INSTITUTO BRASILIENSE DE DIREITO PÚBLICO
ESCOLA DE DIREITO E ADMINISTRAÇÃO PÚBLICA
MESTRADO ACADÊMICO EM DIREITO CONSTITUCIONAL

MATHEUS BARRA DE SOUZA

O FUNDAMENTO CONSTITUCIONAL DA PROTEÇÃO DE DADOS:
FERRAMENTAS CONSTITUCIONAIS DE CONTROLE DO PODER DOS COMUNICADORES FIDUCIÁRIOS

BRASÍLIA/DF
2021

MATHEUS BARRA DE SOUZA

O FUNDAMENTO CONSTITUCIONAL DA PROTEÇÃO DE DADOS

FERRAMENTAS CONSTITUCIONAIS DE CONTROLE DO PODER DOS COMUNICADORES FIDUCIÁRIOS

Dissertação de Mestrado, desenvolvida sob a orientação do Prof. Dr. Gilmar Ferreira Mendes e apresentada como requisito para obtenção do título de Mestre em Direito Constitucional.

BRASÍLIA/DF

2021

MATHEUS BARRA DE SOUZA

O FUNDAMENTO CONSTITUCIONAL DA PROTEÇÃO DE DADOS

FERRAMENTAS CONSTITUCIONAIS DE CONTROLE DO PODER DOS COMUNICADORES FIDUCIÁRIOS

Dissertação de Mestrado, desenvolvida sob a orientação do Prof. Dr. Gilmar Ferreira Mendes e apresentada como requisito para obtenção do título de Mestre em Direito Constitucional.

30 de junho de 2021.

BANCA EXAMINADORA

_____

Prof. Dr. Gilmar Ferreira Mendes
Orientador

_____

Prof. Dr. Georges Abboud
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa
Membro Interno

_____

Prof. Dr. Bruno Dantas Nascimento
Universidade do Estado do Rio de Janeiro
Membro Externo

_____

Prof. Dr. Danilo César Maganhoto Doneda
Universidade do Estado do Rio de Janeiro
Membro Externo

Ao meu querido tio Benes Contente Barra.

A saudade de sua alegria contagiante fica, mas a certeza de que está, agora, alegrando a vida eterna de seus irmãos reconforta a alma. Não elimina a dor da falta, que será permanente, mas também o será a memória dos dias felizes.

AGRADECIMENTOS

Marcado pelas diversas limitações causadas pela pandemia de Covid-19, este trabalho é fruto de um período de minha vida marcado por uma dose relevante de introspecção – forçada, é verdade, mas nem por isso desimportante: em toda dificuldade se esconde uma oportunidade.

É por isso que meus agradecimentos se direcionam, primeiramente, à minha família: minha mãe, Ana Paula, meu pai, Jorge, e meu irmão, Thiago. Passar um ano e meio trancado em casa, trabalhando em um ritmo alucinante, não foi nada fácil. Mas, também, foi uma oportunidade de passar tempo com as pessoas que mais amo nessa vida e lembrar o que é que realmente importa nesse mundo.

Passada a pandemia, provavelmente nunca mais terei a oportunidade de desfrutar tanto tempo com essas três pessoas que foram, são e serão essenciais na formação de quem eu sou e que são indispensáveis à minha felicidade.

Agradeço, portanto, a cada um dos três por todas as conversas, jantares, pseudo-saídas e experiências vividas nesse tempo, além da sempre presente parceria e apoio inegociáveis que tive de todos por esse tempo – só nós sabemos as agruras vividas nesse período como família. Agradeço, em suma, por todo o amor incondicional de vocês. E quero que saibam que eu os amo profundamente.

Também agradeço à minha turma do mestrado do IDP: afirmo, sem qualquer medo de errar, que dei muita sorte em tê-los ao meu lado nessa jornada. Além de valiosas amizades, ganhei, fora da sala de aula, um aprendizado maior do que eu jamais poderia imaginar que alcançaria.

Registro, igualmente, meu agradecimento ao meu orientador, Professor Gilmar Mendes, pela oportunidade de aprender diretamente de um dos maiores constitucionalistas brasileiros da história.

Agradeço, por fim, ao querido amigo João Pedro Mello pelos valorosos comentários que fez a este trabalho, bem como a todos os demais que, de uma forma ou de outra, se fizeram presentes na realização desta dissertação.

RESUMO

Este trabalho teve por tema a proteção de dados pessoais e objetivou analisá-la como desenvolvimento do direito à privacidade diante da realidade tecnológica do século XXI. Por meio de revisão bibliográfica e análise descritiva dos potenciais das inovações tecnológicas, pôde-se estabelecer quais são os riscos de ordem individual que as inovações trouxeram à privacidade. A partir disso, constatou que os riscos à privacidade, originalmente de índole individualista, transmudaram-se para uma preocupação de índole social a partir da expansão das capacidades dos comunicadores fiduciários. A preocupação observada foi, essencialmente, aquela relativa à limitação do poder, a qual relaciona-se com as preocupações verificadas na gênese do constitucionalismo e que a ele foram e permanecem intrínsecos. Então, este trabalho extraiu um fundamento constitucional para a proteção de dados decorrente diretamente do aspecto político da Constituição, de onde decorreu a necessidade de utilização de ferramentas de índole constitucional para o resguardo da privacidade como expressão necessária de uma ordem constitucional.

Palavras-chave: Proteção de dados, privacidade, constitucionalismo, comunicação fiduciária.

ABSTRACT

This work had as its theme the protection of personal data and aimed to analyze it as a development of the right to privacy in light of the technological reality of the 21st century. Through a literature review and descriptive analysis of the potentials of technological innovations, it was possible to establish the individual risks that the innovations brought to privacy. From this, it found that the risks to privacy, originally of an individualistic nature, changed to a concern of a social nature based on the expansion of the capacities of fiduciary communicators. The concern observed was essentially that related to the limitation of power, which is related to the concerns verified in the genesis of constitutionalism and which were and remain intrinsic to it. Then, this work extracted a constitutional foundation for data protection arising directly from the political aspect of the Constitution, which resulted in the need to use tools of a constitutional nature to protect privacy as a necessary expression of a constitutional order.

Keywords: Data protection, privacy, constitutionalism, fiduciary communication.

LISTA DE FIGURAS

LISTA DE SIGLAS

ADI	Ação Direta de Inconstitucionalidade
BVerfG	*Bundesverfassungsgericht*
CADE	Conselho Administrativo de Defesa Econômica
CF/88	Constituição Federal de 1988
CIA	*Central Intelligence Agency*
DF	Distrito Federal
EUA	Estados Unidos da América
GDPR	*General Data Protection Regulation*
LGDP	Lei Geral de Proteção de Dados
MC	Medida Cautelar
SBDE	Sistema Brasileiro de Defesa da Concorrência

SUMÁRIO

INTRODUÇÃO

Os avanços tecnológicos dos últimos anos alteraram por completo a forma de se comunicar do ser humano. A internet e, especialmente, a popularização dos *smartphones*, causou *(i)* um aumento substancial no volume de informações transmitidas entre interlocutores, e *(ii)* ocasionaram um incremento relevante na quantidade de informações comunicadas, objeto de alguma forma de registro e/ou armazenamento.

Ainda, a comunicação humana moderna, inerente à sociedade hiperconectada, passou a depender cada vez mais de terceiros: além do emissor e do receptor, a quantidade de *mensageiros* e, especialmente, *mensageiros com potencial acesso à mensagem* cresceu vertiginosamente.

A privacidade – e deveres e direitos dela decorrentes – defronta-se, hoje, com riscos outrora inexistentes, decorrentes da evolução da tecnologia. Portanto, compreensões do direito ao sigilo pensadas para uma realidade passada não necessariamente possuem aplicabilidade diante dos desafios impostos pela contemporaneidade.

Não se trata, por exemplo, de questão de mera obsolescência hermenêutica,[1] ou de mutação constitucional,[2] visto que a realidade passada *permanece* presente, mas de *complementação* de sentido da norma para abarcar realidades *novas*.

Com respeito a essa nova realidade, Jack Balkin[3] introduz o assunto a partir de seu modelo triangular, o qual parte justamente da premissa de que, hoje, a regulação da fala não consiste simplesmente num modelo dualista, envolvendo o indivíduo e o Estado, mas num modelo pluralista, contendo vários atores diferentes.

A esse respeito, Balkin[4] menciona uma quantidade bastante significativa de atores envolvidos na comunicação – o que é fácil de se observar ao se analisar a troca de mensagens por um aplicativo de celular: há, no mínimo, *(i)* a fabricante do celular; *(ii)* a desenvolvedora do aplicativo utilizado; e *(iii)* a provedora de internet ou a companhia telefônica envolvidas na viabilização da comunicação – tanto para o remetente, quanto para o destinatário. A depender

---

[1] Aqui, entende-se obsolescência hermenêutica como a inadequação da interpretação desenhada para uma realidade antiga face à realidade atual – o que não seria o caso. Na verdade, a interpretação antiga, com relação à realidade antiga, *permanece válida*. As pessoas continuam a enviar cartas e a falar por telefone e não há razão para promover revisão da forma com a qual o ordenamento jurídico lida com tais situações. Hoje, contudo, as pessoas também conversam por WhatsApp e utilizam o Instagram. E, para essas novas realidades, é que é preciso perquirir como a norma antiga deve incidir.

[2] Resumidamente, mutação constitucional é compreendida como a alteração no sentido do texto da própria Constituição ao longo do tempo (Pp. 133.). Com referência à nota de rodapé anterior, não houve *alteração* no sentido do texto, não houve *mudança* do panorama normativo – e sim sua incidência a uma nova realidade.

[3] BALKIN, Jack M. *Free Speech is a Triangle*. ***Columbia Law Review***, Nova York, vol. 118, 2018. P. 2014.

[4] *Ibidem*, p. 2014 – 2015.

do modo de utilização, esse número pode crescer ainda mais: pode-se utilizar uma ferramenta *web*, que envolve tanto o sistema operacional, quanto o navegador, além de uma nova provedora de internet, por exemplo.

Na realidade, o número (e a identidade) *real* de terceiros envolvidos na comunicação que perpassa a internet é absolutamente desconhecido para o usuário – assim como os potenciais riscos decorrentes desse sistema. Um exemplo interessante é a notícia de que o governo dos Estados Unidos espionou vários líderes europeus, inclusive a Chanceler Angela Merkel, por meio de grampos em cabos submarinos dinamarqueses.[5]

Balkin, então, utiliza-se desse paradigma (envolvimento de terceiros na comunicação) para, em seu trabalho, desenvolver diversas questões relacionadas à liberdade de expressão, abordando o que ele chama de *old-school* e *new-school speech regulation*.

O enfoque neste trabalho, todavia, é distinto daquele atribuído por Balkin, muito embora parta exatamente da mesma realidade verificada por ele[6]: enquanto o Balkin enfrenta a questão da *liberdade de expressão*, que diz respeito à intromissão de terceiros nas relações *públicas*, este trabalho tem por enfoque a intromissão de terceiros nas relações *privadas* – e suas repercussões.

O substrato fático, contudo, é rigorosamente o mesmo e decorre das situações estruturais da comunicação e, em geral, da vida humana, derivadas da massificação da utilização de meios eletrônicos conectados à rede mundial de computadores pela população mundial para a comunicação e guarda de arquivos.

Esse fenômeno, caracterizado pela excessiva participação de terceiros/intermediários na comunicação humana, será denominada, para os fins deste trabalho, de *comunicação fiduciária*. Este termo, criado pelo autor deste trabalho, é conceituado com maiores detalhes no início do capítulo 2, mas busca identificar o fenômeno dos meios de comunicação contemporâneos: a proliferação de intermediários nas comunicações humanas torna a segurança das informações trocadas por emissores e receptores dependente dos terceiros responsáveis por viabilizar a troca (os aqui denominados *comunicadores*), como constatado por Balkin e indicado acima.

---

[5] GRONHOLT-PEDERSEN, Jacob; BING, Christopher; JOHNSON, Simon. ***U.S. spied on Merkel and other Europeans through Danish cables - broadcaster DR***. Disponível em: <https://www.reuters.com/world/europe/us-security-agency-spied-merkel-other-top-european-officials-through-danish-2021-05-30/>. Acesso em: 21/06/2021.

[6] *Op. cit.*, p. 2015: "*This is the new structure of speech regulation in the early twenty-First century, and debates about the rights of online free expression must grapple with that structure. To understand how this new system works, we must understand the distinction between old- and new-school speech regulation, explained in Part I, and the emerging system of private governance, discussed in Part II. Parts III and IV offer proposals for protecting freedom of speech in the changed environment. A brief conclusion follows*".

Essa dependência se dá porque emissor e receptor não possuem os meios para averiguarem, por si mesmos, a segurança dos meios de comunicação que utilizam – de onde deriva a qualidade fiduciária dos comunicadores: o funcionamento do sistema de comunicação torna-se indissociável da confiança que os usuários neles depositam. Se o comunicador informa que coleta – ou não – determinado dado, ao usuário não há alternativa a não ser acreditar naquilo que o comunicador lhe diz.

A interação humana, portanto, passa a depender umbilicalmente da confiança no sigilo, na integridade e até mesmo na tecnologia dos diversos responsáveis pela intermediação – em uma palavra: torna-se depende da fidúcia.

Tal conceito, para os propósitos delineados neste trabalho, abrange não somente comunicação *stricto sensu*, como aquela que se dá por meio de aplicativos como *WhatsApp* ou *Telegram* – mas alberga, também, formas de trocas de informações indiretas, como as realizadas por meio de redes sociais como o *Instagram* ou *Facebook* ou mesmo pelo uso de sistemas como o buscador Google: trata-se, em essência, de todos os que coletam e processam dados relativos a humanos.

A amplitude do conceito se dá porque, como será explorado com mais detalhes nos capítulos a seguir, a comunicação moderna (envio e recebimento de informações) ocorre de diversas maneiras distintas – e, muitas vezes, não é nem sequer percebida pelas partes envolvidas na troca, que utilizam algum *software* sem saber que, por meio de seu uso, estão fornecendo determinados dados a alguém.

Nesse sentido, o capítulo 1 realizará, essencialmente, uma análise sobre a privacidade, sua gênese no pensamento jurídico contemporâneo, e estabelecerá conceitos que serão utilizados nas partes seguintes do trabalho.

O capitulo 2, por sua vez, objetivará enunciar os métodos e potencialidades que a realidade da comunicação fiduciária apresenta, analisando seus riscos a partir de uma perspectiva vinculada ao indivíduo.

No capítulo 3, pretende-se observar de que forma os riscos à privacidade transmudaram-se de uma preocupação fortemente atrelada às relações privadas para, com o tempo, e a partir de forte influência decorrente da evolução tecnológica, passar a se preocupar com questões de índole social: poder, democracia, liberdade.

Por fim, o capítulo 4, último deste trabalho, analisará a relação existente entre as preocupações identificadas no capítulo 3 e o constitucionalismo, apresentando ideia para o fundamento constitucional da proteção de dados atrelada não a elementos de direitos

fundamentais constantes em textos constitucionais, mas a uma natureza mais associada à finalidade de controle do exercício do poder que informa as constituições.

Existe, é claro, uma certa tradição brasileira associada às problemáticas que permeiam este trabalho: desde a Constituição de 1824,[7] o Brasil prevê que "O Segredo das Cartas é inviolável". Todavia, a privacidade é questão de preocupação mundial – sobretudo a partir das experiências totalitárias do século XX, as quais marcaram fortemente o modo de abordar diversas questões de cunho social. Em igual sentido, os riscos à privacidade, hoje em dia, extrapolam as fronteiras, uma vez que se originam, com frequência, em empresas multinacionais – a maioria com sede nos Estados Unidos da América.

Portanto, não obstante a existência de uma experiência brasileira de quase duzentos anos com tal direito, não é recomendável passar ao largo da experiência estrangeira. Fazê-lo resultaria em um trabalho míope e incompleto, que deixaria de considerar problemas ainda não ocorridos no Brasil – e, por conseguinte, antecipá-los – e que ignoraria a realidade da internacionalização dos riscos à privacidade, sobretudo originários dos EUA.

A partir de tal cotejo, pretende-se construir um panorama teórico, talvez até filosófico, que discrimine quais são os valores que a proteção ao sigilo/privacidade pretende resguardar, identificando, portanto, a finalidade da tutela de tais direitos no ordenamento jurídico.

A hipótese que se tem, a esse respeito, é que a garantia da privacidade e do sigilo tem duas finalidades: a primeira seria a *social*, que consistiria na proteção do indivíduo contra abusos – seja do Estado, seja de particulares, a partir de enfoque nos *meios* que viabilizam potenciais abusos, *e.g.* o Estado não tem como empreender perseguições contra uma minoria ética se ele não tem uma base de dados relacionando os indivíduos pertencentes a tal minoria (preocupação esta apontada por Danilo Doneda,[8] por exemplo).

Nesse sentido, haveria uma interconexão relevante entre a garantia do sigilo/privacidade e o resguardo de direitos fundamentais, em especial no que tange à liberdade de expressão, uma vez que qualquer pessoa interessada em os cercear ou violá-los disporia de meios para tanto. Passar-se-ia, então, a um enfoque no sentido de que, com respeito a direitos fundamentais, não

[7] Art. 179. A inviolabilidade dos Direitos Civis, e Políticos dos Cidadãos Brazileiros, que tem por base a liberdade, a segurança individual, e a propriedade, é garantida pela Constituição do Império, pela maneira seguinte. [...] XXVII. O Segredo das Cartas é inviolavel. A Administração do Correio fica rigorosamente responsável por qualquer infracção deste Artigo.

[8] DONEDA, Danilo Cesar Maganhoto. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. In: TEPEDINO, Gustavo (org.). **Problemas de direito civil-constitucional.** Rio de Janeiro: Renovar, 2000, pp. 111-136. Disponível em: <https://egov.ufsc.br/portal/sites/default/files/anexos/8196-8195-1-PB.htm>.

seria somente necessário protegê-los, mas voltar uma etapa e proibir até a posse de meios que permitam sua violação.

A esse respeito, os ensinamentos de Hannah Arendt[9] quanto ao totalitarismo e de sua característica essencial de destruição da individualidade iluminarão o debate, relacionando a possibilidade de vigilância completa com a eliminação da diversidade social.

A segunda finalidade que se supõe seria a individual, caracterizada pela proteção do indivíduo contra a exposição de sua vida particular por razões eminentemente morais[10] (como destacado no artigo *The Right to Privacy* de Warren e Brandeis,[11] de 1890). Tal finalidade consistiria em uma espécie de valoração, pelo Direito, de normas de natureza moral[12] voltada à proteção do indivíduo.

Em seguida, a análise passará à Constituição Federal de 1988, realizando-se estudo sobre a forma pela qual o direito ao sigilo foi e é tutelado e compreendido no Brasil sob a égide da Constituição atualmente vigente, comparando-o com a estrutura teórica delineada anteriormente.

Por fim, o trabalho encerrará com a apresentação de ideias acerca da interpretação da proteção constitucional ao sigilo/privacidade para que, à luz da realidade fática e do panorama teórico desenvolvido, seja implementada proteção eficaz aos direitos e deveres decorrentes das previsões constitucionais.

Não será feita uma escolha de casos específicos, nem mesmo de empresas, mas de problemáticas, visto que companhias bastante distintas possuem meios para intervir na privacidade de forma bastante similar – especialmente quando houver cruzamento de dados. Além disso, também não haverá grandes distinções entre setor público e setor privado – ao contrário do que fez Balkin[13] – uma vez que as previsões constitucionais aplicam-se também ao Estado. Essas problemáticas serão delineadas com maior profundidade no Capítulo 1.

---

[9] ARENDT, Hannah. **Origens do totalitarismo.** Trad. Roberto Raposo. 1ª ed. São Paulo: Companhia das Letras, 2012. P. 441.

[10] Escrevem os autores: "*For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of the invasion of privacy by the newspapers, long keenly felt, has been but recently discussed by an able writer* […] *Of the desirability – indeed of the necessity – of some such protection, there can, it is believed, be no doubt The press is overstepping in every direction the obvious bounds of propriety and decency*".

[11] WARREN, Samuel D.; BRANDEIS, Louis D. *The Right to Privacy*. ***Harvard Law Review*****,** Cambridge, vol. 4, n. 5, 1890.

[12] N'A Teoria Pura do Direito, Hans Kelsen trata com profundida sobre o tema, demonstrando a separação do Direito e da Moral. Todavia, o faz com respeito ao fundamento de validade do Direito, porque, se fosse a Moral, pressuporia a existência de uma Moral absoluta. Na verdade, ao reconhecer a pluralidade e relatividade da Moral, Kelsen abre espaço para que o Direito confira validade a uma delas, albergando juridicamente uma realidade social (Trad. João Baptista Machado. 8ª ed. São Paulo: Martins Fontes, 2009. Pp. 75-78). Não obstante, é fato que existe esse tipo de reconhecimento, e que danos morais merecem resguardo pelo ordenamento jurídico.

[13] *Op. cit*, p. 2014.

Este trabalho, então, pretende partir de uma análise das transformações pelas quais a comunicação humana passou em razão dos avanços tecnológicos do século XXI, com um recorte abarcando as infraestruturas de comunicação contemporâneas.

Em seguida, passar-se-á abordagem dogmática, realizando-se revisão bibliográfica e utilizando-se metodologia lógico-dedutiva, tendo como pressuposto a força normativa da constituição[14] para construir panorama hermenêutico que possibilite a adequada tutela das finalidades do direito à privacidade à luz da Constituição Federal de 1988.

[14] HESSE, Konrad. **A Força Normativa da Constituição.** Trad. Gilmar Ferreira Mendes. Porto Alegre: Sérgio Antônio Fabris Editor, 1991.

1. REALIDADE DA COMUNICAÇÃO CONTEMPORÂNEA

Neste capítulo, pretende-se realizar análise descritiva das atuais formas de comunicação e dos riscos à privacidade dos indivíduos decorrentes dos avanços tecnológicos popularizados no terceiro milênio.

O capítulo focará em uma análise fática da realidade contemporânea, com especial atenção aos meios disponíveis e às inseguranças e aos riscos a que ficam submetidos os indivíduos, evidenciando, sempre que possível, a concretude do risco e/ou do dano por meio de exemplos de casos reais.

Nesse sentido, demonstrar-se-á, sem pretensão de exaurir o tema, os riscos derivados de uma característica intrínseca aos modelos de comunicação e registro de dados contemporâneos: a necessidade intransponível da confiança em terceiros, o que, para os fins deste trabalho, será fenômeno denominado de comunicação fiduciária.

Fundamental ressaltar que, na categoria de comunicadores fiduciários, incluem-se não somente os intermediários responsáveis pela transmissão de informações, mas, também, todos aqueles envolvidos no registro e arquivamento de informações. Destaca-se, a esse respeito, que não haverá grandes distinções entre o transmissor e o registrador, visto que a característica essencial a ambos é a possibilidade de acesso aos dados em virtude do fornecimento da infraestrutura essencial à troca e registro de informações.

Nesse sentido, Seth Stephens-Davidowtiz[15] define o que ele chama de quatro grandes poderes do Big Data:

(i) A oferta de novos tipos de dados, tornando acessíveis informações que, outrora, não o eram;

(ii) A honestidade dos dados coletados, diante da dificuldade, inviabilidade e/ou pouca probabilidade de serem mentirosos e/ou falsos;

(iii) A possibilidade de se analisar pequenos subconjuntos de dados, separando as pessoas por categorias; e

(iv) A viabilidade da realização de experimentos causais (testagem da população).

[15] STEPHENS-DAVIDOWITZ, Seth. **Todo mundo mente: o que a internet e os dados dizem sobre quem realmente somos**. Trad. Wendy Campos. Rio de Janeiro: Alta Books, 2018. Pp. 53-54.

Como se pôde ver, a possibilidade de se reduzir a análise de dados a subconjuntos é um dos poderes do Big Data. Se levado ao extremo, o menor subconjunto é o indivíduo. Assim, neste trabalho, não haverá o estabelecimento de distinção quanto ao volume de dados, uma vez que os riscos coletivos são mera exasperação dos riscos individuais.

Assim, com respeito à natureza dos riscos, será possível identificar o principal risco decorrente da comunicação fiduciária: o aumento significativo na *eficiência* do acesso a informações relativas aos indivíduos.

Esse risco de eficiência, como se verá, é caracterizado pelos elementos apontados por Stephens-Davidowitz, indicados acima, e é agravado pela dificuldade (ou pouca praticidade) dos mecanismos de defesa/segurança do indivíduo.

No entanto, para que se identifiquem os riscos a algo, é necessário, anteriormente, identificar *o que é* esse "algo" que está sob risco. Portanto, será feita, inicialmente, a diferenciação entre os conceitos de *i*) privacidade; *ii*) sigilo; e *iii*) proteção de dados.

A partir da identificação do *objeto* do risco, passaremos a uma análise das formas pelas quais tais riscos se implementam, identificando os perigos decorrentes da atuação dos comunicadores fiduciários.

1.1. Privacidade, Sigilo e Proteção De Dados

Embora, à primeira vista, possam parecer conceitos similares, talvez até sinônimos, tais categorias, na dogmática jurídica contemporânea, referem-se a conceitos e situações distintas umas das outras. A gênese de todos, no entanto, reside na ideia de privacidade – da qual derivam o sigilo e a proteção de dados.

1.1.1. Privacidade

O conceito de privacidade é certamente de difícil definição. Daniel Solove[16] ressalta que, "por um bom tempo, acadêmicos sustentaram que privacidade é um conceito tão confuso que é de pouca utilidade". Pontua o autor que

> "Frequentemente, o discurso filosófico acerca da conceptualização da privacidade é ignorado em debates jurídicos e de políticas públicas. Muitos juristas, políticos e

[16] Tradução livre. SOLOVE, Daniel. "***I've Got Nothing To Hide***" and Other Misunderstandings of Privacy. San Diego Law Review**,** vol. 44, p. 745-772, 2007, p. 754: "*For quite some time, scholar have proclaimed that privacy is so muddled a concept that it is of litte use*".

> acadêmicos simplesmente analisam as questões sem articularem um conceito sobre o significado de privacidade".

Este trabalho, portanto, busca não incorrer na crítica acima. Para se tratar da privacidade, é preciso, antes, desenhar um panorama do que é, para que serve e qual o seu objetivo. Trata-se, evidentemente, de uma construção histórica e social, razão pela qual é necessário remontar às suas origens.

Assim, o presente capítulo visa construir um conceito de privacidade em cima do qual se possa trabalhar. Trata-se, sem dúvida, de uma pretensão ambiciosa, razão pela qual não se pretende dar uma resposta definitiva, um conceito final para a privacidade.

Pretende-se, na verdade, definir a privacidade não como um conceito abstrato, quiçá metafísico, mas, como um direito humano que serve a finalidades tidas como universais – como expressamente consignado na Declaração Universal dos Direitos Humanos, adotada pela Assembleia Geral das Nações Unidas em 1948.[17]

Conceituar o direito à privacidade, nesse cenário, é tarefa árdua que é objeto de controvérsia na academia e nos tribunais há mais de um século. Este trabalho, portanto, não possui a pretensão de defini-la como um conceito genérico e abstrato, mas tão somente defini-la, como dito, para os fins deste trabalho, diferenciando-a das demais categorias que serão utilizadas ao longo deste estudo.

Alan Westin,[18] em seus estudos, realiza um rastreamento da privacidade aos aspectos biológicos, partindo de estudos sobre o comportamento animal na natureza:

> "Uma descoberta básica dos estudos dos animais é que praticamente todos os animais procuram momentos de reclusão individual ou de intimidade em grupos pequenos.
> [...]
> Cientistas descobriram que esses padrões territoriais servem a uma quantidade de propósitos importantes. Eles garantem a propagação da espécie por meio da regulação da densidade populacional aos recursos disponível. Eles aprimoram a seleção de "machos aptos" e fornecem bases de reprodução para espécies que demandam assistência masculina na criação do s filhotes. Eles também fornecem um ponto físico de referência para atividades de grupo tais como o aprendizado, a diversão, e o esconderijo, e fornecem contato entre os membros do grupo contra a entrada de invasores. Os paralelos entre regras territoriais na vida animal e conceitos de intrusão

[17] Artigo 12: Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.

[18] WESTIN, Alan. ***Privacy and Freedom*.** New York: Ig Publishing, 1967. Tradução livre. Texto original: "*One basic finding of animal studies is that virtually all animals seek periods of individual seclusion or small group intimacy. […] These territorial patterns have been found by scientists to serve a cluster of important purposes. They ensure propagation of the species by regulating density to available resources. They enhance selection of "worthy males" and provide breeding stations for animals that require male assistance in raising the young. They also provide a physical frame of reference for group activity such as learning, playing, and hiding, and provide contact for group members against the entry of intruders. The parallels between territory rules in animal life and trespass concepts in human society are obvious: in each, the organism lays claim to private space to promote individual well-being and small-group intimacy*".

> na sociedade humana são óbvios: em ambos, um organismo reivindica um espaço privado para promover bem-estar individual e intimidade em grupos pequenos".

Hannah Arendt, em sua obra "A Condição Humana", dedica o Capítulo 2 para tratar das esferas pública e privada. A autora remontava à antiguidade clássica, identificando a origem da separação entre as ideias de vida pública e vida privada na separação entre família e política:[19]

> "A distinção entre uma esfera de vida privada e uma esfera de vida pública corresponde à existência das esferas da família e da política como entidades diferentes e separadas, pelo menos desde o surgimento da antiga cidade-estado; mas a ascendência da esfera social, que não era nem privada nem pública no sentido restrito do termo, é um fenômeno relativamente novo, cuja origem coincidiu com o surgimento da era moderna e que encontrou sua forma política no estado nacional".

Na exposição de Hannah Arendt, teríamos Platão[20] e Aristóteles[21] como principais filósofos gregos a enfrentarem o tema. O pensamento grego, contudo, possuía particularidades muito distintas daquela que se poderia esperar. Com respeito ao pensamento platônico, Peres-Neto[22] leciona o seguinte:

> "Em primeiro lugar há uma manifesta vontade de contrapor à noção de privacidade o conceito de vida pública, limitando a primeira ao âmbito da vida doméstica. Mais do que situar uma fronteira, a vida privada e a vida íntima não teriam nenhum interesse para a vida da (e na) polis, razão pela qual todo aquele que não fosse cidadão seria um "idiota", alguém que deveria ficar circunscrito à vida doméstica e, portanto, despido da capacidade política. A vida privada não representava uma esfera que requeresse qualquer tipo de atenção e, consequentemente, de reflexão. Indiretamente Platão constrói uma moralidade negativa à privacidade. Essa erige-se ao despir de interesse público e político tudo aquilo que for privado. O mundo da privacidade seria, portanto, uma dimensão menor da vida humana. Para Platão, apenas na "cidade justa", no espaço público, podem ser desenvolvidas as boas artes do governo e do conhecimento. Por seu turno, e a raiz do anteriormente exposto, as reflexões platônicas sobre a privacidade não buscam edificar uma separação dialética entre público e privado já que esta última esfera não é de interesse. A virtude - e, portanto, a vida justa, capaz de construir o bem comum – se dá unicamente na *polis*. De tal sorte, não há uma ética da/para a privacidade".

Platão, portanto, recusa a existência das esferas pública e privada – e, como diz Hannah Arendt, chega até mesmo a prever "a abolição da propriedade privada e a expansão da esfera pública ao ponto de aniquilar completamente a vida privada".[23]

Aristóteles, a seu turno, realiza divisão entre as esferas públicas e privada – o que se observa claramente em sua obra "A Política" quando afirma que "os Estados são formados de

---

[19] ARENDT, Hannah. **A Condição Humana.** Trad. Roberto Raposo. 10. ed. Rio de Janeiro: Forense Universitária, 2007. P. 37.
[20] PLATÃO. **A República.** Tradução: Ciro Mioranza. São Paulo: Lafonte, 2017.
[21] ARISTÓTELES. **A Política**. Trad. Roberto Leal Ferreira. 3ª ed. São Paulo: Martins Fontes, 2006.
[22] PERES-NETO, Luiz. Ética e privacidade: múltiplos olhares a partir do campo da comunicação. In: BRANCO, S. TEFFÉ, C. (Org.). **Privacidade em Perspectivas**. 1ª ed. Rio de Janeiro: Lumen Juris, 2018. Pp. 201-221. Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Luiz-Peres-Neto-V-revisado.pdf>. P. 7.
[23] PLATÃO. **A República.** P. 39.

famílias", passando, então, a discorrer sobre o governo doméstico.[24] Não obstante a diferenciação, o filósofo grego coloca a vida privada como de natureza inferior à vida pública.[25]

Todavia, a visão grega sobre as concepções de público e privado partia de formas de pensamento bastante distintas daquelas que hoje se apresentam. A esfera privada, familiar, era compreendida como "animal", essencial à sobrevivência e, assim, não consistiria em característica essencial ao conceito de ser humano, já que aplicável também aos animais.[26]

Contudo, isso não significava um desprezo à esfera privada: a concepção grega, sobretudo a aristotélica, via a *polis* – a vida pública – como sendo o ambiente no qual o particular era livre para tratar com iguais. Mas o pressuposto disso era vida privada, sem a qual o homem não poderia pertencer à *polis*[27].

E, aqui, apresenta-se uma questão interessantíssima, trazida por Peres-Neto[28] – afinal, o propósito do retorno ao pensamento da antiguidade clássica não é o de uma mera menção ao Código de Hamurábi:[29]

> "Como aponta McStay (2014),[30] nasce a partir das reflexões de Platão e Aristóteles a visão de que só se requer da privacidade quando há algo a ser escondido do público. Dito de outro modo, a privacidade apenas é necessária para quem tem algo a ser ocultado. Ambos ignoram a possibilidade de que parte da consciência moral se dá precisamente na microfísica da intimidade, na solidão privada do eu".

Observa-se, de modo geral, a existência de uma aparente contradição no pensamento grego, já indicada por Hannah Arendt:[31] diminuem a esfera privada mas, ao mesmo tempo, atribuíam-na certa sacralidade e deferência. E, como se viu no raciocínio de McStay *apud* Peres-Neto, citado acima, este é um raciocínio que, na essência, persiste até a contemporaneidade, em suas mais diversas formas, e que sofreu profundas alterações a partir das revoluções burguesas

---

[24] ARISTÓTELES. **A Política**. Trad. Roberto Leal Ferreira. 3ª ed. São Paulo: Martins Fontes, 2006.
[25] Peres-Neto, *op.cit.*, p. 8: "Neste sentido, a ação moral é a base para a ação política não havendo cabida para uma ética privada já que a mesma se dá na vida na polis. A vida boa não se encontra na vida privada e sim na vida pública"
[26] Hannah Arendt, *op. cit.*, pp. 33 e 39: "Não que Aristóteles ou Platão ignorasse ou não desse importância ao fato de que o homem não pode viver fora da companhia dos homens; simplesmente não incluíam tal condição entre as características especificamente humanas. Pelo contrário, ela era algo que a vida humana tinha em comum com a vida animal – razão suficiente para que não pudesse ser fundamentalmente humana. A companhia natural, meramente social, da espécie humana era vista como limitação imposta pelas necessidades da vida biológica, necessidades estas que são as mesmas para o animal humano e para outras formas de vida animal. [...] O que distinguia a esfera familiar era que nela os homens viviam juntos por serem a isso compelidos por suas necessidades e carências".
[27] Hannah Arendt, *op. cit.*, p. 39: "O que impediu que a *polis* violasse as vidas privadas dos seus cidadãos e a fez ver como sagrados os limites que cercavam cada propriedade não foi o respeito pela propriedade privada tal como concebemos, mas o fato de que, sem ser dono de sua casa, o homem não podia participar dos negócios do mundo porque não tinha nele lugar algum que lhe pertencesse".
[28] *Ibidem*,
[29] OLIVEIRA, Luciano. **Não fale do Código de Hamurábi!** Anuário dos Cursos de Pós-Graduação em Direito (UFPE), v. 13, 2003, p. 299-330.
[30] McSTAY, Andrew. ***Privacy and philosophy***. Nova Iorque: Peter Lang, 2014.
[31] Hannah Arendt, *op. cit.*, p. 39.

no século XVIII, com o advento do liberalismo e sua característica essencial de enfoque no indivíduo.

A esse respeito, e em atenção à continuidade histórica, cabe ressaltar que a Idade Média, como ensina Mikhail Cancelier,[32] começou-se a notar uma certa necessidade de isolamento, ainda que distante da concepção atual. Logo, foi período de pouco progresso nessa questão. Nesse sentido, anota Danilo Doneda:[33]

> "Durante a Idade Média, ainda não é possível reconhecer um anseio sistemático das pessoas pela privacidade ou isolamento; pode-se ao máximo constatar que alguns poucos podiam isolar-se dos demais, como os senhores feudais que o desejassem, ou então pessoas que optassem pela solidão em detrimento da vida pública, como alguns religiosos, místicos, bandidos ou banidos. Ao fim da Idade Média, entretanto, podemos identificar entre os senhores feudais mais bem colocados na sociedade manifestações que podem ser entendidas como indícios do surgimento de uma esfera privada em moldes vagamente similares aos atuais".

As teorias políticas que se seguiram à Idade Média, renascentistas, trouxeram o ser humano ao centro do debate filosófico e, posteriormente, em conjunto com o pensamento iluminista, conduziram a filosofia europeia para um enfoque no indivíduo.

Como igualmente ressaltado por Doneda,[34] a privacidade, por sua própria natureza, depende necessariamente de uma teorização acerca da relação entre o individual e o coletivo, assim como uma evidente valorização do individualismo, razão pela qual sofreu grande expansão com as teorias liberais do século XVIII, reações ao absolutismo e excesso estatal.

Surge, então, a necessidade de tutela de tal direito, inicialmente fortemente vinculada à noção de propriedade privada.[35]

Nesse sentido, a discussão sobre a privacidade é intrinsecamente ligada à filosofia política – porque não há como se falar em vida privada se não existir vida pública para a ela se contrapor. Este será o ponto de partida deste capítulo.

De qualquer maneira, na concepção contemporânea, as origens de tal direito são rastreáveis ao já mencionado artigo de Warren e Brandeis, de 1890, como ensina Danilo

---

[32] CANCELIER, Mikhail Vieira de Lorenzi. O Direito à Privacidade hoje: perspectiva histórica e cenário brasileiro. **Sequência,** Florianópolis, n. 76, p. 213-240, 2017.

[33] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados**. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019.

[34] Afirma Doneda: "A bem da verdade, qualquer noção de privacidade deve fundar-se em uma percepção da relação do indivíduo com a sociedade, e a gênse de sua atual concepção evoca duas causas principais: a emergência do estado-nação, da sociedade civil e das teorias de sua soberania nos séculos XVI e XVII, que formaram a noção moderna do ente público; e também o estabelecimento de uma esfera privada livre de ingerências desse ente público, como reação ao absolutismo, tendências aceleradas pelo fim da sociedade feudal e, posteriormente, pela revolução industrial".

[35] WARREN, Samuel D.; BRANDEIS, Louis D. *The Right to Privacy.* ***Harvard Law Review*****,** Cambridge, vol. 4, n. 5, 1890.

Doneda.[36] Em tal trabalho, os autores desenvolvem o direito à privacidade a partir da proteção da personalidade da seguinte maneira:[37]

> "Que o indivíduo deve ter proteção total de sua pessoa e de sua propriedade é um princípio tão antigo quanto a lei comum; mas, de tempos em tempos, se fez necessário redefinir a exata natureza e extensão de tal proteção. Mudanças políticas, sociais e econômicas ensejam o reconhecimento de novos direitos, e a lei comum, em sua eterna juventude, cresce para atender às demandas da sociedade.
> [...]
> O escopo desses direitos se expandiu gradualmente; e, agora, o direito à vida passou a significar o direito de aproveitar a vida, - o direito de ser deixado em paz, o direito à liberdade assegura o exercício de diversos privilégios civis; e o termo "propriedade" evoluiu para abarcar toda forma de possessão – intangível, assim como tangível.
> [...]
> É nosso propósito considerar se a lei existente fornece um princípio que possa ser adequadamente invocado para proteger a privacidade do indivíduo; e, caso forneça, qual é a natureza e a extensão de tal proteção.
> [...]
> O princípio que protege escritos privados e todas as outras formas de produções pessoais, não contra furto ou apropriação física, mas contra publicação de qualquer forma, é, na realidade, não o princípio da propriedade privada, mas o da inviolabilidade da personalidade.
> [...]
> Nós devemos, portanto, concluir que os direitos, assim protegidos, qualquer que seja sua natureza exata, não são direitos oriundos de contrato ou de confiança especial, mas são direitos contra o mundo".

Como reconhecem os próprios autores, o artigo objetivava analisar se, a partir do ordenamento jurídico existente à época nos Estados Unidos, seria possível extrair-se um direito à privacidade. Os autores preocupam-se, então, em procurar a sua fonte, e, ao final, estabelecerem as exceções a tal direito. Entretanto, Warren e Brandeis não chegam, propriamente, a conceituar o direito à privacidade.

Depositam, no conceito, uma nítida e elevada carga *moral*, iniciando o trabalho com críticas aos tabloides de então. E isso finda em um trabalho no qual os autores *partem* do raciocínio de que as novas tecnologias (do final do século XIX) violam direitos – ou, no

---

[36] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados**. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019. P. 30.

[37] Tradução livre. WARREN, Samuel D.; BRANDEIS, Louis D. *The Right to Privacy.* ***Harvard Law Review*****,** Cambridge, vol. 4, n. 5, 1890. Texto original: "*That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social and economic changes entail the recognition of new right, and the common law, in its eternal youth, grows to meet the demands of society. […] Gradually, the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life, - the right to be left alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession – intangible, as well as tangible. […] It is our purpose to consider whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual; and, if it does, what the nature and extent of such protection is; […] The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality. […] We must therefore conclude that the rights, so protected, whatever their exact nature, are not rights arising from contract or from special trust, but are rights as against the world;*".

mínimo, têm o potencial de violarem direitos – para, então, procurarem em qual direito essa violação pré-definida se encaixa. Ou para construí-lo.

Essa análise, que se distancia de um raciocínio jurídico lógico-dedutivo e se aproxima de uma juridificação da moralidade, decorre, em grande medida, do contexto em que tal artigo se insere: tanto o contexto específico, quanto o contexto histórico-social, no qual tal obra está inserida. Não é, de forma alguma incompreensível.

Em termos específicos, a causa direta e imediata do trabalho de ambos foi a exploração, pelos jornais da época, da vida[38] de Samuel Warren e sua família, o que lhe causou muito incômodo. Por ter se casado com uma mulher da alta sociedade estadunidense, eventos de família de Samuel Warren eram, frequentemente, objeto de fofocas em jornais de relevante circulação na Nova Inglaterra no final do século XIX.

No aspecto histórico-social, por outro lado, tal trabalho se insere em um período de auge da democracia liberal e de ascensão da burguesia, no qual a diferenciação entre as esferas pública e privada se desenvolve e se acentua:[39]

> "De toda forma, a partir do século XVI, observa-se o início de uma mudança nos costumes no que concerne à vida cotidiana. A nova disposição arquitetônica das casas e das cidades, que se tornam mais propícias à separação por classes e categorias e mesmo ao isolamento tornaram-se regra. Começa a se delinear então a atual noção de privacidade, que só poderia se desenvolver com essa nova situação do homem diante da sociedade. Esse enriquecimento da esfera privada ocorre como consequência do individualismo, de acordo com Hannah Arendt – mais propriamente, em razão da moderna privacidade estruturar-se em oposição à esfera social, e não à esfera política, como o foi para o homem antigo. A bem da verdade, qualquer noção de privacidade deve fundar-se em uma percepção da relação do indivíduo com a sociedade, e a gênese de sua atual concepção evoca duas causas principais: a emergência do estado-nação, da sociedade civil e das teorias de sua soberania nos séculos XVI e XVII, que formaram a noção moderna do ente público; e também o estabelecimento de uma esfera privada livre das ingerências desse ente público, como reação ao absolutismo, tendências aceleradas pelo fim da sociedade feudal e, posteriormente, pela Revolução Industrial.

---

[38] Alpheus Thomas Mason, professor de política da Universidade de Princeton, publicou, em 1946, a biografia "*Brandeis. A Free Man's Life*" sobre a vida de Louis Brandeis, o qual se tornara Ministro associado da Suprema Corte dos Estados Unidos da América em 1916, por indicação do então Presidente Woodrow Wilson, e falecera em 1941. No trabalho, o biógrafo relata a conhecida história do casamento de Warren como motivação para o trabalho dele e de Brandeis, conforme indicado por Edward Bloustein em artigo publicado em 1960 na *New York University Law Review*, no qual relata, citando Mason, que o fator motivacional do artigo foi a cobertura invasiva, pela mídia, do casamento entre Samuel Warren e a Srta. Mabel Bayard, em 1883. William Prossner, em artigo de 1960 publicado na *California Law Review*, referenda a história, afirmando que a motivação para o artigo foi o casamento da filha de Warren. Essa história é refutada por Amy Gajda, em artigo de 2008 publicado na *Michigan State Law Review*, após extensa pesquisa em jornais da época: a autora assevera que a causa do artigo, idealizado por Warren, não foi uma reportagem específica, mas uma coletânea de atividades dos jornais da época, entre 1883 e 1890, sobre casamentos, funerais, encontros sociais, históricos médicos e momentos íntimos de sua família em razão da "fama" de sua esposa, filha de um poderoso Senador dos Estados Unidos e futuro Secretário de Estado, Thomas F. Bayard.

[39] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados**. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019. P. 117-118.

> A privacidade passa a ser prerrogativa de uma emergente classe burguesa que, com seu forte componente individualista, dela se utiliza para marcar sua identidade na sociedade e também para que o solitário burguês se isole dentro de sua própria classe".

De certo modo, portanto, o trabalho de Warren e Brandeis pode ser compreendido como um produto das evoluções tecnológicas – e sociais – de seu tempo,[40] decorrente, em grande medida, da inovação nos meios de obtenção, registro e circulação de informações: principalmente as fotografias instantâneas e a ampla circulação de jornais.

Assim, é possível compreender a falta de conceituação do direito à privacidade por seus "criadores", uma vez que não era seu objetivo conceituá-lo – mas lidar com uma nova realidade que a eles se apresentava.

Richard Posner, quase um século depois,[41] ao tratar do direito à privacidade, qualifica-o como vago e mal definido. Por isso, o autor afirma que não pretenderá definir a privacidade, mas trabalhá-la a partir de um de seus aspectos: a retenção/ocultação de informações.

Outro autor estadunidense, William Prosser,[42] que antecedeu Posner nessa discussão, publicou artigo em agosto de 1960 afirmando que o direito à privacidade possui quatro aspectos distintos:

> "O que surgiu a partir das decisões não é algo simples. Não é um dano, mas um complexo de quatro. O direito da privacidade compreende quatro espécies distintas de invasão a quatro interesses diferentes do querelante, os quais estão ligados pelo nome comum, mas, fora isso, não têm praticamente nada em comum a não ser o fato de que cada um deles representa uma interferência no direito do querelante, na frase cunhada pelo Juiz Cooley, "*de ser deixado em paz*". Sem qualquer pretensão de uma definição exata, esses quatro danos podem ser descritos da seguinte maneira:
> 1. Intrusão na solidão e no isolamento do querelante, ou em seus assuntos particulares.
> 2. Divulgação pública de fatos pessoais embaraçosos para o querelante.
> 3. Publicidade que coloca o querelante sob uma falsa imagem para o público.
> 4. Apropriação, para a vantagem do réu, do nome ou da aparência do querelante.

---

[40] Evidentemente, o pensamento humano no geral é um produto de seu tempo. Mas, existem questões, principalmente de natureza política, filosófica, jurídica, sociológica e antropológica que perseguem a humanidade desde a antiguidade clássica e que, mesmo no século XXI, permanecem atuais. A observação feita em relação ao artigo de Warren e Brandeis, entretanto, tem o condão de ressaltar que ela é caracterizada pelo seu tempo – uma vez que, por óbvio, não haveria tanta relevância em se discutir a privacidade em uma sociedade na qual existem poucos meios de registro, como jornais, fotografias, filmes e vídeos.

[41] POSNER, Richard A. *The Right of Privacy.* ***Georgia Law Review*****,** Athens, vol. 12, n. 3, 1978, p. 393: "*The concept of 'privacy' is elusive and ill defined. Much ink has been spilled in trying to clarify its meaning. I will avoid the definitional problem by simply noting that one aspect of privacy is the withholding or concealment of information. This aspect is of particular interest to the economist now that the study of information has become an important field of economics*".

[42] PROSSER, William L. *Privacy.* ***California Law Review*****,** Berkeley, vol. 38, n. 3, 1960. Tradução livre, com o seguinte original: "*What has emerged from the decisions is no simple matter. It is note one tort, but a complex of four. The law of privacy comprises four distinct kinds of invasion of four different interests of the plaintiff, which are tied together by the common name, but otherwise have almost nothing in common except that each represents an interference with the right of the plaintiff, in the phrase coined by Judge Cooley, 'to be let alone'. Without any attempt to exact definition, these four torts may be described as follows: 1. Instrusion upon the plaintiff's seclusion or solitude, or into his private affairs. 2. Public disclosure of embarrassing private facts about the plaintiff. 3. Publicity which places the plaintiff in a false light in the public eye. 4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.*

Dentre as quatro categorias de Prosser, principalmente a primeira, mas, também a segunda, são as que mais se aproximam da questão em discussão neste trabalho. A quarta característica assemelha-se mais com a ideia de propriedade intelectual, e a terceira, com a questão das *fake news*.

A segunda, todavia, é uma espécie de particularidade, ou uma consequência, um agravamento da primeira: afinal, não há como publicar fatos particulares sem antes ter acesso a eles, por qualquer meio que seja.

Nesse contexto, as duas primeiras espécies categorizadas por Prosser assemelham-se bastante à ideia de Posner: trabalhar a privacidade como um direito individual de reter e ocultar informações.

Por outro lado, Jack Hirshleifer,[43] em resposta ao artigo de Posner, busca definir a privacidade como uma ideia de *autonomia dentro da sociedade*:

> "(...) eu estarei sustentando que a terra firme de "privacidade" não é a ideia de *sigilo* em que nossos pioneiros aparentemente acreditavam – sigilo é apenas uma península periférica. A ideia central do que nós queremos dizer por "privacidade" é, na verdade, um conceito que pode ser descrito como *autonomia dentro da sociedade*. Privacidade, então, significa algo muito maior do que sigilo; ela sugere, como eu irei sustentar em maiores detalhes abaixo, um tipo específico de estrutura social, conectada com a ética social que a suporta".

O autor, de modo bastante interessante, traz a privacidade como *um meio de organizar a sociedade*, destacando o aspecto de autonomia pessoal do indivíduo: a sua independência ao controle exercido por terceiros.[44] A privacidade, afirma Hirschleifer, estaria ligada à ética social associada ao liberalismo. A maior problemática associada à questão, dessa forma, estaria na autonomia contra o *estado*, e a dependência dele para a defesa de tal autonomia.

---

[43] HIRSHLEIFER, Jack. *Privacy: its origin, function, and future.* ***Journal of Legal Studies*****,** vol. 9, n. 4, 1980, p. 649-664. Tradução livre. Texto original: "*I will be contending that the mainland of 'privacy' is not the idea of* secrecy *as our pioneers appear to believe – secrecy is only an outlying peninsula. The central domain of what we mean by 'privacy' is, rather, a concept that might be described as* autonomy within society. *Privacy thus signifies something much broader than secrecy, it suggests, as I shall be maintaining in detail below, a particular kind of social structure together with its supporting social ethic*".

[44] HIRSHLEIFER, Jack. *Privacy: its origin, function, and future.* ***Journal of Legal Studies*****,** vol. 9, n. 4, 1980, p. 649-664. Texto original: "*The desire for seclusion is regarded by Posner as a more or less inexplicable 'taste' – and one that is not, probably, very widely shared. 'Seclusion' approaches but does not yet arrive at what I take to be the heart meaning of privacy; seclusion denotes* withdrawal from *society, whereas I am speaking of privacy as a* way of organizing society. *Still, seclusion does suggest one of the major aspects of the situation, the human desire for autonomy – for independence from control by others. Among the group of us assembled here today, due respect for this desire should not be difficult to find. Autonomy of the individual is the bedrock value of that classical liberalism still popular hereabouts. […] Autonomy as against the* state *is more than the leading special case of the general problem of privacy. (...) But for defending privacy we rely, for the most part, upon the support of* law".

Julie Cohen[45] cuida da temática de modo similar, situando a privacidade no âmbito da teoria política liberal como instrumento de proteção da subjetividade, da autodeterminação e da evolução da sociedade:

> "No entanto, a percepção da privacidade como antiquada e socialmente retrógrada está errada. É o resultado de uma inversão conceitual que se relaciona ao modo no qual o propósito da privacidade foi concebido. Assim como a teoria política liberal mais ampla na qual a privacidade está situada, a academia jurídica concebeu a privacidade como uma forma de proteção do "eu" liberal. Assim caracterizada, a privacidade é reativa e, em uma análise, não essencial. Sua ausência pode, em alguns momentos, esfriar o exercício de liberdades constitucionalmente protegidas, mas, uma vez que o "eu" liberal possui de modo inerente a capacidade de escolha autônoma e autodeterminação, a perda da privacidade não vulnera tal capacidade. Como esse artigo explica, no entanto, tal raciocínio está equivocado.
> Na realidade, o "eu" liberal que é o sujeito da teoria da privacidade e da formulação de políticas públicas sobre privacidade não existe. Como discutido na Parte II, o "eu" que é o real sujeito das leis e políticas de privacidade é socialmente construído, surgindo gradualmente de um substrato cultural e relacional preexistente. Para esse "eu", a privacidade exerce uma função que não tem nada a ver com a estase. A privacidade protege uma subjetividade dinâmica e emergente dos esforços de agentes comerciais e governamentais que visam manter indivíduos e comunidades fixos, transparentes e previsíveis. Ela protege as práticas situadas de gerenciamento de limites por meio das quais a capacidade para autodeterminação se desenvolve".

A privacidade, portanto, só pode ser compreendida se analisada dentro de seu contexto social e histórico, intimamente ligada às democracias liberais ocidentais. Com o tempo e com a experiência histórica, a privacidade, vista por Warren e Brandeis como uma proteção contra jornais de fofoca, passa a assumir contornos muito mais significativos.

As experiências totalitárias e autocráticas do século XX passaram a transformar a preocupação com a privacidade não tanto mais como uma garantia da intimidade pura e simples, mas como um instrumento de proteção do indivíduo contra os excessos do Estado, e, mais recentemente, com os Big Data e as *big techs*, uma proteção necessária contra o aparente poder excessivo que passou a ser detido por um rol pequeno de indivíduos.

Esse ponto será aprofundado no capítulo 2. Não obstante, verifica-se, na temática da privacidade, uma pluralidade de sentidos que sofreu enfoques distintos com o passar do tempo.

---

[45] COHEN, Julie. *What Privacy is For.* ***Harvard Law Review*****,** v. 126, n.7, 2014, p. 1904-1933. Tradução livre. Texto original: "*Yet the perception of privacy as antiquated and socially retrograde is wrong. It is the result of a conceptual inversion that relates to the way in which the purpose of privacy has been conceived. Like the broader tradition of liberal political theory within which it is situated, legal scholarship has conceptualized privacy as a form of protection for the liberal self. So characterized, privacy is reactive and ultimately inessential. Its absence may at times chill the exercise of constitutionally protected liberties, but because the liberal self inherently possesses the capacity for autonomous choice and self-determination, loss of privacy does not vitiate that capacity. As this Article explains, however, such thinking is mistaken. In fact, the liberal self who is the subject of privacy theory and privacy policymaking does not exist. As Part II discusses, the self who is the real subject of privacy law and policy is socially constructed, emerging gradually from a preexisting cultural and relational substrate. For this self, privacy performs a function that has nothing to do with stasis. Privacy shelters dynamic, emergent subjectivity from the efforts of commercial and government actors to render individuals and communities fixed, transparent, and predictable. It protects the situated practices of boundary management through which the capacity for self-determination develops*".

Um direito que, em sua gênese, servia, grosso modo, a uma finalidade específica (proteção do modo de vida liberal-burguês), passou a ter novas utilidades "descobertas" ao longo da história.

Aqueles que sobreviveram ao Nacional-Socialismo alemão, por exemplo, passaram a observar que a privacidade também tinha o potencial de lhes salvaguardar contra a repetição da história, como se verá adiante ao se analisar o caso do censo alemão da década de 1980.

Essa "descoberta" de novas utilidades da privacidade ao longo dos séculos ajuda a explicar a observação feita por Danilo Doneda[46] quando ressalta a indefinição que acompanhou e ainda acompanha o conceito ao longo da história:

> "Preferimos afirmar, portanto, que a indefinição quanto ao conteúdo do direito à privacidade deve ser tomada mais como uma característica intrínseca da matéria do que como um defeito ou obstáculo. Talvez uma "definição" do que seja a privacidade não seja propriamente a principal questão a ser enfrentada".

Outro autor que se dedicou a tal tarefa foi Daniel Solove,[47] em extenso artigo acadêmico no âmbito do qual analisa o assunto a partir de uma pluralidade de perspectivas distintas, conclui que todas pecam ou pela excessiva abrangência, ou pela exagerada restritividade. Por isso, ele advoga por um conceito pluralístico de privacidade, sustentando que as diversas acepções de privacidade se interseccionam umas com as outras, mas carecem de um núcleo duro, ou de uma ideia guarda-chuva, que não seja bastante ampla:

> "Até o momento, as tentativas de localizar um denominador comum para conceituar privacidade foram insatisfatórias. Conceitos que tentam localizar o núcleo ou a essência da privacidade acabam sendo muito amplos ou muito estreitos. (...)
> Uma abordagem contextualizada de baixo para cima voltada à conceituação de privacidade se provará bastante proveitosa no mundo moderno caracterizado pelas mudanças velozes da tecnologia".

De fato, como se viu, conceituar a privacidade é tarefa, não inviável, mas, potencialmente ineficaz. Dada a pluralidade de significados atribuídos historicamente ao conceito, defini-lo seria limitá-lo, abrindo as discussões tecidas neste trabalho às críticas eminentemente terminológicas.[48] Diante disso, adotar-se-á, para seu tratamento, a conceituação de Posner, considerando-a como o direito individual de reter e ocultar informações.

---

[46] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados**. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019. P. 101-102.

[47] SOLOVE, Daniel. *Conceptualizing Privacy.* ***California Law Review*****,** v. 90, n. 4, 2002, 1087-1156. Tradução livre. Texto original: "*Thus far, attempts to locate a common denominator for conceptualizing privacy have been unsatisfying. Conceptions that attempt to locate the core or essence of privacy wind up being too broad or too narrow. (...) A bottom-up contextualized approach toward conceptualizing privacy will prove quite fruitful in today's world of rapidly changing technology*".

[48] É comum, na academia, que um autor seja criticado por outro que afirma que o conceito utilizado está equivocado e/ou impreciso quando, na realidade, trata-se de confusão meramente terminológica. Enquanto um autor dá um nome a algo, outro dá o mesmo nome a outra coisa, surgindo o debate. Ou, como no caso da privacidade, quando um conceito é demasiado amplo, tentam falsear-lhe por meio da indicação de características e consequências condizentes com um de seus aspectos, mas incompatíveis com outros. Nesses casos, a melhor saída, e que privilegia o conteúdo do debate, ao invés de perder-se em filigranas gramaticais, é tratar o tema a

É a partir dessa acepção, então, que se torna possível a contraposição entre os conceitos de privacidade, sigilo e proteção de dados.

1.1.2. Sigilo

Tércio Sampaio Ferraz Júnior, ao tratar do tema,[49] afirma que o direito à privacidade possui por objeto "*a liberdade de 'negação' de comunicação do pensamento*", ao passo que seu conteúdo seria a faculdade de manter o sigilo:

> "Como direito subjetivo fundamental aqui também há de se distinguir entre o objeto e o conteúdo. O objeto, o bem protegido, é, no dizer de Pontes, a liberdade de "negação" de comunicação do pensamento. O conteúdo, a faculdade específica atribuída ao sujeito, é a faculdade de resistir ao devassamento, isto é, de manter o sigilo (da informação materializada na correspondência, na telegrafia, na comunicação de dados, na telefonia). A distinção é importante. Sigilo não é o bem protegido, não é o objeto do direito fundamental. Diz respeito à faculdade de agir (manter sigilo, resistir ao devassamento), conteúdo estrutural do direito.
> [...]
> Seria, portanto, um equívoco falar em *direito ao sigilo*, tomando a faculdade (conteúdo) pelo bem protegido (objeto), como se se tratasse em si de um único direito fundamental. Ao contrário, é preciso ver e reconhecer que o sigilo, a faculdade de manter sigilo, diz respeito a informações privadas (inciso XII do art. 5º) ou de interesse da sociedade ou do Estado (inciso XXXIII do mesmo artigo). No primeiro caso, o bem protegido é uma liberdade de "negação". No segundo, a segurança coletiva.
> [...]
> Ou seja, se não houver inviolabilidade do sigilo não há privacidade, mas se houver inviolabilidade do sigilo isto não significa que haja privacidade (pode haver outra coisa, como a segurança do Estado ou da sociedade). O direito à privacidade, em consequência, sendo um fundamento em si mesmo, permite dizer que a privacidade de um indivíduo só se limita pela privacidade de outro indivíduo (como a liberdade de um só encontra limite na liberdade do outro). O mesmo, porém, não vale para a inviolabilidade do sigilo, cuja instrumentalidade remete à avaliação ponderada dos fins, à chamada "*Abwägung*" (sopesamento) da dogmática constitucional alemã" (Grabitz, p.5).

O raciocínio do autor, nessa toada, coloca o sigilo como uma faculdade da privacidade, mas não como um direito em si mesmo. Isso significa dizer que, para Tércio Sampaio, o sigilo será um *atributo* da privacidade, a qual o titular do direito pode – ou não – decidir por abrir mão no momento em que informa a terceiros algo protegido pelo direito à privacidade. Menciona, a esse respeito, a ligação da faculdade do sigilo à defesa da segurança da sociedade

---

partir de seu conteúdo, localizando-o o no debate, mas sem dispender esforço excessivo na tentativa de estabelecer uma definição geral a algo que pode significar várias coisas. No caso da privacidade, em específico, sua polissemia é evidente e já foi objeto de estudo por diversos outros autores – mas ainda não se chegou a um consenso, e não é esse o objetivo deste trabalho.

[49] FERRAZ JR., Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito,** Universidade de São Paulo**,** n. 88, p. 439-459, 1993.

e do Estado, afirmando tratar-se de cenário no qual o sigilo liga-se a um direito outro que não a privacidade em si.

A categorização do autor, no entanto, é de pouca utilidade prática para este trabalho, eis que redunda em discussão meramente terminológica. Afinal, toda faculdade é, necessariamente, um direito: afirmar que a alguém é facultado fazer algo (manter sigilo) significa dizer, rigorosamente, que aquela pessoa tem o direito de fazê-lo – ou não.

Na realidade, o que Tércio parece querer dizer é que o sigilo não é um direito de existência autônoma, mas dependente: não existiria, para ele, um direito atribuível a determinado sujeito que o permitisse omitir/reter informações de modo puro e simples, sem condicionantes. Para Tércio, esse direito se vincularia, sempre, a algum outro, juridicamente protegido.

Isso, entretanto, não passa de um jogo de palavras. Em primeiro lugar, porque o fato de determinado direito possuir um âmbito de incidência[50] específico não retira a sua qualidade de direito subjetivo – do contrário, só seriam direitos aqueles entendidos como absolutos: todo o restante seria mera "faculdade".

Em segundo lugar, porque a existência de direitos de conteúdo análogo em contextos distintos do ordenamento jurídico não lhes retira sua qualidade de direitos. A autotutela, por exemplo, existe tanto na seara cível,[51] quanto na criminal[52] – e isso não a transforma em faculdade de outros direitos: é, simplesmente, um direito subjetivo cuja hipótese de incidência ocorre em mais de uma situação.

E, em terceiro lugar, porque todo direito necessariamente se vincula ao seu objeto. O desforço necessário na defesa da posse se vincula ao objeto posse (não se aplica à mera detenção). A legítima defesa no âmbito criminal pressupõe direito subjetivo violado. Ambas são modalidades de autotutela – que é um direito que o sujeito tem quando verificadas as situações específicas previstas na norma de regência da matéria.

---

[50] FERRAZ JR., Tércio Sampaio. **Introdução ao estudo do direito: técnica, decisão, dominação**. 7ª ed. São Paulo: Atlas, 2013. P. 293.

[51] Um bom exemplo é a autorização para o desforço imediato, por parte do possuidor, na hipótese de esbulho, como previsto pelo Código Civil de 2002 no§ 1º do art. 1.210: "*§ 1º O possuidor turbado, ou esbulhado, poderá manter-se ou restituir-se por sua própria força, contanto que o faça logo; os atos de defesa, ou de desforço, não podem ir além do indispensável à manutenção, ou restituição da posse*".

[52] O Código Penal Brasileiro prevê a legítima defesa como excludente de ilicitude, nos termos do artigo 23, inciso II, e do artigo 25 do Código: "*Art. 23 – Não há crime quando o agente pratica o fato: [...] II – em legítima defesa; [...] Art. 25 – Entende-se em legítima defesa quem, usando moderadamente dos meios necessários, repele injusta agressão, atual ou iminente, a direito ou de outrem. Parágrafo único. Observados os requisitos previstos no* ***caput*** *deste artigo, considera-se também em legítima defesa o agente de segurança pública que repele agressão ou risco de agressão a vítima mantida refém durante a prática de crimes*".

Portanto, a distinção realizada entre "faculdade" e "objeto" é inócua. Ter a faculdade de manter o sigilo, sob determinada circunstância, é situação de conteúdo idêntico ao direito de manter o sigilo. Tércio buscou realizar uma distinção terminológica que, na realidade, não passa de mero juízo de subsunção/incidência do direito às hipóteses verificadas na prática forense.

Por isso, sua categorização não será adotada neste trabalho, eis que não se refuta a nomenclatura "direito ao sigilo": a "definição" de privacidade que se optou por adotar neste trabalho, extraída dos estudos de Posner, necessariamente o engloba. Afinal, possuir o direito de reter/ocultar informações, atributo caracterizador da privacidade, significa, necessariamente, poder guardar sigilo quanto a tais assuntos.

Não obstante, a terminologia do sigilo se mostra mais adequada para tratar não o *direito*, mas o dever: o titular da privacidade pode, se assim desejar, divulgar e/ou abrir informações protegidas pela privacidade para terceiros. Todavia, isso não significa que esses terceiros passem a ser os titulares dessa privacidade. Pelo contrário: possuem o dever de manter sigilo quanto às informações protegidas pelo direito à privacidade que recebem em razão de algum dever legal e/ou contratual.

Essa compreensão se coaduna com o tratamento da matéria no ordenamento jurídico brasileiro, de onde podemos extrair, como exemplos, o sigilo bancário,[53] o sigilo fiscal[54] e o sigilo telefônico.[55]

Em todos esses casos, terceiros – no caso, empresas ou o Fisco – possuem acesso a informações ou a meios de se obter informações cobertas pelo direito à privacidade por força de contrato e/ou lei. Diante disso, sobre elas recai o dever de guardar sigilo quanto às informações a que tiverem acesso em virtude de suas atividades.

Essa, então, será a perspectiva relativa ao sigilo adotada neste trabalho: a de um *dever*, ao que se sujeitam terceiros, que, por alguma razão, obtém acesso legítimo a informações protegidas pela privacidade, mas sob o dever de a respeitarem.

1.1.3. Proteção de Dados

Isso leva à terceira e última definição que se busca fazer neste capítulo: a de proteção de dados. Entretanto, para enfrentar tal tema, é necessário, primeiramente, destrinchar os

[53] Vide Lei Complementar nº 105/2001.
[54] Conforme previsão Código Tributário Nacional, art. 198.
[55] Regulamentado pela lei nº 9.296/1996.

conceitos de "dados" e "informações". Para tanto, socorremo-nos, mais uma vez, ao ensinamento de Danilo Doneda:[56]

> "Em relação à utilização dos termos "dado" e "informação", é necessário notar preliminarmente que o conteúdo de ambos se sobrepõe em várias circunstâncias, o que justifica uma certa promiscuidade na sua utilização. Ambos os termos servem a representar um fato, um determinado aspecto de uma realidade. Não obstante, cada um deles possui suas peculiaridades a serem levadas em conta.
> Assim, o "dado" apresenta conotação um pouco mais primitiva e fragmentada, como se observa em um autor que o entende como uma informação em estado potencial, antes de ser transmitida. O dado, assim, estaria associado a uma espécie de "pré-informação", anterior à interpretação e a um processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição. Mesmo sem aludir ao seu significado, na informação, já se pressupõe a depuração de seu conteúdo – daí que a informação carrega em si também um sentido instrumental, no sentido de redução de um estado de incerteza.
> A doutrina e mesmo a lei, não raro, tratam estes dois termos indistintamente.
> Deve-se lembrar, ainda, que o termo "informação", em certos contextos, está muito fortemente associado a determinadas ordens de valor. Nesse sentido, mencione-se a "liberdade de informação" como fundamento de uma imprensa livre, bem como seu correspectivo "direito à informação", que possuem conteúdo bastante específico, assim como ocorre no caso do dever de informação pré-contratual do Código de Defesa do Consumidor, entre outras menções ao conceito.
> De fato, o que hoje destaca a informação de seu significado histórico é a maior desenvoltura na sua manipulação, desde a sua coleta e tratamento até a sua comunicação. E o vetor que faz esta diferença é justamente o tecnológico: ao incrementar a capacidade de armazenamento e comunicação, cresce também a variedade de formas pelas quais a informação pode ser apropriada ou utilizada. E, à medida que expande a sua utilidade, mais ela se torna elemento fundamental para um crescente número de relações, como também aumentam as suas possibilidades de influir em nosso cotidiano. Conforme notou Stefano Rodotà, ainda em 1973, "(...) a novidade fundamental introduzida pelos computadores é a transformação de informação dispersa em informação organizada".

A definição trazida pelo autor, portanto, coloca os "dados" como uma etapa *anterior* à obtenção da informação. É um conteúdo "cru", "bruto", sem passar por um processo de "refinamento" que o permita ser utilizado. A informação, a seu turno, consiste nos dados organizados, o que possibilita sua utilização para determinada finalidade.

Em igual sentido, Nathan Shedroff,[57] em trabalho de 1999, define dados como "o produto de pesquisa, criação, coleção e descoberta. É o material cru que encontramos ou criamos e usamos para construir nossas comunicações". O autor ressalta que dados não são, em si, valiosos, porque não são mensagens completas. Servem a processos produtivos, e só.

---

[56] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados**. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019. P. 136.

[57] SHEDROFF, Nathan. *Information interaction design: an unified field theory of design. In: JACOBSON, Robert (Org.).* ***Information design*****.** Cambridge: The MIT Press, 1999. P. 272. Tradução livre. Texto original: "*Data is the product of research, creation, collection, and discovery. It is the raw material we find or create that we use to build our communications*".

Informação, por outro lado, como coloca o autor[58], constitui material bruto já trabalhado, assim definindo-a:

> "Informação é o primeiro nível no qual se torna apropriado comunicar com o público. Ela representa a transmissão de mensagens pensadas que revelam as relações e padrões (o contexto) no âmbito dos dados apresentados. Transformar dados em informação é algo que se faz ao organizá-los de uma forma significativa, apresentando-os em maneiras apropriadas, e comunicando o contexto que os cerca".

De toda sorte, há, na doutrina e na legislação, um grande intercâmbio entre as expressões "dados" e "informações" – estando a questão longe de consenso acadêmico. Como coloca por Marcos Balster,[59] há uma pluralidade de significados especialmente para a ideia de "informação", a qual muda conforme o contexto em que é utilizada. Assemelha-se, no caso, ao problema mencionado alhures com respeito ao artigo[60] de Tércio Sampaio quando tratava da ideia de sigilo como faculdade.

Aidan Forde[61] também destaca tal preocupação quando afirma que:

> É uma tarefa onerosa identificar um conceito unificado de privacidade. Sua relação com proteção de dados é cercada por controvérsias. Não obstante, a luta para identificar um entendimento conceitual unificado de privacidade, elucidando a relação entre privacidade e proteção de dados, é algo que gera um claro benefício à democracia e à sociedade.

Dessa forma, não há como escapar a uma certa dose de arbitrariedade quando da escolha do significado que se lhe atribuirá no âmbito de determinado trabalho acadêmico. Não há um consenso preciso sobre o conteúdo de tal termo e não é a pretensão deste trabalho criá-lo – mas, tão somente, defini-lo de maneira condizente com os estudos sobre o tema, de modo a ter-se uma definição que seja útil e utilizável ao longo do trabalho para fins de exposição e contraposição de ideias.

Diante disso, entender "informação" como "dado utilizável" mostra-se bastante adequado para as finalidades deste estudo, eis que servirá para ressaltar um elemento que, como se verá adiante, será de fundamental importância para o prosseguimento deste estudo: a tomada

---

[58] SHEDROFF, Nathan. *Information interaction design: an unified field theory of design. In: JACOBSON, Robert (Org.).* ***Information design*****.** Cambridge: The MIT Press, 1999. P. 272-273. Tradução livre. Texto original: "*Information is the first level at which it is appropriate to communicate with audiences. It represents the transmission of thoughtful messages that reveal the relationships and patterns (the context) among the data presented. Transforming data into information is accomplished by organizing them into a meaningful form, presenting them in appropriate ways, and communicating the context around them*".

[59] CORREIA, Marcos Balster Fiore. **A comunicação de dados estatísticos por intermédio de infográficos: uma abordagem ergonômica**. Rio de Janeiro: Pontifícia Universidade Católica do Rio de Janeiro, 2009. P. 41-45.

[60] FERRAZ JR., Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito,** Universidade de São Paulo, n. 88, p. 439-459, 1993.

[61] FORDE, Aidan. *The Conceptual Relationship between Privacy and Data Protection*. ***Cambridge Law Review***, v. 1, n. 135, 2016. P. 136. Tradução livre. Texto original: "*It is an onerous task to identify a unified conceptual understanding of privacy. Controversy surrounds its relationship with data protection. Notwithstanding the battle to identify such a unified conceptual understanding of privacy, elucidating the relationship between privacy and data protection is something of clear benefit to democracy and society*".

de decisão humana (por meios automatizados ou não) capaz de influir na realidade e afetar, em sentido amplo, a vida de indivíduos e sociedades.

O que se está a afirmar é que dados, por si só, têm pouca ou nenhuma relevância se não for possível convertê-los em informações que possam subsidiar a tomada de decisão humana (ainda que tal decisão consista no desenvolvimento de um algoritmo que toma decisões). De tal raciocínio decorre a utilidade do conceito de informação que ora se elege, visto que possui, como elemento central, o destaque conferido ao aspecto utilitário que os dados podem vir a assumir.

A ideia de proteção de dados, então, surge como uma consequência natural dos conceitos delineados acima. Como se verá no capítulo 3, há um reconhecimento acerca das potencialidades e dos riscos a uma sociedade livre resultantes da amplitude de informações decorrentes da massificação no uso dos dados.

Ao passo em que a privacidade se mostra como um direito de reter/ocultar informações, a proteção de dados vai além, reconhecendo os dados como uma realidade externa ao sujeito que pode implicar vulneração de sua privacidade e, assim, dando ao sujeito o direito de decidir o que terceiros fazem com tais dados que a ele se referem. Como coloca Danilo Doneda,[62] "*a proteção de dados pessoais, em suma, propõe o tema da privacidade, porém modifica seus elementos; aprofunda seus postulados e toca nos pontos centrais dos interesses em questão*".

A Lei Geral de Proteção de Dados – LGPD,[63] em seu artigo 1º, quando estabelece que o objetivo da proteção de dados é "*proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural*" corrobora o raciocínio acima por meio da positivação, no ordenamento jurídico, da proteção de dados com enfoque em tais finalidades.

1.2.Conclusões Provisórias

Este capítulo buscou, de modo sucinto, situar o debate relativo à privacidade para o fim de estabelecer ideias de privacidade, sigilo e proteção de dados com as quais possa-se trabalhar.

A ideia de privacidade, desde a sua gênese contemporânea em 1890, é carregada de controvérsia e polissemia. As diversas ramificações que tal direito adquiriu não permitiram que

[62] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados**. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019. P. 173.
[63] BRASIL, República Federativa do. **Lei nº 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Diário Oficial da União: Brasília, 15 de agosto de 2018.

a academia ou os tribunais alcançassem um único conceito definidor de privacidade e que fosse capaz de abarcar todas as situações nas quais afirmou-se que tal direito estava presente e que deveria ser resguardado.

As tentativas de defini-la resultavam em ideias ou muito estreitas, ou muito amplas, o que eliminava a sua utilidade como conceito para fins de utilização prática. Viu-se que, ao invés de um conceito único, a privacidade é uma rede de ideias que se sobrepõem parcialmente umas às outras.

Diante disso, optou-se por adotar uma ideia de privacidade a partir de sua finalidade e do direito que o sujeito tem: o de reter e ocultar informações, sem perquirir qual seria o motivo específico para cada situação e sem tentar extrair uma ideia abstrata comum a todos.

Adotado um modo de trabalhar com a privacidade, passou-se à ideia de sigilo. Não obstante exista também uma certa polissemia em tal conceito, que é frequentemente usado como sinônimo de privacidade, distingui-lo da privacidade por meio da definição do sujeito a que se refere mostrou-se mais adequada. Tal distinção destina-se tanto a evitar a sinonímia, quanto para, ao longo do texto, identificar, por meio de terminologia adequada, a quem se está referindo ao tratar de temas relacionados à privacidade.

Por fim, passou-se à ideia de proteção de dados, que, assim como os demais conceitos que orbitam a temática da privacidade, também é difícil de se estabelecer. Nesse sentido, definiu-se a ideia de "dados" como elementos informativos brutos sobre determinados fatos, que, após processo de análise, tornam-se "informações", a qual é dotada de conteúdo utilizável. Diante disso, pôde-se entender proteção de dados, para os fins deste trabalho, e sem a pretensão de definir um conceito universal, como a disciplina que rege a coleta, uso e disseminação de dados com vistas à proteção das informações que deles se pode obter e que possuem aptidão de vulnerar a privacidade.

Estabelecidas estas ideias, o próximo capítulo irá, a partir de uma ótica pragmática, verificar quais são os potenciais dos dados e quais as informações que deles se pode obter no contexto tecnológico do século XXI, elencando os riscos à privacidade daí derivados a partir de uma análise concreta.

2. RISCOS À PRIVACIDADE

O conceito de comunicador fiduciário, apresentado na introdução, abrange as entidades, geralmente personalidades jurídicas, que atuam, na sociedade contemporânea, como intermediários da comunicação humana.

Partiu-se da concepção da realidade delineada por Jack Balkin[64] para a liberdade de expressão, mas, que, dado o diagnóstico preciso dos meios pelo qual se dá a interação humana na realidade do século XXI, aplica-se, também, às questões concernentes à privacidade.

Neste capítulo, busca-se partir dos conceitos delineados no capítulo anterior, somando-os a uma análise crítica dos potenciais decorrentes da utilização de dados na contemporaneidade, para, assim, identificar quais são os elementos de preocupação sob um ponto de vista eminentemente pragmático.

Tal identificação é fundamental porque, no capítulo 3, será realizada análise teórica dos riscos identificados neste capítulo a partir de uma perspectiva concreta dos potenciais tecnológicos hoje existentes no âmbito de atuação dos comunicadores fiduciários.

Este capítulo, portanto, iniciará com a definição da ideia de comunicador fiduciário, que nada mais é do que o responsável pela viabilização do fenômeno hoje existente que é a comunicação fiduciária.

Em seguida, realizar-se-á um levantamento taxonômico a partir do trabalho de Daniel Solove[65] para o fim de definir categorias de riscos às pessoas decorrentes do uso de informações, que é o que a proteção de dados visa resguardar por meio da atenção à etapa que lhe antecede.

Depois, o trabalho focará nas potencialidades das novas tecnologias, partindo dos quatro grandes poderes do Big Data definidos por Seth Stephens-Davidowitz[66] e identificando os riscos que elas apresentam.

---

[64] BALKIN, Jack M. *Free Speech is a Triangle.* ***Columbia Law Review*****,** Nova York, vol. 118, 2018, p. 2011-2056. P. 2014.

[65] SOLOVE, Daniel. *A Taxonomy of Privacy.* ***University of Pennsylvania Law Review*****,** v. 154, n. 3, 2006, p. 477-564.

[66] STEPHENS-DAVIDOWITZ, Seth. **Todo mundo mente:** o que a internet e os dados dizem sobre quem realmente somos. Trad. Wendy Campos. Rio de Janeiro: Alta Books, 2018. P. 53-54: (i) a oferta de novos tipos de dados, tornando acessíveis informações que, outrora, não o eram; (ii) a honestidade dos dados coletados, diante da dificuldade, inviabilidade e/ou pouca probabilidade de serem mentirosos e/ou falsos; (iii) a possibilidade de se analisar pequenos subconjuntos de dados, separando as pessoas por categorias; e (iv) a viabilidade da realização de experimentos causais (testagem da população).

Em seguida, serão apresentadas as preocupações manifestadas ao longo do tempo sobre o tema, realizando-se cotejo no intuito de verificar se os poderes apresentados por Stephens-Davidowitz evidenciam uma materialização desses riscos de ordem pragmática.

2.1.Comunicação Fiduciária

Quando a comunicação humana e o arquivamento de informações se davam exclusivamente em meios físicos, como cartas, bibliotecas e arquivos, a preocupação com a violação à privacidade era restrita a um rol específico e controlável de situações.

A dependência de comunicadores fiduciários era bastante reduzida, limitando-se, no caso de cartas, aos próprios carteiros – seja por mão própria, seja em virtude da interceptação por parte de terceiros.

De toda sorte, a utilização de meios rudimentares de criptografia, como a aposição de selos com cera, por exemplo, ou até mesmo a utilização de códigos acessíveis a qualquer pessoa, como a Cifra de César,[67] permitia ao destinatário que verificasse a ocorrência de invasão ao sigilo da missiva e ao remetente que garantisse, mesmo nessa hipótese, o segredo do conteúdo.

Com respeito a arquivos, a situação era bastante parecida: a privacidade era garantida por fechaduras e paredes. A dependência de terceiros era mínima e limitada aos frequentadores do local, identificados ou identificáveis. Além disso, eventuais violações não seriam de difícil percepção: qualquer ser humano é capaz de identificar um arrombamento. E a entrada subreptícia pode ser facilmente coibida por meio de vigilância.

Acrescente-se a isso a limitação no número de envolvidos: uma pessoa só poderia violar a privacidade de outra se estivesse fisicamente presente no local, com acesso ao recinto ou à comunicação. Ocorrendo violação, a pessoa cuja privacidade foi vilipendiada saberia quem seriam os potenciais suspeitos – o arquivista, o secretário, o segurança etc. O rol de pessoas com potencial acesso à informação era limitado, identificado ou identificável *pelo* titular.

Em contraposição a esse cenário, com o arquivamento de informações em aparelhos informatizados e expansão da comunicação fiduciária, o controle do indivíduo sobre a própria privacidade torna-se significativamente mais frágil.

Suponha-se um cenário em que um indivíduo se comunica com o outro por um aplicativo de mensagens, como o WhatsApp, conectado pelo navegador de um computador.

[67] Método de criptografia atribuído a Júlio César, que consiste no "deslocamento" de letras do alfabeto. O destinatário, ciente do número de letras deslocadas, era capaz de corrigir a criptografia e construir o texto da mensagem original.

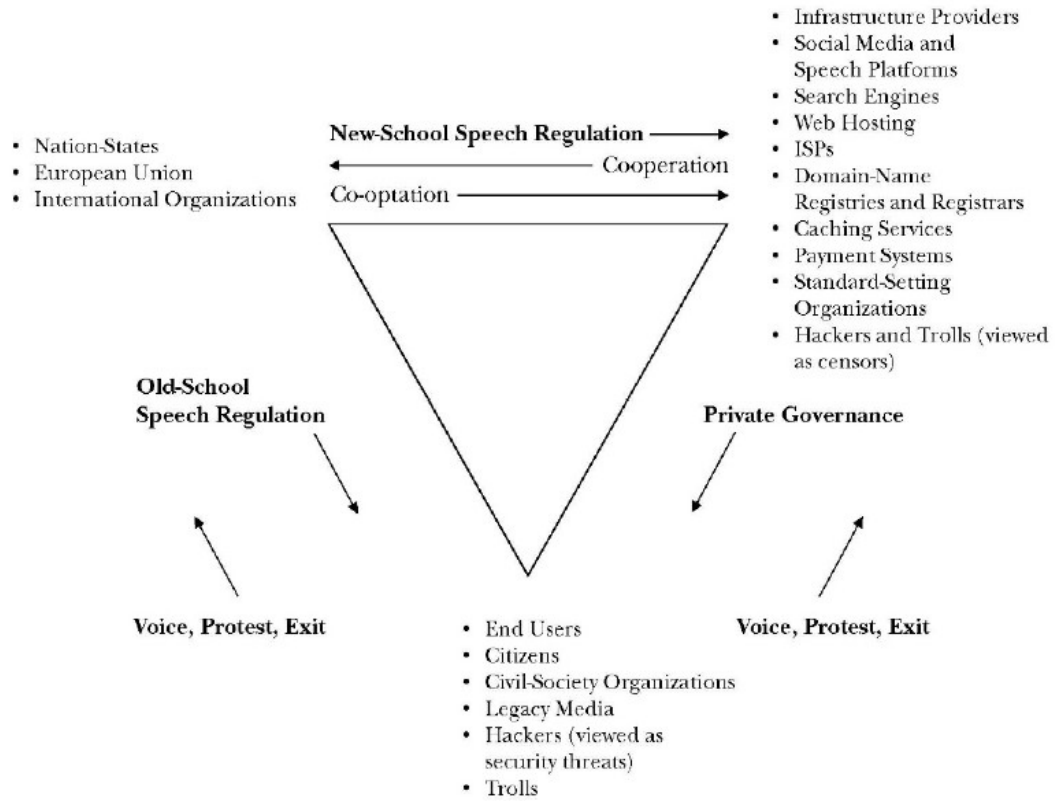
Tudo o que for digitado passará pelo desenvolvedor do sistema (como a Microsoft), pelo desenvolvedor do navegador (e.g. Google Chrome), pelo provedor de internet (e.g. GVT), pela empresa desenvolvedora do aparelho celular (e.g. Apple), pela companhia telefônica (e.g. Vivo) e, naturalmente, pelo próprio *WhatsApp*, que pertence ao Facebook. Além disso, como toda comunicação tem, no mínimo, dois envolvidos, a situação se repete para o destinatário da mensagem, que terá intermediários análogos viabilizando a comunicação do seu lado. E existem, ainda, os diversos fornecedores de infraestrutura, que também possuem acesso potencial ao fluxo de dados – como a recente controvérsia acerca da rede 5G[68] e da empresa de tecnologia Huawei demonstram.

O que se tem, assim, e que é seu elemento caracterizador, é que qualquer dos comunicadores fiduciários possui acesso potencial às informações que tramitam por seus sistemas, e a limitação a esse acesso depende única e exclusivamente de configurações de *software* dificilmente auditáveis pelo cidadão comum.

Jack Balkin desenha o que ele chama de modelo pluralista da regulação da fala a partir do estabelecimento dos seguintes agentes:

[68]OLIVEIRA, Eliane. China reage a nova provocação de Eduardo Bolsonaro sobre 5G e afirma que deputado perturba parceria com Brasil. **O Globo.** Rio de Janeiro, 24 de novembro de 2020. Disponível em: https://oglobo.globo.com/economia/china-reage-nova-provocacao-de-eduardo-bolsonaro-sobre-5g-afirma-que-deputado-perturba-parceria-com-brasil-1-24763500. Acesso em: 18 de janeiro de 2021.

Figura 1: Modelo Triangular de Balkin



Fonte: BALKIN, Jack M. Free Speech is a Triangle. **Columbia Law Review**, Nova York, vol. 118, 2018. P. 2014. P. 2014.

Os vértices, na definição de Balkin,[69] são compostos da seguinte maneira:

> "Em um vértice do triângulo estão os estados-nações, estados, municípios e organizações supranacionais como a União Europeia.
> No segundo vértice do triângulo estão as empresas de infraestrutura da internet. (...) Cada um desses elementos da infraestrutura da internet é importante, se não for crucial, à possibilidade prática de as pessoas falarem. Na maior parte dos países, essa infraestrutura da internet, ou partes importantes dela, pertencem ao setor privado.
> No terceiro vértice do triângulo, bem na base, nós temos os falantes e a mídia, incluindo organizações de mídia de massa, manifestantes, organizações da sociedade civil, *hackers* e *trolls*".

[69] BALKIN, Jack M. *Free Speech is a Triangle.* ***Columbia Law Review***, Nova York, vol. 118, 2018. P. 2014. P. 2014-2015. Tradução livre. Texto original: "*On one corner of the triangle are nation-states, states, municipalities, and supranational organizations like the European Union. On the second corner of the triangle are internet-infrastructure companies. (...) Each of these elements of the internet infrastructure is important, if not crucial, to people's practical ability to speak. In most countries, this internet infrastructure, or important parts of it, are privately owned. On the third corner of the triangle, at the very bottom, we have speakers and legacy media, including mass-media organizations, protesters, civil society organizations, hackers, and trolls*".

Como se vê a partir de Balkin, os intermediários são pessoas jurídicas, multinacionais – as quais, por natureza, contam com milhares de funcionários. O indivíduo utilizador do sistema não possui qualquer condição de saber quem dentro das empresas detém meios para acessar as informações. Ocorrendo violação da privacidade de determinado indivíduo, ele (*i*) não necessariamente saberá, já que a empresa pode esconder a ocorrência; e (*ii*) se souber, não terá como identificar os responsáveis – afinal, o usuário não conhece os sistemas de gestão internos da empresa desenvolvedora dos sistemas que ele utiliza.

O *WhatsApp*, por exemplo, com o intuito de apaziguar as preocupações, assevera que a comunicação é criptografada de ponta-a-ponta,[70] e que nem a própria empresa teria acesso ao conteúdo das mensagens trocadas por meio de seu sistema. Porém, em última análise, não há mudança no elemento fiduciário: o usuário pode confiar que ninguém da empresa violará sua privacidade, ou pode confiar que o sistema da empresa não permitirá que ninguém viole sua privacidade. De qualquer maneira, precisa confiar no que a empresa lhe diz.

Em última análise, contudo, o usuário comum continua a ter sua privacidade baseada na confiança nos intermediários – que, não necessariamente, estão bem-intencionados. A imposição de criptografia pode servir somente para impedir que terceiros se aproveitem dos dados, mantendo o acesso próprio no caso de má-fé do intermediário, como se fosse uma espécie de estratégia monopolista, garantindo a um dos comunicadores fiduciários exclusividade na violação à privacidade.

Quando o risco afeta instituições de grande porte, que possuem os meios para testar os sistemas de intermediários, os perigos tornam-se conhecidos para a população. Um exemplo disso é a recente alteração[71] nos termos de uso do *WhatsApp* – que acarretou a migração das comunicações da Comissão Europeia[72] para o Signal. A Comissão Europeia, naturalmente, possui meios para averiguar os riscos a que está submetida que são melhores do que aqueles ordinariamente à disposição do cidadão comum. Todavia, nem mesmo grandes instituições estatais estão seguras.

---

[70] Sobre a criptografia de ponta a ponta. **FAQ do Whatsapp.** Disponível em: <https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption/?lang=pt_br>. Acesso em: 18 de janeiro de 2021.

[71] LAVADO, Thiago. WhatsApp: o que muda com os novos termos de uso? É hora de trocar de app? **Exame.** São Paulo, 14 de janeiro de 2021. Disponível em: <https://exame.com/tecnologia/whatsapp-o-que-muda-com-os-novos-termos-de-uso-e-hora-de-trocar-de-app/>. Acesso em: 13 de março de 2021.

[72] Comissão Europeia troca WhatsApp por Signal para aumentar segurança. **Consultor Jurídico.** São Paulo, 11 de janeiro de 2021. Disponível em: <https://www.conjur.com.br/2021-jan-11/comissao-europeia-troca-whatsapp-signal-aumentar-seguranca>. Acesso em: 17 de março de 2021.

Um bom exemplo é caso[73] da empresa Crypto AG, sediada na Suíça e especializada na elaboração de sistemas de criptografia: a agência de inteligência/espionagem dos Estados Unidos da América – CIA (*Central Intelligence Agency*) era, secretamente, dona da empresa. Ao longo de 50 (cinquenta) anos, a empresa forneceu sistemas de criptografia para mais de 120 (cento e vinte) países. Naturalmente, todos possuíam falhas propositais que permitiam acesso ao conteúdo das comunicações. Além de realizar espionagem em larga escala, a CIA ainda lucrou milhões de dólares com a operação.

A comunicação fiduciária, consequentemente, deixa o usuário duplamente refém dos intermediários: tanto com respeito à própria garantia da privacidade, quanto no que tange à identificação dos responsáveis por eventual violação e acesso indevido a dados privados. Em última análise, o usuário se torna inteiramente dependente da *confiança* em terceiros para a garantia de um direito seu, razão pela qual a adoção da qualificação "*fiduciário*" para identificar os intermediários da comunicação.

Assim, a ideia de "comunicador fiduciário" é um pouco mais ampla, mas, na essência, consiste nos atores privados identificados por Jack Balkin[74] como os ocupantes do segundo vértice de seu triângulo comunicacional: as empresas de infraestrutura de internet responsáveis por viabilizar as conexões humanas.

2.2. Dados, Metadados e Cruzamento De Informações

A etapa seguinte dessa problemática é o registro dos chamados *metadados*: são dados indiretos, periféricos, que acompanham arquivos informatizados e transmissões de informações – como a data, horário e localização de uma fotografia. Carrington e Vandewiele[75] os definem, sinteticamente, como sendo "dados sobre dados".

Kevin Butterfield[76] aprofunda a questão nos seguintes termos:

---

[73] MILLER, Greg. *The intelligence coup of the century.* ***The Washington Post.*** Washington, 11 de fevereiro de 2020. Disponível em: <https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/>. Acesso em: 18 de abril de 2021.

[74] BALKIN, Jack M. *Free Speech is a Triangle.* ***Columbia Law Review***, Nova York, vol. 118, 2018. P. 2014.

[75] CARRINGTON, David; VANDEWIELE, Alida. *What Is Metadata?* ***International In-House Counsel Journal*****,** v. 8, n. 31, 2015, p. 1-7. Texto original: "*Put shortly, metadata is 'data about data'.*".

[76] BUTTERFIELD, Kevin. Metadata: An Overview. **AALL Spectrum,** v. 6, n. 3, 2001, p. 24-28. Tradução livre. Texto original: "*Metadata is commonly defined as data about data. It may be further defined as na expansion of bibliographic cataloging practices in a digital environment. In particular communities and contexts, however, the word is used with much narrower definitions. For example, it may mean only cataloging, or only data about digital resources, or only information structured to be understood by computers*".

> "Metadados são comumente definidos como dados sobre dados. O conceito pode ser melhor definido como uma expansão de práticas de catalogação bibliográfica em um ambiente digital. Em determinadas comunidades e contextos, no entanto, a palavra é usada com definições muito mais precisas. Por exemplo, pode significar somente catalogação, ou somente dados sobres fontes digitais, ou somente informação estruturada para ser compreendida por computadores".

Anne Gilliland[77] categoriza os metadados conforme seus usos em cinco tipos distintos, destacando que sua constituição pode ser fluida porque o que seria um dado em um contexto pode ser um metadado em outro contexto:

(i) Administrativos: utilizados para gerenciar e administrar coleções e informações;

(ii) Descritivos: utilizados para identificar e descrever coleções e informações relacionadas;

(iii) Preservativos: relacionados ao gerenciamento da preservação de coleções e informações;

(iv) Técnicos: relacionados ao modo de funcionamento de um sistema ou ao comportamento dos metadados;

(v) Utilitários: relacionados ao nível e espécie de uso de coleções e informações.

Os metadados consistem em uma categoria especial de dados, que variam conforme o contexto em que utilizadas, e que possibilitam a descoberta e manutenção de uma série de informações – principalmente quando realizado o cruzamento de dados.

Como exemplo, há o sistema operacional de *smartphones* da Apple, o iOS, que possui mecanismos de registro de localização geográfica (dados georreferenciais do aparelho). A empresa informa[78] que é dado ao usuário decidir – ou não – por ativar a funcionalidade que permite a coleta de tais dados, bem como em que termos e em que situações. Novamente, o elemento fiduciário entra em cena: o usuário não tem opção a não ser acreditar que, se ele optar por não compartilhar seus dados geográficos, os dados realmente não serão utilizados pela empresa.

---

[77] GILLILAND, Anne J. *Setting the Stage. In:* ***Introduction to Metadata*****,** BACA, Murtha. 2ª ed. Los Aangeles: Getty Research Institute, 2008. P. 9. Tradução livre. Original: "*Administrative: Metadata used in managing and administering collections and information resources [...] Descriptive: Metadata used to identify and describe collections and related information resources [..] Preservation: Metadata related to the preservation management of collections and information resources [...] Technical: Metadata related to how a system functions or metadata behaves [...] Use: Metadata related to the level and type of use of collections and information resources [...]* One information object's metadata can simultaneously be another information object's data, depending on the kind of aggregations of and dependencies between information objects and systems".

[78] Controle as informações de localização compartilhadas no iPhone. **Manual do Usuário do iPhone.** Disponível em: <https://support.apple.com/pt-br/guide/iphone/iph3dd5f9be/ios>. Acesso em: 18 de janeiro de 2021.

Em segundo lugar, há um outro problema: ainda que a empresa cumprisse com a obrigação assumida, ela poderia obter exatamente a mesma informação por meio de outros dados. É possível coletar registros dos pontos de conexão e das redes de internet a que o usuário se conecta – o que, efetivamente, permite a localização geográfica do usuário,[79] ainda que com um grau menor de precisão. Nesse cenário, o indivíduo nega seu consentimento à coleta e uso de determinados dados acreditando que a informação deles decorrente também estará protegida. No entanto, isso não necessariamente é verdade.

Ian James Samuel,[80] em trabalho de 2008, explica como funciona o rastreamento de aparelhos celulares, que funcionam na base de ondas de rádio, a partir de metadados:

> "Para enviar e receber ligações, mensagens de texto ou e-mails, telefones celulares se comunicam com torres de rádio, conhecidas como torres de celular. As torres de celular são distribuídas por uma área de cobertura; usuários de celulares frequentemente estão dentro do alcance de mais de uma.
> A qualidade do sinal de e para essas torres é o que é medido pelas características "barras" em telefones celulares. Como usuários de telefones celulares sabem, as barras indicativas da qualidade do sinal estão presentes quer uma ligação esteja em curso ou não, uma vez que os telefones permanecem em contato frequente com as torres de celular próximas. Pela comparação do tempo e ângulo de chegada do sinal do telefone em várias torres de celular é possível descobrir o local da transmissão. Isso é conhecido como triangulação de rádio. Quanto mais densamente colocadas forem as torres de telefone, mais precisos serão os dados de localização".

O cenário acima é apenas um exemplo do potencial dos metadados. Enquanto o registro de chamadas é um dado vinculado à utilização do aparelho celular, a identificação das antenas e ângulos de conexão é o metadado – por meio do qual torna-se possível obter informações "extra" sobre o usuário do telefone.

Um elemento importante que caracteriza o metadado é que, com frequência, o usuário não tem como, por meios próprios, evitar sua coleta: o uso de aparelho celular necessariamente demanda a conexão por meio de antenas, o que, por si só, dá à companhia telefônica o potencial de, unilateralmente, optar – ou não – por manter registro de tais metadados.

---

[79] ROHR, Altieres. Localização de endereço de IP: entenda como poder feito o rastreamento e o que é mito. **G1.** Rio de janeiro, 2 de março de 2021. Disponível em: <https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2021/03/02/localizacao-de-endereco-de-ip-entenda-como-pode-ser-feito-o-rastreamento-e-o-que-e-mito.ghtml>. Acesso em: 7 de junho de 2021.

[80] SAMUEL, Ian James. *Warantless Location Tracking.* ***New York University Law Review*****,** v. 83, n. 4, 2008, p. 1324-1352. Tradução livre. Texto original: "*A cell phone is 'a radio-an extremely sophisticated radio, but a radio nonetheless.' To send and receive calls, text messages, or email, cell phones communicate with radio towers, known as cell towers. The cell towers are distributed throughout a coverage area; cell phone users are often in range of more than one. The quality of the signal to and from these towers is what's measured by the characteristic 'bars' on cell phones. As users of cell phones know, the signal quality bars are present whether or not a call is in progress, as the phones remain in regular contact with nearby cell towers.' By comparing the phone signal's time and angle of arrival at several cell towers, the location of the broadcast can be figured out. This is known as radio triangulation. The more densely placed the phone towers, the more accurate the location data will be*".

Hoje, a possibilidade de rastreamento geográfico por meio do uso de antenas de aparelhos celulares é razoavelmente pública – vale dizer, não é uma informação secreta ou de conhecimento de poucos. Mas, isso nem sempre foi assim. Quando do surgimento da tecnologia, os primeiros usuários não sabiam que, ao utilizarem um serviço que os permitia conversar com pessoas distantes, estavam, ao mesmo tempo, permitindo que determinadas companhias mantivessem um registro perene de todos os locais frequentados pelo usuário.

Quando os metadados entram em cena, os riscos à privacidade aumentam, os quais são agravados pelo cruzamento de dados: é possível identificar com quem uma pessoa estava reunida simplesmente a partir do cruzamento de dados de localização – e o usuário jamais saberá que alguém possui tais informações.

Nos métodos antigos, para descobrir com quem um cidadão se reunia, era imprescindível um estabelecimento de vigilância física. A pessoa sendo seguida teria meios para identificar a violação de sua privacidade: observaria carros seguindo seus trajetos, fotógrafos suspeitos nas cercanias, dentre outros elementos indiciários. Hoje, contudo, tais elementos tecnológicos permitem que a violação ocorra sem que o sujeito nem sequer suspeite que sua privacidade está sob perigo.

Outra situação é que uma empresa como a *Google* pode saber o assunto tratado em uma conversa particular por meio de inferências decorrentes do uso de metadados e do cruzamento de informações: se os dados geográficos indicam que duas pessoas estavam reunidas em determinado local por determinado período de tempo, e se os dados do *Google* demonstram que uma delas fez uma pesquisa por determinado assunto naquele tempo, há uma razoável inferência dos temas objeto de discussão naquela ocasião.

O registro da formatação de páginas *web* permite identificar o sistema operacional utilizado e, assim, saber se a pessoa está usando o computador de terceiro para acessar determinado serviço. O registro de *timestamps*[81] de mensagens, ainda que o conteúdo seja criptografado, permite que se descubra se determinada pessoa estava dormindo ou acordada em algum horário específico, assim como possibilita que desvendem os hábitos de sono do indivíduo.[82] De igual modo, tal mecanismo permite que se saiba se duas pessoas conversaram entre si, a julgar pelo horário em que permaneceram ativas no sistema.

---

[81] Registro de data e horário da ocorrência de determinado fato.

[82] As tentativas de descobrir a identidade de Satoshi Nakamoto, pseudônimo do criador da criptomoeda Bitcoin, envolveram análise dos horários de suas postagens na internet, para, a partir de um cotejo entre os horários mais comuns de atividade e inatividade, desvendar o provável fuso horário em que residia o inventor da tecnologia. STEPHENS, Randall. *The Creator os Bitcoin, Satoshi Nakamoto, Is Most Likely This Guy.* ***Medium*****,** 9 de março de 2019. Disponível em: <https://medium.com/swlh/the-creator-of-bitcoin-satoshi-nakamoto-is-most-likely-this-guy-8723eddb517c>. Acesso em: 10 de junho de 2021.

Sob essa perspectiva, é fundamental destacar que os problemas ora apontados não existiam no século XX, ou, ao menos, não na mesma escala. Um terceiro não teria como inferir o assunto de uma conversa entre particulares sem estar fisicamente presente no local – já que a pesquisa seria feita em uma enciclopédia, e não no Google.

Um outro exemplo bastante recente da utilização de metadados é o da invasão ao Capitólio nos Estados Unidos: a polícia,[83] a partir de localizadores geográficos de aparelhos celulares, procurou identificar os invasores. Todavia, essa mesma tecnologia, que permite a identificação de criminosos, também viabiliza a identificação e perseguição de participantes em protestos legítimos, como se viu em Hong Kong:[84]

> "Lojas de aparelhos eletrônicos em Hong Kong viram um rápido aumento na demanda por telefones descartáveis baratos na medida em que o governo da cidade, dominado pela China, reduz as restrições causadas pelo coronavírus, mas fortalece o uso de um aplicativo rastreador de contatos que gerou preocupações com a privacidade.
> A antiga colônia britânica viu protestos anti-governo e anti-China surgirem em 2019 e uma lei de segurança nacional rígida imposta por Pequim como resposta, junto com a prisão da maioria de seus ativistas pró-democracia mais proeminentes.
> A brusca virada autoritária do governo, que nega cercear os direitos e liberdades dos 7.5 milhões de habitantes da região administrativa especial, resultou em profunda desconfiança de políticas públicas, incluindo medidas voltadas à contenção do coronavírus.
> A Secretária de Saúde Sophia Chan disse que o aplicativo não apresenta nenhum risco de privacidade, uma vez que salva dados somente no telefone dos usuários e nenhum terceiro os coleta. O aplicativo notifica os usuários caso eles tenham estado no mesmo local em que uma pessoa diagnosticada com COVID-19".

Nesse sentido, o que se vê é que os metadados – e o cruzamento de informações – ocasionam uma ampliação dos riscos à privacidade porque possibilitam a violação da privacidade de modo sub-reptício. São situações que geralmente passam despercebidas para o usuário e que apresentam riscos tão grandes quanto, ou até maiores, do que o acesso propriamente dito ao conteúdo das comunicações.

---

[83] YANG, Allie. *Many Capitol rioter implicated by their own social media posts.* ***ABC News*****.** Nova York, 11 de janeiro de 2021. Disponível em: <https://abcnews.go.com/Technology/capitol-rioters-implicated-social-media-posts/story?id=75177672>. Acesso em: 18 de janeiro de 2021.

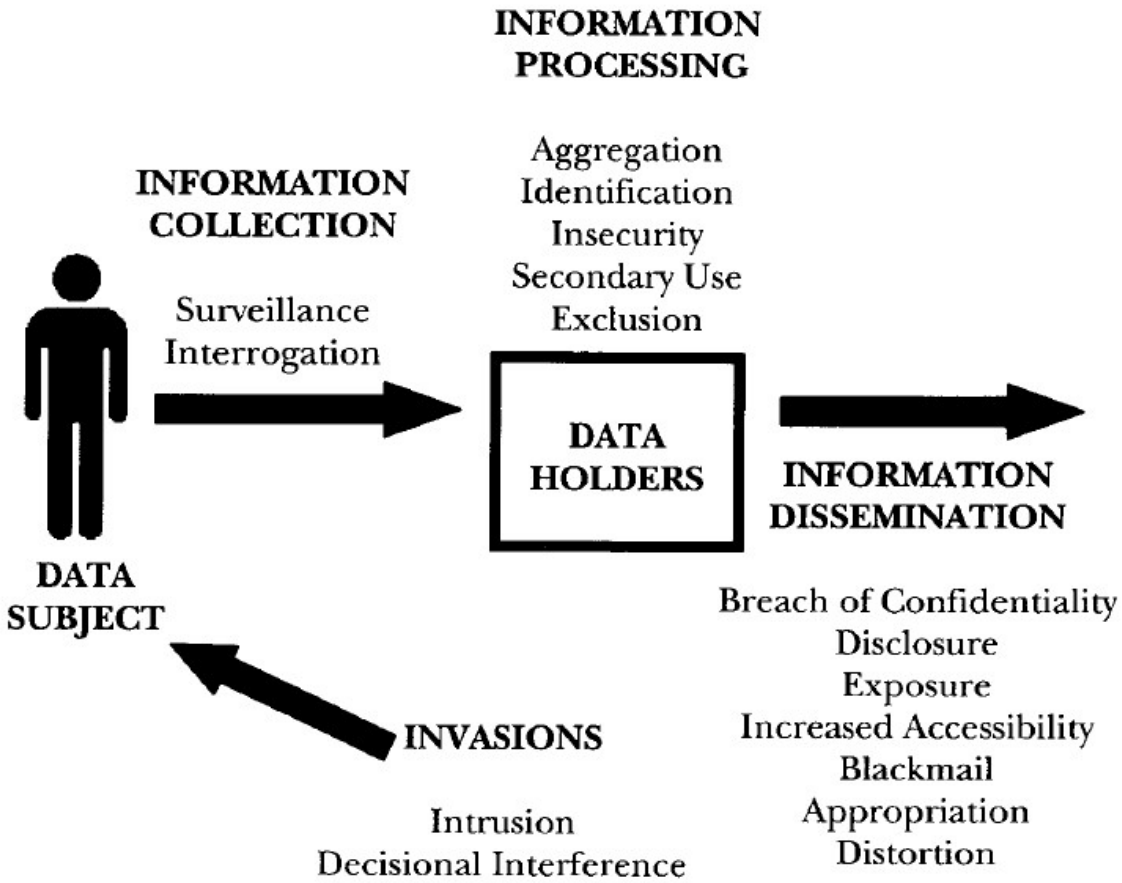
[84] CHAN, Justin. *Hong Kong sees rush for burner phones as government pushes contact-tracing app.* ***Reuters*****.** 18 de fevereiro de 2021. Disponível em: <https://www.reuters.com/article/us-health-coronavirus-hongkong-idUSKBN2AI0I8>. Acesso em: 7 de junho de 2021. Tradução livre. Texto original: "*Electronics shops in Hong Kong have seen a sharp increase in demand for cheap burner phones as the Chinese-ruled city's government eases coronavirus restrictions but pushes the use of a contact-tracing app which has raised privacy concerns. The former British colony saw anti-government and anti-China protests erupt in 2019 and a sweeping national security law imposed by Beijing in 2020 in response, along with the arrest of most of its prominent pro-democracy activists. The swift authoritarian turn taken by the government, which denies curbing the rights and freedoms of the special administrative region's 7.5 million residents, has resulted in deep-seated mistrust of public policies, including of measures to curb the coronavirus. Health Secretary Sophia Chan said the app poses no privacy risks as it only stores data on users' phones and no third party collects it. The app notifies users if they had been in the same place with a person confirmed with COVID-19*".

2.3. Taxonomia De Daniel Solove

Diante dessas ponderações, Daniel Solove[85] estabeleceu uma *taxonomia* dos riscos à privacidade, visando categorizá-las no intuito de poder, com elas, trabalhar, e dividindo-as nas seguintes quatro categorias principais, posteriormente detalhadas: (*i*) coleta de informações; (*ii*) processamento de informações; (*iii*) disseminação de informações; e (*iv*) invasão. Não é pretensão nem objetivo deste trabalho aprofundar demasiado nas taxonomias, mas, tão somente, explicá-las, de modo sucinto, para que possam ser utilizadas posteriormente.

Assim, inicialmente, é preciso situar em qual momento da atuação dos comunicadores fiduciários cada uma delas se situa, o que Daniel Solove faz de modo bastante didático por meio da figura constante na página seguinte:

Figura 2: Posicionamento da taxonomia da privacidade



[85] SOLOVE, Daniel. A Taxonomy of Privacy. **University of Pennsylvania Law Review,** v. 154, n. 3, 2006, p. 477-564. P. 478.

Fonte: SOLOVE, Daniel. *A Taxonomy of Privacy.* ***University of Pennsylvania Law Review*****,** v. 154, n. 3, p. 477-564, 2006. P. 490.

2.3.1. Coleta de Informações

A categoria (*i*), atinente à coleta de informações, compreende riscos de duas naturezas distintas: (a) vigilância; e (b) interrogatório. A primeira, como o nome indica, consiste no monitoramento constante das atividades de uma pessoa, e pode levar à autocensura, inibição de comportamento do sujeito observado e cerceamento da liberdade.[86] A segunda, a seu turno, diz respeito à não autoincriminação (direito de ficar em silêncio), que, para Solove,[87] além de poder gerar uma "auto coação", também gera um risco de distorção da informação.

2.3.2. Processamento de Informações

No que tange ao processamento das informações, este se refere à forma como dados coletados são usados, armazenados e manipulados. Diz respeito ao que se faz com eles quando já foram obtidos.[88] As subcategorias nas quais se divide tal espécie de risco são as seguintes: (a) agregação; (b) identificação; (c) insegurança; (d) uso secundário; e (e) exclusão.

Agregação, como classifica Daniel Solove,[89] é o risco de combinação de diversos tipos de informação relativas a uma pessoa em um mesmo ambiente de análise. É algo que sempre foi possível, mas, como ele coloca, se tornou mais fácil na era da informatização. O problema que cerca a agregação é a possibilidade de, por meio da combinação de dados (ainda que publicamente disponíveis), obter-se novas informações. Isso pode conduzir tanto a informações errôneas, a partir de dados incompletos, quanto a poder e à tomada de decisões sobre a vida do sujeito sem que ele tenha qualquer ingerência sobre a questão.

---

[86] *Ibidem,* p. 491-493.
[87] *Ibidem,* p. 501-502. Trecho do texto original: "*However, for interrogation generally, the compulsion need not be direct; nor must it rise to the level of outright coercion. Compulsion can consist of the fear of not getting a job or of social opprobrium. People take offense when others ask an unduly probing question-even if there is no compulsion to answer. One explanation may be that people still feel some degree of compulsion because not answering might create the impression that they have something to hide. This is why, I believe, there are social norms against asking excessively probing or prying questions: they make the person being questioned feel uncomfortable. Interrogation forces people to be concerned about how they will explain themselves or how their refusal to answer will appear to others*".
[88] *Ibidem*, p. 505.
[89] *Ibidem*, p. 506-511.

Identificação, a seu turno, consiste na vinculação de informações a pessoas.[90] Possui diversas utilidades, como a verificação de identidades para acesso a determinados locais ou serviços, ou a descoberta de pessoas responsáveis por atos ilícitos. Contudo, pode vincular pessoas a informações passadas, impossibilitando mudança, pode servir para finalidades discriminatórias, a depender de quais informações são vinculadas à identidade, e também pode cercear a liberdade de expressão ao inviabilizar o anonimato, nos países em que é permitido.

Insegurança,[91] por sua vez, são falhas na segurança dos dados e das informações, sob o ponto de vista tecnológico. Diz respeito aos mecanismos digitais utilizados, do qual a criptografia é exemplo. Os riscos são auto evidentes, como roubo de identidade, fraude bancária, alteração de dados, entre outros.

Uso secundário[92] diz respeito à utilização de dados para finalidades outras que não aquelas específicas para as quais eles foram coletados. Causa um sério risco de desconfiança e prejudica a dignidade dos sujeitos ao negar-lhes controle sobre suas próprias informações, além de viabilizar interpretações equivocadas decorrentes da retirada dos dados do contexto original em que foram obtidos.

Exclusão,[93] a última subcategoria dos riscos no processamento das informações, consiste na confidencialidade dos dados e das informações em relação ao sujeito, que permanece ignorante em relação à manutenção desses elementos por alguma entidade. Quanto a essa característica, causa uma falta de *accountability* por parte dos detentores dos dados, o que expõe o sujeito aos riscos descritos anteriormente, além de ocasionar graves problemas de confiança decorrentes da sensação de impotência causada por uma potencial e significativa assimetria de informações entre agentes na sociedade.

2.3.3. Disseminação de Informações

Quanto aos riscos de disseminação de informações,[94] estes subdividem-se em (a) quebra de confidencialidade; (b) divulgação; (c) exposição; (d) facilidade de acesso; (e) chantagem; (f) apropriação; e (g) distorção.

---

[90] *Ibidem*, p. 511-515.
[91] *Ibidem*, p. 517.
[92] *Ibidem*, p. 520-522.
[93] *Ibidem*, p. 523.
[94] *Ibidem*, p. 525.

O primeiro deles, a quebra de confidencialidade,[95] consiste na abertura de informações, para terceiros, por profissionais que possuem algum dever específico de sigilo, como médicos, advogados, banqueiros, entre outros. Esse tipo de risco é visto como uma violação a uma relação fiduciária: o problema não é meramente a divulgação da informação, mas a traição à confiança – voltando-se, portanto, à preservação da confiança social no sigilo decorrente de determinadas atividades.

Com respeito à divulgação,[96] esta se assemelha à preocupação de Samuel Warren que ensejou a gênese do direito à privacidade: é a divulgação pública de fatos particulares, com o consequente dano à reputação, e que pode implicar riscos à segurança ou inibir comportamentos do sujeito, além de causar uma potencial distorção ou fomentar preconceitos a partir da divulgação parcial de informações.

Por outro lado, a exposição[97] consiste na mostra, a terceiros, de atributos de uma pessoa vistos como vergonhosos ou embaraçosos – tal como nudez ou morte, por exemplo. O dano advém da publicização de situações íntimas, porém consideradas impróprias a partir de regras sociais e que, se divulgadas, possam causar humilhação, vergonha ou outros sentimentos análogos.

Já com respeito à facilidade de acesso,[98] esta consiste no incremento da facilidade com a qual dados de natureza pública se tornam acessíveis. Um bom exemplo é a divulgação indiscriminada, na internet, de autos de processos findos e em andamento. O problema, nesse aspecto, é que a facilidade de acesso incrementa os riscos decorrentes da divulgação pública de tais informações.

Em relação à chantagem,[99] definida como "coagir uma pessoa a ceder às demandas do chantageado sob a ameaça de exposição de segredos", e, na visão de Solove, é penalizada em razão da relação de poder que cria, subjugando uma pessoa à vontade de outra – e isso independe da veracidade da assertiva que fundamenta a chantagem.

Apropriação,[100] por outro lado, significa a utilização de atributos de outro em vantagem própria – como a utilização de uma foto de um artista famoso em uma propaganda sem que ele

---

[95] *Ibidem*, p. 526-527.
[96] *Ibidem*, p. 530-533.
[97] *Ibidem*, p. 536-537.
[98] *Ibidem*, p. 539-540. No que tange a processos judicias, por exemplo: a divulgação, na internet, de cópia dos autos torna o endereço de pessoas facilmente identificável e seu patrimônio, a depender da natureza da informação. Isso facilita, por exemplo, o trabalho de um assaltante. Nesse sentido, dados públicos não teriam um tratamento binário (público/privado), mas o *quão* público ou o *quão* privado passa a se tornar um ponto relevante de debate.
[99] *Ibidem*, p. 542-543. Tradução livre. Texto original: "*Blackmail involves coercing and individual by threatening to expose her personal secrets if she does not accede to the demands of the blackmailer*".
[100] *Ibidem*, p. 546-548.

consinta. A despeito da controvérsia sobre se o dano vem da afronta à dignidade ou aos direitos de propriedade, Solove sustenta existir uma violação à liberdade e ao desenvolvimento pessoal decorrente de se *usar* uma pessoa contra sua vontade, alterando a forma pela qual ela se apresenta à sociedade.

Distorção,[101] por fim, consiste na manipulação da forma pela qual uma pessoa é percebida pela sociedade. Apresenta os mesmos riscos de dano que a divulgação, mas dela difere porque, na distorção, a informação é falsa, destruindo ou comprometendo a reputação de alguém.

2.3.4. Invasão

A última das categorias que Solove estabelece em sua taxonomia é a invasão[102], cujas subdivisões são (a) intrusão; e (b) interferência decisional. A intrusão seria o intrometimento na vida das pessoas[103], violando seu direito de ser deixado em paz – cujos danos potenciais já foram explorados por Warren e Brandeis e indicados no capítulo anterior. A interferência decisional,[104] por derradeiro, consistiria na indevida intromissão de terceiros no âmbito das decisões que uma pessoa toma para sua própria vida. Solove indica que esse tipo de risco agrega espécies de danos decorrentes de vários dos demais, de modo que realizar detalhamento, aqui, seria excessivo. Não obstante, os problemas decorrentes de indevida intromissão do Estado nas decisões privadas é bastante auto evidente.

2.3.5. Importância da Taxonomia

Como mencionado no início deste subtópico, a taxonomia de Daniel Solove tem por objetivo criar palavras, termos e expressões dotadas de significado próprio no âmbito das discussões relativas à privacidade *lato sensu*. No caso, ele o faz com respeito aos diferentes tipos de riscos existentes à privacidade – que, como se viu, são muitos.

É nesse cenário que o subtópico seguinte utilizará a nomenclatura explicada acima para, em cada caso, exemplificar quais desses riscos podem advir da massificação do uso de dados com maior ou menor facilidade, a partir das ponderações de Seth Stephens-Davidowitz.

---

[101] *Ibidem*, p. 550-551.
[102] *Ibidem*, p. 552.
[103] *Ibidem*, p. 553.
[104] *Ibidem*, p. 557-

2.4. Classificação de Stephens-Davidowitz

Em sua obra "Todo Mundo Mente", Seth Stephens-Davidowitz exemplifica, de modo prático, as utilizações que tais dados podem ter, o que faz por meio de suas classificações dos quatro poderes do Big Data.

Neste tópico, partiremos dos exemplos concretos do autor, para cada um dos poderes por ele descritos, no intuito de exemplificar formas de desvirtuamento do uso dos dados, os quais consistiriam nos riscos decorrentes da atividade dos comunicadores fiduciários – tanto de modo coletivo, quanto de modo individual.

Em seguida, iremos comparar de que forma os perigos antecipados pela academia decorrentes de riscos à privacidade e à proteção de dados mostraram-se – ou não – justificados.

2.4.1. Acesso a novos tipos de dados

O primeiro "poder" apresentado pelo autor[105] é o que ele conceitua como o oferecimento de novos tipos de dados (e, portanto, de informações) a quem quer que seja que venha, eventualmente, a utilizá-los.

Uma explicação de Stephens-Davidowitz, que sintetiza um bom exemplo dos novos dados disponibilizados por meios digitais, diz respeito ao diferencial do sistema de buscas do Google:

> "O que os fundadores do Google, Sergey Brin e Larry Page fizeram de diferente?
> Outros mecanismos de busca localizavam para seus usuários os sites que continham mais ocorrências da frase pela qual buscaram. Se estivesse procurando por informação sobre "Bill Clinton", aqueles mecanismos de busca encontrariam, pela internet inteira, os sites que continham mais ocorrências para Bill Clinton. Havia muitos motivos para esse sistema de classificação ser imperfeito, e um deles era o fato de ser muito fácil manipulá-lo. Um site de piada com o texto "Bill Clinton Bill Clinton Bill Clinton Bill Clinton Bill Clinton" Escondido em algum lugar de sua página seria mais bem classificado do que o site oficial da Casa Branca.
> O que Brin e Page fizeram foi encontrar uma forma de registrar um novo tipo de informação muito mais valiosa do que uma mera contagem de palavras. Sites normalmente, ao discutir um assunto, criam links para sites que entendem ser mais úteis para o entendimento do assunto. Por exemplo, o *New York Times*, se mencionasse Bill Clinton, poderia permitir que os leitores clicassem no nome para ser direcionado para o site oficial da Casa Branca.
> Cada site criando esses tipos de links estava, de certa forma, fornecendo uma opinião sobre onde encontrar a melhor informação sobre Bill Clinton. Brin e Page conseguiram reunir todas essas opiniões sobre todos os assuntos. Isso permitiu processas as opiniões do *New York Times*, milhões de Listservs, centenas de bloggers e todo o restante da internet. Se todo um grupo de pessoas pensasse que o link mais

[105] STEPHENS-DAVIDOWITZ, Seth. **Todo mundo mente: o que a internet e os dados dizem sobre quem realmente somos**. Trad. Wendy Campos. Rio de Janeiro: Alta Books, 2018.

> importante para "Bill Clinton" fosse o seu site oficial, esse provavelmente seria o site que a maioria das pessoas buscando por "Bill Clinton" gostaria de visualizar.
> Esses tipos de links eram dados que outros mecanismos de busca ignoravam, mas que eram incrivelmente preditivos sobre a informação mais útil sobre determinado tópico".

O sucesso do *Google* derivou de um novo tipo de dado que, a partir das inovações tecnológicas ocorridas a partir dos anos 1990, tornou-se acessível: as opiniões e as referências das pessoas.

No entanto, não é propriamente correto afirmar que tais dados se tornaram disponíveis somente com o advento e popularização da internet: evidentemente, o ser humano emite opiniões sobre tudo e todos desde os primórdios da civilização, assim como as referências em trabalhos acadêmicos, jornais e escritos de modo geral há séculos.

A mudança, na realidade, foi mais quantitativa do que qualitativa. Existem muito mais opiniões registradas (e acessíveis ao público) no ambiente virtual do que jamais existiu ao longo da história humana.

Warren e Brandeis[106] reclamaram da fofoca em jornais escritos, em tabloides de grande circulação, afirmando que violariam a privacidade dos cidadãos. Mas, nos Estados Unidos dos anos 1890, a quantidade de fofoca escrita era, sem sombra de dúvidas, infinitamente menor do que a que se tem hoje. E passava por filtros editoriais de seus veículos de propagação.

Por outro lado – e mantendo o exemplo da fofoca, que tanto incomodou Samuel Warren – os aparelhos de celulares, especialmente os aplicativos de mensagens, estão repletos de informações pessoais – e todos conectados à internet. Enquanto que, em 1890, para saber de fofocas relacionadas a um casamento da *high society* (e vazá-las) era necessário comparecer ao casamento, ou obter diretamente a informação a partir de alguém que compareceu. Isto se torna desnecessário no contexto tecnológico atual, ao menos em tese.

Os denominados *keyloggers*[107] são *softwares* que registram as teclas pressionadas em um aparelho eletrônico, principalmente um computador. Geralmente é um vírus de computador, o qual pode ser combatido por *softwares* antivírus. E, a princípio, desenvolvedoras de *softwares* instalam *keyloggers* "de fábrica" nos computadores de clientes. Se fazem, certamente não assumem.

No entanto, como garantir que, por meio de uma simples linha de código, a desenvolvedora do *software* não está bisbilhotando tudo o que seus usuários digitam? Neste

---

[106] WARREN, Samuel D.; BRANDEIS, Louis D. *The Right to Privacy.* ***Harvard Law Review***, Cambridge, vol. 4, n. 5, 1890. P. 196.

[107] KASPERSKY. **O que é keylogger?** Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/keylogger>. Acesso em: 11 de junho de 2021.

ponto, deve-se diferenciar *softwares* de código aberto e de código fechado, assim feito por Carla Michler:[108]

> "Um *software* é, em termos amplos, constituído por dois elementos, notadamente o "código fonte" e o "código objeto". O "código fonte" e o "código objeto" referem-se às versões "antes" e "depois" de um programa de computador que é compilado antes de estar pronto para rodar em um computador. O código fonte consiste em um grupo de frases de programação legíveis por humanos que são criadas por um programador com um editor de texto ou uma ferramenta de programação visual e salvas em um arquivo. O código fonte não pode ser executado por si só por um computador, mas é compilado com um programa especial chamado compilador, e o arquivo compilado de saída é frequentemente denominado de "código objeto". O código objeto consiste em uma sequência de instruções que o microprocessador do computador pode entender, mas que é difícil para um humano ler ou modificar.
> Em um modelo de *software* "código fechado" ou "proprietário", o vendedor do *software* retém o código fonte e vende ou licencia somente o código objeto componente do programa para os usuários do *software*. Sob os termos das licenças de código fechado, os usuários do *software* podem rodar o código objeto, mas não podem ver ou modificar o código fonte e, portanto, modificar o comportamento do programa sem se consultar com os vendedores do *software*. Nesse modelo de código fechado, o código fonte somente pode ser definido por meio de recompilação ou engenharia reversa, embora recompilação e engenharia reversa do código objeto seja frequentemente proibida pelos termos de licença de códigos fechados. Como consequência, o usuário pode apenas utilizar o que quer que seja a ele fornecido pelo vendedor do *software*, junto de eventuais modificações que eles possam fazer o vendedor do *software* incorporar. O modelo de código fechado continua a ser usado pela maioria das empresas desenvolvedoras de *softwares* comerciais e é o modelo de *software* mais comum adotado tanto pelo setor público, quanto pelo setor privado.
>
> *Softwares* de código aberto são baseado em um rol de princípios fundamentalmente distintos daqueles em que se baseiam os *softwares* de código fechado e dão aos usuários uma liberdade muito maior em relação ao modo com o qual eles lidam com o *software*. Em termos gerais, *softwares* de código aberto são *softwares* onde o código fonte é livremente distribuído e está amplamente disponível para os usuários de modo a ser usado, copiado, modificado e redistribuído. *Softwares*

[108] MICHLER, Carla. *The Procurement Decision – Open or Closed Source Software.* ***Deakin Law Review*****,** v. 10, n. 1, 2005, p. 261-270. Tradução livre. Texto original: "*In order to appreciate the differences between 'open' and 'closed' source software it is necessary to understand what actually constitutes 'software'. Software is, in broad terms, constituted by two elements, namely the 'source code' and the 'object code'. The 'source code' and the 'object code' refer to the 'before' and 'after' versions of a computer program that is compiled before it is ready to run in a computer. The source code consists of a set of human readable programming statements that are created by a programmer with a text editor or a visual programming tool and then saved in a file. The source code cannot itself be executed by a computer but is compiled with a specialised program called a compiler and the resulting output, the compiled file, is often referred to as the 'object code'. The object code consists of a sequence of instructions that the computer's microprocessor can understand but that is difficult for a human to read or modify. In a 'closed source' or 'proprietary' software model, software vendors retain the source code and sell or licence only the object code component of the program to the software users. Under the terms of the closed source licences, software users are permitted to run the object code but cannot view or modify the source code and, hence, modify the behaviour of the program without consulting with the software vendors. In this closed source model the source code can only be ascertained through recompilation or reverse engineering, however recompilation or reverse engineering of the object code is commonly prohibited by closed source licence terms. As a result, the user can only use whatever is provided to them by the software vendor, along with any modifications that they could prevail upon the software vendor to incorporate. The closed source model continues to be used by the majority of commercial software companies and is the most common software model adopted by both the private and public sector. Open source software is based on a set of fundamentally different principles than closed source software and provides users with a greater freedom in the way in which they deal with the software. In general terms, open source software is software where the source code is freely distributed and widely available to users so it may be used, copied, modified and redistributed.' Open source software is licensed with certain common restrictions which generally differ from closed source software. Frequently, open source licenses require users who distribute open source software, whether in its original form or as modified, to make the source code widely available*".

> de código aberto são licenciados com certas restrições comuns que geralmente diferem daquelas dos *softwares* de código fechado. Frequentemente, licenças de código aberto requerem que usuários que distribuem *softwares* de código aberto, quer na sua forma original, quer modificados, façam o código fonte amplamente disponível".

Em *softwares* de código aberto, pessoas com conhecimento técnico adequado podem verificar o que é processado por conta própria. Os leigos, por outro lado, precisam confiar em quem possui tal conhecimento. Nos de código fechado, entretanto, nem técnicos, nem leigos possuem meios para saber todas as nuances do *software* utilizado. Ou seja, retomando o exemplo anterior: em um *software* de código fechado é impossível, para a maior parte da população, saber se o desenvolvedor embutiu de fábrica, ou não, uma linha de código que faça as vezes de um *keylogger*.

Tem-se, dessa forma, um cenário no qual o comunicador fiduciário pode salvar *mais* dados, mas, paradoxalmente, o usuário não possui meio *nenhum* para saber *quais* dados (ou metadados) são esses. E, se o usuário não sabe quais são os dados, ele fica completamente ignorante quanto às informações que o comunicador fiduciário possui em relação a ele.

Os riscos que daí decorrem podem ser categorizados, sinteticamente, em duas categorias: (*i*) riscos públicos; e (*ii*) riscos particulares. Ambos, como se verá, são variações sobre o mesmo tema, uma vez que consistem no abuso da fidúcia. A diferença reside, somente, na natureza do abusador e no que ele pode fazer com a informação. Enquanto um particular pode usar a informação para, por exemplo, levar um concorrente à falência, ou revelar um caso extraconjugal de um desafeto por pura inimizade, o setor público, valendo-se destas mesmas informações, pode perseguir dissentes, prender opositores, armar golpes de Estado e cometer genocídio.

Em artigo[109] anônimo publicado no portal *Medium*, em 8 de janeiro de 2021, o autor discute a já mencionada política de dados do *WhatsApp*, mencionando a alegada criptografia ponta-a-ponta implementada pela empresa.

No decorrer do artigo, contudo, o autor chama a atenção para dois pontos fundamentais: a criptografia ponta-a-ponta protege as *mensagens* contra invasores *externos*. Não há proteção contra invasores externos[110] e a proteção limita-se ao conteúdo das mensagens, sem qualquer garantia de resguardo da privacidade quanto aos metadados – os quais, como se viu, têm o

---

[109] MAGNET, Pen. *WhatsApp Doesn't Read Your Messages, It Doesn't Need To.* ***Medium*****,** 8 de janeiro de 2021. Disponível em: <https://medium.com/swlh/whatsapp-doesnt-read-your-messages-it-doesn-t-need-to-7ce0ec2846f9>. Acesso em: 11 de junho de 2021.

[110] O autor coloca, com certa dose de ironia nas palavras, que o WhatsApp considera seu próprio servidor "sacrossanto".

potencial de fornecer informações tão particulares quanto os dados em comento. Quanto ao armazenamento do conteúdo das mensagens, aduz o autor:[111]

> "É altamente improvável que ele [Whatsapp] tenha armazenado mensagens. A razão não é a privacidade, mas a capacidade de servidores e a largura de banda, as quais tem relação direta (às vezes não-linear) com custos excessivos.
> Que companhia pagaria uma fortuna para a nuvem, somente para armazenar petabytes de **Olás** e **Saudades** escritos pelos usuários, somente para incorrer em processos judiciais devastadores sobre privacidade?
> Para tornar economicamente viável o armazenamento de mensagens dos usuários, seria preciso criar um serviço dedicado de mensagens utilizado somente por bilionários.
> O que importa para os usuários do WhatsApp é a informação no fundo: **Conexões.** Eles não dizem que não as armazenam, e nunca disseram isso, creio eu. E estava tudo OK porque isso nunca havia sido monetizado (ao menos não publicamente).
> Agora, com a divulgação, suas conexões do WhatsApp, tal qual seus amigos do Facebook, são propriedade do Facebook.
> WhatsApp sempre registra suas mensagens e telefonemas. Se você deletar suas mensagens de texto, ele ainda assim registra o *timestamp* da mensagem. Isso significa que sua mensagem nunca vai sem ser deixar rastros..".

Além desses elementos, destaca[112] que outro serviço do *Facebook*, o *Facebook Messenger*, pode ler as mensagens do *WhatsApp* em razão de uma funcionalidade no sistema iOS, da Apple, decorrente do fato de que *Facebook* e *WhatsApp* são aplicativos pertencentes à mesma organização – embora ressalte o autor que isso é uma mera possibilidade, e que não está afirmando que o *Facebook Messenger* efetivamente faz isso.

De qualquer maneira, esses são dados novos, que, no atual contexto tecnológico, o comunicador fiduciário passa a deter: a lista de contatos e os relacionamentos pessoais dos usuários.

O problema, aqui, mostra-se importante sob a perspectiva do Big Data: rastrear comunicações pode permitir identificar usuários socialmente mais "relevantes", líderes comunitários, através da análise do fluxo de informações. Somando-se a informação sobre os fluxos de comunicação a uma potencial leitura do conteúdo das mensagens, tem-se que uma

---

[111] Tradução livre. Texto original: "*It's highly unlikely it ever stored message content. The reason is not privacy but server + bandwidth capacity which is directly (sometimes nonlinearly) coupled with cost overruns. Which company will pay a fortune to the cloud, only to store petabytes of user's **Hellos** and **Miss Yous**, only to get into devastating privacy lawsuits? To make it economically viable to store users' messages, one has to create a dedicated messenger used by billionaires only. What matters to users of WhatsApp is the information at the bottom: **Connections.** It doesn't say it doesn't store them, and it never said so, I believe. And it was OK because it was (at least publicly) never monetized. Now, with the disclosure, your WhatsApp connections, just like your Facebook friends, is the property of Facebook. WhatsApp always stores your message and call logs. If you delete your text message, it still stores the message timestamp. This means that your communication never goes untraced*".

[112] MAGNET, Pen. *WhatsApp Doesn't Read Your Messages, It Doesn't Need To.* ***Medium*****,** 8 de janeiro de 2021. Disponível em: <https://medium.com/swlh/whatsapp-doesnt-read-your-messages-it-doesn-t-need-to-7ce0ec2846f9>. Acesso em: 11 de junho de 2021.

empresa na posse de tais dados pode conseguir convertê-los em informação que permita, por exemplo, identificar concorrentes ou tentativas de greve de funcionários.

Essas mesmas informações, nas mãos do poder público, podem servir para reprimir manifestações, perseguir opositores, identificar líderes de movimentos sociais, e, de modo geral, reprimir quem se oponha ao *establishment*.

Sob outra perspectiva, é preocupante o risco de *identificação de indivíduos* decorrente do uso de tais dados. Isso porque, naturalmente, pessoas pertencentes a determinados grupos tendem a se comunicar mais, e a religião é um bom exemplo: é possível identificar muçulmanos por meio dos *timestamps*, eis que, nos horários do Salá, naturalmente haverá redução no uso de aplicativos de mensagens com certa regularidade. Judeus podem ser identificados a partir dos contatos regulares realizados por um Rabino conhecido. Católicos, em virtude da atividade nos feriados de Páscoa e Natal.

Sob a ótica individual, o problema é praticamente idêntico, com a diferença de que as informações terão por objeto alvos pré-determinados. Uma empresa pode, por exemplo, monitorar o Presidente da concorrente e realizar espionagem industrial, ou descobrir um caso extraconjugal de um alto executivo e chantageá-lo – e medidas idênticas, ou análogas, podem também ser adotadas por autoridades públicas contra opositores, cerceando a liberdade de expressão e a democracia por meio da violação à privacidade dos indivíduos decorrente do acesso a novos tipos de dados.

2.4.2. Honestidade dos dados

Em um segundo momento,[113] Stephens-Davidowitz aponta que os dados disponíveis têm outra vantagem fundamental: eles são *honestos* – seja por "dolo", seja por "culpa" dos usuários dos sistemas.

Isso ocorre porque as pessoas, mesmo quando garantido o anonimato, tendem a exagerar as próprias virtudes e a reduzir os próprios defeitos – ainda que inconscientemente, o que podem fazer, por exemplo, por questões de autoimagem.[114] Assim explica Stephens-Davidowitz:

---

[113] STEPHENS-DAVIDOWITZ, Seth. **Todo mundo mente: o que a internet e os dados dizem sobre quem realmente somos**. Trad. Wendy Campos. Rio de Janeiro: Alta Books, 2018.

[114] Stephens-Davidowitz menciona estudo conduzido com graduandos da Universidade de Maryland no qual menos de 2% (dois por cento) alegam terem se formado com média inferior a 2,5 e 44% (quarenta e quatro por cento) afirmaram ter doado dinheiro para a Universidade – enquanto os dados oficiais são, respectivamente, 11% (onze por cento) e 28% (vinte e oito por cento). STEPHENS-DAVIDOWITZ, Seth. **Todo mundo mente: o que a internet e os dados dizem sobre quem realmente somos**. Trad. Wendy Campos. Rio de Janeiro: Alta Books, 2018, p. 106-107.

> "Por que as pessoas omitem informações em pesquisas anônimas? Perguntei a Roger Tourangeau, pesquisador emérito da Universidade de Michigan e talvez o maior especialista do mundo em desvio de desejabilidade social. "Nossa inclinação para as 'mentiras brancas' é uma importante parte do problema", explicou Tourangeau. "Cerca de um terço do tempo, as pessoas mentem na vida real. Esse hábito é transferido para as pesquisas."
> Além disto, às vezes temos o estranho hábito de mentir para nós mesmos. "Existe uma relutância em admitir para si mesmo que, digamos, fomos um fracasso como alunos", diz Tourangeau.
> [...]
> Entretanto, em assuntos delicados, todos os métodos de pesquisa evocarão uma quantidade substancial de informação incorreta. Tourangeau usou aqui uma palavra que é frequentemente empregada por economistas: incentivo. As pessoas não têm qualquer incentivo para dizer a verdade.
> Como, então, podemos aprender o que nossos colegas seres humanos estão realmente pensando ou fazendo?
> Em alguns casos, existem fontes de dados oficiais que podemos consultar para obter a verdade. Mesmo que as pessoas mintam sobre as doações para caridade, por exemplo, podemos conseguir os números reais de doação em determinada região das próprias entidades. Mas quando tentamos conhecer comportamentos que não são listados em registros oficiais ou descobrir o que as pessoas pensam – suas verdadeiras crenças, sentimentos e desejos –, não há outra fonte de informação, exceto o que as pessoas se permitem dizer nas pesquisas. Isto é, até agora.
> Este é o segundo poder do Big Data: determinadas fontes online conseguem fazer com que as pessoas admitam coisas que não admitiriam em nenhum outro lugar. Elas agem como um soro digital da verdade. Pense nas buscas do Google. Lembre-se das condições que tornam as pessoas mais honestas. Online? Sim. Sozinha? Sim. Ninguém conduzindo a pesquisa? Sim.
> E há outra imensa vantagem que as buscas no Google têm em fazer as pessoas dizerem a verdade: incentivos. Se você gosta de piadas racistas, tem zero incentivo de compartilhar este fato politicamente incorreto em uma pesquisa. No entanto, existe um incentivo para buscar novas piadas racistas online. Se pensa que pode estar sofrendo de depressão, não tem incentivo algum para admitir isso para uma pesquisa. Mas sim para perguntar ao Google sobre os sintomas e potenciais tratamentos.
> Mesmo que esteja mentindo para si mesmo, ainda assim o Google pode saber a verdade. Alguns dias antes da eleição, você e seus vizinhos poderiam legitimamente achar que compareceriam à seção de votação para votar. Mas se você ou eles não buscaram qualquer informação sobre como ou onde votar, cientistas de dados como eu podem estimar que a taxa de comparecimento em sua região será baixa. Da mesma forma, talvez você não tenha admitido sequer para si mesmo que sofre de depressão, mesmo fazendo buscas no Google sobre crises de choro e dificuldades de sair da cama. Entretanto, você apareceria nas buscas relacionadas à depressão de determinada região, analisadas anteriormente neste livro".

Embora Stephens-Davidowitz foque seu trabalho nas pesquisas do *Google*, os comunicadores fiduciários podem ter acesso a dados ainda mais particulares ou específicos, especialmente quando se tratar de comunicação não criptografada (e lembrando que, frequentemente, o usuário não tem muita opção a não ser acreditar que a criptografia existe, e que, além de existir, é eficaz).

Um estudo de Matthew Gentzkow, Jesse Shapiro e Matt Taddy mencionado por Stephens-Davidowitz identifica palavras e expressões mais associadas a políticos Democratas

ou Republicanos[115] a partir de discursos realizados no Capitólio em 2005. Democratas tenderiam mais a falar em "imposto imobiliário" e "Rosa Parks", ao passo que Republicanos utilizavam mais as expressões "imposto 'de morte'" e "Saddam Hussein".

Os autores que embasaram a assertiva de Stephens-Davidowitz, Matthew Gentzkow e Jesse Shapiro, uniram-se a Matt Taddy e realizaram novo estudo[116], publicado em julho de 2019 na Econometrica, aprofundando os estudos – e no qual constatam que houve uma segregação relevante no modo como Democratas e Republicanos falam a partir da década de 1990:

> "Em 1874, um observador escutando tal espécie de discurso esperaria ter uma chance de aproximadamente 0.54 de deduzir corretamente o partido a que pertencia o orador, muito pouco acima do 0.5 anterior. Em 1990, esse valor havia subido ligeiramente, para 0.57. Entre 1990 e 2008, no entanto, saltou para 0.73".

Os autores fornecem, também, uma informação bastante relevante ao comparar a expectativa de acerto da posição política do orador, ao longo dos séculos, quando a estabelecem em função do tempo de discurso (e número de frases). Com um horizonte de 100 (cem) frases, o que daria algo em torno de 3 (três) minutos de fala, a taxa de acerto do partido do orador, em 2007-2008, alcançaria espantosos 90% (noventa por cento), contra pouco menos de 60% (sessenta por cento) no Congresso estadunidense de 1873-1874, e pouco menos de 70% (setenta por cento) no de 1989-1990. Isso tudo com base em uma análise sistematizada das palavras utilizadas nos discursos de políticos.

Se, em um discurso de 3 (três) minutos, com 100 (cem frases), já é possível identificar, na contemporaneidade, a vinculação político-ideológica de uma pessoa com 90% (noventa por cento) de precisão, quanto mais verdade isso não é a partir da análise de dias, meses, anos e décadas de mensagens postadas em redes sociais, conversas por meio de aplicativo, mensagens de texto ou até mesmo análise de áudios por meio de *softwares* que os convertam em textos.

E, se isso serve para a política, também serve para a religião, orientação sexual, ou para coisas mais simplórias, como uma preferência por vinhos alentejanos em detrimento dos oriundos de Bordeaux, ou um gosto acentuado por funk carioca que se contrapõe a um desgosto por pagode, música sertaneja ou Bossa Nova.

---

[115] GENTZKOW, Matthew; SHAPIRO, Jesse; TADDY, Matt. *Measuring Polarization in High-Dimensional Data: Method and Application to Congressional Speech*. ***Stanford Institute for Economic Policy Research*****.** *Working Paper*, 2016.

[116] GENTZKOW, Matthew; SHAPIRO, Jesse; TADDY, Matt. *Measuring Group Differences in High-Dimensional Choices: Method and Application to Congressional Speech*. ***Econometrica*****,** v. 87, n. 4, 2019, p. 1307-1340. Citação em tradução livre. Texto original: "*In 1874, an observer hearing such a speech would expect to have a posterior of around 0.54 on the speaker's true party, only slightly above the prior of 0.5. By 1990, this value increased slightly to 0.57. Between 1990 and 2008, however, it leaped up to 0.73*".

Em um primeiro momento, mostra-se razoavelmente difícil imaginar motivos que a maioria das pessoas consideraria relevantes para que alguém esconda seu gosto musical ou sua bebida predileta (mais sobre isso adiante). Não obstante, é um direito da pessoa manter tais informações reservadas se assim desejar, sem revelá-las a terceiros, por quaisquer motivos que lhe aprouver – privacidade, afinal, significa exatamente isso, como expusemos anteriormente. Com religião ou orientação sexual, por outro lado, já é possível vislumbrar uma maior sensitividade da questão.

De toda sorte, ao longo da vida, essas preferências invariavelmente deixarão registros: despesas com cartões de crédito, localizações geográficas, pessoas com as quais se comunica, pesquisas no *Google* – e, tudo isso, fica ao alcance dos comunicadores fiduciários.

Durante o Macarthismo,[117] uma pessoa poderia simplesmente optar por, quando questionada, mentir e negar ser comunista. Hoje, sua compra d'O Manifesto Comunista na Amazon, registrada por tempo indefinido, poderia entregá-la. No Nazismo,[118] um judeu poderia afirmar-se católico para escapar à perseguição e ao horror do Holocausto. Mas, contatos telefônicos frequentes e históricos com um conhecido Rabino poderiam revelá-lo.

É "fácil" mentir por um dia, uma semana, um mês, ou, até mesmo, um ano. Por outro lado, é impossível mentir por uma vida inteira. E, em vários casos, as pessoas tem razões legítimas para mentirem. A comunicação fiduciária, entretanto, fragiliza por completo essa possibilidade de autopreservação.

Os dados, como indica o título deste subtópico, são honestos, em razão, principalmente, da quantidade e da variedade que é coletada, somada à duração da coleta. Uma pessoa pode afirmar publicamente que ama sua esposa, mas traí-la às escondidas. Dados georreferenciais dos aparelhos celulares, bem como contatos telefônicos, certamente podem denunciar as aventuras amorosas. Isso pode configurar um problema atinente exclusivamente às pessoas envolvidas. Mas, dependendo do contexto, relacionamentos amorosos podem ter repercussões gigantescas. Bill Clinton e Monica Lewinsky que o digam.

Em síntese, o fato é que, com a proliferação de intermediários digitais nas relações humanas, saber com precisão o que as pessoas fizeram no verão passado, ou o que pensam e fazem na intimidade de sua vida, com segurança, tornou-se mais fácil do que nunca.

---

[117] Período na história estadunidense, ao longo dos anos 1950, caracterizado por extensa perseguição a comunistas, capitaneadas pelo Senador Joseph McCarthy. ACHTER, Paul J. McCarthyism. **Britannica.** Disponível em: <https://www.britannica.com/topic/McCarthyism>. Acesso em: 12 de junho de 2021.

[118] Mais adiante, como se verá, as políticas nazistas causaram trauma na sociedade alemã quando da realização de censo da população na década de 1980.

Hoje, cidadãos mais preocupados com sua privacidade recorrem a meios alternativos, como o uso de aplicativos de mensagens como o Signal, mencionado anteriormente, ou navegadores como o Tor.[119] Entretanto, tais medidas são utilizadas por poucos usuários. O Chrome, navegador da Google, por exemplo, detém um espantoso *market share* de 70% (setenta por cento) dos usuários de internet a nível global.[120]

A honestidade dos dados, além disso, é aprofundada pela *ignorância* dos usuários, os quais simplesmente não sabem quais são os seus dados que estão sendo coletados, e, por isso, não se preocupam em protegê-los. Em 2013, por exemplo, um homem foi interrogado pela polícia[121] em razão de suas pesquisas, no *Google*, por bombas similares àquelas utilizadas no então recente atentado à bomba na maratona de Boston, ocorrido em abril daquele ano.

Certamente, tal homem, quando pesquisou por tais informações – às vezes, por mera curiosidade – nem sequer poderia imaginar que seus dados de pesquisa estariam sendo registrados, e, posteriormente, seriam utilizados contra ele. Afinal, caso vislumbrasse o que de fato ocorreu como uma possibilidade real, muito provavelmente não teria feito o que fez.

O mesmo se aplica a outras formas de interação humana que envolvem comunicadores fiduciários. Quando se fala em aplicativos de mensagens, a tendência da preocupação é com a leitura das mensagens, como o histórico da evolução da política de privacidade do *WhatsApp* demonstrou: os dados propriamente ditos é que são o foco.

Mas, como visto, o "ouro digital" não é o conteúdo das conversas em si, mas as pessoas com as quais se conversa. O metadado. E, justamente por frequentemente não saber quais são os metadados coletados (ou nem sequer saber que existem) é que a pessoa não se protege contra eles – e é por isso que os dados digitais coletados no século XXI são tão honestos, e, consequentemente, tão úteis. E é isso que os faz perigosos.

Desse modo, e resumidamente, o fato é que a ilusão de anonimato na internet, somada ao desconhecimento dos dados efetivamente coletados, gera, no usuário, uma sensação de segurança, liberdade, anonimato e, portanto, privacidade. O resultado disso é um comportamento mais honesto e pouco enviesado por parte dos usuários que, por meio de usos

---

[119] Software destinado à navegação na internet que, por meio de mecanismos de segurança, garante com razoável segurança o anonimato dos usuários na internet. **Tor Project.** Disponível em: <https://www.torproject.org/>. Acesso em: 12 de junho de 2021.

[120] DE VYNK, Gerrit. Google is totally changing how ads track people around the Internet. Here's what you need to know. **The Washington Post,** 18 de junho de 2021. Disponível em: <https://www.washingtonpost.com/technology/2021/06/18/google-is-totally-changing-how-ads-track-people-around-internet-heres-what-you-need-know/>. Acesso em: 18 de junho de 2021.

[121] **NBC News.** Man questioned by police for Google search history. 1º de Agosto de 2013. Disponível em: <https://www.nbcnews.com/technolog/man-questioned-police-google-search-history-6c10824803>. Acesso em: 14 de junho de 2021.

secundários no futuro, por exemplo, pode os prejudicar de maneiras absolutamente impensáveis.

Georges Bernanos,[122] ainda em 1947, tinha um alerta extremamente pertinente a esse respeito, quando afirma que, a princípio, só o criminoso levaria vantagem em esconder-se. O problema, contudo, é que o conceito de criminoso pode se expandir – e muito. E a honestidade de dados do passado, mantida registrada, pode servir, por exemplo, para viabilizar uma autoincriminação posterior em um contexto de perseguição. Afinal, como poderia um cidadão afirmar que não se filia a determinada corrente política, ou que não lhe é simpático, se, nos dez anos anteriores, seu cartão de crédito registrou doações mensais a entidades sabidamente vinculadas a tal pensamento?

2.4.3. Diferenciação dos dados

O terceiro poder dos dados, conforme Seth Stephens-Davidowitz,[123] é a possibilidade de diferenciação decorrente do excessivo volume de dados, o que permite analisar subconjuntos desses dados para, então, extrair conclusões com segurança.

Dois exemplos do autor são a escolha do time de beisebol dos estadunidenses e a preferência política. A partir de quantidades massivas de dados, ele pôde realizar setorizações e descobrir que há uma tendência na população masculina de torcer para o time de beisebol que foi campeão quando o indivíduo tinha oito anos de idade, assim como há uma correlação entre a filiação política dos indivíduos e a popularidade (ou sua falta) do partido Republicano ou Democrata aos dezoito anos de idade do indivíduo.[124]

No entanto, a principal capacidade desse terceiro poder é a formação de *dúplices*. Eis o que são explicados a partir do caso de David Ortiz, jogador de beisebol:[125]

> "Então, em 2003, o estatístico Nate Silver introduziu um novo modelo, que batizou de PECOTA, para prever o desempenho de um jogo. Ele se mostrou o melhor – e, também, o mais arrojado de todos. Silver procurou por dúplices de jogadores. Funciona da seguinte forma: crie uma base de dados de todos os jogadores da Liga

[122] BERNANOS, Georges. **A França contra os robôs.** Trad. Lara Christina de Malimpensa. 1ª ed. São Paulo: É Realizações, 2018 [1947]. P. 33.
[123] STEPHENS-DAVIDOWITZ, Seth. **Todo mundo mente: o que a internet e os dados dizem sobre quem realmente somos**. Trad. Wendy Campos. Rio de Janeiro: Alta Books, 2018, p. 170.
[124] STEPHENS-DAVIDOWITZ, Seth. **Todo mundo mente: o que a internet e os dados dizem sobre quem realmente somos**. Trad. Wendy Campos. Rio de Janeiro: Alta Books, 2018, p. 166: "Mais uma vez, vemos que o ano mais importante na vida de um homem, para efeito de sedimentar sua preferência por determinado time de beisebol quando adultado, é aquele em que ele tem mais ou menos 8 anos", e p. 169: "Com todos esses dados, os pesquisadores foram capazes de determinar um único ano crucial para o desenvolvimento das visões políticas: os 18 anos".
[125] STEPHENS-DAVIDOWITZ, Seth. **Todo mundo mente: o que a internet e os dados dizem sobre quem realmente somos**. Trad. Wendy Campos. Rio de Janeiro: Alta Books, 2018, p. 198-199.

> Principal de Beisebol de todos os tempos, são mais de 18 mil homens. E inclua tudo que você sabe sobre eles: altura, idade, posição, médias de *home runs*, de rebatimento, *walks* e *strikeouts* para cada ano de suas carreiras. Agora, encontre os vinte jogadores que mais se pareçam com Ortiz até aquele momento de sua carreira – aqueles que jogaram como ele quando tinha 24, 25, 26, 27, 28, 29, 30, 31, 32 e 33 anos. Em outras palavras, encontre seus dúplices e depois veja como foram suas carreiras.
> Uma busca por dúplice é outro exemplo de foco. Ela se concentra em um pequeno subconjunto de pessoas mais parecidas com determinada pessoa. E, assim como todo foco, quanto mais dados, melhor. Ocorre que os dúplices de Ortiz ofereceram uma previsão muito diferente para o futuro de Ortiz. Seus dúplices incluíam Jorge Posada e Jim Thorne. Esses jogadores começaram suas carreiras mais devagar; tiveram explosões fantásticas aos vinte e tantos anos, com potencial para elite, e declinaram logo após os trinta.
> Silver então previu como Ortiz se sairia com base nos resultados de seus dúplices. E descobriu que eles recuperaram o poder. Para as esposas troféus, Simmons pode estar certo: quando despencam, despencam de uma vez. Mas para os dúplices de Ortiz, quando despencaram, recuperaram a forma.
> A busca por dúplices, a melhor metodologia usada para prever o desempenho de jogadores de beisebol, mostrou que o Red Sox deveria ter paciência com Ortiz. E o time, de fato, foi muito paciente com seu jogador "maduro". Em 2010, a média de Ortiz subiu para .270. Ele acertou 32 *home runs* e chegou ao time All-Star. Esse foi o primeiro de uma sequência de 4 jogos All-Star para Ortiz. Em 2013, rebatendo em sua posição tradicional, aos 37 anos, a média de rebatimento de Ortiz foi .688 na vitória do Boston Red Sox sobre o St. Louis, 4 games a 2 na Série Mundial".

A metodologia dos dúplices pode ser considerada uma identificação de *estereótipo*. Por meio de Big Data, os analistas de dados constroem os estereótipos. Posteriormente, utilizando os mesmos tipos de dados, porém de um indivíduo determinado, comparam-nos com os estereótipos construídos e verificam em qual deles o indivíduo se encaixa. Então, de posse dessa informação, utilizam-na para o que julgarem necessário.

Pode ser algo bastante útil para identificar bons jogadores de beisebol, para definir escores de crédito ou para fazer melhores recomendações de livros e filmes para usuários. Não obstante, imaginar os problemas decorrentes de estereotipação em massa não é tarefa difícil.

Um artigo de 2016,[126] de autoria de Julia Angwin, Jeff Larson, Surya Mattu e Lauren Kirchner, analisou um *software* utilizado nos Estados Unidos para prever a chance de reincidência de criminosos:

---

[126] ANGWIN, Julia et al. Machine Bias. **ProPublica,** 23 de maio de 2016. Disponível em: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>. Acesso em: 12 de junho de 2021. Tradução livre. Texto original: "*When a full range of crimes were taken into account — including misdemeanors such as driving with an expired license — the algorithm was somewhat more accurate than a coin flip. Of those deemed likely to re-offend, 61 percent were arrested for any subsequent crimes within two years We also turned up significant racial disparities, just as Holder feared. In forecasting who would re-offend, the algorithm made mistakes with black and white defendants at roughly the same rate but in very different ways. * The formula was particularly likely to falsely flag black defendants as future criminals, wrongly labeling them this way at almost twice the rate as white defendants. * White defendants were mislabeled as low risk more often than black defendants. Could this disparity be explained by defendants' prior crimes or the type of crimes they were arrested for? No. We ran a statistical test that isolated the effect of race from criminal history and recidivism, as well as from defendants' age and gender. Black defendants were still 77 percent more likely to be pegged as at higher risk of committing a future violent crime and 45 percent more likely to be predicted to commit a future crime of any kind*".

> "Quando um rol amplo de crimes foi considerado – incluindo contravenções como dirigir com uma habilitação vencida – o algoritmo era pouco mais preciso do que um "cara ou coroa". Dentre aqueles tidos como prováveis reincidentes, 61% foram presos por algum crime subsequente nos dois anos seguintes.
> Nós também verificamos disparidades raciais significativas, exatamente como Holder havia temido. Ao prever quem iria reincidir, o algoritmo cometeu erros com réus brancos e pretos aproximadamente na mesma proporção, mas de maneiras muito distintas:
>
> - A fórmula era particularmente propensa a identificar réus pretos como futuros criminosos, identificando-os assim de modo errôneo em proporção quase duas vezes superior do que os réus brancos.
>
> - Réus brancos foram erroneamente identificados como de baixo risco com mais frequência do que réus pretos.
>
> Poderia essa disparidade ser explicada pelos crimes anteriores pelos quais os réus haviam sido presos? Não. Nós rodamos um teste estatístico que isolou o efeito racial do histórico criminal e da taxa de reincidência, assim como da idade e gênero dos réus. Réus negros ainda assim tinham uma chance 77% maior de serem identificados como de maior risco de cometimento futuro de crimes violentos e 45% maior de receberem uma previsão de cometimento futuro de um crime qualquer".

Este tipo de análise decorre de uma convergência entre Big Data e os dados individualmente considerados: Big Data serve para construir os estereótipos. Mas, é com os dados de indivíduos – coletados de diversas formas distintas – que eles são encaixados nos estereótipos e perfis pré-construídos.

Essas formações de estereótipo podem ter vários níveis: desde o agrupamento de indivíduos que moram no mesmo Estado, ou que se mudaram de uma cidade específica para outra, até aqueles que moram em bairros específicos, estudaram em determinada escola, fizeram faculdade no mesmo local, são amigos das mesmas pessoas, e assim por diante.

Não há como saber qual o conteúdo do perfil formado: pode identificar pessoas que estudaram em uma escola como de maior poder aquisitivo (e cobrar mais caro por produtos), como, também, estereotipá-las como usuárias de drogas, caso haja uma incidência elevada do vício entre os egressos.

A máxima popular "diga-me com quem andas e te direi quem és", por meio de tal poder dos dados, é levada a extremos. E, mais do que isso, vincula os indivíduos ao passado, eis que os estereótipos são construídos com base em dados históricos. A possibilidade de mudança fica restrita.

O usuário, a seu turno, tem dados seus coletados pelos comunicadores fiduciários (não necessariamente completos) que são utilizados para estereotipá-lo sem que levante quaisquer suspeitas.

Em última análise, isso consiste em uma efetiva segregação que causa a completa anulação da individualidade. O indivíduo passa a ser identificado como parte de um grupo com base em retratos parciais de sua vida e sem ter qualquer ingerência sobre o perfil que é feito dele. É bom frisar que (*i*) dados parciais podem gerar probabilidade, mas nunca certeza; e (*ii*) é impossível obter *todos* os dados; e (*iii*) esses perfis são construídos necessariamente com base em dados do passado, de modo que realizam um julgamento da pessoa com base em elementos desatualizados e estranhos a ela.

2.4.4. Testagem da população

O último poder dos dados apontado por Stephens-Davidowitz é bastante simples: consiste na ampla possibilidade de testagem por meio dos denominados "testes A/B"[127]:

> "Como, então, estabelecemos causalidade de modo mais preciso? O método mais confiável é um experimento aleatório controlado. Veja como funciona. Divide-se as pessoas aleatoriamente em dois grupos. A um deles, o grupo de tratamento, pede-se que tome ou faça determinada coisa. O outro, o grupo de controle, não faz nada. Então, observa-se como cada um deles responde. A diferença nos resultados entre os dois grupos é o efeito causal".

Esse tipo de teste, geralmente, tem como finalidade definir questões de natureza simplória: qual a melhor manchete para uma notícia, qual a melhor cor para um anúncio, qual o melhor design para uma propaganda, por meio da comparação entre os resultados gerados entre grupos de teste e de controle.[128]

Pode, entretanto, possuir feições mais delicadas. O Facebook, em 2014, realizou teste[129] com cerca de 700 (setecentos) mil usuários de sua rede social, submetendo-os a exposição controlada de emoções positivas e negativas para, a partir disso, concluir se havia, ou não, algum grau de "contágio" emocional. A conclusão foi a seguinte:

> "Nós demonstramos, por meio de um experimento massivo (N = 689,003) no Facebook, que estados emocionais podem ser transferidos a outras pessoas por meio de contágio emocional, levando pessoas a experimentarem as mesmas emoções sem terem consciência disso. Nós fornecemos evidência experimental de que contágio emocional ocorre sem interação direta entre pessoas (exposição a um amigo

---

[127] STEPHENS-DAVIDOWITZ, Seth. **Todo mundo mente: o que a internet e os dados dizem sobre quem realmente somos**. Trad. Wendy Campos. Rio de Janeiro: Alta Books, 2018, p. 206.
[128] *Ibidem*, Capítulo 6.
[129] KRAMER, Adam; GUILLORY, Jamie; HANCOCK, Jeffrey. Experimental evidence of massive-scale emotional contagion through social networks. **PNAS,** v. 111, n. 24, 2014. Tradução livre. Texto original: "*We show, via a massive (N = 689,003) experiment on Facebook, that emotional states can be transferred to others via emotional contagion, leading people to experience the same emotions without their awareness. We provide experimental evidence that emotional contagion occurs without direct interaction between people (exposure to a friend expressing an emotion is sufficient), and in the complete absence of nonverbal cues*".

> expressando uma emoção é suficiente), e na completa ausência de elementos não-verbais".

Tal estudo foi objeto de enorme polêmica – em grande medida porque nenhuma das pessoas usadas como "cobaia" foi informada de que era objeto de um teste que, objetivamente, visava manipular suas emoções, e de fato manipulou, por meio do controle escamoteado de suas relações e interações sociais.

A despeito da controvérsia, houve defesa[130] da prática do Facebook ao argumento de que a realização de testes A/B nesses moldes seriam a melhor opção para se alcançar o resultado desejado, dentre as alternativas existentes, e desde que realizada análise ética caso a caso.

Os testes, a princípio, podem parecer inócuos. Mas, o elemento central a eles é: o que é que se está testando. Uma coisa é testar qual a melhor cor ou o melhor desenho para um aplicativo. Outra coisa muito diferente da anterior é testar qual tipo de discurso político é mais apto a influenciar pessoas, ou qual espécie de *fake news* tem mais chance de induzir determinado comportamento. Se o mundo todo vira um laboratório, ele vira um laboratório para todo e qualquer tipo de experimento.

2.5. Conclusões Provisórias

Neste capítulo, definiu-se a noção dos comunicadores fiduciários, caracterizados como as entidades que fornecem infraestrutura para a realização da comunicação e troca de dados e informações entre indivíduos no contexto tecnológico do século XXI.

Em seguida, explicitou-se a taxonomia da privacidade desenvolvida por Daniel Solove. Isso foi feito com um intuito específico: descrever, na medida do detalhe necessário, as formas pelas quais dados (e, por conseguinte, informações) podem ser mal utilizadas e gerar danos aos indivíduos titulares de dados.

Na etapa seguinte, a partir das explicações de Stephens-Davidowitz, elencou-se os poderes que os dados possuídos pelos comunicadores fiduciários têm. O objetivo foi realizar uma análise descritiva das potencialidades dos dados no cenário tecnológico contemporâneo.

---

[130] A esse respeito, MEYER, Michelle N. Two Cheers for Corporate Experimentation: The A/B Illusion and the Virtues of Data-Driven Innovation. ***Colorado Technology Law Journal*****,** v. 13, n. 2, 2015, p. 329: "*But Facebook's primary and perfectly financially tenable alternative to conducting an experiment-to simply change its business practice once and for all, without collecting any data to guide its decision, and dismissing others' probative (but not dispositive) evidence that News Feed was, one way or another, harming users-seems worse on all these scores. […] None of this means, of course, that every corporate experiment, even every experiment designed to investigate the safety or efficacy of a company's products, services, or practices, is ethically laudable or even permissible*".

É preciso reconhecer: as informações que os dados que comunicadores fiduciários possuem (real ou potencial) não são, propriamente, novas na história humana. Para saber a etnia de uma pessoa, basta olhar para ela. A religião pode ser descoberta por meios tradicionais: indo a uma igreja, uma sinagoga ou uma mesquita e vendo quem está lá. Preferências alimentares, sentando em uma mesa ao lado dentro de um restaurante. Opiniões e ideologias poderiam ser descobertas simplesmente conversando com o indivíduo, ou perguntando a alguma pessoa de seu relacionamento.

O que se verifica, contudo, é que os riscos decorrentes da posse excessiva de dados por comunicadores fiduciários não residem na natureza das informações passíveis de obtenção, mas em dois elementos essenciais: (*i*) na massificação dos riscos, que, hoje, estendem-se de modo indistinto à população; e (*ii*) no ganho incalculável de eficiência, se comparados os métodos novos aos antigos, tanto na obtenção de dados quanto na transformação deles em informações.

Nesse sentido, não é difícil perceber que todos os riscos elencados na taxonomia de Solove estão presentes nas discussões relacionadas aos comunicadores fiduciários, porém em escala muito maior do que no passado.

Entretanto, essa constatação ainda não se mostra completa: a taxonomia de Solove descreve preocupações de ordem pragmática muito ligadas ao indivíduo. São questões relativas à intimidade de quem tem sua vida revelada nos jornais, fica envergonhada, é chantageada ou tem sua imagem pública manipulada, por exemplo.

Mas o que é essencial à massificação dos dados, como Stephens-Davidowitz mostrou, é o aspecto generalizado: uma quantidade enorme de pessoas está sujeita a esses riscos, de modo generalizado, sistematizado e indiscriminado.

Se a extrapolação de tais problemas à coletividade decorrente da ampliação causada pela tecnologia contemporânea traz – ou não – preocupações que também extrapolem o indivíduo é assunto que será abordado no capítulo a seguir.

3. RISCOS DOS DADOS

Nas páginas anteriores, demonstrou-se quais são potencialidades dos dados, a partir de suas características, e partir das informações que, com origem neles, podem ser obtidas por entidades que os analisarem.

Neste capítulo, o objetivo é analisar se os riscos descritos pela taxonomia de Solove, quando vistos sob a ótica massificada, constituem, em si, uma nova espécie de problema. Ou, talvez, não uma nova, mas uma bem mais grave do que aquela individualmente considerada.

A esse respeito, cabe mencionar entrevista de Stephens-Davidowitz[131] na qual afirma que o Big Data não é bom ou ruim: é, simplesmente, poderoso. E, quando se fala de poder, existem sempre duas perguntas fundamentais: (*i*) qual poder?; e (*ii*) sob o controle de quem?

Este capítulo busca responder à primeira pergunta,[132] indicando qual, exatamente, é a dimensão desse poder, o que se faz a partir da apresentação de diversas perspectivas distintas, situadas em locais diferentes no tempo, na história e no mundo.

Por questões metodológicas, é importante ressaltar que foram escolhidos, como referências de pensamento, a tradição jurídica estadunidense e o paradigma alemão. Não foram escolhas aleatórias: os Estados Unidos têm uma longa tradição com o direito da privacidade, e, no Vale do Silício, estão localizadas as *big techs*. O debate, em tal país, está em estágio avançado – e não se pode olvidar que, desde Ruy Barbosa,[133] no mínimo, o direito brasileiro bebe das fontes do pensamento jurídico estadunidense.

A eleição da Alemanha, a seu turno, decorre do fato de que a gênese do direito de autodeterminação informativa se deu naquele país e influenciou a *General Data Protection Regulation – GDPR*[134] europeia, que, por sua vez, influenciou a Lei Geral de Proteção de Dados brasileira. Além disso, o histórico alemão, caracterizado por graves experiências totalitárias e os traumas delas decorrentes (notadamente, nazismo e comunismo, este último na Alemanha oriental), foi e é chave de pensamento daquele país – o que implica um arcabouço de

---

[131] FONTEVECCHIA, Agustino. Seth Stephens-Davidowitz: "*Big data isn't good or bad, it's powerful*". ***Buenos Aires Times*****,** 26 de outubro de 2019. Disponível em: <https://www.batimes.com.ar/news/culture/seth-stephens-davidowitz-big-data-isnt-good-or-bad-its-powerful.phtml>. Acesso em: 8 de junho de 2021.

[132] A segunda será objeto do próximo capítulo.

[133] A título exemplificativo, ver BARBOSA, Ruy. ***Os Actos Inconstitucionales do Congresso e do Executivo ante a Justiça Federal*****.** Rio de Janeiro: Companhia Impressora, 1893.

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

pensamento atento aos *meios* essenciais de garantia da democracia, da liberdade e dos direitos humanos.

3.1.Preocupações

Aidan Forde, em trabalho acadêmico,[135] traz a proteção de dados como uma preocupação central relacionada à defesa de princípios básicos das sociedades ocidentais, como democracia, pluralismo e autonomia:

> "Uma cultura concentrada em proteger a privacidade dentro da Europa foca no pluralismo, na democracia e na autonomia. Autonomia é central para conceituar tanto privacidade quanto proteção de dados. Deve-se observar diferenças entre privacidade substancial e informacional. Proteção substancial permite ao indivíduo conduzir suas atividades diárias livre da ameaça de dano ou coerção estatal. Privacidade cria o ambiente por meio do qual autonomia informacional pode ser exercitada. Mecanismos de proteção de dados, tais como portabilidade de dados, retificação e limpeza dão ao indivíduo maior controle sobre o conteúdo de informações pessoais. Na ausência de tais controles, a vulnerabilidade humana aumenta. (...) Provisões efetivas de proteção de dados auxiliam os cidadãos a alcançar o desenvolvimento humano e florescer dentro da sociedade. Isso, em última análise, contribui para a manutenção de uma democracia saudável e encoraja o engajamento cívico. Proteção de dados reduz os males da vigilância e o sentimento de viver dentro de uma sociedade panóptica. (...) Mecanismos de proteção de dados levam os cidadãos rumo à realização de maior liberdade pessoal. Ferramentas de proteção de dados como o direito de ser informado, de acesso, de retificação, de limpeza e objeto colocam restrições ao armazenamento de dados pessoais por estados e por monopolistas da informação. Tais ferramentas de proteção de dados sujeitam os estados e companhia a maior escrutínio, promovem uma cultura focada em liberdades civis e previnem o fortalecimento de sociedades "focadas em vigilância". Proteção de dados, portanto, tem um efeito positivo na privacidade substancial. Tais mecanismos incrementam o bem-estar geral da sociedade e fornecem ferramentas valiosas por meio das quais o indivíduo pode remediar a relação assimétrica entre cidadão e estado, quando necessário".

É nítida, no raciocínio acima transcrito, a preocupação com a liberdade e autonomia dos cidadãos, com democracia, com o livre desenvolvimento do cidadão no seio da sociedade. É

---

[135] FORDE, Aidan. *The Conceptual Relationship between Privacy and Data Protection*. ***Cambridge Law Review***, v. 1, n. 135, 2016, p. 135-149. Tradução livre. Texto original: "*A culture concentrated on protecting privacy within Europe focuses on pluralism, democracy and autonomy. Autonomy is central to conceptualising both privacy and data protection. Differences are to be observed between substantive and informational privacy." Substantive protection allows the individual to engage in daily affairs free from the threat of state coercion or harm. Privacy creates the environment through which informational autonomy can be exercised." Data protection mechanisms such as data portability, rectification and erasure hand the individual greater control over content personal information. In the absence of such controls, human vulnerability increases. (...) Effective data protection provisions assist citizens to achieve human development and flourish within society. This ultimately contributes to the maintenance of healthy democracy and encourages civic engagement. Data protection lessens surveillance woes and the feeling of living within a panoptical society. (...) Data protection mechanisms lead citizens towards actualising greater personal freedom. Data protection tools such as right to be informed, access, rectification, erasure and object place constraints on information monopolists and states' storage of personal data. Such data protection tools subject states and corporates to greater scrutiny, promote a culture focused on civil liberties and prevent the fuelling of 'surveillance focused' societies." Data protection therefore has a positive effect on substantive privacy. Such mechanisms increase societal well-being overall and provide valuable tools through which the individual can remedy the asymmetric relationship between the citizen and state, where appropriate*".

uma preocupação, aliás, que já se manifestava no caso do censo alemão de 1983 e que, pela sua importância, merece ser esclarecida aqui.

A situação de fundo era a seguinte: a Alemanha Ocidental (*Bundesrepublik Deutschland*) possuía uma Lei Federal de Proteção de Dados (*Bundesdatenschutzgesetz*)[136] desde 1977. Em 1982, foi aprovada uma outra Lei Federal determinando a realização de um censo nacional (*Volkszählungsgesetz*),[137] a qual gerou enorme controvérsia, na ocasião, por prever 160 (cento e sessenta) perguntas, além de outras medidas controversas relativas, por exemplo, ao compartilhamento de dados.[138]

A questão chegou ao Tribunal Constitucional Federal Alemão (*Bundesverfassungsgericht – BverfG*), que declarou[139] a lei inconstitucional em acórdão assim ementado:

> "1. Nas condições do moderno processamento de dados, a proteção do indivíduo contra a coleta, armazenamento, uso e divulgação ilimitados de seus dados pessoais é coberta pelo direito geral de personalidade da Lei Básica Art. 2 Abs. 1 em conexão com a Lei Básica Art. 1 Abs. 1. Nesse sentido, o direito fundamental garante ao indivíduo o poder de determinar de maneira geral a divulgação e o uso de seus dados pessoais.

---

[136] ALEMANHA, República Federal da. *Bundesdatenschutzgesetz*, de 27 de janeiro 1977. *Mißbrauch personenbezogener Daten bei der Datenverarbeitung.* ***Bundesgesetzblatt*****:** Berlim, 1º de fevereiro de 1977, seção I, n. 7 p. 201.

[137] ALEMANHA, República Federal da. *Volkszählungsgesetz*, de 25 de março de 1982. *Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung.* ***Bundesgesetzblatt*****:** Berlim, 31 de março de 1982, seção I, n. 13, p. 369.

[138] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados**. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019, p.166-167.

[139] ALEMANHA, República Federal da. ***Bundesverfassungsgericht***, sentença do Primeiro Senado de 15 de dezembro de 1983. Karlsruhe, 1 BvR 209/83, Rn. 1-215. Tradução livre. Texto original: "*1. Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des GG Art 2 Abs. 1 in Verbindung mit GG Art 1 Abs. 1 umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. 2. Einschränkungen dieses Rechts auf "informationelle Selbstbestimmung" sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muß. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken. 3. Bei den verfassungsrechtlichen Anforderungen an derartige Einschränkungen ist zu unterscheiden zwischen personenbezogenen Daten, die in individualisierter, nicht anonymer Form erhoben und verarbeitet werden, und solchen, die für statistische Zwecke bestimmt sind. Bei der Datenerhebung für statistische Zwecke kann eine enge und konkrete Zweckbindung der Daten nicht verlangt werden. Der Informationserhebung und Informationsverarbeitung müssen aber innerhalb des Informationssystems zum Ausgleich entsprechende Schranken gegenüberstehen. 4. Das Erhebungsprogramm des Volkszählungsgesetzes 1983 (§ 2 Nr. 1 bis 7, §§ 3 bis 5) führt nicht zu einer mit der Würde des Menschen unvereinbaren Registrierung und Katalogisierung der Persönlichkeit; es entspricht auch den Geboten der Normenklarheit und der Verhältnismäßigkeit. Indessen bedarf es zur Sicherung des Rechts auf informationelle Selbstbestimmung ergänzender verfahrensrechtlicher Vorkehrungen für Durchführung und Organisation der Datenerhebung. 5. Die in VoZählG 1983 § 9 Abs.1 bis 3 vorgesehenen Übermittlungsregelungen (unter anderem Melderegisterabgleich) verstoßen gegen das allgemeine Persönlichkeitsrecht. Die Weitergabe zu wissenschaftlichen Zwecken (VoZählG 1983 § 9 Abs. 4) ist mit dem Grundgesetz vereinbar*".

> 2. Restrições a este direito de "autodeterminação informativa" são permitidas apenas no interesse geral predominante. Exigem uma base jurídica constitucional, que deve corresponder ao requisito do Estado de direito de clareza das normas. Nos seus regulamentos, o legislador também deve respeitar o princípio da proporcionalidade. Ele também deve tomar precauções organizacionais e processuais que neutralizem o risco de violação dos direitos pessoais.
> 3. No que diz respeito aos requisitos constitucionais para tais restrições, deve ser feita uma distinção entre os dados pessoais recolhidos e tratados de forma individualizada e não anónima e os que se destinam a fins estatísticos. Ao coletar dados para fins estatísticos, uma finalidade específica dos dados não pode ser exigida. A coleta e o processamento da informação devem, entretanto, ser contrabalançados por barreiras correspondentes dentro do sistema de informação.
> 4. O programa de pesquisa da Lei do Censo de 1983 (§ 2 No. 1 a 7, §§ 3 a 5) não leva a um registro e catalogação da personalidade que seja incompatível com a dignidade humana; atende também aos requisitos de clareza de normas e proporcionalidade. No entanto, a fim de garantir o direito à autodeterminação informativa, precauções processuais adicionais são necessárias para a implementação e organização da coleta de dados.
> 5. Os regulamentos de transmissão previstos em VoZählG 1983 Seção 9 (1) a (3) (incluindo a comparação do registro da população) violam direitos pessoais gerais. A transmissão para fins científicos (VoZählG 1983 § 9, § 4) é compatível com a Lei Fundamental".

Nas razões do acórdão, o *BVerfG* expressamente menciona, por exemplo, a preocupação dos recorrentes de que, sem a garantia do anonimato, o cidadão poderia "ser privado de livre autodeterminação e se tornar objeto do exercício de vontade e controle de outra pessoa".[140] A decisão do *BVerfG*, como um todo, é brilhante e demonstra as seguintes ponderações:

(a) A velocidade do processamento de dados decorrente da automatização computacional, além da possibilidade de armazenamento indefinido e do potencial de cruzamento de dados para formar perfis de personalidade sem que o sujeito possa controlar a correção e uso dos perfis, viabilizando uma pressão para forçar um *compliance* do indivíduo com a opinião pública;[141]

(b) A impossibilidade de um sujeito saber, com certa razoabilidade, o que as demais pessoas sabem dele pode significar ter sua liberdade

---

[140] Tradução livre. Texto original: "*Dadurch könne die Einzelperson der freien Selbstbestimmung beraubt und zum Gegenstand fremder Willensausübung und Kontrolle warden*".

[141] Texto original do acórdão: "*Diese Befugnis bedarf unter den heutigen und künftigen Bedingungen der automatischen Datenverarbeitung in besonderem Maße des Schutzes. Sie ist vor allem deshalb gefährdet, weil bei Entscheidungsprozessen nicht mehr wie früher auf manuell zusammengetragene Karteien und Akten zurückgegriffen werden muß, vielmehr heute mit Hilfe der automatischen Datenverarbeitung Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (personenbezogene Daten [vgl. § 2 Abs. 1 BDSG]) technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar sind. Sie können darüber hinaus - vor allem beim Aufbau integrierter Informationssysteme - mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne daß der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann. Damit haben sich in einer bisher unbekannten Weise die Möglichkeiten einer Einsicht- und Einflußnahme erweitert, welche auf das Verhalten des Einzelnen schon durch den psychischen Druck öffentlicher Anteilnahme einzuwirken vermögen*".

significativamente restringida – e a falta de conhecimento sobre os riscos decorrentes da coleta de informações de determinado comportamento divergente pode cercear a liberdade do cidadão de exercê-lo;[142]

(c) Não existem dados "irrelevantes", uma vez que quaisquer dados podem ser utilizados e/ou cruzados de modo a se tornarem relevantes;[143]

(d) O uso de dados deve ser limitado à finalidade legalmente específica, em virtude dos perigos do processamento automático de dados;[144]

(e) Em razão da falta de transparência para o cidadão, é necessária auditoria por terceiros;[145]

(f) Os dados estatísticos devem resguardar o fornecimento/divulgação de dados que possam causar rotulagem social;[146]

(g) De modo geral, a necessidade de anonimização e garantia da anonimização dos dados.

Apesar de se tratar de uma decisão tomada por um Tribunal Constitucional há quase quatro décadas, as preocupações do *BVerfG* que conduziram à consolidação do direito à autodeterminação informativa (*recht auf informationelle selbstbestimmung*) permanecem extremamente atuais.

O ponto de maior interesse, aqui, é que o *BVerfG* tratou de um censo organizado pelo *Estado* alemão. Não obstante, os assuntos tratados guardam enorme semelhança com os debates

---

[142] Texto original do acórdão: "*Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. (...) Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen*".

[143] Texto original do acórdão: "*Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein "belangloses" Datum mehr*".

[144] Texto original do acórdão: "*Die Verwendung der Daten ist auf den gesetzlich bestimmten Zweck begrenzt. Schon angesichts der Gefahren der automatischen Datenverarbeitung ist ein - amtshilfefester - Schutz gegen Zweckentfremdung durch Weitergabe- und Verwertungsverbote erforderlich. Als weitere verfahrensrechtliche Schutzvorkehrungen sind Aufklärungs-, Auskunfts- und Löschungspflichten wesentlich*".

[145] Texto original do acórdão: "*Wegen der für den Bürger bestehenden Undurchsichtigkeit der Speicherung und Verwendung von Daten unter den Bedingungen der automatischen Datenverarbeitung und auch im Interesse eines vorgezogenen Rechtsschutzes durch rechtzeitige Vorkehrungen ist die Beteiligung unabhängiger Datenschutzbeauftragter von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung*".

[146] Texto original do acórdão: "*Es kann auch hier nicht jede Angabe verlangt werden. Selbst bei der Erhebung von Einzelangaben, die für statistische Zwecke gebraucht werden, muß der Gesetzgeber schon bei der Anordnung der Auskunftspflicht prüfen, ob sie insbesondere für den Betroffenen die Gefahr der sozialen Abstempelung (etwa als Drogensüchtiger, Vorbestrafter, Geisteskranker, Asozialer) hervorrufen können und ob das Ziel der Erhebung nicht auch durch eine anonymisierte Ermittlung erreicht werden kann*".

que, hoje, cercam as comunicadoras fiduciárias (*big techs*, sobretudo), as quais são entidades eminentemente privadas.

O estudo das controvérsias contemporâneas sobre o tema nos permite notar um certo padrão: as preocupações, habitualmente, têm uma natureza voltada ao *poder* que as comunicadoras fiduciárias possuem. Questões como termos de uso, quebras de contrato, entre outras, têm sua relevância, assim como os debates sobre necessidade de regulação de mercado. No entanto, as principais inquietudes derivam de questões como o temor de, por meio do uso indiscriminado de dados pessoas, viabilizar-se um Estado totalitário.

Matthew Slaughter e David McCormick não poderiam deixar isso mais claro ao escrevem um artigo[147] intitulado "Dados São Poder", quando afirmam que "Mais até do que outros elementos da economia global, os dados são interconectados com poder". Além de discutir a perspectiva do trânsito internacional de dados a partir da ótica do comércio internacional, os autores ressaltam os riscos transnacionais à privacidade decorrentes do potencial mau uso de dados em prejuízo de direitos e garantias fundamentais:

> "A ausência de uma estrutura internacional também ameaça a privacidade das pessoas. Quem irá garantir que governos e outros atores não farão mau uso dos dados das pessoas e não violarão seus direitos econômicos, políticos e humanos? Como podem os governos protegerem a privacidade de seus cidadãos ao mesmo tempo em que permitem que dados se movam através das fronteiras?"

A preocupação é apresentada, também, por Hina Sarfaraz,[148] a qual ressalta que uma situação de completa falta de privacidade decorrente do uso de dados pessoais poderia fazer um Estado se assemelhar à ideia do Panóptico de Jeremy Bentham,[149] assumindo viés totalitário e eliminando por completo a dissidência e a liberdade – elementos indissociáveis de qualquer regime que se pretenda dizer democrático.

---

[147] SLAUGHTER, Matthew J.; MCCORMICK, David H. *Data Is Power.* ***Foreign Affairs*****,** v. 100, n. 3, maio/junho 2021, p. 54-63. Tradução livre. Texto original: "*Even more than other elements of the global economy, data is intertwined with power. […] The absence of an international framework also threatens people's privacy. Who will ensure that governments or other actors do not misuse people's data and violate their economic, political and human rights? How can governments protect their citizens' privacy while allowing data to move across borders?*".

[148] SARFARAZ, Hina. Surveillance, *Privacy and Cyber Law.* ***Computer and Telecommunications Law Review*****,** v. 20, n. 7, 2014, p. 189-194.

[149] BENTHAM, Jeremy. **O Panóptico.** Belo Horizonte: Autêntica, 2000: o Panóptico seria uma prisão na qual o vigia conseguiria observar todas as celas, mas os detentos não teriam como saber se estavam efetivamente sendo vigiados em qualquer dado momento. Diante disso, haveria um comportamento de conformidade constante derivado do medo da vigilância, a qual jamais teria como ser afastada.

Essa perspectiva também é adotada por Daniel Solove,[150] o qual, a partir de um paralelo principalmente com a obra O Processo, de Franz Kafka,[151] conclui o seguinte:

> "Sob essa perspectiva, o problema com bases de dados e as práticas atualmente associadas a elas é que elas tiram poder das pessoas. Elas deixam as pessoas vulneráveis por tirar delas controle sobre sua própria informação pessoal. Não existe um motivo diabólico ou um plano secreto para dominação; na verdade, há uma rede de decisões impensadas tomadas por burocratas de baixo escalão, políticas padronizadas, procedimentos rígidos, e uma maneira de lidar com indivíduos e suas correspondentes informações que frequentemente se torna indiferente ao bem-estar deles. [...]
> Privacidade envolve a habilidade de evitar a impotência de ter outros controlando informações que afetam as chances de uma pessoa conseguir um emprego, uma licença para exercer uma profissão ou um empréstimo importante. Envolve a habilidade e evitar compilação e circulação desse tipo de informação importante na vida de alguém sem que esse alguém possa dizer algo a respeito, sem saber quem possui qual informação, com quais propósitos ou motivos essas entidades as tem, ou o que será feito com tal informação no futuro. Privacidade envolve o poder de recusar ser tratado com indiferença burocrática quando alguém reclama sobre erros ou quando alguém quer certos dados excluídos. Não é meramente a coleção de dados que é o problema – é a nossa completa falta de controle sobre as formas em que é usado ou pode ser usado no futuro".

Similar compreensão é manifestada por Richard Posner,[152] o qual ressalta que a publicidade coíbe comunicação sincera, até mesmo por temor dos indivíduos de serem mal interpretados. Por isso o autor afirma que "há um valor social em comunicações francas, incluindo a possibilidade de testar nossas ideias com amigos e colegas sem imediatamente expô-las a ataques de rivais ou pessoas mal-intencionadas".

Neil Richards[153] também adota raciocínio semelhante, reforçando a importância de se permitir um espaço de liberdade, distante da vigilância, justamente para que se possam

---

[150] SOLOVE, Daniel. *Privacy and Power: Computer Databases and Metaphors for Information Privacy.* ***Stanford Law Review*****,** v. 53, n. 6, 2001, p. 1393-1462. Tradução livre. Texto original: "*Under this view, the problem with databases and the practices currently associated with them is that they disempower people. They make people vulnerable by stripping them of control over their personal information. There is no diabolical motive or secret plan for domination; rather, there is a web of thoughtless decisions made by low-level bureaucrats, standardized policies, rigid routines, and a way of relating to individuals and their information that often becomes indifferent to their welfare. […] Privacy involves the ability to avoid the powerlessness of having others control information that can affect whether an individual gets a job, becomes licensed to practice in a profession, or obtains a critical loan. It involves the ability to avoid the collection and circulation of such powerful information in one's life without having any say in the process, without knowing who has what information, what purposes or motives those entities have, or what will be done with that information in the future. Privacy involves the power to refuse to be treated with bureaucratic indifference when one complains about errors or when one wants certain data expunged. It is not merely the collection of data that is the problem-it is our complete lack of control over the ways it is used or may be used in the future.*".

[151] KAFKA, Franz. **O Processo.** Trad. Marcelo Backes. Porto Alegre: L&PM, 2018 [1925]. O julgamento de Josef K. pode até ser visto como um exemplo de potencial prejuízo decorrente da estereotipação decorrente da imperfeição na formação de perfis.

[152] POSNER, Richard. ***Not a Suicide Pact: The Constitution in a Time of National Emergency***. Oxford, Oxford University Press, 2006, p. 131. Tradução livre. Texto original: "*There is a social value in frank communications, including being able to try out ideas on friends or colleagues without immediate exposure to attacks from rivals or ill-wishers*".

[153] RICHARDS, Neil. *The Dangers of Surveillance.* ***Harvard Law Review*****,** v. 126, n. 7, 2013, p. 1934-1965. Tradução livre. Texto original: "*Intellectual-privacy theory suggests that new ideas often develop best away from*

construir ideias e possibilitar a evolução social e a mudança, além de evitar a disparidade de forças entre vigilante e vigiado. A vigilância, afirma o autor, ameaça o que ele denomina de "privacidade intelectual":

> "A teoria da privacidade intelectual sugere que novas ideias frequentemente se desenvolvem melhor distantes do escrutínio intenso da exposição pública; que pessoas deveriam poder fazer suas cabeças em tempos e lugares de sua própria escolha; e que uma garantia significativa da privacidade – proteção contra vigilância ou interferência – é necessária para promover este tipo de liberdade intelectual. Isso se assenta na ideia de que mentes livres são a fundação de uma sociedade livre, e que a vigilância das atividades de formação de crenças e geração de ideias podem afetar profunda e negativamente tais atividades".

Em adendo, uma preocupação trazida por Richards é a de que, em razão dessa falta de clareza sobre a importância da privacidade intelectual, quando ocorrem conflitos entre a privacidade e a vigilância, esta costuma vencer – em nome da segurança e do combate ao terrorismo, por exemplo.[154]

A partir de um ponto de vista similar, Glenn Negley,[155] em trabalho de 1966, destaca que o problema da privacidade, para ser sanado, demanda o cumprimento de um requisito dúplice: a definição de valores, por meio da filosofia moral e a especificação de procedimentos, por meio da lei: "Falha ou negligência em qualquer uma dessas tarefas deixa como alternativa unicamente o incremento da discricionariedade administrativa arbitrária que pode ativamente contornar quaisquer valores alcançados pelo indivíduo". A necessidade, portanto, e como diz o autor, é a de um julgamento de valor sobre quais *devem* ser os direitos morais e políticos do indivíduo.

E, sobre o julgamento de valor que embasa a privacidade, Solove[156] enfrenta uma discussão muito comum, que decorre do que ele indica como sendo o principal argumento

---

the intense scrutiny of public exposure; that people should be able to make up their minds at times and places of their own choosing; and that a meaningful guarantee of privacy - protection from surveillance or interference - is necessary to promote this kind of intellectual freedom. It rests on the idea that free minds are the foundation of a free society and that surveillance of the activities of belief formation and idea generation can affect those activities profoundly and for the worse".

[154] RICHARDS, Neil. *The Dangers of Surveillance.* ***Harvard Law Review*****,** v. 126, n. 7, 2013, p. 1951. Texto original: "*Despite often displaying an intuitive understanding that surveillance might be potentially harmful, courts have struggled to understand why. This absence of clarity has led to courts misunderstanding and diminishing privacy interests that conflict with other values. When faced with balancing a vague and poorly articulated privacy right against state interests such as the prevention of terrorist attacks, surveillance tends to win. Courts also make the mistake that the ACLU v. NSA court made and cast surveillance as solely a Fourth Amendment issue of crime prevention, rather than as one that also threatens intellectual freedom and First Amendment values of the highest order*".

[155] NEGLEY, Glenn. *Philosophical Views on the Value of Privacy.* ***Law and Contemporary Problems*****,** v. 31, n. 2, 1966, 319-325. Tradução livre. Texto original: "*Failure in or neglect of either of these tasks leaves only the alternative of an increasing latitude of arbitrary administrative discretion that can actively circumvent any achievement of values by the individual*".

[156] SOLOVE, Daniel. *"I've Got Nothing To Hide" and Other Misunderstandings of Privacy*. ***San Diego Law Review*****,** vol. 44, p. 745-772, 2007.

utilizado em debates envolvendo a garantia da privacidade: a alegação de que "não tenho nada a esconder".

A resposta do autor[157] a tal argumento é a de que a privacidade não é, nem deve ser tratada, como um direito *individual*, e sim como um valor social. Isso porque, para ele, a vigilância é uma prática que afeta não somente o indivíduo que, na ocasião, teve sua privacidade lesionada. Solove afirma que tal vigilância "define o tipo de sociedade em que vivemos. Ainda, o governo pode implementar vigilância sistêmica que aumenta dramaticamente seus poderes e tem efeito generalizado na liberdade das pessoas".

Ele deriva essa conclusão deriva de diversos fatores, como, por exemplo, da constatação de Bruce Schneier[158] de que o argumento do "nada a esconder" parte da premissa equivocada de que a privacidade se destina a esconder alguma coisa. Schneier coloca que "a privacidade nos protege de abusos por parte daqueles que estão no poder, mesmo que nós não estivéssemos fazendo nada de errado à época da vigilância".

Charles Fried[159] também influencia as conclusões de Solove ao relacionar a privacidade com o que, no Brasil, conhecemos como a dignidade da pessoa humana, colocando-a como um interesse do indivíduo, contraposto aos interesses da sociedade, e que deve ser privilegiado. Esse pensamento, contudo, é objeto de crítica parcial por parte de Solove, como se verá.

É de se notar que o raciocínio de Fried – que não é exclusivo dele, pelo contrário, constitui um entendimento bastante popular – também fundamenta abordagens como a Amitai Etizioni,[160] que parte de uma perspectiva que ele denomina como sendo comunitarista liberal.

---

[157] SOLOVE, Daniel. ***Nothing to Hide: The False Tradeoff between Privacy and Security***. New Haven: Yale University Press, 2011. P. 51-52. Tradução livre. Texto original: "*The power of the government to engage in this kind of surveillance without adequate oversight affects everyone. It shapes the kind of society we live in. Moreover, the government can engage in systemic surveillance that dramatically increases its power and has widespread effects on people's freedom*".

[158] SCHNEIER, Bruce. *The Eternal Value of Privacy.* ***Schneier on Security*****,** 18 de maio de 2006. Disponível em: https://www.schneier.com/essays/archives/2006/05/the_eternal_value_of.html. Acesso em 15 de junho de 2021. Tradução livre. Texto original: "*Privacy protects us from abuses by those in power, even if we're doing nothing wrong at the time of surveillance*".

[159] FRIED, Charles. *Privacy.* ***Yale Law Journal*****,** v. 77, n. 3, 1968, p.475-493. Fried afirma seguir a linha teórica de John Rawls no sentido de que devem ser desenhadas instituições sociais de modo a permitir o máximo de liberdade individual possível que seja compatível com os interesses gerais.

[160] ETZIONI, Amitai. *A Liberal Communitarian Conception of Privacy.* ***John Marshall Journal of Computer and Information Law*****,** v. 29, n. 3, 2012, p. 419-462. Tradução livre. Texto original: "*A liberal communtarian conception of privacy starts by taking for granted that citizens face two or more fully legitimate concerns (or conceptions of utility), and hence citizens should not a priori privilege any. (...) This liberal communitarian approach differs from those approaches which strongly advocate for individuals' rights in general, particularly privacy rights, set a very high bar that must be cleared before rights can be limited, and put the onus of proof on those who seek such concessions. The liberal comunitarian approach also parts from those who hold that security must be protected and when needs conflict with rights, security should be privileged. Authoritarian communities and East Asian communitarians tend to be concerned with either the common good or rights to the extent that the rights are upheld to serve the rulers*".

De fato, o autor tenta se situar no que seria uma perspectiva de "centro", afirmando existirem duas preocupações sociais em conflito (interesses individuais *versus* coletivos), mas se distanciando da premissa de que nenhum deles deva ser privilegiado em detrimento do outro:[161]

> "Um conceito comunitarista liberal da privacidade começa partindo da premissa de que cidadãos enfrentam duas ou mais preocupações totalmente legítimas (ou conceitos de utilidade), e, portanto, cidadão não deveriam *a priori* privilegiar nem um, nem outro. (...)
> Esta abordagem comunitarista liberal difere daquelas abordagens que advogam fortemente a favor de direitos individuais em geral, particularmente direitos de privacidade, estabelecem um critério muito alto que precise ser superado antes que seja possível limitar direitos, e colocam o ônus da prova naqueles que buscam tais concessões. A abordagem comunitária liberal também se separa daqueles que creem que a segurança deve ser protegida e que, quando a necessidade conflita com direitos, a segurança deve ser privilegiada. Comunidades autoritárias e comunitaristas da Ásia oriental tendem a estar preocupados seja com o bem comum, seja com direitos comuns na medida em que tais direitos são mantidos para servir àqueles em posição de poder".

Etzioni, no entanto, encontra resultado tão lacônico quanto sua premissa: a resposta que dá ao dilema, em apertada síntese, é que cada conflito entre privacidade e interesse público deve ser resolvido casuisticamente, em função do contexto histórico no qual a sociedade se insere – partindo, até mesmo, de um controle moral no intuito de evitar o controle estatal, o qual só seria viabilizado mediante a instauração de poucos controles de privacidade sociais.[162] Colocando o raciocínio do autor em outras palavras, ele advoga por uma espécie de "princípio da proporcionalidade"[163] aplicável à privacidade.

Em trabalho anterior, Etzioni[164] já estabelecia as bases que veio a desenvolver nos anos seguintes, ressaltando sua visão de que, para se ter menos controle estatal, seria necessário

---

[161] O que não passa indene de críticas, afinal, há um evidente desequilíbrio nos conflitos entre o indivíduo e a coletividade, além da lógica decorrente de uma realidade facilmente observável: o interesse coletivo é composto por interesses individuais. Um existe em função do outro. Mais sobre isso com John Dewey, adiante.

[162] ETZIONI, Amitai. *A Liberal Communitarian Conception of Privacy.* ***John Marshall Journal of Computer and Information Law*****,** v. 29, n. 3, 2012, p. 461-462. É interessante notar que o raciocínio do autor é bastante circular, e, por vezes, a etapa seguinte de sua lógica anula a anterior. Sustenta Entzioni que, ao superar os controles morais, passa-se ao estatal, que deve ser mínimo. Contudo, logo em seguida, afirma que, quanto mais vigilância sobre os agentes estatais existir, mais vigilância o Estado pode exercer: seriam os guardas guardando os guardas. Mas, se a extensão da intromissão estatal é uma mera função dos sistemas de *accountability*, então esvazia-se tudo o que veio antes. Ao fim e ao cabo, a resposta de Etzioni ao problema é a de que deve haver pouca privacidade entre os cidadãos, e que tudo é permitido, desde que seja necessário. Porém, quanto menos necessário, melhor. À toda evidência, isso não auxilia na resolução de problema algum e carrega elevada dose de subjetivismo e suscetibilidade do indivíduo aos ventos do tempo. Aliás, é de se destacar que a lógica de Etzioni de controle comunitário é não a da proteção da privacidade em si, mas a da alteração do controlador – do Estado para a comunidade. A privacidade, no entanto, continua vilipendiada. Só o que muda é *por quem*.

[163] ALEXY, Robert. **Teoria dos Direitos Fundamentais.** Trad. Virgílio Afonso da Silva. 2ª ed. São Paulo: Malheiros, 2012. Pp. 116-120. Claro que a analogia é feita com diversas ressalvas. Visa somente evidenciar a lógica de Etzioni quanto à necessidade de se analisar, em concreto, a situação de conflito, ponderando os interesses em conflito numa tentativa de melhor compatibilizá-los.

[164] ETZIONI, Amitai. *A Communitarian Perspective on Privacy.* ***Connecticut Law Review*****,** v. 32, n. 3, 2000, p. 897-906.

implementar menos privacidade social, por meio do controle comunitário mencionado anteriormente.

Esse conflito entre interesses individuais e públicos também pode ser visto na obra de Richard Posner,[165] que trata do direito à privacidade sob a perspectiva dos Estados Unidos no contexto da Guerra ao Terror que se seguiu aos atentados de 11 de setembro de 2001. O autor, levado por uma lógica de autopreservação dos Estados Unidos enquanto nação diante de um inimigo externo (como o título da obra sugere), acaba por realizar, no capítulo 6 do livro, uma efetiva defesa de uma intrusão estatal na privacidade – não tanto com base em argumentos teóricos, mas, muito mais, a partir de considerações de ordem prática.[166]

Daniel Solove,[167] entretanto, repele justamente a lógica do raciocínio que estabelece um *tradeoff* entre privacidade e interesse público por entender que resguardar a privacidade é um interesse público – não obstante ele, assim como Posner, também veja um valor social na garantia da privacidade.

É importante destacar que a lógica de Solove remonta a John Stuart Mill,[168] que, em sua *magnum opus* sobre o utilitarismo, traz a ideia de que o homem é incapaz de se conceber em como um ser alheio ao seu corpo social:

> "O estado social é ao mesmo tempo tão natural, tão necessário, e tão habitual ao homem, que, exceto em algumas circunstâncias incomuns ou por um esforço voluntário de abstração, ele nunca se concebe de outra forma a não ser como um membro de um corpo social; e esta associação é soldada mais e mais, à medida que a humanidade é removida do estado de independência selvagem".

John Dewey[169] elabora nesse pensamento, destacando que, com Mill, há uma mudança em relação ao pensamento anterior de Jeremy Bentham, que considerava a motivação de se

---

[165] POSNER, Richard. ***Not a Suicide Pact: The Constitution in a Time of National Emergency***. Oxford, Oxford University Press, 2006, Capítulo 6,

[166] Posner, resumidamente, diz que, apesar de privacidade ser importante, segurança nacional também o é, e, com respeito ao que ele analisa, as intrusões eram razoáveis, tinha mecanismos de controle, não difeririam muito do que acontece normalmente e do que o cidadão médio costuma revelar em seu dia-a-dia, e que dava para confiar nos *bureaus* de segurança pública nos anos 2000 – tudo isso na opinião dele, é claro.

[167] SOLOVE, Daniel. *"I've Got Nothing To Hide" and Other Misunderstandings of Privacy.* ***San Diego Law Review*****,** vol. 44, p. 745-772, 2007, p. 763, texto original: "*Privacy, then, is not the trumpeting of the individual against society's interests, but the protection of the individual based on society's own norms and values*". É aqui onde reside a crítica parcial ao pensamento de Charles Fried.

[168] MILL, John Stuart. ***Utilitarianism*****.** The Floating Press, 2009 [1861]. Ebook. P. 57. Texto original: "*The social state is at once so natural, so necessary, and so habitual to man, that, except in some unusual circumstances or by an effort of voluntary abstraction, he never conceives himself otherwise than as a member of a body; and this association is riveted more and more, as mankind are further removed from the state of savage independence*".

[169] DEWEY, John; TUFTS, James H. ***Ethics*****.** New York: Henry Holt and Company, 1908. Pp. 293-295. Tradução livre. Texto original: "*To state the doctrine is almost to criticize it. It comes practically to saying that a sensible and prudent self-love will make us pay due heed to the effect of our activities upon the welfare of others. We are to be benevolent, but the reason is that we get more pleasure, or get pleasure more surely and easily, that way than in any other. We are to be kind, because upon the whole the net return of pleasure is greater that way. This does not mean that Bentham denied the existence of "disinterested motives" in man's make-up; or that he held that all sympathy is coldly calculating. On the contrary, he held that sympathetic reactions to the well-being and*

fazer algo bom a outra pessoa como o resultado do bem-estar que isso causaria, por sua vez, ao agente. Com o pensamento de Mill, e havendo, na visão dele, uma "unificação" entre o indivíduo e a sociedade, a motivação para o agir no sentido do bem comum passa a ser decorrente da identidade entre o bem-estar individual e o social:

> "Afirmar a doutrina [de Bentham] é quase criticá-la. Ela praticamente diz que um amor próprio sensato e prudente nos fará prestar a devida atenção ao efeito de nossas atitudes sobre o bem-estar dos outros. Devemos ser benevolentes, mas a razão é que obteremos mais prazer, ou obteremos prazer com mais segurança e facilidade, dessa forma do que de qualquer outra. Devemos ser gentis porque, no geral, o retorno líquido do prazer é maior dessa forma. Isso não significa que Bentham negou a existência de "motivos desinteressados" na constituição do homem; ou que ele sustentava que toda simpatia é friamente calculista. Pelo contrário, ele sustentava que reações simpáticas ao bem-estar e ao sofrimento de outras pessoas estão envolvidas em nossa constituição. Mas no que se refere aos *motivos* para a ação, ele sustenta que as afeições simpáticas nos influenciam apenas sob a forma de desejo para o nosso próprio prazer: elas nos fazem regozijar na alegria dos outros, e nos fazer agir para que os outros se regozijem para que possamos, assim, regozijarmo-nos ainda mais. [...]
> A importância dessa visão modificada reside no fato de que ela nos obriga a considerar certos desejos, afeições e motivos como inerentemente valiosos, porque são fatores constituintes intrínsecos da felicidade. Assim, permite-nos *identificar* a nossa felicidade com a felicidade dos outros, encontrar o nosso bem no bem alheio, ao invés de apenas procurar a felicidade dos outros como, em geral, a forma mais eficaz de assegurar a nossa. Nossas afeições sociais são interesses diretos no bem-estar dos outros; seu cultivo e expressão são, ao mesmo tempo, uma fonte de bem para nós mesmos e, inteligentemente guiados, para os outros. [...]
> Se for perguntado o *porquê* de o indivíduo dever considerar o bem-estar dos outros como um objeto inerente de desejo, há, de acordo com Mill, apenas uma resposta: não podemos pensar em nós mesmos, exceto em certa medida, como seres *sociais*. Portanto, não podemos separar a ideia de nós mesmos e do nosso próprio bem de nossa ideia dos outros e do bem alheio. […]
> É uma questão de encontrar o bem no bem dos outros".

Em trabalho seguinte, Dewey,[170] buscando aprofundar na ideia de "direitos civis"[171] traz a ideia de liberdades civis como restrições ao poder governamental decorrentes de um suposto

---

suffering of others are involved in our make-up. But as it relates to motives *for action he holds that the sympathetic affections influence us only under the form of desire for our own pleasure: they make us rejoice in the rejoicing of others, and move us to act that others may rejoice so that we may thereby rejoice the more. […] The importance of this changed view lies in the fact that it compels us to regard certain desires, affections, and motives as inherently worthy, because intrinsic constituent factors of happiness. Thus it enables us to* identify *our happiness with the happiness of others, to find our good in their good, not just to seek their happiness as, upon the whole, the most effective way of securing our own. Our social affections are direct interests in the well-being of others; their cultivation and expression is at one and the same time a source of good to ourselves, and, intelligently guided, to others. […] If it is asked* why *the individual should thus regard the well-being of others as an inherent object of desire, there is, according to Mill, but one answer: We cannot think of ourselves save as to some extent* social *beings. Hence we cannot separate the idea of ourselves and of our own good from our idea of others and of their good. […] It is a question of finding one's good in the good of others*".

[170] DEWEY, John. ***Problems of Men.*** New York: Philosophical Library, 1946. P. 118-121. Tradução livre. Texto original: "*A consistente social philosophy of the various rights that go by this name has never existed*

[171] A ideia de "direitos civis" na tradição jurídica estadunidense pode induzir a um falso cognato, uma vez que induz o pensamento rumo às normas de Direito Civil. Na realidade, na tradição jurídica brasileira, tais direitos seriam melhor compreendidos na tradição jurídica brasileira sob nomenclaturas como "direitos individuais" ou "direitos fundamentais de 1ª geração", embora a identidade não seja perfeita, eis que constituem liberdades do cidadão oponíveis contra o Estado.

antagonismo entre este e as liberdades do cidadão. Contudo, o autor rejeita esse raciocínio: considera que só é possível falar em direitos civis no âmbito de uma civilização, de modo que, em sua análise, eles seriam justificados não por um antagonismo ao governo e consequente proteção ao indivíduo, mas, pelos benefícios que geram à comunidade. Desse modo, a forma adequada de defendê-los, coloca Dewey, é por meio de suas bases e justificações sociais.[172]

E, nesse ponto do pensamento, retorna-se à preocupação manifestada por Daniel Solove[173] em defesa da privacidade para lhe completar o significado, mas, com um ponto de vista mais apurado: a característica da privacidade como um interesse individualista lhe dá, na realidade, um contorno social: é interesse da sociedade defender esse individualismo.

Isso ocorre porque a privacidade, como se viu, é um mecanismo de liberdade e inovação. Hannah Arendt falava[174] no "perigo para a existência humana decorrente da eliminação da esfera privada", destacando que uma "existência vivida inteiramente em público, na presença de outros, torna-se, como diríamos, superficial". E esse individualismo, afirma a outra em outra obra,[175] é um elemento incompatível com regimes totalitários – e, como se pode observar, ainda é reputado como uma característica essencial às democracias liberais.[176]

Em arremate, Kirsty Hughes[177] sintetiza os valores sociais da privacidade:

---

[172] O trabalho, escrito em 1936, e originalmente publicado sob o título "*Liberalism and Civil Liberties*" na revista "*Social Frontier*" apresentava, na realidade, uma crítica de ordem pragmática ao tempo em que vivia o autor. Analisando as restrições sistemáticas aos direitos civis que se seguiram à 1ª Guerra Mundial, bem como a hipocrisia de certos ditos liberais – que só o eram na economia –, Dewey ressalta a postura dos *Justices* Holmes e Brandeis como defensores das liberdades civis, mas destacando que o fizeram com base na defesa da imprescindibilidade de alguns tais direitos para o bem-estar social. Ao final, Dewey assenta que, dada a realidade, deveriam os liberais reconhecer que a garantia da liberdade não é independente do arranjo social e, de modo pragmático, defendê-la a partir de seus benefícios sociais. Interessante notar que "estratégia" similar é utilizada por Daniel Solove.

[173] SOLOVE, Daniel. *"I've Got Nothing To Hide" and Other Misunderstandings of Privacy.* ***San Diego Law Review*****,** vol. 44, p. 745-772, 2007: seja com respeito à perspectiva Kafkiana, seja no que tange à perspectiva Orwelliana apontada por Solove. Ambas as preocupações (inibição do pensamento e perda de ingerência sobre a própria vida) manifestam valores sociais a serem protegidos, eis que revelam, cada uma à sua maneira, um plexo de riscos à democracia e à liberdade como um todo.

[174] ARENDT, Hannah. A Condição Humana. Trad. Roberto Raposo. 10. ed. Rio de Janeiro: Forense Universitária, 2007. P. 80-81.

[175] ARENDT, Hannah. **Origens do totalitarismo.** Trad. Roberto Raposo. 1ª ed. São Paulo: Companhia das Letras, 2012. P. 441.

[176] COHEN, Julie. *What Privacy is For.* ***Harvard Law Review*****,** v. 126, n.7, 2014, p. 1905. Texto original: "*Privacy shelters dynamic, emergent subjectivity from the efforts of commercial and government actors to render individuals and communities fixed, transparent, and predictable. It protects the situated practices of boundary management through which the capacity for self-determination develops.[...] Privacy therefore is an indispensable structural feature of liberal democratic political systems*".

[177] HUGHES, Kirsty. *The Social Value of Privacy***.** In: ROESSLER, Beate; MOKROSINSKA, Dorota (Org.). **Social Dimensions of Privacy: Interdisciplinary Perspectives**. Cambridge: Cambridge University Press, 2015. P. 226-227. Tradução livre. Texto original: "*There are at least three ways in which society benefits from privacy. The first is that privacy precludes the dissent into a totalitarian regime. The second is that privacy cultivates the intellectual development of society by providing the emotional and physical space in which ideas can be formed, developed and explored. The third is that privacy fosters social relations by enabling us to form different sorts of relationships with different levels of intimacy. Such relations are important to human well-being and happiness,*

> "Existem pelo menos três formas pelas quais a sociedade se beneficia da privacidade. A primeira é que a privacidade impede a dissidência para um regime totalitário. A segunda é que a privacidade cultiva o desenvolvimento intelectual da sociedade ao fornecer o espaço físico e emocional no qual ideias podem ser formadas, desenvolvidas e exploradas. O terceiro é que a privacidade alimenta relações sociais ao nos permitir formar diferentes tipos de relacionamentos com diferentes graus de intimidade. Tais relações são importantes para o bem-estar e a felicidade humanas, assim como para a harmonia social. Cada um desses valores enfatiza o papel que a privacidade exerce para contribuir na formação do tipo de sociedade que desejamos: uma sociedade democrática, reflexiva e harmônica".

A exposição de Hughes é elucidativa ao evidenciar e sumarizar os benefícios à sociedade decorrentes das garantias inerentes à privacidade em três elementos básicos. A seguir, ver-se-á o que eles significam.

3.2. Conclusões Provisórias

A pretensão deste capítulo era a de observar, além dos elementos individuais intrínsecos à proteção da privacidade em suas mais diversas formas, se também haveriam preocupações de cunho social.

O julgamento do *BVerfG* quanto ao censo alemão de 1983 lançou luzes iniciais relevantes sobre o tema. É possível extrair do acórdão do tribunal uma preocupação relevante com o poder que estaria nas mãos do Estado como resultado de um censo realizado nos moldes originalmente previstos.

Considerando o histórico alemão do século XX e o fato de que a lei do censo foi aprovada à unanimidade pelo *Reichstag*, essa preocupação do *BVerfG* não era nem um pouco trivial. A corte, à toda evidência, demonstrou relevante sensibilidade e atenção à problemática do poder que os dados podem conceder ao seu titular, privilegiando uma política de intromissão reduzida e adstrita ao mínimo necessário à consecução das finalidades a que se destinava.

É interessante observar que isso se estende até hoje: a Alemanha praticamente não aparece no sistema Google Street View[178] dada a enorme resistência de seus cidadãos ao que viram como uma violação de sua privacidade.

Essa preocupação manifestada pelo *BVerfG* é a ideia que, como se pôde ver, subjaz ao pensamento dos envolvidos no debate sobre privacidade. Além da Alemanha ocidental da década de 1980 preocupada com o poder derivado do excesso de informações, viu-se pensamentos análogos manifestados por Hannah Arendt na década de 1950 e Richard Posner

---

as well as to social harmony. Each of these values emphasizes the role that privacy plays in contributing to the sort of society to which we aspire: a democratic, reflective and harmonious society".

[178] ***Google Street View.*** Disponível em: >https://www.google.com.br/maps>. Acesso em: 17 de junho de 2021.

nos anos 2000, no contexto da Guerra ao Terror, por exemplo. E a eles se filiam tantos outros autores, mencionados neste trabalho ou não.

A literatura sobre o tema – e a quantidade de autores que assim pensam – é tão extensa que tentar abordá-la por completo redundaria em tarefa impossível e redundante; é uma preocupação que pulula a mente de uma quantidade incomensurável de profissionais das mais diversas áreas que se debruçam sobre o assunto.

A esse respeito, o exemplo de Hong Kong é paradigmático: a Região Administrativa Especial era uma democracia. Até que deixou de ser[179] em uma velocidade impressionante. E os dados dos cidadãos se tornaram uma relevante preocupação[180] diante das ofensivas despóticas do Partido Comunista Chinês – PCCh.

Considerando os poderes dos dados e os riscos que eles apresentam, uma perseguição de indivíduos pró-democracia em Hong Kong, nos moldes do que o PCCh promove contra a etnia Uigur[181], é um risco – e cidadão pró-democracia, que assim se comportaram durante o período de "normalidade", correm risco de sofrerem graves consequências.

De todo modo, o que se depreende sem grandes dificuldades é que, no âmbito do debate atual sobre a privacidade, ela é considerada de interesse não mais exclusivamente individual, mas se reveste de um caráter de interesse social.

E esse caráter social decorre de sua funcionalidade como instrumento de preservação de liberdades fundamentais, da democracia e da restrição de poder, como se viu no pensamento dos diversos agentes abordados neste capítulo.

Em termos concretos: a privacidade, no contexto de 1890 em que surgiu, evidenciava preocupações essencialmente com direitos dos indivíduos oponíveis contra outros indivíduos. A motivação de Warren para escrever o artigo, como dito, era a excessiva fofoca de que sua família era vítima. Era uma questão, essencialmente, de direito privado, a ser resolvida por meio da responsabilidade civil.

Mas, hoje, o enfoque se expandiu substancialmente, ao ponto em que as preocupações individuais com a privacidade alcançam um caráter fortemente social – muito embora permaneçam direcionadas contra entidades privadas: os comunicadores fiduciários.

---

[179] PANG, Jessie; SIU, Tyrone. *Closure looms for Hong Kong's pro-democracy Apple Daily after raids.* ***Reuters*****,** 21 de junho de 2021. Disponível em: <https://www.reuters.com/world/asia-pacific/hong-kongs-apple-daily-board-may-stop-publication-this-week-memo-2021-06-21>. Acesso em: 21 de junho de 2021.

[180] CHAN, Justin. *Hong Kong sees rush for burner phones as government pushes contact-tracing app.* ***Reuters*****.** 18 de fevereiro de 2021. Disponível em: <https://www.reuters.com/article/us-health-coronavirus-hongkong-idUSKBN2AI0I8>. Acesso em: 7 de junho de 2021.

[181] **BBC,** 21 de junho de 2021. Disponível em: <https://www.bbc.com/news/world-asia-china-22278037>. Acesso em: 21 de junho de 2021.

É esse o diagnóstico de Stefano Rodotà:[182]

> "Talvez seja possível traçar um esquema deste processo, ressaltando que parece cada vez mais frágil a definição de "privacidade" como o "direito a ser deixado só", que decai em prol de definições cujo centro de gravidade é representado pela possibilidade de cada um controlar o uso das informações que lhe dizem respeito. Não que este último aspecto estivesse ausente das definições tradicionais: nelas, porém, ele servia muito mais para sublinhar e exaltar o ângulo individualista, apresentando a privacidade como mero instrumento para realizar a finalidade de ser deixado só; enquanto hoje chama a atenção sobretudo para a possibilidade de indiviíduos e grupos controlarem o exercício dos poderes baseados na disponibilização de informações, concorrendo assim para estabelecer equilíbrios sócio-políticos mais adequados".

Ocorre que tais preocupações – controle do poder, garantia da democracia e de liberdades individuais... não são discussões típicas de direito privado. Na realidade, esses debates costumam ser vistos no âmbito das discussões que cercam o constitucionalismo.

É dizer: não se afirma habitualmente que as leis de divórcio, sucessão, ou normas societárias ou consumeristas destinam-se ao controle do poder de quem quer que seja. O direito privado comumente passa ao largo dessas questões.

Porém, a frequência com que aparecem nos debates que cercam a temática da privacidade destoa da área de pensamento jurídico em que está inserida, e, por isso, salta aos olhos, levando à seguinte conclusão: o debate sobre a privacidade, no contexto tecnológico do século XXI, não é um debate que enfrenta (apenas) problemas de direito privado; é um debate cujo ponto fulcral alcançou e alcança problemas de direito constitucional – mais especificamente, de constitucionalismo.

É importante ressaltar que a perplexidade que o debate sobre privacidade causa não comporta reducionismo à natureza de questão regulatória – cujo enfoque é afeito a elementos técnicos e/ou de mercado de determinadas atividades econômicas. As preocupações sobre proteção de dados são de natureza distinta. É dizer, a título exemplificativo: o setor aeroportuário não é regulado por temor de que, se assim não o fosse, uma companhia aérea poderia conseguir instalar um regime totalitário – os motivos são outros e até soa cômico pensar em um cenário desses. Por outro lado, a preocupação que se tem com os comunicadores fiduciários (especialmente as *big techs*) é exatamente essa, junto de suas ramificações.

Essa constatação não é trivial: o constitucionalismo possui mecanismos próprios, existentes há séculos, que servem para lidar com a problemática do poder e da política[183]. São exemplos a separação dos poderes, a transparência, os direitos fundamentais, entre tantos outros

---

[182] RODOTÀ, Stefano. **A Vida na Sociedade da Vigilância: A privacidade hoje**. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. P. 24.

[183] Poder, na concepção de Zygmunt Bauman, como a capacidade de fazer coisas, e política, como a de escolher quais coisas serão feitas. Em BAUMAN, Zygmunt. **Vigilância Líquida.** Trad. Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013. P. 105.

mecanismos de desenho institucional que se prestam à finalidade de controle do exercício de poder na sociedade.

Se os riscos que os comunicadores fiduciários apresentam são de essência constitucional, então os mecanismos para enfrentá-los devem ser os mesmos. Insistir em dar soluções de direito privado a problemas que são enfrentados pelo direito constitucional há séculos é seguir pela trilha da ineficiência e assegurar a não resolução dos problemas: esses perigos não são tão novos quanto poderiam parecer à primeira vista; a humanidade já se debruçou sobre essas questões.

A saída, certamente, não é a de um ludismo moderno: a tecnologia evolui, a roda do tempo gira e o mundo caminha para frente. É impossível querer se apegar à falsa e ilusória segurança do passado e guardá-la como se imutável fosse, buscando congelar a evolução da humanidade no tempo.

Por outro lado, é possível e é devido aprender com a experiência humana passada, e, para problemas análogos, dar soluções análogas. Não há a necessidade de reinventar a roda: somente adaptá-la ao novo veículo; de madeira, para borracha vulcanizada.

Nesse contexto, o capítulo 4, último deste trabalho, visa pensar e analisar de que forma as técnicas do constitucionalismo servem à proteção da privacidade, porém em caráter meramente inaugural e sem a pretensão de exaurir o tema, mantendo enfoque nas principais e mais prementes ferramentas que o constitucionalismo nos dá para lidar com os riscos à privacidade no século XXI.

4. FERRAMENTAS DO CONSTITUCIONALISMO

Como se demonstrou nos capítulos anteriores, as preocupações relacionadas à privacidade transmudaram-se de sua natureza original, fortemente vinculada a preocupações de ordem individual, para assumirem um caráter de ordem social, voltado à proteção da sociedade e do regime democrático – sem, no entanto, perder sua essência original, que continuou e continua a persistir.

Essa ampliação do escopo da privacidade se deu, em grande medida, à massificação dos meios de coleta de dados e obtenção de informações. Com a informatização, a partir da segunda metade do século XX, o ganho de eficiência no processamento de dados atingiu patamares antes inimagináveis. Viu-se, nesse sentido, que a nova realidade vem acompanhada de poderes significativos que passam a ser detidos pelos comunicadores fiduciários.

Isso altera o paradigma anterior, no qual as preocupações de ordem democrática e de contenção do poder dirigiam-se, essencialmente, à figura do Estado. Os atores privados passam a incutir preocupações similares: seja por eles próprios, seja em razão do temor de figurarem, eventualmente, como auxiliares do Estado, por meio do uso secundário de informações que possam vir a servir para viabilizar o poder excessivo.

Nesse sentido, o que se constata é que as preocupações contemporâneas relacionadas à privacidade, especialmente no que tange ao processamento de dados, possuem natureza assemelhada àquela que informou a história do constitucionalismo.

Neste capítulo final, então, busca-se, partindo das ideias acima, posicionar o constitucionalismo como uma linha de pensamento humana que se preocupa com o poder e sua forma de exercício com o objetivo de resguardar direitos humanos fundamentais.

A partir disso, poder-se-á concluir que as normas protetivas da privacidade têm raiz diretamente na essência dos textos constitucionais – aqui, com atenção ao texto constitucional brasileiro.

A proteção da privacidade (sob a perspectiva da proteção de dados), portanto, não será questão fundada meramente em pensamentos constitucionais de natureza privatista ou com base infralegal, mas uma decorrência necessária dos fundamentos mais basilares da Constituição Federal brasileira como um instrumento de contenção do poder – que, agora, passa a ter o uso massificado de dados como uma ameaça.

Entretanto, haverá o cuidado de não se refutar o avanço da tecnologia, evitando concepções ludistas: deve-se, na realidade, buscar meios de viabilizá-la ao mesmo tempo em

que se resguardam os princípios constitucionais democráticos e limita-se o poder dos comunicadores fiduciários.

Ver-se-á, também, que a questão não será de mera horizontalização dos direitos fundamentais, uma vez que possui fundamento diverso, nem será de mera *regulação* nos moldes do direito regulatório, eis que não derivará de questões meramente técnicas ou mercadológicas: a preocupação (e o fundamento) abarca, porém, extrapola tais questões.

Sem embargo, serão ponderadas, ao final, duas ferramentas do Direito Constitucional que, na avaliação deste autor, são de importância destacada para a privacidade e não encontram resguardo suficiente na normatização atualmente vigente no Brasil: (*i*) a separação dos poderes; e (*ii*) a transparência.

4.1. Constitucionalismo e Privacidade

O constitucionalismo, se compreendido como pensamento voltado à contenção do poder político, remonta à antiguidade clássica.[184] No entanto, nos moldes contemporâneos, tal filosofia política tem suas origens nas revoluções liberais do século XVIII[185], muito embora possua elementos rastreáveis à Idade Média ou à Antiguidade Clássica, no que convencionou-se chamar de constitucionalismo antigo.[186]

Desse modo, Canotilho[187] entende ser inadequado falar em constitucionalismo como uma ideia geral e unívoca no tempo e no espaço. O autor sustenta ser mais adequado "dizer que existem diversos movimentos constitucionais com corações nacionais, mas também com alguns momentos de aproximação entre si, fornecendo uma complexa tessitura histórico-culturais". Nas palavras do autor:

---

[184] Nesse sentido, a título exemplificativo, Aristóteles já falava na tripartição entre os poderes deliberativo, executivo e judiciário, que é elemento intrínseco ao constitucionalismo decorrente das revoluções liberais. Platão, que foi professor de Aristóteles e aluno de Sócrates, também traz noções similares em sua defesa do governo de filósofos, ao dar as bases teóricas para o que se desenvolveu até se tornar a concepção moderna de realização do controle de constitucionalidade por um grupo de pessoas esclarecidas. Tratam-se de elementos que se relacionam com as noções atuais que acompanham o constitucionalismo sob a perspectiva do conteúdo da ideia e suas finalidades. A esse respeito, ver: ARISTÓTELES. **A Política**. Trad. Roberto Leal Ferreira. 3ª ed. São Paulo: Martins Fontes, 2006; PLATÃO. **A República.** Tradução: Ciro Mioranza. São Paulo: Lafonte, 2017; e VALE, André Rufino do. *Reis-juízes* ou *reis-legisladores*? O dilema platônico e o problema da legitimação democrática da Jurisdição Constitucional. **Caderno Virtual,** v. 3, n. 9, 2004, p. 1-15.

[185] MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional.** 13ª ed. São Paulo: Saraiva Educação, 2018. P. 39: "*A ideia de Constituição, como a vemos hoje, tem origem mais próxima no tempo e é tributária de postulados liberais que inspiraram as Revoluções Francesa e Americana do século XVIII*".

[186] A esse respeito, ver a lição de Canotilho: CANOTILHO, J. J. Gomes. **Direito Constitucional e Teoria da Constituição.** 7ª ed. Coimbra: Almedina, 2000. P. 52.

[187] CANOTILHO, J. J. Gomes. **Direito Constitucional e Teoria da Constituição.** 7ª ed. Coimbra: Almedina, 2000. P. 51.

> "E dizemos ser mais rigoroso falar de vários *movimentos constitucionais* do que de vários constitucionalismos porque isso permite recortar desde já uma noção básica de *constitucionalismo*. **Constitucionalismo** é a teoria (ou ideologia) que ergue o princípio do governo limitado indispensável à garantia dos direitos em dimensão estruturante da organização político-social de uma comunidade. Neste sentido, o constitucionalismo moderno representará uma *técnica específica de limitação do poder com fins garantísticos*. O conceito de constitucionalismo transporta, assim, um claro juízo de valor. É, no fundo, uma *teoria normativa da política*, tal como a teoria da democracia ou a teoria do liberalismo".

Sobre esse tema, José Afonso da Silva[188] ensina que a Declaração de Direitos do Bom Povo da Virgínia, firmada em 1776 e anterior à Declaração de Independência dos EUA foi a primeira declaração de direitos em sua acepção moderna; diferenciava-se dos textos anteriores por constituir não uma limitação ao poder do rei, mas ao próprio poder estatal, assim considerado. Partia-se, nas palavras do autor, da premissa da existência de "direitos naturais e imprescritíveis do homem", insuscetíveis de qualquer espécie de ingerência estatal – os quais podem ser identificados com a ideia dos assim denominados direitos fundamentais de primeira geração.[189] Nesse contexto, portanto, teve gênese o constitucionalismo moderno.

Foi nesse contexto, portanto, em que teve gênese o constitucionalismo moderno, caracterizado, conforme anota Canotilho[190] pelas seguintes três características essenciais: (*i*) a existência de um documento escrito; (*ii*) a presença de declaração de direitos e do modo de garanti-los; e (*iii*) a forma pela qual seria organizado o poder político de modo a assegurar sua moderação e limitação.

Daí decorre a constatação feita por Canotilho[191] no sentido de que o constitucionalismo moderno é caracterizado pelas ideias básicas de regulação do poder político e de reconhecimento e garantia dos direitos e liberdades de primeira geração.

Posteriormente, o advento do Estado de Bem-Estar Social, associado ao constitucionalismo, desembocou em constituições que passavam a expandir as declarações de direitos e prever, também, prestações estatais e direitos difusos, consubstanciando os direitos fundamentais de segunda e terceira gerações.[192]

---

[188] SILVA, José Afonso da. **Curso de direito constitucional positivo.** 42ª ed. São Paulo: Malheiros, 2019. P. 155-156.

[189] Paulo Bonavides define os direitos fundamentais de primeira geração como sendo os direitos de liberdade: "Os direitos de primeira geração são os direitos da liberdade, os primeiros a constarem do instrumento normativo constitucional, a saber, os direitos civis e políticos, que em grande parte correspondem, por um prima histórico, àquela fase inaugural do constitucionalismo do Ocidente". BONAVIDES, Paulo. **Curso de Direito Constitucional.** 34ª ed. São Paulo: Malheiros, 2019. P. 576.

[190] CANOTILHO, J. J. Gomes. **Direito Constitucional e Teoria da Constituição.** 7ª ed. Coimbra: Almedina, 2000. P. 52.

[191] *Ibidem*, p. 54-55.

[192] BONAVIDES, Paulo. **Curso de Direito Constitucional.** 34ª ed. São Paulo: Malheiros, 2019. P. 577-585.

A evolução seguinte, os chamados direitos de quarta geração, seriam aqueles que ainda aguardam reconhecimento e positivação[193], mas que seriam fruto da globalização dos direitos fundamentais – os direitos à democracia, ao pluralismo e à informação.[194] O reconhecimento desta quarta geração, todavia, não passa indene de ponderações sobre sua real concretude e sua essência meramente derivativa das gerações anteriores, como anota Ingo Sarlet.[195]

As constituições contemporâneas, e, no caso do Brasil, especialmente a Constituição Federal de 1988 – CF/88,[196] preveem diversos direitos, os quais podem ser categorizados em todas as quatro supracitadas gerações. Não obstante, no que tange à privacidade (com enfoque na proteção de dados), não é preciso socorrer-se à segunda, terceira ou quarta gerações para encontrá-lo; sua razão de ser é intrínseca à gênese do constitucionalismo.

O capítulo anterior demonstrou que, com a contemporaneidade, a proteção de dados se tornou um interesse social voltado à limitação do poder, como colocam Serge Gutwirth e Paul de Hert.[197] A doutrina constitucional, a seu turno, evidencia que a gênese do fenômeno constitucional se preocupa com o controle do poder e garantia das liberdades civis. A ligação entre uma coisa e outra é evidente.

O que se está a dizer é que a proteção de dados, no contexto atual, deve ter por fundamento justamente tais paradigmas, os quais são intrínsecos ao constitucionalismo moderno.

No entanto, o direito brasileiro tratou, por muito tempo, a proteção de dados a partir do paradigma de Tércio Sampaio,[198] considerando que o artigo 5º, inciso XII da CF/88 resguardava somente a *comunicação* de dados, mas não os dados em si, como se vê a partir de o julgamento do *habeas corpus* nº 91.867, do Pará, em abril de 2012:[199]

---

[193] MARTINS FILHO, Ives Gandra. Direitos Fundamentais. In: MARTINS, Ives Gandra da Silva/ MENDES, Gilmar Ferreira; NASCIMENTO, Carlos Valder (Org.). **Tratado de Direito Constitucional.** Vol. 1. 2ª ed. São Paulo: Saraiva, 2012. P. 317.

[194] BONAVIDES, Paulo. **Curso de Direito Constitucional.** 34ª ed. São Paulo: Malheiros, 2019. P. 585-587.

[195] SARLET, Ingo. **A Eficácia dos Direitos Fundamentais.** 13ª ed. Porto Alegre: Livraria do Advogado, 2018. P. 50-51.

[196] BRASIL, República Federativa do. Constituição (1988). **Constituição da República Federativa do Brasil de 1988.** Diário Oficial da União, Brasília, 5 de outubro de 1988.

[197] GUTWIRTH, Serge; DE HERT, Paul. *Privacy, Data Protection and Law Enforcement: Opacity of the individual and Transparency of the Power*. In: CLAES, E; DUFF, A; GUTWIRTH, S. (Ed.). ***Privacy and the Criminal Law*.** Antwerp/Oxford: Intersentia, 2006. P. 16. Texto original: "*As such these regulations implicitly accept that a processing of personal data is closely linked to the exercise of power and that it facilitates its establishment*".

[198] FERRAZ JR., Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito,** Universidade de São Paulo, n. 88, p. 439-459, 1993.

[199] BRASIL, República Federativa do. Supremo Tribunal Federal. ***Habeas Corpus* nº 91.867/PA.** Rel. Min. Gilmar Mendes. Segunda Turma, julgado em 24/04/2012, ACÓRDÃO ELETRÔNICO DJe-185 DIVULG 19-09-2012 PUBLIC 20-09-2012.

> "Não se confundem comunicação telefônica e registros telefônicos, que recebem, inclusive, proteção jurídica distinta. Não se pode interpretar a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral. A proteção constitucional é da comunicação de dados e não dos dados".

Recentemente, no entanto, o Supremo Tribunal Federal (STF), ao julgar o referendo da medida cautelar (MC) na ação direta de inconstitucionalidade (ADI) 6.387 do Distrito Federal (DF),[200] reconheceu o direito fundamental à proteção de dados, mas o fez com fundamento nas garantias constitucionais à liberdade, à privacidade e ao desenvolvimento da personalidade, a despeito das ponderações acerca de sua importância para a garantia da democracia:[201]

> "2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados".

É curioso notar que, a despeito de o STF ter demonstrado significativa preocupação com a garantia democrática, ainda se ateve, nos fundamentos adotados, às disposições constitucionais de índole individual, enquanto a garantia democrática se apresenta como preocupação de índole social e constitucionalista.

A preocupação com a razão de ser, que aqui se apresenta, não consiste em mero preciosismo jurídico; não é uma preocupação inócua. A base teórica que se adota possui repercussões que extrapolam a mera resolução do problema.

Isso se dá porque, no âmbito jurídico, mais de um fundamento distinto pode conduzir a uma tutela específica. É possível, por exemplo, absolver um réu criminal por falta de provas ou por prova negativa. O resultado prático é o mesmo: o réu vai solto. Mas não é possível negar que a razão de decidir possui relevância que extrapola o caso concreto.

A fundamentação teórica, o princípio constitucional do qual se extrai o direito à proteção de dados influencia fortemente nas ferramentas jurídicas colocadas à disposição do intérprete para resguardá-lo.

Uma concepção puramente privatista poderia conduzir à equivocada ideia de que, aqui, o que se está a abordar é uma espécie do gênero "eficácia horizontal dos direitos fundamentais". No entanto, não é disso que se trata.

---

[200] BRASIL, República Federativa do. Supremo Tribunal Federal. **Referendo da Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6.387/DF.** Rel. Min. Rosa Weber. Tribunal Pleno, julgado em 07/05/2020, PROCESSO ELETRÔNICO DJe-270 DIVULG 11-11-2020 PUBLIC 12-11-2020.

[201] MENDES, Laura Schertel Ferreira. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais. **Jota.** Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020>. Acesso em: 18 de junho de 2021.

A eficácia horizontal dos direitos fundamentais consiste, em síntese, na aplicação, às relações privadas, de direitos fundamentais constitucionalmente assegurados. Daniel Sarmento[202] a coloca como necessária à proteção do indivíduo diante dos poderes sociais, "que podem oprimir tanto ou até mais que os Estado".

Virgílio Afonso da Silva,[203] em sentido similar, anota que a eficácia horizontal dos direitos fundamentais derivou do "reconhecimento de que, ao contrário do que uma arraigada crença sustentava, não é somente o Estado que pode ameaçar os direitos fundamentais dos cidadãos, mas também outros cidadãos, nas relações horizontais entre si".

Também se debruça sobre tema, de modo similar, Thiago Sombra,[204] quando assenta que a horizontalização dos direitos fundamentais veio a partir da constatação de que a complexidade das relações sociais ensejou situações nas quais um particular passou a estar em "constante posição de ingerência aos direitos fundamentais de seus pares".

De fato, à primeira vista, há aparente similaridade entre a ideia de eficácia horizontal dos direitos fundamentais e os fundamentos constitucionais para a privacidade que ora se propõe. No entanto, essa identidade é meramente superficial.

É que, como indicado acima, o constitucionalismo moderno foi caracterizado em sua gênese pela contenção do poder e pelas enunciações de direitos. A eficácia horizontal dos direitos fundamentais diz respeito à aplicação, no âmbito das relações privadas, do último.

Veja-se, nesse sentido, que nem sequer faria sentido falar em eficácia horizontal dos direitos fundamentais quando se está tratando de um direito que surgiu como um direito eminentemente privado, na acepção de Warren e Brandeis. A proteção de dados, que vem da privacidade, tem origem no direito privado, e não no direito público. O nome do direito não é mero acaso ou coincidência.

De maneira diversa, o que aqui se sustenta diz respeito à primeira característica do constitucionalismo moderno: a contenção do poder. Em certo aspecto, seria, talvez, melhor definir a lógica que ora se apresenta como uma verticalização do direito privado, ao invés de uma horizontalização de direitos fundamentais.

A partir de outra perspectiva, poder-se-ia afirmar que a resolução da questão se daria pela via do direito regulatório, mediante simples regulação das *big techs*. Essa, contudo, é uma

---

[202] SARMENTO, Daniel. **Direitos Fundamentais e Relações Privadas.** Rio de Janeiro: Lumen Juris, 2004. Asdasd P. 66-67. 275-276.
[203] SILVA, Virgílio Afonso da. A **Constitucionalização do Direito: Os direitos fundamentais nas relações entre particulares**. São Paulo: Malheiros, 2005. P. 52.
[204] SOMBRA, Thiago Luís Santos. **A Eficácia dos Direitos Fundamentais nas Relações Privadas.** 2ª ed. São Paulo: Atlas, 2011. P. 35.

saída pela perspectiva pragmática, mas não pela perspectiva teórica. Como dito, não importa, para o direito, apenas o resultado alcançado; os motivos pelos quais se decide também são relevantes e devem ser considerados.

Márcio Iorio Aranha,[205] ao tratar do tema, assenta que "[o] cerne da regulação reside em outra seara qualificadora do mercado: o direito à igualdade". Trata-se de garantir, na visão do autor, "o direito à igualdade de condições concorrenciais" no mercado, no que acrescenta, também, que "o conjunto dos direitos fundamentais apresenta-se como a razão de ser da regulação".

Ocorre que nenhum dos dois fundamentos se aplica ao raciocínio aqui desenvolvido: a proteção da igualdade no mercado não é relevante porque o objeto das preocupações é o poder social – e não o poder econômico. Um pode ter relação com o outro, ou derivar do outro, a depender do caso, mas são espécies essencialmente distintas e sem inter-relação necessária.

A garantia dos direitos fundamentais, por outro lado, faz incidir na mesma observação feita anteriormente quando se abordava a horizontalização dos direitos fundamentais: a preocupação é com o *poder* social, e não com os direitos enunciados nas cartas políticas.

Assim, a solução também não se dá pela via do direito regulatório. Dá-se, na realidade, como consequência direta da força normativa da Constituição, conforme ensinamento de Konrad Hesse.[206] A Constituição, como instrumento do constitucionalismo, possui sua própria força de contenção do poder, e essa força implica o reconhecimento da proteção de dados como direito intrínseco à concepção moderna de constitucionalismo desde a sua gênese.

Entretanto, e como sobressai evidente, no século XVIII, os *founding fathers* estadunidenses, ou os *sans-culottes* franceses nem sequer cogitavam a possibilidade de ser necessário falar em privacidade, nos moldes atuais de proteção de dados, para assegurar limitação do poder estatal.

Porém, no contexto de distanciamento de regimes absolutistas, especialmente no âmbito francês, para os revolucionários de outrora a limitação do poder era, de fato, uma preocupação relevante – se não a mais relevante – daqueles momentos históricos e movimentos constitucionais. E, por isso, foram desenvolvidos diversos mecanismos de controle do poder.

---

[205] ARANHA, Márcio Iorio. **Manual de Direito Regulatório: Fundamentos de Direito Regulatório**. 4ª ed. Londres: Laccademia Publishing, 2018. P. 13, 15-16.

[206] HESSE, Konrad. **A Força Normativa da Constituição.** Trad. Gilmar Ferreira Mendes. Porto Alegre: Sérgio Antônio Fabris Editor, 1991.

Dentre esses, um que se destaca no constitucionalismo moderno – e que tem raízes que remontam a Aristóteles, como visto – é a separação dos poderes, iniciada em sua concepção moderna por Charles de Secondat, o Barão de Montesquieu.[207]

Além da separação, a transparência no exercício do poder também é ferramenta utilizada para seu controle, embora sem uma gênese tão marcada e identificável quanto a separação. Não obstante, em qualquer concepção de constitucionalismo que se possa imaginar, ela é fundamental: se o constitucionalismo é técnica de limitação do poder, então é indissociável a ideia de conhecimento sobre a forma como ele está sendo exercido. Afinal, é impossível controlar algo sem saber o que se passa.

Como, no caso da comunicação fiduciária, a concentração e opacidade do funcionamento das *big techs* são elementos característicos – dada a concentração de dados por poucas empresas e a necessidade intransponível de confiança, de onde derivou-se a expressão qualificadora fiduciária – elegeu-se essas duas ferramentas para um olhar mais aprofundado.

4.2. Ferramentas Constitucionais

O objetivo deste subtópico consiste em, a partir do raciocínio desenvolvido anteriormente, realizar, sucintamente, análise de duas ferramentas de natureza fortemente atrelada ao constitucionalismo que, em razão de suas

A separação dos poderes no contexto do constitucionalismo é tema que foi abordado com maior profundidade por este autor em trabalho monográfico,[208] razão pela qual não há a necessidade de revisitar o tema desde os seus primórdios.

Não obstante, é importante ressaltar que a ideia de separação de poderes, no constitucionalismo, é trazida por Montesquieu como um instrumento necessário à proteção contra a tirania, mas, ao falar sobre o tema, o francês não dá grandes explicações, limitando-se, na realidade, a realizar espécie de petição de princípio nesse sentido.[209]

Posteriormente, Jeremy Waldron[210] reconhece a separação dos poderes como um instrumento de garantia da liberdade política, mas deu-lhe uma definição como uma teoria articulada de governança estatal, enfatizando seu caráter procedimental: a lógica por detrás da

---

[207] MONTESQUIEU, Charles de Secondat, Baron de. **O Espírito das Leis.** São Paulo: Martins Fontes, 2005 [1748].
[208] BARRA DE SOUZA, Matheus. ***A Political Question Doctrine* no Direito Brasileiro.** Monografia (Bacharelado em Direito). Faculdade de Direito, Universidade de Brasília. Brasília, p. 79, 2018.
[209] *Op. cit.*, p. 167-178.
[210] WALDRON, Jeremy. *Separation of Powers in Thought and Practice?* ***Boston College Law Review*,** v. 54, n. 2, 2013, p. 433-468. P.

separação de poderes seria a necessidade de que, antes de o poder impactar o indivíduo, cada um dos poderes manifeste separadamente seu "posicionamento" sobre isso.

A partir disso, exsurge um questionamento sobre a aplicabilidade dessa lógica às questões concernentes à privacidade. Também, e especificamente com respeito ao direito brasileiro, aparece o questionamento sobre se a LGPD já não prevê tal espécie de procedimento, ou ao menos de modo análogo. E, ainda, poder-se-ia indagar, caso se esteja afirmando que a separação de poderes aplicada à privacidade diria respeito à separação entre empresas, se tal questão não seria resolvida simplesmente pelo direito antitruste. Todas perguntas relevantes e que merecem ser avaliadas.

Começando pela última, há uma resposta mais imediata: o Conselho Administrativo de Defesa Econômica – CADE cuida,[211] grosso modo, de duas espécies de problemas: (*i*) infrações à ordem econômica; e (*ii*) atos de concentração.

Ambos, no entanto, preocupam-se especificamente com o problema da dominância e do poder de particulares exclusivamente sob a ótica econômica. A privacidade, a seu turno, se importa com o aspecto social. Pode até haver sobreposição em casos específicos, mas não será necessária.

A título exemplificativo: ninguém dirá que uma empresa produtora de arroz que detenha monopólio da produção e comércio do importante cereal poderá, em tese, ser uma ameaça à democracia ou um veículo para a instauração de um regime totalitário.

Por outro lado, uma empresa com baixo faturamento (portanto, escapando da incidência do artigo 88 da Lei do Sistema Brasileiro de Defesa da Concorrência – SBDE) e que não pratique nenhuma infração à ordem econômica (não incorrendo nas prescrições do artigo 26 da Lei do SBDE) pode, ainda assim, deter uma quantidade relevantíssima de dados e informações, por exemplo, sobre a religião de cada um dos brasileiros, orientação sexual e/ou visão político-ideológica.

É claro que há uma *tendência*, já que dados possuem valor econômico e é natural que a empresa que os detenha em grande quantidade tente explorá-los, além do que existe a possibilidade de que tenham sido obtidos por meio de infrações à ordem econômica. Contudo, a relação entre uma coisa e outra não obrigatória.

A LGPD, por sua vez, prevê diversos instrumentos de restrição ao uso de dados pelos controladores e operadores. As medidas, contudo, tem natureza eminentemente individual. O enfoque que a LGPD dá é na proteção dos direitos subjetivos do titular de dados.[212]

---

[211] A esse respeito, a Lei Federal nº 12.529, de 30 de novembro de 2011, artigos 36 e 53.
[212] Nesse sentido, o Capítulo III da LGPD foca, especificamente, nos direitos do titular, como seu nome indica.

A separação de poderes, por outro lado, tem conotação procedimental e se destinaria ao controle a ser exercido sobre o comunicador fiduciário,[213] o qual seria o destinatário da norma. As proteções aos titulares, é certo, restringem as possibilidades de mau uso dos dados e protegem os cidadãos de diversos dos riscos enfrentados e narrados ao longo do capítulo 2 deste trabalho, principalmente.

No entanto, para que haja um efetivo controle do poder dos comunicadores fiduciários, que é a preocupação que se depreende a partir dos estudos desenvolvidos no capítulo 3, é imprescindível, também, que os processos de tomada de decisão quanto ao uso dos dados sejam objeto de atenção.

A pretensão, aqui, não é a de elencar formas pelas quais isso deva ou possa ocorrer; não obstante, uma preocupação que exsurge da LGPD é seu caráter eminentemente reativo: se o poder for mal utilizado, é possível combatê-lo. A história do constitucionalismo, contudo, nos mostrou que o mau uso do poder não é uma questão de *se*, mas uma questão de *quando*.[214]

Por isso, uma lógica de proteção e dados que se funde fortemente na enunciação de direitos do titular, passando ao largo do controle do poder em si, permanece insuficiente e não elimina, por completo, os riscos existentes na quantidade massiva de informações detidas pelos comunicadores fiduciários.

É possível, por exemplo, valer-se da ferramenta da separação de poderes para impedir o agrupamento de dados de espécies distintas em um mesmo comunicador fiduciário: um mesmo comunicador não poderia operar com dados oriundos de comunicação, saúde e educação, por exemplo. Essa solução seria análoga (porém distinta nos fundamentos) àquela que a Suprema Corte dos EUA deu, em 1911, à *Standard Oil Co. of New Jersey*.[215]

De qualquer maneira, o objetivo, neste trabalho, não é o de adentrar aplicações específicas de tais ferramentas constitucionais, mas de posicioná-las como efetivas possibilidades dotadas de utilidade e que devem, no cenário prático, ter sua aplicabilidade ponderada, inclusive como decorrência direta da Constituição Federal.

---

[213] Aqui, usaremos uma identidade entre o termo "comunicador fiduciário" e as ideias de controlador e operador definidas pelo artigo 5º da LGPD.

[214] No ponto, o alerta atribuído a Lord Acton de que "O poder corrompe. O poder absoluto corrompe absolutamente".

[215] ESTADOS UNIDOS DA AMÉRICA. Suprema Corte. ***Standard Oil Co. of New Jersey v. United Stades***, 221 U.S. 1 (1911): a gigante *Standard Oil*, de John D. Rockefeller, e que controlava desde a produção do petróleo até sua venda, passando pelas refinarias, foi cindida, com fundamento nas leis antitrustes, em trinta e quarto companhias distintas.

Nessa linha, é por isso que se elegeu a transparência[216] também como um elemento essencial derivado do constitucionalismo: aqui, entendida a transparência como a possibilidade de a sociedade saber o que é que se faz por detrás das portas do poder. A Declaração de Direitos da Virgínia, a esse respeito, já previa a liberdade de imprensa – que é um instrumento de transparência – como essencial à liberdade.[217]

No entanto, essa opção tem menos raízes na história do constitucionalismo – funda-se, mais, no elemento fiduciário caracterizados do fenômeno da comunicação contemporânea, que gera uma assimetria entre comunicadores e comunicantes e coloca a população à mercê justamente da fidúcia.

Sendo a relação de confiança um elemento essencial, e sendo o poder dela derivado, na geração do Big Data, bastante significativo, esse instrumento do constitucionalismo serve para se assegurar que, aquilo que se diz, é. Sem ela, mesmos os direitos de ordem individual, garantidos pela LGPD, tornam-se inócuos. Porque a questão, aqui, não é o direito de saber um determinado fato: mas de saber se não se está sendo enganado.

A LGPD, em seu artigo 18, garante, ao titular, o direito de confirmar a existência dos dados, acessá-los e corrigi-los. Como, no entanto, que um comunicador fiduciário não faltará com a verdade quando solicitado?

A solução está em um conceito explorado no capítulo 2: código aberto. A possibilidade de qualquer cidadão analisar a tecnologia por detrás dos comunicadores fiduciários é o único meio de assegurar a quais riscos a sociedade está se expondo – e, a partir disso, decidir, ou não, por corrê-los.

Metadados, por exemplo, podem ser utilizados para obter informações sensíveis de modo sub-reptício. Se isso ocorre, ou não, só uma análise aprofundada dos códigos permitirá concluir.

É bom destacar que o fato de o código ser aberto não implica violação de propriedade intelectual: havendo tal proteção, nenhum terceiro poderá utilizar o código. Mas todos poderão saber o que ele faz.

Essa, aliás, é uma medida condizente com uma sociedade que visa manter o poder sobre controle, e não é uma saída nova no Brasil: o STF, em algumas ocasiões, já destacou a

---

[216] Aqui, o termo é utilizado não sob a lógica de publicidade das atividades governamentais nos moldes o artigo 37 da CF/88, mas no sentido de informação acerca do exercício do poder: saber quem são os representantes, o que decidem, como fazem, enfim, conhecer as atividades desempenhadas pelos detentores de poder.

[217] SILVA, José Afonso da. **Curso de Direito Constitucional Positivo.** 42ª ed. São Paulo: Malheiros, 2019. P. 156.

necessidade de abertura de informações em prol de preocupações coletivas.[218] Não se pode pretender o exercício do poder indene de ônus.

4.3. Conclusões Provisórias

Neste derradeiro capítulo, pôde-se constatar a íntima ligação entre a moderna preocupação que permeia a privacidade – o controle do poder – e as preocupações intrínsecas ao constitucionalismo.

A proteção de dados, portanto, exsurgiu como uma consequência direta da Constituição Federal, mas indo além das tradicionais concepções que a atrelam a direitos individuais: a proteção de dados é, na essência, indissociável de qualquer Estado que pretenda não ser despótico – e assim se manter.

Viu-se, também, que a necessidade de se estabelecer uma relação teórica entre ambas as ideias guarda relação com outras linhas de pensamento jurídicas, porém possui suas próprias particularidades, com elas não se confundindo.

Por fim, este capítulo pretendeu indicar, sem pretensão de exaurir o debate, duas espécies de preocupações intimamente associadas ao controle do poder e que podem, às suas maneiras, servir como ferramentas úteis ao controle do poder derivado da massificação da coleta e do processamento de dados que resulta das tecnologias do século XXI.

[218] Um bom exemplo disso é a divulgação de salários de servidores públicos na internet, conforme decidido pelo STF no julgamento do recurso extraordinário com agravo nº 652.777/

CONCLUSÃO

Este trabalho pretendeu partir de um estudo sobre a privacidade para estabelecer conceitos utilizáveis: viu-se que o tema goza de grande polissemia: existem vários tipos de direitos, por vezes classificados de formas distintas, que são, habitualmente, tratados sob a rubrica da "privacidade".

Ao revés, pôde-se ver que a privacidade constitui uma espécie de "rede" que conecta diversos direitos tutelados com espaços de sobreposição. Defini-la, contudo, redundaria em conceitos ou muito amplos, ou muito estreitos, sem grandes utilidades práticas.

Por isso, acolheu-se a ideia de Richard Posner de tratá-la não a partir do que a privacidade é, mas a partir do que ela permite: como direito, a privacidade permite a um sujeito manter informações restritas.

Pôde-se, então, trazer o sigilo como uma ideia similar, porém focada não no sujeito titular da privacidade em uma dada hipótese, mas no terceiro que se obriga a mantê-la privada, analisando o sigilo a partir de sua ideia de *dever*.

Em seguida, buscou-se definir dados como elementos relativos a fatos, de natureza bruta, que, após passarem por procedimento de análise, podem ser convertidos em informações, as quais seriam os dados utilizáveis.

Diante disso, pôde-se compreender a proteção de dados como a disciplina desses elementos informativos brutos com vistas a proteger não apenas os dados em si, mas as informações que deles podem ser obtidas.

O capítulo 2 objetivou perquirir acerca das potencialidades dos dados, assim considerados a partir de uma perspectiva pragmática que objetivava analisar de que forma a tecnologia atual permite expandir a capacidade de obtenção de dados, e, a partir deles, de informações.

Utilizou-se, também, taxonomia para identificar quais riscos exsurgem dessas potencialidades, exemplificando os potenciais derivados do mau uso de dados e evidenciando os perigos que os dados apresentam – e que decorrem de seu poder como ferramenta.

Passando-se ao capítulo 3, logrou-se demonstrar que a preocupação com privacidade, inicialmente atrelada a uma perspectiva bastante individualista, mudou seu foco para passar a centralizar em uma discussão relativa ao controle do poder. O direito, antes de ordem individual, adquiriu um elemento social e político. O dilema da informação deixou de ser o conflito entre o indivíduo e a sociedade porque proteger o indivíduo passou a ser, também, um interesse da sociedade.

Essa constatação causou perplexidade porque dilemas relativos ao controle do poder não são típicos de direito privado; ao contrário, essa é a temática de que se ocupa o direito constitucional há vários séculos. Isso conduziu ao pensamento de que, se o problema é o mesmo, talvez o direito constitucional tenha instrumentos utilizáveis voltados à resolução e mitigação dos riscos que o tratamento de dados contemporâneo apresenta à sociedade.

Desse assunto ocupou-se o derradeiro capítulo 4, onde se estabeleceu um vínculo entre o constitucionalismo moderno e a problemática atinente à proteção de dados. Nessa toada, a proteção de dados sobressaiu como uma consequência direta do constitucionalismo não somente na perspectiva de proteção de direitos individuais – uma vez que esta, de cunho mais individualista, ainda se manteve – mas, também, como o resultado da preocupação constitucional central com a limitação do poder.

Sem pretensão de exaurir o tema, o capítulo 4 também se ocupou em demonstrar a importância da diferenciação teórica, destacando a sua não trivialidade: muito embora outras linhas de pensamento jurídico possam dar soluções que satisfaçam o problema, nenhuma delas terá o embasamento teórico na Constituição que permite lidar com o problema de forma completa. Podem servir para tratar o sintoma, mas, para curar a doença, é preciso diagnosticá-la adequadamente.

Ao final, apresentou-se ideias, oriundas do pensamento constitucional, que podem ter aplicabilidade nos debates que permeiam a proteção de dados. O atual plexo normativo, consubstanciado, principalmente, na LGPD, é bastante evoluído, mas não é capaz, por si só, de dar um ponto final aos riscos que o processamento massificado de dados apresenta.

Em última análise, portanto, a preocupação é democrática: proteção de dados deve ser vista, e tratada, como uma temática indissociável de qualquer Estado que preze pela limitação do poder e que não deseje se sujeitar aos riscos do despotismo. É uma questão constitucional.

BIBLIOGRAFIA

ACHTER, Paul J. McCarthyism. ***Britannica*.** Disponível em: <https://www.britannica.com/topic/McCarthyism>.

ALEMANHA, República Federal da. *Bundesdatenschutzgesetz*, de 27 de janeiro 1977. *Mißbrauch personenbezogener Daten bei der Datenverarbeitung*. ***Bundesgesetzblatt* I:** Berlim, 1º de fevereiro de 1977, seção I, n. 7 p. 201. Em vigor a partir de 1º de janeiro de 1978.

_____. ***Bundesverfassungsgericht***, sentença do Primeiro Senado de 15 de dezembro de 1983. Karlsruhe, 1 BvR 209/83, Rn. 1-215.

_____. *Volkszählungsgesetz*, de 25 de março de 1982. *Gesetz über eine Volks-, Berufs, Wohnungs- und Arbeitsstättenzählung*. ***Bundesgesetzblatt*:** Berlim, 31 de março de 1982, seção I, n. 13, p. 369.

ALEXY, Robert. **Teoria dos Direitos Fundamentais.** Trad. Virgílio Afonso da Silva. 2ª ed. São Paulo: Malheiros, 2012.

ANGWIN, Julia, et al. Machine Bias. **ProPublica,** 23 de maio de 2016. Disponível em: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.

APPLE. **Controle as informações de localização compartilhadas no iPhone**. Manual do Usuário do iPhone. Disponível em: <https://support.apple.com/pt-br/guide/iphone/iph3dd5f9be/ios>.

ARANHA, Márcio Iorio. **Manual de Direito Regulatório: Fundamentos de Direito Regulatório**. 4ª ed. Londres: Laccademia Publishing, 2018.

ARENDT, Hannah. **A Condição Humana.** Trad. Roberto Raposo. 10. ed. Rio de Janeiro: Forense Universitária, 2007.

_____. **Origens do totalitarismo.** Trad. Roberto Raposo. 1ª ed. São Paulo: Companhia das Letras, 2012.

ARISTÓTELES. **A Política**. Trad. Roberto Leal Ferreira. 3ª ed. São Paulo: Martins Fontes, 2006.

BALKIN, Jack M. *Free Speech is a Triangle.* ***Columbia Law Review***, Nova York, vol. 118, 2018, p. 2011-2056.

BARBOSA, Ruy. ***Os Actos Inconstitucionaes do Congresso e do Executivo ante a Justiça Federal*.** Rio de Janeiro: Companhia Impressora, 1893.

BARRA DE SOUZA, Matheus. **A *Political Question Doctrine* no Direito Brasileiro.** Monografia (Bacharelado em Direito). Faculdade de Direito, Universidade de Brasília. Brasília, p. 79, 2018.

BAUMAN, Zygmunt. **Vigilância Líquida.** Trad. Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

BBC, 21 de junho de 2021. Disponível em: <https://www.bbc.com/news/world-asia-china-22278037>.

BENTHAM, Jeremy. **O Panóptico.** Belo Horizonte: Autêntica, 2000.

BERNANOS, Georges. **A França contra os robôs.** Trad. Lara Christina de Malimpensa. 1ª ed. São Paulo: É Realizações, 2018 [1947].

BLOUSTEIN, Edward. *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser.* ***New York University Law Review*****,** Nova York, vol. 39, n. 6, 1964, p. 962-1007.

BONAVIDES, Paulo. **Curso de Direito Constitucional.** 34ª ed. São Paulo: Malheiros, 2019.

BRASIL, República Federativa do. Constituição (1824). **Constituição Política do Império do Brazil (de 25 de março de 1824).** Coleção de Leis do Império do Brasil, página 7, vol. 1, Rio de Janeiro, 1824.

_____. **Constituição da República Federativa do Brasil de 1988.** Diário Oficial da União, Brasília, 5 de outubro de 1988.

_____. **Decreto-Lei nº 2.848**, de 7 de dezembro de 1940. Código Penal. Diário Oficial da União: Rio de Janeiro, 31 de dezembro de 1940.

_____. **Lei Complementar nº 105**, de 10 de janeiro de 2001. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Diário Oficial da União: Brasília, 11 de janeiro de 2001.

_____. **Lei nº 10.406**, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, ano 139, n. 8, p. 1-74, 11 jan. 2002.

_____. **Lei nº 12.529**, de 30 de novembro de 2011. Estrutura o Sistema Brasileiro de Defesa da Concorrência; dispõe sobre a prevenção e repressão às infrações contra a ordem econômica; altera a Lei nº 8.137, de 27 de dezembro de 1990, o Decreto-Lei nº 3.689, de 3 de outubro de 1941 - Código de Processo Penal, e a Lei nº 7.347, de 24 de julho de 1985; revoga dispositivos da Lei nº 8.884, de 11 de junho de 1994, e a Lei nº 9.781, de 19 de janeiro de 1999; e dá outras providências. Diário Oficial da União: Brasília, 1º de novembro de 2011.

_____. **Lei nº 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Diário Oficial da União: Brasília, 15 de agosto de 2018.

_____. **Lei nº 5.172**, de 25 de outubro de 1966. Dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios. Diário Oficial da União: Brasília, 27 de outubro de 1966.

_____. **Lei nº 9.296**, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Diário Oficial da União: Brasília, 25 de julho de 1996.

_____. Supremo Tribunal Federal. ***Habeas Corpus* nº 91.867/PA.** Rel. Min. Gilmar Mendes. Segunda Turma, julgado em 24/04/2012, ACÓRDÃO ELETRÔNICO DJe-185 DIVULG 19-09-2012 PUBLIC 20-09-2012.

_____. Supremo Tribunal Federal. **Referendo da Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6.387/DF.** Rel. Min. Rosa Weber. Tribunal Pleno, julgado em 07/05/2020, PROCESSO ELETRÔNICO DJe-270 DIVULG 11-11-2020 PUBLIC 12-11-2020.

BUTTERFIELD, Kevin. *Metadata: An Overview*. ***AALL Spectrum*,** v. 6, n. 3, 2001, p. 24-28.

CANCELIER, Mikhail Vieira de Lorenzi. O Direito à Privacidade hoje: perspectiva histórica e cenário brasileiro. **Sequência,** Florianópolis, n. 76, p. 213-240, 2017.

CANOTILHO, J. J. Gomes. **Direito Constitucional e Teoria da Constituição.** 7ª ed. Coimbra: Almedina, 2000.

CARRINGTON, David; VANDEWIELE, Alida. *What Is Metadata?* ***International In-House Counsel Journal***, v. 8, n. 31, 2015, p1-7.

CHAN, Justin. *Hong Kong sees rush for burner phones as government pushes contact-tracing app.* ***Reuters*.** 18 de fevereiro de 2021. Disponível em: <https://www.reuters.com/article/us-health-coronavirus-hongkong-idUSKBN2AI0I8>.

COHEN, Julie. *What Privacy is For.* ***Harvard Law Review*,** v. 126, n.7, 2014, p. 1904-1933.

CONSULTOR JURÍDICO. **Comissão Europeia troca WhatsApp por Signal para aumentar segurança**. São Paulo, 11 de janeiro de 2021. Disponível em: <https://www.conjur.com.br/2021-jan-11/comissao-europeia-troca-whatsapp-signal-aumentar-seguranca>.

CORREIA, Marcos Balster Fiore. **A comunicação de dados estatísticos por intermédio de infográficos: uma abordagem ergonômica**. Rio de Janeiro: Pontifícia Universidade Católica do Rio de Janeiro, 2009.

DE VYNK, Gerrit. *Google is totally changing how ads track people around the Internet. Here's what you need to know.* ***The Washington Post*,** 18 de junho de 2021. Disponível em: <https://www.washingtonpost.com/technology/2021/06/18/google-is-totally-changing-how-ads-track-people-around-internet-heres-what-you-need-know/>.

DEWEY, John. ***Problems of Men*.** New York: Philosophical Library, 1946

DEWEY, John; TUFTS, James H. ***Ethics*.** New York: Henry Holt and Company, 1908.

DONEDA, Danilo. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. In: TEPEDINO, Gustavo (org.). **Problemas de direito civil-constitucional.** Rio de Janeiro: Renovar, 2000, pp. 111-136.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados**. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019.

ESTADOS UNIDOS DA AMÉRICA. Suprema Corte. ***Standard Oil Co. of New Jersey v. United Stades*****,** 221 U.S. 1 (1911).

ETZIONI, Amitai. *A Communitarian Perspective on Privacy.* ***Connecticut Law Review*****,** v. 32, n. 3, 2000, p. 897-906.

ETZIONI, Amitai. *A Liberal Communitarian Conception of Privacy.* ***John Marshall Journal of Computer and Information Law*****,** v. 29, n. 3, 2012, p. 419-462.

FERRAZ JR., Tércio Sampaio. **Introdução ao estudo do direito:** técnica, decisão, dominação. 7ª ed. São Paulo: Atlas, 2013.

_____. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito, Universidade de São Paulo,** n. 88, p. 439-459, 1993.

FONTEVECCHIA, Agustino. *Seth Stephens-Davidowitz: "Big data isn't good or bad, it's powerful".* ***Buenos Aires Times*****,** 26 de outubro de 2019.

FORDE, Aidan. *The Conceptual Relationship between Privacy and Data Protection.* ***Cambridge Law Review*****,** v. 1, n. 135, 2016, p. 135-149.

FRIED, Charles. *Privacy.* ***Yale Law Journal*****,** v. 77, n. 3, 1968, p.475-493

GAJDA, Amy. What if Samuel D. *Warren hadn't married a Senator's daughter? uncovering the press coverage that led to "The Right to Privacy".* ***Michigan State Law Review*****,** n. 35, 2008, p. 35-60.

GENTZKOW, Matthew; SHAPIRO, Jesse; TADDY, Matt. *Measuring Group Differences in High-Dimensional Choices: Method and Application to Congressional Speech.* ***Econometrica*****,** v. 87, n. 4, 2019, p. 1307-1340.

GENTZKOW, Matthew; SHAPIRO, Jesse; TADDY, Matt. *Measuring Polarization in High-Dimensional Data: Method and Application to Congressional Speech.* ***Stanford Institute for Economic Policy Research*****.** Working Paper, 2016.

GILLILAND, Anne J. *Setting the Stage*. In: ***Introduction to Metadata*****,** BACA, Murtha. 2ª ed. Los Angeles: Getty Research Institute, 2008.

GOOGLE. **Google Street View.** Disponível em: <https://www.google.com.br/maps>.

GRONHOLT-PEDERSEN, Jacob; BING, Christopher; JOHNSON, Simon. ***U.S. spied on Merkel and other Europeans through Danish cables - broadcaster DR***. Disponível em: <https://www.reuters.com/world/europe/us-security-agency-spied-merkel-other-top-european-officials-through-danish-2021-05-30/>.

GUTWIRTH, Serge; DE HERT, Paul. *Privacy, Data Protection and Law Enforcement: Opacity of the individual and Transparency of the Power*. In: CLAES, E; DUFF, A; GUTWIRTH, S. (Ed.). ***Privacy and the Criminal Law*****.** Antwerp/Oxford: Intersentia, 2006.

HESSE, Konrad. **A Força Normativa da Constituição.** Trad. Gilmar Ferreira Mendes. Porto Alegre: Sérgio Antônio Fabris Editor, 1991.

HIRSHLEIFER, Jack. *Privacy: its origin, function, and future.* ***Journal of Legal Studies*****,** vol. 9, n. 4, 1980, p. 649-664.

HUGHES, Kirsty. *The Social Value of Privacy***.** In: ROESSLER, Beate; MOKROSINSKA, Dorota (Org.). ***Social Dimensions of Privacy: Interdisciplinary Perspectives***. Cambridge: Cambridge University Press, 2015.

KAFKA, Franz. **O Processo.** Trad. Marcelo Backes. Porto Alegre: L&PM, 2018 [1925].

KELSEN, Hans. **Teoria Pura do Direito.** 8ª ed. São Paulo: Martins Fontes, 2009.

KRAMER, Adam; GUILLORY, Jamie; HANCOCK, Jeffrey. *Experimental evidence of massive-scale emotional contagion through social networks.* ***PNAS*****,** v. 111, n. 24, 2014.

LAVADO, Thiago. WhatsApp: o que muda com os novos termos de uso? É hora de trocar de app? **Exame.** São Paulo, 14 de janeiro de 2021. Disponível em: <https://exame.com/tecnologia/whatsapp-o-que-muda-com-os-novos-termos-de-uso-e-hora-de-trocar-de-app/>.

MAGNET, Pen. *WhatsApp Doesn't Read Your Messages, It Doesn't Need To.* ***Medium*****,** 8 de janeiro de 2021. Disponível em: <https://medium.com/swlh/whatsapp-doesnt-read-your-messages-it-doesn-t-need-to-7ce0ec2846f9>.

MARTINS FILHO, Ives Gandra. Direitos Fundamentais. In: MARTINS, Ives Gandra da Silva/ MENDES, Gilmar Ferreira; NASCIMENTO, Carlos Valder (Org.). **Tratado de Direito Constitucional.** Vol. 1. 2ª ed. São Paulo: Saraiva, 2012.

MASON, Alpheus Thomas. ***Brandeis: A Free Man's Life*****.** New York: The Viking Press, 1946.

MCSTAY, Andrew. ***Privacy and philosophy*****.** Nova Iorque: Peter Lang, 2014.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional.** 13ª ed. São Paulo: Saraiva Educação, 2018.

MENDES, Laura Schertel Ferreira. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais. **Jota.** Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020>.

MEYER, Michelle N. *Two Cheers for Corporate Experimentation: The A/B Illusion and the Virtues of Data-Driven Innovation.* ***Colorado Technology Law Journal*****,** v. 13, n. 2, 2015, p. 273-332.

MICHLER, Carla. *The Procurement Decision – Open or Closed Source Software.* ***Deakin Law Review*****,** v. 10, n. 1, 2005, p. 261-270.

MILL, John Stuart. ***Utilitarianism*.** The Floating Press, 2009 [1861]. Ebook.

MILLER, Greg. *The intelligence coup of the century.* ***The Washington Post*.** Washington, 11 de fevereiro de 2020. Disponível em: <https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/>.

MONTESQUIEU, Charles de Secondat, Baron de. **O Espírito das Leis.** São Paulo: Martins Fontes, 2005 [1748].

NBC News. ***Man questioned by police for Google search history***. 1º de Agosto de 2013. Disponível em: <https://www.nbcnews.com/technolog/man-questioned-police-google-search-history-6c10824803>.

NEGLEY, Glenn. *Philosophical Views on the Value of Privacy.* ***Law and Contemporary Problems*,** v. 31, n. 2, 1966, 319-325.

OLIVEIRA, Eliane. China reage a nova provocação de Eduardo Bolsonaro sobre 5G e afirma que deputado perturba parceria com Brasil. **O Globo.** Rio de Janeiro, 24 de novembro de 2020. Disponível em: <https://oglobo.globo.com/economia/china-reage-nova-provocacao-de-eduardo-bolsonaro-sobre-5g-afirma-que-deputado-perturba-parceria-com-brasil-1-24763500>.

OLIVEIRA, Luciano. Não fale do Código de Hamurábi! **Anuário dos Cursos de Pós-Graduação em Direito (UFPE)**, v. 13, 2003, p. 299-330.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Assembleia Geral das Nações Unidas. **Declaração Universal dos Direitos Humanos**, de 10 de dezembro de 1948. Disponível em: <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>.

PANG, Jessie; SIU, Tyrone. *Closure looms for Hong Kong's pro-democracy Apple Daily after raids.* ***Reuters*,** 21 de junho de 2021. Disponível em: <https://www.reuters.com/world/asia-pacific/hong-kongs-apple-daily-board-may-stop-publication-this-week-memo-2021-06-21>.

PERES-NETO, Luiz. Ética e privacidade: múltiplos olhares a partir do campo da comunicação. In: BRANCO, S. TEFFÉ, C. (Org.). **Privacidade em Perspectivas**. 1ª ed. Rio de Janeiro: Lumen Juris, 2018.

PLATÃO. **A República.** Tradução: Ciro Mioranza. São Paulo: Lafonte, 2017.

POSNER, Richard A. *The Right of Privacy.* ***Georgia Law Review*,** Athens, vol. 12, n. 3, 1978, p. 393.

POST, Robert. *The Social Foundations of Privacy: Community and Self in the Common Law Tort.* ***California Law Review*,** v. 77, n. 5, 1989, p. 957-1010.

PROSSER, William L. *Privacy.* ***California Law Review*,** Berkeley, vol. 38, n. 3, 1960.

RICHARDS, Neil. *The Dangers of Surveillance.* ***Harvard Law Review*,** v. 126, n. 7, 2013, p. 1934-1965.

RODOTÀ, Stefano. **A Vida na Sociedade da Vigilância: A privacidade hoje**. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SAMUEL, Ian James. *Warantless Location Tracking.* ***New York University Law Review*****,** v. 83, n. 4, 2008, p. 1324-1352.

SARFARAZ, Hina. *Surveillance, Privacy and Cyber Law.* ***Computer and Telecommunications Law Review*****,** v. 20, n. 7, 2014, p. 189-194.

SARLET, Ingo. **A Eficácia dos Direitos Fundamentais.** 13ª ed. Porto Alegre: Livraria do Advogado, 2018.

SARMENTO, Daniel. **Direitos Fundamentais e Relações Privadas.** Rio de Janeiro: Lumen Juris, 2004.

SCHNEIER, Bruce. *The Eternal Value of Privacy.* ***Schneier on Security*****,** 18 de maio de 2006. Disponível em: <https://www.schneier.com/essays/archives/2006/05/the_eternal_value_of.html>.

SHEDROFF, Nathan. *Information interaction design: an unified field theory of design*. In: JACOBSON, Robert (Org.). ***Information Design*****.** Cambridge: The MIT Press, 1999.

SILVA, José Afonso da. **Curso de direito constitucional positivo.** 42ª ed. São Paulo: Malheiros, 2019.

SILVA, Virgílio Afonso da. A **Constitucionalização do Direito: Os direitos fundamentais nas relações entre particulares**. São Paulo: Malheiros, 2005.

SLAUGHTER, Matthew J.; MCCORMICK, David H. *Data Is Power.* ***Foreign Affairs*****,** v. 100, n. 3, maio/junho 2021, p. 54-63.

SOLOVE, Daniel. *"I've Got Nothing To Hide" and Other Misunderstandings of Privacy.* ***San Diego Law Review*****,** vol. 44, p. 745-772, 2007.

_____. *A Taxonomy of Privacy.* ***University of Pennsylvania Law Review*****,** v. 154, n. 3, 2006, p. 477-564.

_____. *Conceptualizing Privacy.* ***California Law Review*****,** v. 90, n. 4, 2002, 1087-1156.

_____. ***Nothing to Hide: The False Tradeoff between Privacy and Security***. New Haven: Yale University Press, 2011.

_____. *Privacy and Power: Computer Databases and Metaphors for Information Privacy.* ***Stanford Law Review*****,** v. 53, n. 6, 2001, p. 1393-1462.

STEPHENS, Randall. *The Creator of Bitcoin, Satoshi Nakamoto, Is Most Likely This Guy.* ***Medium*****,** 9 de março de 2019. Disponível em: <https://medium.com/swlh/the-creator-of-bitcoin-satoshi-nakamoto-is-most-likely-this-guy-8723eddb517c>.

STEPHENS-DAVIDOWITZ, Seth. **Todo mundo mente: o que a internet e os dados dizem sobre quem realmente somos**. Trad. Wendy Campos. Rio de Janeiro: Alta Books, 2018.
Tor Project. Disponível em: <https://www.torproject.org/>.

UNIÃO EUROPEIA. Regulamento nº 679, de 27 de abril de 2016. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de Abril de 2016:** relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados. Bruxelas, Bélgica.

VALE, André Rufino do. Reis-juízes ou reis-legisladores? O dilema platônico e o problema da legitimação democrática da Jurisdição Constitucional. **Caderno Virtual,** v. 3, n. 9, 2004, p. 1-15.

WALDRON, Jeremy. *Separation of Powers in Thought and Practice?* ***Boston College Law Review*****,** v. 54, n. 2, 2013, p. 433-468.

WARREN, Samuel D.; BRANDEIS, Louis D. *The Right to Privacy.* ***Harvard Law Review*****,** Cambridge, vol. 4, n. 5, 1890.

WESTIN, Alan. ***Privacy and Freedom*****.** New York: Ig Publishing, 1967.

WHATSAPP. **FAQ do *WhatsApp*.** Disponível em: <https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption/?lang=pt_br>.

YANG, Allie. *Many Capitol rioters implicated by their own social media posts.* ***ABC News*****.** Nova York, 11 de janeiro de 2021. Disponível em: <https://abcnews.go.com/Technology/capitol-rioters-implicated-social-media-posts/story?id=7517767>2.