECK, Ulrich. **Sociedade de Risco:** rumo à uma nova modernidade. São Paulo: Editora 34, 2a ed, 2011.

BIONI, Bruno. **Autodeterminação Informacional: Paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet.** 2016. 309 f. Dissertação (Mestrado) - Curso de Direito, Universidade de São Paulo, São Paulo, 2016.

BIONI, Bruno. Proteção de Dados, Fluxo Transnacional, GDPR. In: Seminário Governança das Redes, 3, Belo Horizonte, 2018, Anais [s.l.], 2018, p. 50 - 69.

BOLOGNA, Silvio; CORSO, Pietro; BELLAVISTA, Alessandro; ZANGARA, Gianluca. Electronic Health Record in Italy and Personal Data Protection. **European Journal of Health Law,** v. 23, n. 3, 2016, p. 265–277.doi:10.1163/15718093-12341403

BRANDEIS, Louis; WARREN, Samuel. The Right to Privacy. Nova Orleans: Quid Pro LLC, 2010.

BRUNO, Fernanda. **Máquinas de ver, Modos de Ser**: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013.

CANCLINI, Nestor García. **Consumidores e cidadãos:** conflitos multiculturais da globalização. Rio de Janeiro: UFRJ, 2001.

CARVALHO FILHO, José dos Santos. **Manual de Direito Administrativo**. 32 ed. São Paulo: Atlas, 2018.

CHILDRESS, Steven Alan. **Prefácio** In: Louis; WARREN. Samuel. **The Right to Privacy.** Nova Orleans: Quid Pro LLC, 2010.

CLARKE, Roger. Information Technology and Dataveillance. **ACM** 31, no. 5, p. 498–512, 1998.

CLARKE, Roger. The Digital Persona and Its Application to Data Surveillance. **Information Society** [s.l.], v 10, n. 2, p. 77–92, 1994.

COHEN, Julie. Examined Lives: Informational Privacy and the Subject as Object. **Standford Law Review** [s.l], v. 52, p. 1373-1438, 2000.

DANNA, Anthony; GANDY JUNIOR, Oscar H.. All That Glitters is Not Gold: Digging Beneath the Surface of Data Mining. **Journal Of Business Ethics**, [s.l.], v. 40, n. 4, p.373-386, 2002. Springer Nature. http://dx.doi.org/10.1023/a:1020845814009.

DARDOT, Pierre; LAVAL, Christian. **A Nova Razão do Mundo.** 1 ed. São Paulo: Boitempo, 2016.

DEBAETS, Emilie. Personal Data Protection in Tumor Banks. In: BIOY, Xavier. **Public Regulation of Tumor Banks Establishment, Heritage Status, Development and Sharing of Human Biological Samples**. Londres: Springer, 2018. p. 19 - 30.

DELEUZE, Gilles. **Conversações**. 1 ed. São Paulo: Editora 34, 1992.

DIXON, Pam; GELLMAN, Robert. **The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future.** In: World Privacy Forum Report. Abril, 2014. Disponível em:https://www.worldprivacyforum.org/2014/04/wpf-report-the-scoring-of-america-how-secret-consumer-scores-threaten-your-privacy-and-your-future/. Acesso em: 18 de dezembro de 2018

FARIA, José Eduardo. **O Direito na Economia Globalizada.** São Paulo: Malheiros, 1999.

FARIAS, Cristiano Chaves de; ROSENVALD, Nelson. **Curso de Direito Civil.** 16a ed. Salvador: 2018.

FOUCAULT, Michel. **Vigiar e Punir:** Nascimento da prisão. Petrópolis: Vozes, 2005.

FOUCAULT, Michel. **Microfísica do poder**. 13 ed. Rio de Janeiro: Graal, 1998.

FOUCAULT, Michel. **Nascimento da Biopolítica.** 1a ed. São Paulo: Martins Fontes, 2008.

FREUD, Sigmund. **O Mal-Estar na Civilização.** Rio de Janeiro: Imago, 1997.

GANDY, Oscar H. The Surveillance Society: Information Technology and Bureaucratic Social Control. **Journal Of Communication**, [s.l.], v. 39, n. 3, p.61-76, 1 set. 1989. Oxford University Press (OUP). http://dx.doi.org/10.1111/j.1460-2466.1989.tb01040.x.

GONZALEZ FUSTER, Gloria. **The Emergence of Personal Data Protection as a Fundamental Right of the EU**. Londres: Springer, 2016.

GONZALEZ FUSTER, Gloria.**Beyond the GDPR, above the GDPR.** Disponível em: https://policyreview.info/articles/n\A\Zews/beyond-gdpr-above-gdpr/385

GOULART, Guilherme. Proteção de Dados, Fluxo Transnacional, GDPR. In: Seminário Governança das Redes, 3, Belo Horizonte, 2018, Anais [s.l.], 2018, p. 50 - 69.

GRAEFF, Timothy; HARMON, Susan. Collecting and using personal data: consumers awareness and concerns, **Journal of Consumer Marketing**, 2002, v. 19, n. 4, pp.302-318, https://doi.org/10.1108/07363760210433627

GREENWALD, Glenn. **No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State.** Nova Iorque: Metropolitan, 2014.

GUADAMUZ, Andres. Habeas Data: The Latin-American Response to Data Protection. The Journal of Information, Law and Technology, v. 20 2000 Disponível em: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_2/guadamuz/.

HAN, Byung-Chul. **La Sociedade de la Transparencia.** Barcelona: Herder Editorial, 2013.

HAN, Byung-Chul. **Psicopolítica**. Barcelona: Herder Editorial, 2014.

HAN, Byung-Chul. **No enxame.** Petrópolis: Vozes, 2018.

HAN, Byung-Chul. **Sociedade do Cansaço**. Petrópolis: Vozes, 2015

HARVEY, David. **Condição Pós-Moderna**: Uma Pesquisa sobre as Origens da Mudança Cultural. 17 ed. São Paulo: Loyola, 2008.

HILBERT, Martin; LOPEZ, Priscila. **The World's Technological Capacity to Store, Communicate, and Compute Information.** Science. Disponível em: http://www.martinhilbert.net/WorldInfoCapacity.html/

HUR, Domenico Uhng. Da biopolítica à noopolítica: contribuições de Deleuze. **Lugar comum**, v. 10, n. 40, dez.2013, pp. 201-215. Disponível em: https://goo.gl/Y1prLc.

HUSTINX, Peter. **EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation.** Disponível em: https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_en.pdf
HUXLEY, Aldous. **Admirável Mundo Novo**. São Paulo: Globo, 2009.

JENSEN, Carlos; POTTS, Colin; JENSEN, Christian. Privacy practices of Internet users: Self-reports versus observed behavior. **Human Computer Studies**, v. 63, 2005, p. 203-227.

LACE, Susanne. **The glass consumer**: life in a surveillance society. Bristol: Policy Press, 2005.

LEMOS, Ronaldo; DOUEK, Daniel; ADAMI, Mateus Piva; LANGENEGGER, Natalia; FRANCO, Sofia Lima. **A criação da Autoridade Nacional de Proteção de Dados pela MP nº 869/2018.** Disponível em: https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/artigos/a-criacao-da-autoridade-nacional-de-protecao-de-dados-pela-mp-no-869-2018-29122018

LEONARDI, Marcel. A garantia fundamental do direito à privacidade e à liberdade de expressão nas comunicações como condição ao pleno exercício do direito de acesso à internet. In: LEITE, George Salomão; LEMOS, Ronaldo. **Marco Civil da Internet.** São Paulo: Atlas, 2014. p. 621-633.

LESSIG, Lawrence. **Code 2.0.** Nova Iorque: Basic Books, 2006.

LESSIG, Lawrence. Privacy as Property **Social Research** Vol. 69, No. 1, pp. 247-269. Disponível em: http://www.jstor.org/stable/40971547

LIPOVETSKY, Gilles. **A Felicidade Paradoxal**: Ensaio sobre a Sociedade do Hiperconsumo. Lisboa: Edições 70, 2006.

LIPOVETSKY, Gilles. **O Império do Efêmero**. Companhia de Bolso

LIPOVETSKY, Gilles. **Os Tempos Hipermodernos.** São Paulo: Barcarolla, 2004.

LIPOVETSKY, Gilles**;** SERROY, Jean. **A Estetização do Mundo: Viver na Era do Capitalismo Artista**. 1ª ed. São Paulo: Companhia das Letras, 2015.

LINKSEY, Orla. **The Foundations of EU Data Protection Law.** Oxford: Oxford University Press, 2015.

LOGAN, Robert. **O que é informação: a propagação da informação na biosfera, na simbolosfera, na tecnosfera e na econosfera**. Rio de Janeiro: Contraponto,. 2012.

LYON, David. **The electronic eye: The Rise of Surveillance Society.** Minneapolis: University of Minnesota Press, 1994.

LYON, David. **Surveillance as Social Sorting.** Nova Iorque: Routledge, 2003.

LYON, David. Facing the future:: Seeking ethics for everyday surveillance. **Ethics And Information Technology**, [s.l.], v. 3, n. 3, p.171-180, mar. 2001. Springer Nature. http://dx.doi.org/10.1023/a:1012227629496.

MACHADO, Roberto. Apresentação. In: FOUCAULT, Michel. **Microfísica do poder**. 13 ed. Rio de Janeiro: Graal, 1998.

MACHADO, Diego; DONEDA, Danilo. **Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados.** Disponível em:

https://www.researchgate.net/publication/330401277_Protecao_de_dados_pessoais_e_criptografia_tecnologias_criptograficas_entre_anonimizacao_e_pseudonimizacao_de_dados

MARQUES, Claudia Lima, BENJAMIN, Antonio Herman; MIRAGEM, Bruno. **Comentários ao Código de Defesa do Consumidor**. 3a ed. São Paulo: RT. 2010, p. 297.

MARTINS, Leonardo. (org.) **Cinquenta Anos de Jurisprudência do Tribunal Constitucional Alemão**. Montevidéu: Fundação Konrad Adenauer, 2005.

MARX, Gary. **Windows into the Soul: Surveillance and Society in an age of High Technology.** Chicago: The University of Chicago Press, 2016. DOI: 10.7208/chicago/9780226286075.001.0001

MATHIESEN, Thomas. **The Viewer Society: Michel Foucault's Panopticon Revisited.** Londres: Theoretical criminology : an international journal, v. 1, 1997, pp.215-232.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big Data: The Essential Guide to Work, Life and Learning in the Age of Insight.** John Murray Publishers: Londres, 2017.

MAYER-SCHÖNBERGER, Viktor. Generational Development of Data Protection in Europe. In: AGRE, Philip E.; ROTENBERG, Marc. **Technology and Privacy: The New Landscape.** Cambridge: MIT Press, 1997. p. 219-242.

MENDES, Gilmar; BRANCO, Paulo Gonet. **Curso de Direito Consticional.** 14a ed. São Paulo: Saraiva, 2013.

MENDES, Laura Schertel. **Privacidade, Proteção de Dados e Defesa do Consumidor.** São Paulo: Saraiva, 2014.

MENDES, Laura Schertel. **Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo.** 156 f. Dissertação (Mestrado) - Curso de Direito, Universidade de Brasília, Brasília, 2008

MENDES, Laura Schertel. **Uso de softwares espiões pela polícia: prática legal? Disponível em:** https://www.jota.info/autor/laura-schertel-mendes

MENDES, Laura Schertel; DONEDA; Danilo. Reflexões iniciais sobre a nova lei geral de proteção de dados pessoais. **Revista do Direito do Consumidor.** v. 120, ano 27, São Paulo, nov - dez, 2018, p. 469 - 483.

MENDES, Laura Schertel; DONEDA; Danilo. Comentário à nova Lei de Proteção de Dados: o novo paradigma de proteção de dados no Brasil. **Revista do Direito do Consumidor.** v. 120, ano 27, São Paulo, nov - dez, 2018, p. 555 - 587.

MONCAU, Luiz Fernando et al. **Contribuição do Centro de Tecnologia e Sociedade da FGV Direito Rio ao debate público sobre o Anteprojeto de Lei de Proteção de Dados Pessoais.** Disponível em: http://bibliotecadigital.fgv.br/dspace/handle/10438/17472

MORAES, Maria Celina Bodin de. Apresentação. In: RODOTÀ, Stefano. **A vida na sociedade de vigilância:** A privacidade hoje. Rio de Janeiro: Renovar, 2008.

MORAES, Maria Celina Bodin de; TEFFÉ, Chiara. Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. **Revista Pensar**, v. 22, n. 1 2017, p. 108 - 146.

MORAIS, José Luiz Bolzan; MENEZES NETO, Elias Jacob de. A insuficiência do marco civil da internet na proteção das comunicações privadas armazenadas e do fluxo de dados a partir do paradigma da surveillance, In: LEITE, George Salomão; LEMOS, Ronaldo. **Marco Civil da Internet.** São Paulo: Atlas, 2014. p. 417 - 429.

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).** Disponível em: https://www.researchgate.net/publication/330000896_Dados_pessoais_sensiveis_e_a_tutela_de_direitos_fundamentais_uma_analise_a_luz_da_lei_geral_de_protecao_de_dados_Lei_1370918

NISSENBAUM. Helen. **Privacy in Context.** Standford University Press: Standford, 2010.

NOUGRÈRES, Ana Brian. Data Protection and Enforcement in Latin America and in Uruguay. In: WRIGHT, David; HERT, Paul de. **Enforcing Privacy Regulatory, Legal and Technological Approaches.** Londres: Springer, 2017. p. 145-182.

OLIVEIRA, Ricardo Alexandre.Lei Geral de Proteção de Dados Pessoais e seus impactos no ordenamento jurídico. **Revista dos Tribunais.** v. 107, n. 998, nov - dez 2018.

O'NEIL, Cathy. Weapons of Math Destruction: How big data increases inequality and threatens democracy. Nova Iorque: Broadway Book, 2018.

ORWELL, George. **1984**. 29ª ed. São Paulo: Ed. Companhia Editora Nacional, 2005.

OST, François. El reflejo del Derecho en La Literatura. **Doxa: Cuadernos de Filosofía del Derecho**, Alicante, v. 29, n. 26, p.333-348, 2006.

PASQUALE, Frank. **The Black Box Society**: The Secret Algorithms That Control Money and Information.Cambridge: Harvard University Press, 2015.

PASQUALE, Frank. Redescribing Health Privacy: The Importance of Information Policy (November 3, 2015). **Houston Journal of Health Law and Policy,** Vol. 14, p. 95, 2014; U of Maryland Legal Studies Research Paper No. 2015-40. Disponível em: https://ssrn.com/abstract=2685696

POSTER, Mark. **The Second Media Age**. Cambridge: Polity, 1995.

PRIDMORE, Jason Hart. **Loyal Subjects?:** Consumer surveillance in the personal information economy. 2008. 240 f. Tese (Doutorado) - Curso de Sociologia, Queen's University, Kingston, 2008.

RICHARDSON, Megan. **The Right to Privacy:** Origins and Influence of a Nineteenth-Century Idea. Cambridge: Cambridge Press, 2017.

RODOTÀ, Stefano. **A vida na sociedade de vigilância:** A privacidade hoje. Rio de Janeiro: Renovar, 2008.

SANTOS, Fabíola Meira de Almeida; TALIBA; Rita. Lei Geral de Proteção de Dados no Brasil e os possíveis impactos. **Revista dos Tribunais.** v. 107, n. 997, nov-dez 2018, p.

SARAIVA, Raquel. Inteligência Artificial. In: **Seminário Governança das Redes**, 3, Belo Horizonte, 2018, Anais [s.l.], 2018, p. 86 - 95.

SHMATIKOV, Vitaly; NARAYANAN, Arvind. **How To Break Anonymity of the Netflix Prize Dataset.** Disponível em: https://arxiv.org/abs/cs/0610105

SCHMITZ, Amy. Secret Consumer Scores and Segmentations: Separating Consumer 'Haves' from 'Have-Nots'. **Michigan State Law Review,** v. 15, n. 6, jun, 2015, p. 1411 - 1476.

SCHNEIER, Bruce. **Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.** W. W. Norton & Company: Nova Iorque, 2015.

SCHREIBER, Anderson. **Direitos da Personalidade.** 3a ed. São Paulo: Atlas, 2014.

SCHWARTZ, Paul. **Privacy and Democracy in Cyberspace.** Disponível em: http://dx.doi.org/10.2139/ssrn.205449

SCHWARTZ, Paul; PEIFER, Karl-Nikolaus. **Transatlantic Data Privacy Law.** Disponível em: https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3913&context=facpubs

SMITH, Andrew; SPARKS, Leigg. Making Tracks: Loyalty Cards As Consumer Surveillance. In: TURLEY, Darach; BROWN, Stephen. **E - European Advances in Consumer Research.** 6. ed. Provo: Association For Consumer Research, 2002. p. 368-373.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo.** 36 ed. São Paulo: Malheiros, 2012

SILVEIRA, Sergio Amadeu da. **Tudo sobre Todo@s: redes digitais, privacidade e venda de dados pessoais**. São Paulo: SESC, 2017.

SILVEIRA, Sérgio Amadeu; AMBRIOLA, Amanda Yumi. **As implicações políticas dos algoritmos.** Tecnopolítica. 7min 28s. Disponível em: https://www.youtube.com/watch?v=aRkqfx_XTVY. Acesso em: 30 de dezembro de 2018.

SOLOVE, Daniel. **A Brief History of Information Privacy Law.** Washington: GW Law Faculty Publications, 2006

SOLOVE, Daniel. A taxonomy of privacy. **University Of Pennsylvania Law Review.** Filadélfia, p. 477-560. jan. 2006.

SOLOVE, Daniel.**The Digital Person: technology and privacy in the information age.** New York University Press. Nova Iorque: 2004.

SOUZA, Joyce Ariana de. **A saúde dos dados pessoais e o município de São Caetano do Sul.** 2018. 189 f. Dissertação (Mestrado) - Curso de Ciências Humanas e Sociais, Universidade Federal do Abc, Santo André, 2018.

TARTUCE, Flavio; NEVES, Daniel Amorim Assumpção. **Manual de Direito do Consumidor.** 6 ed. São Paulo: Forense, 2017.

TATARU, Stefan Razvan. **Personal Data Protection in the Commercial Operations of e-Pharmacies.**Disponível em: <https://www.researchgate.net/publication/330411037_Protectia_datelor_cu_caracter_personal_in_activitatea_farmaciilor_online_Personal_Data_Protection_in_the_Commercial_Operations_of_e-Pharmacies>. Acesso em: 23 jan. 2019.

VOIGT, Paul; Bussche, Axel von dem. **The EU General Data Protection Regulation (GDPR).** Londres: Springer, 2017.

YAKOVITZ BAMBAUER, Jane R. Tragedy of the Data Commons. **Harvard Journal of Law and Technology,** Vol. 25, mar 2011, Disponível em: https://ssrn.com/abstract=1789749

WARAT, Luis Alberto. **O Direito e a Sua Linguagem.** 2a ed. Porto Alegre: Sergio Antonio Fabris Editor, 1995.

WONG, Rebecca. The Data Protection Directive 95/46/EC: Idealisms and Realisms. **International Review Oflaw, Computers & Technology**: Routledge, Nova Iorque, v. 26, n. 2-3, p.229-244, nov. 2012.

WRIGHT, David; Hert, Paul de. **Enforcing Privacy: regulatory, legal and technological approaches**. Springer: Londres, 2016.

ZANATTA, Rafael. A proteção de dados pessoais entre leis, códigos e programação: os limites do Marco Civil da Internet. In: De LUCCA, Newton; SIMÃO FILHO, Adalberto; PEREIRA DE LIMA, Cintia Rosa. **Direito e Internet III: Marco Civil da Internet**, São Paulo, Quartier Latin, 2015, p. 447 - 470.

ZUBOFF, Shoshana. **The Secrets of Surveillance Capitalism.** Frankfurt: Allgemeine Zeitung GmbH, 2016.

ZUBOFF, Shoshana. **Big other: surveillance capitalism and the prospects of an information civilization.** London: Journal of Information Technology, 2015, 75– 89. Disponível em: http://ssrn.com/abstract=2594754. Acesso em 01 de abril de 2017.

ZURAWSKI, Nils. Local Practice and Global Data: Loyalty Cards, social practices, and consumer surveillance. **The Sociological Quarterly**, [s.i], v. 4, n. 52, p.509-527, ago. 2011.