

# ESTADO, REGULAÇÃO E TRANSFORMAÇÃO DIGITAL

O FUTURO DAS DEMOCRACIAS: HIPERVIGILÂNCIA,  
FAKE NEWS E OUTRAS AMEAÇAS

## ORGANIZADORES

ANDRÉ KARAM TRINDADE  
ELDA COELHO DE AZEVEDO BUSSINGUER  
INGO WOLFGANG SARLET

## COORDENADORES

ALEXANDRE BARBOSA DA SILVA  
ALFREDO COPETTI NETO

**tirant**  
lo blanch

Organizadores

**André Karam Trindade**  
**Elda Coelho de Azevedo Bussinguer**  
**Ingo Wolfgang Sarlet**

Coordenadores

**Alexandre Barbosa da Silva**  
**Alfredo Copetti Neto**

# ESTADO, REGULAÇÃO E TRANSFORMAÇÃO DIGITAL

O FUTURO DAS DEMOCRACIAS: HIPERVIGILÂNCIA, FAKE NEWS E OUTRAS AMEAÇAS



**tirant**  
lo blanch

**Copyright**© Tirant lo Blanch Brasil

*Editor Responsável:* Aline Gostinski

*Assistente Editorial:* Izabela Eid

*Diagramação e Capa:* Analu Brettas

**CONSELHO EDITORIAL CIENTÍFICO:**

**EDUARDO FERRER MAC-GREGOR POISOT**

*Presidente da Corte Interamericana de Direitos Humanos. Investigador do Instituto de Investigações Jurídicas da UNAM - México*

**JUAREZ TAVARES**

*Catedrático de Direito Penal da Universidade do Estado do Rio de Janeiro - Brasil*

**LUIS LÓPEZ GUERRA**

*Ex Magistrado do Tribunal Europeu de Direitos Humanos. Catedrático de Direito Constitucional da Universidade Carlos III de Madrid - Espanha*

**OWEN M. FISS**

*Catedrático Emérito de Teoria de Direito da Universidade de Yale - EUA*

**TOMÁS S. VIVES ANTÓN**

*Catedrático de Direito Penal da Universidade de Valência - Espanha*

C895

Estado, regulação e transformação digital : o futuro das democracias: hipervigilância, fake news e outras ameaças [livro eletrônico] / Aldacy Rachid Coutinho ... [et. al.]; André Karam Trindade, Elda Coelho de Azevedo Bussinguer, Ingo Wolfgang Sarlet (org.); Alexandre Barbosa da Silva, Alfredo Copetti Neto (coord.). -1.ed. – São Paulo : Tirant lo Blanch, 2023.

1Kb; livro digital

ISBN: 978-65-5908-630-6.

1. Estado. 2. Regulação. 3. Tecnologia. I. Título.

CDU: 342.727

Bibliotecária responsável: Elisabete Cândida da Silva CRB-8/6778

DOI: 10.53071/boo-2023-07-27-64c1c4f33a6ec

*É proibida a reprodução total ou parcial, por qualquer meio ou processo, inclusive quanto às características gráficas e/ou editoriais. A violação de direitos autorais constitui crime (Código Penal, art. 184 e §§, Lei n° 10.695, de 01/07/2003), sujeitando-se à busca e apreensão e indenizações diversas (Lei n° 9.610/98).*



***Todos os direitos desta edição reservados à Tirant lo Blanch.***

Fone: 11 2894 7330 / Email: editora@tirant.com / atendimento@tirant.com  
tirant.com/br - editorial.tirant.com/br/

Organizadores

**André Karam Trindade**  
**Elda Coelho de Azevedo Bussinguer**  
**Ingo Wolfgang Sarlet**

Coordenadores

**Alexandre Barbosa da Silva**  
**Alfredo Copetti Neto**

# ESTADO, REGULAÇÃO E TRANSFORMAÇÃO DIGITAL

O FUTURO DAS DEMOCRACIAS: HIPERVIGILÂNCIA, FAKE NEWS E OUTRAS AMEAÇAS

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) – Código de Financiamento 001

Autores

Aldacy Rachid Coutinho  
Alfredo Copetti Neto  
Amanda Antonelo  
André Karam Trindade  
Clarissa Tassinari  
Danilo Pereira Lima  
Elda Coelho de Azevedo Bussinguer  
Eugênio Facchini Neto  
Fabio Luis Celli  
Georges Abboud  
Ingo Wolfgang Sarlet  
Jacinto Nelson de Miranda Coutinho  
Jorge Pereira da Silva  
Lenio Luiz Streck  
Luigi Ferrajoli  
Marcos Ehrhardt Jr.  
Milton Pereira de França Netto  
Phillip Gil França  
Thiago Santos Rocha



**tirant**  
lo blanch



# NOMINATA DE AUTORES

## **Aldacy Rachid Coutinho**

Doutora em Direito (UFPR). Professora Titular de Direito do Trabalho da Universidade Federal do Paraná (aposentada). Professora do Programa de Pós-Graduação em Direito, Inovação e Regulação da UNIVEL.

## **Alfredo Copetti Neto**

Pós-doutorado em Direito (UNISINOS). Doutor em Direito (UNIROMA3/ITÁLIA). Coordenador do Programa de Pós-Graduação em Direito, Inovação e Regulação da UNIVEL. Professor Adjunto de Teoria do Direito da Universidade Estadual do Oeste do Paraná.

## **Amanda Antonelo**

Mestre em Direito, Inovação e Regulações (UNIVEL).

## **André Karam Trindade**

Doutor em Teoria e Filosofia do Direito (UNIROMA3/ITÁLIA). Professor do Programa de Pós-Graduação em Direito, Inovação e Regulação da UNIVEL. Professor Visitante da Università Degli Studi Roma Tre.

## **Clarissa Tassinari**

Pós-doutorada em Direito (UNISINOS). Professora do Programa de Pós-Graduação em Direito da UNISINOS.

## **Danilo Pereira Lima**

Doutor em Direito Público (UNISINOS). Professor do Curso de Direito do Centro Universitário Claretiano de Batatais.

## **Elda Coelho de Azevedo Bussinguer**

Doutora em Bioética (UnB). Coordenadora do Programa de Pós-Graduação em Direito da Faculdade de Direito de Vitória. Presidente da Sociedade Brasileira de Bioética.

## **Eugênio Facchini Neto**

Doutor em Direito Comparado (UNIFI/ITÁLIA). Professor da Escola de Direito e dos Cursos de Mestrado e Doutorado em Direito da Pontifícia Universidade Católica do Rio Grande do Sul.

## **Fabio Luis Celli**

Mestrando em Direito, Inovação e Regulações (UNIVEL).

## **Georges Abboud**

Livre-docente e doutor em Direito (PUC/SP). Professor do Programa de Pós-Graduação em Direito do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa e da Pontifícia Universidade Católica de São Paulo.

## **Ingo Wolfgang Sarlet**

Doutor em Direito pela Universidade de Munique (LMUM/ALEMANHA). Professor Titular da Escola de Direito e Coordenador dos Cursos de Mestrado e Doutorado em Direito da Pontifícia Universidade Católica do Rio Grande do Sul.

## **Jacinto Nelson de Miranda Coutinho**

Doutor em Direito (LA SAPIENZA/ITÁLIA). Professor dos Programas de Pós-Graduação em Direito da UNIVEL e da DAMAS. Professor Colaborador do Programa de Pós-Graduação em Ciências Criminais da PUCRS.

## **Jorge Pereira da Silva**

Doutor em Direito (UCP/PORTUGAL). Professor da Faculdade de Direito da Universidade Católica Portuguesa, onde atualmente dirige a Escola de Direito.

## **Lenio Luiz Streck**

Pós-doutorado em Direito Constitucional (FDUL/PORTUGAL). Doutor e Mestre em Direito do Estado (UFSC). Professor Titular dos Cursos de Mestrado e Doutorado dos Programas de Pós-Graduação em Direito da UNISINOS/RS e da UNESA/RJ.

## **Luigi Ferrajoli**

Livre Docente em Filosofia do Direito. Professor Emérito da Università Degli Studi Roma Tre. Doctor Honoris Causa em inúmeras Universidades da América Latina.

## **Marcos Ehrhardt Jr.**

Doutor em Direito (UFPE). Professor de Direito Civil da Universidade Federal de Alagoas (UFAL). Professor do Centro Universitário Cesmac.

## **Milton Pereira de França Netto**

Mestrando em Direito (CESMAC).

## **Phillip Gil França**

Pós-doutorado em Direito (PUCRS). Professor do Programa de Pós-Graduação em Direito, Inovação e Regulação da UNIVEL. Professor da Escola da Magistratura do Paraná.

## **Thiago Santos Rocha**

Doutorando em Direito (PUCRS/OVIEDO).

# COMPLIANCE JURÍDICO: ENTRE EFICÁCIA, EFETIVIDADE E EFICIÊNCIA

ALDACY RACHID COUTINHO

## 1. INTRODUÇÃO

*Compliance* é, sobretudo, a afirmação de um compromisso com valores éticos e com a integridade. E, como anotado por Rotsch, “ha protagonizado una carrera vertiginosa” representando “por completo un nuevo objeto de trabajo de la Ciencia jurídica<sup>1</sup>”. Não se trata, pois, da externalização da manifestação de um desejo ou um conselho, nem uma aposta dirigida a um futuro incerto. O agir em conformidade pressupõe, então, um padrão comportamental ditado por regras presentes na sociedade e advindas da cultura em relação às quais a observância e a obediência se traduz em um mandamento imperativo.

A ordem jurídica revela, então, sua constituição mandatória. Assim também toda ordem ética, como ressalta Ascensão, pois estando baseada em uma noção de dever ser, se traduz em regras caracterizadas pela imperatividade, tomada no sentido de revelação da exigência de sua aplicação<sup>2</sup>.

As regras que ditam os comportamentos advêm tanto de uma normatividade jurídica vigente emanada do poder público, quanto daquelas fixadas no campo privado no espaço reconhecido da autonomia pela autorregulação:

Si la autorregulación es el resultado imprevisto de la necesaria evolución del modo en el que el Estado regula el mundo empresarial, debemos preguntarnos entonces por qué razón se ha convenido que la pura heterorregulación no es suficiente ni adecuada, al menos con carácter general, para disciplinar de forma conveniente la actividad empresarial. La respuesta al uso es simple: el Estado ya no está en disposición de hacerlo, o al menos, de hacerlo en solitario<sup>3</sup>.

Autonomia não mais se situa nos marcos do dogma da vontade; superada na modernidade, hoje tem-se que a autonomia privada constitucional é externalização de um dado jurídico, pelo poder limitado assegurado a sujeitos de direito dentro da ordem jurídica para que, autorizados, sejam estabelecidas normati-

---

1 ROTSCH, Thomas. Criminal compliance. InDret – Revista para el analisis del derecho, Barcelona, jan. 2012, p. 1-11. Disponível em: <https://indret.com/wp-content/themes/indret/pdf/876a.pdf> Acesso em: 20nov. 2022, p. 2; p. 9.

2 ASCENSÃO, José de Oliveira. O direito: introdução e teoria geral. Uma perspectiva luso-brasileira. 11. ed. Coimbra: Almedina, 2001, p. 37.

3 VILA, Ivó Coca. ¿Programas de cumplimiento como forma de autorregulación regulada? In: Criminalidad de empresa y compliance: prevención y reacciones corporativas. SÁNCHEZ, Jesús-María Silva (dir.); FÉRNANDEZ, Raquel Montaner (coord.) Barcelona : Atelier libros, 2013, p. 45.

vidades imperativas com coercibilidade no campo da gestão dos seus interesses particulares e coletivos: um poder de autogoverno da vida em sociedade.

Autonomia privada em que se funda a criação de um Programa de Compliance, é ‘o poder que os particulares têm de regular, pelo exercício de sua própria vontade, as relações de que participam, estabelecendo-lhes o conteúdo e a respectiva disciplina jurídica<sup>4</sup>’. Não há, pois, nem superposição de fontes, nem delegação de poder estatal, senão uma atuação correlata e complementar nos espaços autorizados para (auto)regulação. Não é o que se quer, mas o que se pode, e não se pode tudo, menos ainda tudo o que se quer, segundo o direito.

Ordem jurídica se consolida no espaço democrático pela adoção de normas de organização e normas de conduta. A submissão, de todos, à ordem jurídica vem acompanhada da coercibilidade, pelo que é inerente ao Estado o uso da força para ver-se aplicadas consequências a todos os que violam ou desatendem suas normas, assim entendidas as regras e os princípios. O emprego da força volta-se não somente para cumprimento das fontes heterônomas, mas ainda para as autônomas.

No espaço da autorregulação regulada, mais consentânea com a perspectiva de um Estado Regulador<sup>5</sup>, regras sobre ações e procedimentos são então criadas e, dentre outras possibilidades, os Programas de Compliance, Códigos de Conduta, de Boas Práticas, de Integridade ganham juridicidade, com atuação inclusive em investigações e sancionamentos.

Imperioso, de todo modo, ressaltar que o Programa de Compliance não tem o único objetivo de assegurar aplicabilidade e observância às normas jurídicas estatais vigentes, eis que são as detentoras de imperatividade e coercibilidade. Cabe ao próprio Estado a investigação e coerção, inclusive com aplicação de sanções e penas, pela violação de suas normas. Seria, para tal escopo, inútil por desnecessário; talvez uma espécie de manifestação obsessiva e compulsiva pela ordem.

A função de compliance, portanto, volta-se à promoção e à prevenção no espaço de atuação dos interesses da corporação ou organização e não no interesse imediato geral e abstrato; indiretamente pode servir de instrumento auxiliar para conformidade com o sistema normativo estatal. A observância do direito é, afinal, um valor da ética e da cultura empresarial: “[...] el consenso parece total. [...] ‘una cultura empresarial basada en valores’ es un factor del éxito empresarial<sup>6</sup>”.

---

4 AMARAL, Francisco. Direito civil: introdução. 2. ed. Rio de Janeiro : Renovar, 1998, p. 327.

5 JUSTEN FILHO, Marçal. Introdução ao estudo do direito. 2. ed. Rio de Janeiro : Forense, 2021, p. 51.

6 BACIGALUPO, Enrique; HERMIDA, Carmen. El cumplimiento del derecho como valor de la ética y la cultura empresarial. In: Compliance y derecho penal. BACIGALUPO, Enrique; HERMIDA, Carmen. (coord.). Cizur Menor : Aranzadi; Thompson Reuters, 2011, p. 17.

Os Programas de Compliance visam sobremaneira o controle e supervisão de condutas éticas e jurídicas para que desvios, fraudes, ilícitos não sejam cometidos e se o forem, sejam adotadas respostas imediatas para sanar as irregularidades, reduzindo consequentemente os custos da responsabilização pelos comportamentos desconformes.

Não por outra razão indica-se que instaura uma nova cultura no ambiente corporativo apesar de ter existência jurídica, isto é, seja fonte formal autônoma ou não-estatal. É, neste aspecto, instrumental. E, neste sentido, também finalístico. Portanto, gera efeitos irradiados imediatamente, em decorrência do seu conteúdo específico, sem qualquer condicionante, inclusive no campo jurídico. O primeiro efeito decorre da sua própria edição, pois acarreta uma alteração na realidade em relação ao precedente temporal. Um antes e um depois do Programa de Compliance, já indica uma mudança, isto é, algum efeito típico em si considerado. No aspecto jurídico denota a criação de regras e princípios, direitos e deveres, obrigações, procedimentos, diretrizes e sanções. Não se restringe ao âmbito das condutas, abarcando a forma de organização das corporações.

Da mesma forma, deve ainda ser eficaz, efetivo e eficiente. Para se atingir a finalidade pretendida, tem-se que um Programa de Compliance não pode/deve ser apenas um documento ou tampouco ser reduzido à mera materialização em um papel. Nada obstante não se deva tomar como idênticos os Programas de Compliance e Programas de Integridade, para o presente artigo basta a menção de que embora sejam distintos, vem sendo aceitos indistintamente como equivalentes, sobretudo pelos legisladores. Recentemente a edição do Decreto 11.129, de 11 de julho de 2022, que regulamenta a Lei 12.846, de 1º de agosto de 2013, quanto a atos lesivos, conceitua no art. 56 o Programa de Integridade como sendo aquele que “no âmbito de uma pessoa jurídica, no conjunto de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e na aplicação **efetiva** de códigos de ética e de conduta, políticas e diretrizes”. Acrescenta, nos incisos I e II do art. 56, que são objetivos a (i) prevenção, detecção e saneamento de atos desconformes tais como desvios, fraudes, irregularidades e atos ilícitos; e o (ii) fomento e manutenção de uma cultura de integridade no ambiente organizacional.

Referido Decreto define, ainda, critérios para avaliação dos Programas de Integridade quanto à existência e aplicação (art.57) e, dentre os parâmetros, a “gestão adequada de riscos, incluindo sua análise e reavaliação periódica, para a realização de adaptações necessárias do programa de integridade e a alocação **eficiente** de recursos” (grifo nosso). No parágrafo 2º, do citado artigo, há indicação de que “A **efetividade** do programa de integridade em relação ao ato lesivo objeto de apuração será considerada para fins da avaliação de que trata o **caput**”.

As noções conceituais de eficácia, efetividade e eficiência não são imunes de controvérsias no âmbito doutrinário, sendo por vezes empregadas indistintamente. Como indica Tércio Sampaio<sup>7</sup>

na teoria jurídica, tradicionalmente, encontramos dois conceitos diferentes relacionados à efetividade das normas, que nem sempre são usados com a devida especificação. [...] há concepções meramente *sintáticas* da efetividade, caso em que a doutrina usa, embora com certa indecisão, o termo *eficácia*, no sentido de aptidão para produzir efeitos jurídicos por parte da norma [...]

É mister precisar os seus conteúdos, em especial porquanto dispositivos legais determinam, *prima facie*, apenas a análise da efetividade e eficiência e não da eficácia de um Programa de Compliance como condição necessária para incidência de benefícios diante do cometimento de ilícitos criminais ou administrativos. Mas não há efetividade sem eficácia, nem eficiência sem efetividade.

## 2. EFICÁCIA E A GERAÇÃO DE EFEITOS

A compreensão de que o Programa de Compliance seria uma ferramenta da gestão corporativa, para difundir e implementar valores éticos por meio de processos e controles internos, não é de todo equivocada, embora seja reducionista. Na medida em que não é um indiferente jurídico, até porquanto há previsão normativa de sua adoção, consubstancia-se em um ato jurídico – embora há quem o tome como um negócio jurídico –, à semelhança de regulamento empresarial. Desde logo tem-se que é dotado de eficácia.

Ser eficaz, assim, se situa nos marcos da caracterização da existência jurídica. O Compliance não deve ser recebido como parte de uma estrutura da organização, um “departamento”; nem identificado com a função que lhe é inerente, assimilando o conteúdo pela forma. Tem existência enquanto fenômeno jurídico. Há previsão em distintos dispositivos legais, tais como na nova Lei de licitações, Lei 14.133, de 1º de abril de 2021, em seu art. 25, parágrafo 4º; a previsão da hipótese normativa por vezes indica a perspectiva de uma voluntariedade, ou o prevê em algumas situações com caráter mandamental, impositivo. Por conseguinte, ocorrendo um ‘acontecimento’ que estará identificado como um suporte fático, se correspondente à hipótese normativa, a juridicização está caracterizada, com a consequente e infalível incidência da norma que adjetiva o ato como sendo ‘jurídico’. É correspondência do suporte fático à hipótese normativa que implica a existência jurídica e a adequação (não colisão com regras jurídicas vigentes e/ou preenchimento de todos os requisitos legais) que acarreta a sua validade. Ambas determinam as condições para geração de efeitos fáticos e jurídicos.

---

7 FERRAZ JUNIOR, Tercio Sampaio. Teoria da norma jurídica. 2. ed. Rio de Janeiro: Forense, 1986, p. 117.

A concepção do Programa de Compliance deve levar em conta no exercício das atividades os riscos atuais a que se submete, que não será o mesmo em cada organização ou corporação, pois minimizar a responsabilização é o escopo primeiro: “função de assegurar a adequação, o fortalecimento e o funcionamento de controle interno da instituição, em que o intuito é diminuir os riscos dos negócios que serão estabelecidos pela corporação, já que os *stakeholders* perceberão que transmite credibilidade<sup>8</sup>”.

Não por outra razão não há um modelo a ser seguido. Parâmetros para avaliação da existência e aplicação – eficácia – podem, no entanto, serem dessumidos do Decreto 11.129, de 11 de julho de 2022, em seu art. 57, em seus incisos I a XV.

A validade vai ser determinada pela observância de um agente capaz, presença de um objeto jurídico lícito e possível e forma prevista ou não proibida por lei. É assente que não há um “modelo” a ser seguido para os Programas de Compliance, mas seu conteúdo não pode se contrapor ao direito vigente e sua forma deve ser a escrita. Pode resultar de uma declaração de vontade unilateral ou bilateral, no caso em que será formado por vários acordos de vontade.

Poderá ser entendida a eficácia de modo restritivo ao campo do direito ou inserir o impacto da realidade fenomênica. Aqui, então, remete-se à sua concepção, eis que é a se traduziria pela aptidão, enquanto potencialidade, para produção de efeitos jurídicos pretendidos. A concreta geração de efeitos é tão somente uma possível consequência, *post facto* e estará (em princípio) descolada, embora sendo conexa à existência jurídica e sua validade: não se trata de aferir a qualidade de produzir efeitos, mas a efetiva produção destes. Duas distintas acepções, então, podem tomar o vocábulo eficácia.

A aptidão para gerar efeitos, uma idoneidade, pressupõe o reconhecimento pelo direito do poder de acarretar consequências jurídicas acobertadas e garantidas. Não teria nenhum sentido pensar em potencialidade para geração de efeitos na prática, pois a própria presença, *de per se*, de um Programa de Compliance desde logo implica uma alteração na realidade de uma corporação; acarreta mudanças fáticas. A adoção da concepção da aptidão para gerar efeitos se restringiria, então, ao domínio do jurídico e instalaria uma necessária e nem sempre presente correlação entre existência/validade/eficácia. Instalaria, ainda, uma dissonância entre o ato não apto para gerar efeitos jurídicos e os efeitos práticos constatados, que deveriam ser suprimidos da realidade pela desconformidade, sem que se pudesse, por exemplo, voltar no tempo e ao *status quo ante*.

---

8 TOMAZ, Roberto Epifanio. O que é compliance? Histórico, conceito e objetivos. In: Descomplicando o compliance. TOMAZ, Roberto Epifanio (org.) São Paulo : Tirant Lo Blanch, 2018, p. 29.

Desta forma, aceitando a eficácia como a geração de efeitos na concretude, isto é, não a possibilidade, mas a efetiva produção de efeitos, quaisquer que sejam eles, identificamos um Programa de Compliance eficaz quando, uma vez presente, altera uma situação prévia.

Os pilares de um Programa de Compliance, tais como são indicados, mesclam questões da própria existência jurídica, além da eficácia (efetiva produção de efeitos práticos na realidade das corporações) e efetividade (produção de efeitos pretendidos pela prática do ato jurídico). A construção de um Programa de Compliance depende da existência de uma identificação (mapeamento) e análise dos riscos ou *risk assessment*, da adoção de código de conduta ética, da previsão de controles internos e externos, de canais de denúncia. Outras situações, como monitoramento contínuo, *due dilligence*, investigações internas, auditorias ou monitoramento, dizem respeito à efetividade.

### **3. EFETIVIDADE E O ATINGIMENTO DE METAS OU FINS PRÓPRIOS**

A efetividade remete à concretude da geração de efeitos almejados, ou seja, à modificação na realidade no que tange ao atingimento dos fins próprios ou metas, que é, de uma parte, alterar a cultura organizacional e, de outra, prevenir, detectar e sanar irregularidades e atos ilícitos. Não se confunde com a eficácia, que diz respeito à efetiva geração de efeitos, fáticos e/ou jurídicos reconhecidos pelo direito. Se gerou algum efeito, mesmo que não tenha fomentado e mantido uma cultura de integridade no ambiente da organização ou corporação, por exemplo, foi eficaz. Embora possa não ser válido, se tiver sido concebido e aplicado por agente incapaz, pode ter sido efetivo. Isto porquanto não há uma correspondência necessária e imediata entre validade/eficácia e efetividade. Eficaz é se gerou algum efeito; efetivo é se atingiu a finalidade para qual foi concebido.

A efetividade está direcionada não para quaisquer efeitos; se conecta com a aferição do atingimento dos escopos, dos objetivos, das metas pretendidas. E se os fins alcançados o foram com a melhor relação custo/benefício, terá sido então, igualmente eficiente.

Os Programas de Compliance são estabelecidos para uma governança corporativa, prevenção e detecção de condutas desviantes. A resposta à indagação sobre as situações em que eles serão efetivo não pode se resumir apenas e tão somente se nenhuma conduta desconforme ocorrer, pois somente estar-se-ia considerando a meta de prevenção. Por conseguinte, se constatado um desvio, ele puder for descoberto, a finalidade de detecção determina a constatação da sua efetividade.



Ademais, a meta de um Programa de Compliance é reduzir custos e não os eliminar; e o objetivo é instar, como um compromisso, à conformidade ética e jurídica.

Não se tem como critério certo, entretanto, que a análise da efetividade estaria condicionada apenas à aferição da geração de efeitos em relação aos objetivos e metas. Nesse trilhar, tem-se como efetivo o Programa de Compliance quando se constata que houve (i) cumprimento, explicação com treinamento, com exemplo de comprometimento da alta direção; (ii) a presença de documentação e verificabilidade para controle dos atos, produzida e devidamente custodiada pela empresa; (iii) congruência e coerência em todas as ações; (iv) transparência na gestão empresarias; (v) separação de poderes; (vi) imparcialidade e independência dos órgãos de controle; (vii) confidencialidade.

Outrossim, é preciso analisar individualmente cada caso, como prevê o *Guidance Document – Evaluation of Corporate Compliance Programs* do U.S. Department of Justice, Criminal Division, a partir de três questões principais: (i) O Programa de Compliance foi adequadamente concebido? (ii) O Programa de Compliance está sendo aplicado com boa fé e honestidade ou em outras palavras, está sendo implementado efetivamente? E (iii) O Programa de Compliance tem atuado na prática?

#### 4. EFICIÊNCIA E A QUESTÃO DOS CUSTOS - MÉTODOS

A eficiência se caracteriza pela geração dos efeitos pretendidos a partir de uma pauta de maximização dos resultados, levando-se em consideração os meios, ainda uma relação de custo/benefício (ação eficiente). A noção de eficiência está determinada pela adoção de uma episteme neoliberal, que resultou de um cambio de racionalidade de uma perspectiva presente anteriormente, representada pela causalidade (causa/efeito), em favor de uma ação eficiente, o que acarreta uma confusão entre

*“efetividade (que visa fins), com eficiência (que está atrelada a meios).[...] O objetivo do mencionado cambio era o de – abandonando o princípio de falibilidade humana na previsão dos fins próprios da relação causa-efeito – combater fortemente o construtivismo, isto é, as instituições criadas deliberadamente por meio da razão. [...] o Direito [deve] ser pautado por ordens naturais espontâneas sem as ingerências de atos e decisões volitivas que pudessem gerar ‘desordem’. Com o giro provocado, deixa-se de ater aos fins, passando-se a importar única e exclusivamente aos meios”*<sup>9</sup>.

Os meios, então, justificariam os fins. De toda sorte, não se deve confundir, então, com eficácia, na medida em que

eficiência tem o intuito de melhorar o desempenho na consecução de um resultado, agido diretamente nos custos dispendidos para a sua realização, enquanto a eficácia objetiva simples-

---

<sup>9</sup> MARCELLINO JUNIOR, Julio Cesar. Princípio constitucional da eficiência administrativa: (des) encontros entre economia e direito. Florianópolis : Habitus, 2009, p. 185.

mente o atingimento de resultados. [...] Acrescenta-se que os termos também são distintos da definição de efetividade, a qual diz respeito às consequências concretas<sup>10</sup> [...]

Logo, todo Programa de Compliance deve ser eficaz, saindo do papel para alcançar a realidade, importando ainda atingir os objetivos, alcançar as metas, para chegar a ser efetivo e, na busca de um melhor resultado possível (benefício), com o menor custo, poderá ser eficiente. Aponta-se, então, para a imprescindibilidade da adoção dos melhores procedimentos.

A tomada de decisões, então, como expressão de uma governança corporativa comprometida com o menor desperdício de tempo e dinheiro dependerá, certamente de um bom planejamento; e um bom planejamento dependerá certamente de uma correta e consentânea análise dos riscos. Ao final e ao cabo, não haverá Programa de Compliance eficiente sem uma análise de riscos.

É preciso, ademais, levar em consideração que a eficiência é um dado em constante aferição e que depende da adoção de um modelo adequado de avaliação, pois as condições reais em que se insere a corporação na sua atuação são mutáveis e complexas. Portanto, mesmo que tenha havido uma acurada análise dos riscos envolvidos para concepção do Programa de Compliance, como as situações envolvem sempre um número elevado de variáveis mutáveis, o Compliance seguirá sendo constantemente aprimorado diante de mudanças internas e externas e, assim atingir eficiência é um desafio contínuo.

Alvacir Correa dos Santos lembra que “eficiência e eficácia têm que andar juntas, significando que, em qualquer empreendimento ou organização, deve-se sempre buscar o melhor resultado, com o menor esforço ou custo possíveis<sup>11</sup>”. Não somente na atuação de uma corporação no mercado, buscando lucro. A eficiência ingressa como princípio jurídico pela via constitucional (Constituição Federal de 1988), no seu art. 37, *caput*, por meio da Emenda Constitucional 19/1998, para a Administração Pública. Não se trata de um recorte de gestão estratégia no mercado, regido pela via econômica. É um imperativo de ditames constitucionais tais como a função social da propriedade. Na relação meio/fim alguns valores éticos e compromissórios com a sociedade, tais como meio ambiente ou direitos humanos determinam que o recorte de análise não deve se restringir ao filtro financeiro.

## 5. CONCLUSÕES

Por certo que diante da imperatividade das normas jurídicas estatais a sua observância não depende da adoção de qualquer Programa de Compliance. A

---

10 JANNIS, Andre Schmidt. *Compliance* público frente aos princípios da administração pública: a necessidade da atuação do advogado no *compliance* público como pressuposto de efetividade. In: *Compliance: aspectos polêmicos e atuais*. LAMY, Eduardo (org.). Belo Horizonte : Letramento; Casa do Direito, 2018, p. 45.

11 SANTOS, Alvacir Correa dos. Princípio da eficiência da administração pública. São Paulo : LTI, 2003, p. 189.

violação das regras e princípios jurídicos acarretam responsabilizações, que são vistos como riscos que geram custos pelas organizações e corporações.

Diz-se, pois, que o Programa de Compliance se consubstancia em instrumentos de supervisão empresarial, ou melhor, “en última instancia [...el] evidente principio vigente en cada uno de los ordenamientos jurídicos estatales según el cual las empresas y sus órganos deben operar armónicamente con el Derecho vigente<sup>12</sup>.” Esse mecanismo de controle e supervisão no âmbito das corporações tem como finalidade a prevenção de práticas desconformes para redução da responsabilidade pela violação de normas jurídicas. A adoção de um Programa de Integridade, de um Código de Ética, Procedimentos de Boas Práticas, em si já denotam uma mudança de cultura na gestão das organizações, acarretando efeitos. Presente a eficácia.

Sua efetividade vai além, abraçando um compromisso com o atingimento das metas e objetivos na redução dos riscos; não está de forma alguma adstrita à violação “zero”, mas a um compromisso com a cultura do cumprimento das normas e da conduta ética na atuação.

Poderá ainda ser eficiente. Entretanto, a introdução da ação eficiente é legado da episteme neoliberal da lógica dos custos, com prevalência dos meios em detrimento dos fins, pelo que fica o alerta de que a racionalidade jurídica não deve jamais ser suplantada para acolher uma racionalidade econômica, sob pena de abandonarmos um projeto de nação inclusivo para permitir que os interesses privados e egoísticos tenham prevalência.

É certo que a autonomia privada precede e sustenta os negócios jurídicos, com uma nova moldura, mas “circumspeta a novos valores constitucionais e infraconstitucionais [...] sempre mediante autorização concedida pelo Estado para a consecução de tais movimentos do sujeito e a perseguição dos efeitos jurídicos almejados, [...] e sempre] socialmente funcionalizada<sup>13</sup>”.

Os Programas de Compliance não estão à margem do Direito, nem podem desconsiderar a normatividade constitucional. Até mesmo a empresa, como expressão da livre iniciativa e revelação da propriedade privada, deve ater-se à sua função social, exercendo em vista disso o relevante papel de conformação do social para o bem da pessoa humana.

## REFERÊNCIAS BIBLIOGRÁFICAS

AMARAL, Francisco. Direito civil: introdução. 2.ed. Rio de Janeiro : Renovar, 1998.

ASCENSÃO, José de Oliveira. O direito: introdução e teoria geral. Uma perspectiva luso-brasileira. 11. ed. Coimbra : Almedina.

---

12 ROTSCH, Thomas. Criminal compliance. InDret – Revista para el analisis del derecho, Barcelona, jan. 2012, p. 1-11. Disponível em: <https://indret.com/wp-content/themes/indret/pdf/876a.pdf> Acesso em: 20nov. 2022, p. 2.

13 NALIN, Paulo. A autonomia privada na legalidade constitucional. In: A autonomia privada na legalidade constitucional. NALIN, Paulo (coord.) Curitiba : Juruá, 2006, p. 29.

- BACIGALUPO, Enrique; HERMIDA, Carmen. El cumplimiento del derecho como valor de la ética y la cultura empresarial. In: Compliance y derecho penal. BACIGALUPO, Enrique; HERMIDA, Carmen. (coord.). Cizur Menor : Aranzadi; Thompson Reuters, 2011, p. 17-19.
- JANNIS, Andre Schmidt. *Compliance* público frente aos princípios da administração pública: a necessidade da atuação do advogado no *compliance* público como pressuposto de efetividade. In: *Compliance: aspectos polêmicos e atuais*. LAMY, Eduardo (org.). Belo Horizonte : Letramento; Casa do Direito, 2018, p. 33-52.
- JUSTEN FILHO, Marçal. Introdução ao estudo do direito. 2.ed. Rio de Janeiro : Forense, 2021.
- FERRAZ JUNIOR, Tercio Sampaio. Teoria da norma jurídica. 2.ed. Rio de Janeiro : Forense, 1986.
- MARCELLINO JUNIOR, Julio Cesar. Princípio constitucional da eficiência administrativa: (des) encontros entre economia e direito. Florianópolis : Habitus, 2009.
- NALIN, Paulo. A autonomia privada na legalidade constitucional. In: A autonomia privada na legalidade constitucional. NALIN, Paulo (coord.) Curitiba : Juruá, 2006, p. 13-45.
- ROTSCH, Thomas. Criminal compliance. InDret – Revista para el analisis del derecho, Barcelona, jan.2012, p.1-11. Disponível em: <https://indret.com/wp-content/themes/indret/pdf/876a.pdf> Acesso em: 20nov.2022.
- SANTOS, Alvacir Correa dos. Princípio da eficiência da administração pública. São Paulo : LTr, 2003.
- TOMAZ, Roberto Epifanio. O que é compliance? Histórico, conceito e objetivos. In: Descomplicando o compliance. TOMAZ, Roberto Epifanio (org.) São Paulo : Tirant Lo Blanch, 2018, p. 19-45.
- VILA, Ivó Coca. ¿Programas de cumplimiento como forma de autorregulación regulada? In: Criminalidad de empresa y compliance: prevención y reacciones corporativas. SÁNCHEZ, Jesús-María Silva (dir.); FÉRNANDEZ, Raquel Montaner (coord.) Barcelona : Atelier libros, 2013, p. 43-76.

# MUNDO DIGITAL, ALGORITMOS E PERFILIZAÇÃO: DETECTANDO OS PERIGOS DE UM NEM SEMPRE ADMIRÁVEL MUNDO NOVO

EUGÊNIO FACCHINI NETO

## 1. INTRODUÇÃO

Estamos vivendo, em dimensão globalizada, um momento em que inúmeros sensores com os quais convivemos, e dos quais muitas vezes não temos noção, captam nossos dados pessoais e com eles formam nosso corpo eletrônico. Isso permite que se acumulem informações a respeito de cada um de nós a ponto de se garantir o conhecimento sobre quem efetivamente somos, do que gostamos, de nossos hábitos de consumo, do nosso círculo de amizades, de nossas simpatias políticas, de nossas tendências ideológicas, de nossos gostos. Conhecendo quem somos e nossas preferências, é possível nos ‘vender’ produtos e serviços afins aos nossos interesses.

Esses sensores que captam e aglutinam dados, permitindo uma precisa identificação de quem somos, não são somente estatais – a maioria, aliás, é manejada pela sociedade, através de seus agentes econômicos. Ainda que todo o processo tenha iniciado como uma tentativa de ‘vender’ produtos e serviços de uma forma mais eficaz, já que direcionado diretamente ao público potencialmente alvo, fato é que tais dados aglutinados podem ser facilmente transferidos inclusive a agentes não econômicos, com finalidade política e ideológica, como já ocorreu em tempos recentes (fenômenos do Brexit e da eleição de Trump).

O fenômeno permite a manipulação de opiniões e de pessoas, o que significa uma restrição da espontaneidade individual e um enfraquecimento da liberdade de cada um de se conduzir de forma realmente autônoma na vida de relação e nas suas relações com o Estado.

A inteligência artificial, que permite tudo isso, veio para ficar. Cada vez mais impactará nossas vidas. Isso é inevitável e seus resultados são majoritariamente positivos, permitindo ganhos de tempo, de produtividade, de eficácia. Todavia, traz consigo também algumas ameaças, que não podem ser desconsideradas. Ao contrário, impõe-se delas ter consciência, para que se procurem meios de reduzir ou controlar os inevitáveis danos.

Essa modesta contribuição não tem a pretensão de oferecer soluções, mas mais humildemente busca apenas indicar o surgimento e evolução desse proces-

so, pontuar alguns problemas e condensar as ponderações que os especialistas vêm fazendo a respeito.

## 2. A REVOLUÇÃO DIGITAL

A propriedade da terra foi o principal ativo econômico durante boa parte da história da humanidade. Com o crescimento das cidades, a partir da baixa idade média, passou a sofrer a concorrência crescente do comércio. E a partir do último quartel do século XVIII, máquinas e fábricas assumiram o papel de motores econômicos das nações. “No século XXI, a tecnologia da informação e o controle sobre os dados transformaram-se nos grandes ativos.” Um novo estágio é anunciado, em que ocorrerá a “fusão entre a tecnologia da informação e a biotecnologia (...) no qual se antecipa a integração entre o físico e o virtual, o humano e o mecânico. (...) Um mundo de promessas, desafios e novos riscos.”<sup>1</sup>

Em visão concorrente, Klaus Schwab, diretor-presidente do Fórum Econômico Mundial, publicou, em 2016, “A Quarta Revolução Industrial”<sup>2</sup>, que é o nome que ele dá<sup>3</sup> à época em que passamos a viver nas duas últimas décadas, como um aprofundamento da revolução digital. Ela é caracterizada “por uma internet mais ubíqua e móvel, por sensores menores e mais poderosos que se tornaram mais baratos, e pela inteligência artificial e aprendizagem automática (ou aprendizado de máquina).” A razão do seu caráter disruptivo em relação à terceira revolução industrial (relacionada ao advento da computação e da internet) é que essas novas tecnologias estão se tornando mais sofisticadas e integradas, envolvendo a fusão e interação de domínios físicos, digitais e biológicos, envolvendo aspectos tão distintos quanto sequenciamento genético, nanotecnologia, energias renováveis e computação quântica. Tudo isso implicou o advento de tecnologias que estão transformando a maneira como vivemos.

De fato, aos poucos, todos fomos migrando boa parte de nossas vidas para o mundo digital. Esse passou a ser o mercado onde compramos produtos e serviços, nossa fonte primeira de informações sobre o mundo e sobre as pessoas, além de ser o espaço predominante para os contatos pessoais. Suas aplicações são múltiplas e as vantagens infinitas.

A Inteligência Artificial, fenômeno que está na base dessa revolução disruptiva que estamos vivenciando, tornou-se possível, ou ao menos foi potencializada pela possibilidade de acumular informações (dados) sobre tudo e sobre

---

1 BARROSO, Luís Roberto. Revolução tecnológica, crise da democracia e mudança climática: limites do direito num mundo em transformação. *Revista Estudos Institucionais*, v. 5, p. 1262-1313, set./dez. 2019, p. 1278/1279.

2 SCHWAB, Klaus. *A Quarta Revolução Industrial*. Trad. Daniel Moreira Miranda. Bauru/SP: EDIPRO, 2019.

3 Embora em 2014 Luciano Floridi já tivesse publicado obra identificando essa quarta revolução: “*The Fourth Revolution: how the infosphere is reshaping the human reality*” (Oxford: Oxford University Press, 2014).

todos. Essa quantidade imensurável de dados – conhecida pela expressão inglesa *big data*<sup>4</sup> – constitui o combustível (*inputs*) que alimenta os programas de inteligência artificial, que com eles – os dados – aprendem, fazem correlações, e apresentam resultados (*outputs*). *Big data*, assim, passou a ser o novo petróleo (*new oil*), como constou na capa da revista *The Economist*, em edição de 2017. Ou seja, assim como o petróleo fornecia o combustível para impulsionar a antiga indústria, os dados – ou *data* – constitui o combustível que abastece a nova economia digital da sociedade algorítmica.<sup>5</sup>

Na verdade, a coleta de dados pessoais não é algo propriamente novo: o que ocorre é que os fenômenos do *Big Data* e *Big Analytics*<sup>6</sup> “possibilitaram que tais atividades ocorressem de maneira muito mais eficiente, com mais veracidade, velocidade, variedade e volume”.<sup>7</sup>

---

4 Segundo Steve Lohr, citado por Dresch e Faleiros Júnior, “a expressão inglesa *big data* tem sua origem atribuída a John Mashey, que, desde a década de 1990 popularizou seu uso ao utilizá-la para se referir ao conjunto de dados com tamanhos além da capacidade de ferramentas de *software* usuais da época, englobando dados não estruturados, semiestruturados e estruturados, cujo ‘tamanho’ é concebido como uma meta em constante movimento, variando de algumas dezenas de *terabytes* a muitos *zettabytes* de dados” (DRESCH, Rafael de Freitas Vale; FALEIROS JÚNIOR, José Luiz de Moura. Reflexões sobre a responsabilidade civil na Lei Geral de Proteção de Dados (Lei n. 13. 709/2018). In: ROSENVALD, Nelson; DRESCH, Rafael de Freitas Valle; WESENDONCK, Tula (Coord.). **Responsabilidade Civil: novos riscos**. Indaiatuba: Ed. Foco, 2019, p. 66, n. r. 1. Em outra definição, *Big data* é o termo usualmente empregado para descrever “qualquer quantidade volumosa de dados estruturados, semiestruturados ou não estruturados que tem o potencial de ser explorados para obter informações” (MAGRANI, Eduardo; OLIVEIRA, Renan Medeiros de. O Big Data somos nós: novas tecnologias e projetos de gerenciamento pessoal de dados. In: TEPEDINO, Gustavo et al. (Coord.). **Anais do VI Congresso do Instituto Brasileiro de Direito Civil**. Belo Horizonte: Fórum, 2019, p. 405. Nas palavras de Sarlet e Molinaro, *Big data* é uma expressão que descreve um “tratamento de grandes quantidades de dados que visa reconhecer padrões e obter novas percepções a partir deles”, caracterizando-se pela “abundância, diversidade dos dados e rapidez com que são coletados, analisados e revinculados ou reintroduzidos no sistema” – SARLET, Gabrielle Bezerra Sales; MOLINARO, Carlos Alberto. Questões tecnológicas, éticas e normativas da proteção de dados pessoais na área da saúde em um contexto de big data. **Direitos Fundamentais & Justiça**, Porto Alegre, v. 13 (2019), p. 183-213, p. 188. Bruno Bioni esclarece que o enorme volume de dados processados permite “correlacionar uma série de fatos (dados), estabelecendo-se entre eles relações para desvendar *padrões* e, por conseguinte, inferir, inclusive, *probabilidades* de acontecimentos futuros”. De certa forma, “big data não é um sistema inteligente”, pois ele “não se preocupa com a *causalidade* de um evento, mas, tão somente, com a probabilidade de sua ocorrência” - BIONI, Bruno Ricardo. **Proteção de Dados Pessoais** – a função e os limites do consentimento. 2ª ed., rev., atual. e reform. Rio de Janeiro: Forense, 2020, p. 36.

5 BALKIN, Jack M. Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation. **Yale Law School: Faculty Scholarship Series**, n. 5160, 2018. Disponível em [https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=6159&context=fs\\_papers](https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=6159&context=fs_papers). Acesso em 22/10/2022.

6 A simples capacidade técnica de reunir volumes gigantescos de dados pessoais não teria grande significado, pois eles necessitam ser processados e trabalhados para que possam gerar valor, ou seja, há que se transformá-los em informação. É isso que é feito através do que é chamado *big analytics*, ou seja, “a possibilidade de extrair, a partir dos dados, correlações, padrões e associações que possam ser consideradas informações. Para tal objetivo, é grande a importância dos algoritmos e das máquinas responsáveis por tal processamento.” Os fenômenos do *big data* e do *big analytics* apresentam, assim, uma “relação simbiótica”, pois as plataformas digitais “procuram ter o maior acesso possível aos dados dos usuários para depois poder convertê-los em informações e, a partir daí, usar tais informações em seu próprio negócio ou compartilhá-las com parceiros comerciais” – nesses termos, FRAZÃO, Ana. Plataformas digitais, *big data* e riscos para os direitos da personalidade. In: TEPEDINO, Gustavo; MENEZES, Joyceane Bezerra de (Coord.). **Autonomia privada, liberdade existencial e direitos fundamentais**. Belo Horizonte: Fórum, 2019, p. 337.

7 FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais – Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais** – e suas repercussões no Direito Brasileiro. 2. Ed. São Paulo: Thomson Reuters Brasil/Revista dos Tribunais, 2020, p. 24/25. Na verdade, a autora apoia-se em Doug Laney, o qual se refere a *big data* como os “Four Vs”, os Quatro Vs: *volume*, *variety*, *veracity* e *velocity*. Segundo ele, *Data* é considerado “big” porque é produzido e coletado em **volume** gigantesco. Além disso, os dados apresentam-se com uma **variedade** nunca antes vista, abrangendo desde dados banais, como nome, idade, sexo, como outros abarcando dados de saúde e precisa geolocalização a cada momento do dia. A **veracidade** fica por conta da confiabilidade das informações coletadas, fornecidas pelo próprio interessado mesmo que ele não saiba disso. E **velocidade**, em razão da impressionante rapidez com que os dados são coletados, transmitidos, analisados, tratados - LANEY, Doug, disponível em <http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf>. Acesso em 10. 12. 2019. Roberto PFEIFFER acrescenta às quatro características já citadas, mais uma – **valor** (*value*) – diante de sua indiscutível importância econômica para a economia digital – PFEIFFER, Roberto Augusto Castellanos. Digital Economy, Big Data and Competition Law. **Market and Competition Law Review** / volume iii / no. 1 / abril 2019, p. 55/56.

Os dados coletados, que abastecem a economia e sociedade digital, são substancialmente fornecidos ‘voluntariamente’, pelos próprios indivíduos, ao navegarem na rede, inclusive quando participam de espaços de lazer, como ocorre com as redes sociais.<sup>8</sup>

Quase a totalidade dos programas acessados na internet exige fornecimento de alguns dados, ou então a autorização para o responsável pelo programa acessar os dados armazenados nos aplicativos de celulares, nas redes sociais, na galeria de fotos, etc. Esse é o ‘preço’ que se paga para a utilização dos programas e aplicativos oferecidos na rede. Esses dados são valiosíssimos, pois baseados neles é que se montam estratégias publicitárias direcionadas, e é esta publicidade que remunera os serviços disponibilizados na internet<sup>9</sup>. De se notar que “o marketing direcionado promovido nas redes sociais vai muito além de banners e links patrocinados”<sup>10</sup>.

Os impactos da revolução digital são enormes, diversos, amplos e substancialmente positivos. Todavia, também apresentam motivos para preocupação, criando algumas distorções que devem ser enfrentadas. Isso ocorre em grande parte porque a transformação digital em que estamos inseridos está sendo realizada substancialmente por empresas privadas, “que podem exercer considerável influência sobre as liberdades de outros indivíduos privados e as condições reais de uso da liberdade, e que o fazem tendo em vista seus próprios interesses”<sup>11</sup>. Assim, se inicialmente a preocupação era voltada para a proteção da privacidade frente ao Estado e entes governamentais (visto como o *Big Brother*), de algumas décadas para cá percebeu-se que tão importante quanto isso era a proteção de espaços de liberdade frente aos inúmeros operadores privados (*Big Other* ou *little Brothers*), já que o mercado “fez a privacidade passar de um direito a uma *commodity*”<sup>12</sup>. As-

---

8 MEDON, Filipe. Decisões automatizadas: o necessário diálogo entre a Inteligência Artificial e a proteção de dados pessoais para a tutela de direitos fundamentais. In: TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (Coord.). **O Direito Civil na era da Inteligência Artificial**. São Paulo: Thompson Reuters Brasil/Revista dos Tribunais, 2020, p. 343.

9 Como referem Morey e Krajecki, “a ampla disponibilidade de muitos tipos diferentes de dados pessoais, juntamente com a capacidade de armazenar e analisar esses dados, permite que as empresas personalizem a experiência do consumidor. Com tecnologias como os smartphones, redes de sensores e produtos inteligentes conectados, as grandes empresas globais podem interagir com os seus consumidores de uma forma personalizada não mais vista desde que deixamos para trás a loja da aldeia para entrar na era industrial” (trad. nossa) – MOREY, Timothy; KRAJECKI, Kristin. **Personalization, Data and Trust: The Role of Brand in a Data-Driven, Personalized, Experience Economy**. Disponível em <https://www.frogdesign.com/designmind/personalization-data-trust-role-brand-data-driven-personalized-experience-economy>, acesso em 22/12/2020 (originariamente publicado no **Journal of Brand Strategy**, Summer 2016 (V. 5, n. 2, p. 178-185).

10 TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. **Pensar**. Fortaleza, v. 22, n. 1, p. 108-146, jan. -abr. 2017, p. 122/123 e n. r. 23.

11 HOFFMANN-RIEM, Wolfgang. **Teoria Geral do Direito Digital**. Transformação digital – desafios para o direito. Trad. Italo Fuhrmann. Rio de Janeiro: Forense, 2021, p. 44. Em decisão do final de 2019, o Tribunal Constitucional alemão constatou esse fenômeno: “Em todas as áreas da vida, os serviços básicos para o público em geral estão sendo cada vez mais prestados por empresas privadas, muitas vezes poderosas, com base em extensas coletas de dados pessoais e medidas de processamento de dados. Essas empresas desempenham um papel decisivo na formação da opinião pública, na geração e restrição de oportunidades, na participação na vida social ou mesmo em tarefas elementares da vida diária. Os indivíduos dificilmente terão outra escolha senão a de revelar em grande medida seus dados pessoais para as empresas, caso não queiram ser excluídos desses serviços básicos” - HOFFMANN-RIEM, *op. cit.*, p. 46.

12 PAESANI, Líliliana Minardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil**. 4. Ed. São Paulo: Atlas, 2008, p. 36. Segundo uma imagem cada vez mais difundida, os dados pessoais são “considerados o ouro do século XXI” – nesses termos, OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela, Maria Pereira. Os princípios norteadores da proteção de



sim, as ameaças cada vez mais se originam não de um centro maligno e vigilante, mas sim de “milhares de empresas que coletam, armazenam e processam dados de seus clientes, consumidores finais ou não”<sup>13</sup>.

Algumas consequências atingem os indivíduos e impactam suas vidas no ambiente social e econômico. É o que será visto na sequência. Preocupações diversas atingem também a vivência democrática, mas estas não serão objeto desse artigo, em razão da limitação de espaço.

### 3. IMPACTOS DA REVOLUÇÃO DIGITAL NOS ÂMBITOS INDIVIDUAL E SOCIAL

Ao navegarmos na rede, deixamos pegadas, rastros, em quantidades imensas. Isso envolve desde nossas atividades mais simples (como digitar na barra de ferramentas do Google um assunto qualquer para pesquisa) às mais complexas (como transações financeiras) – tudo fica armazenado, revelando nossas “pegadas digitais”. Diferentemente do mundo “físico”, onde nem sempre nossas ações são registradas, no mundo “virtual” nada se perde, tudo fica guardado. Nesse mundo, nada é passado – tudo é presente contínuo, permanentemente acessível aos nossos dedos<sup>14</sup>. Com o uso de tecnologia, é possível agrupar e tratar esses dados esparsos, a ponto de fazê-los revelar quem somos, do que gostamos, o que pensamos. De fato, por meio das redes sociais, criamos perfis e participamos das mais diversas comunidades e grupos, compartilhando uma série de dados relativos a nossas características pessoais, preferências e gostos. Essa ânsia de visibilidade que constitui o *ethos* (ou *zeitgeist*)<sup>15</sup> de nossa era, todavia, traz consigo uma potencialidade de importantes danos<sup>16</sup>, inclusive à privacidade, “haja vista a coleta e

---

dados pessoais no Brasil e sua otimização pela Lei 13. 709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados** – e suas repercussões no Direito Brasileiro. 2. ed. São Paulo: Ed. Revista dos Tribunais/Thompson Reuters Brasil, 2020, p. 53-82, p. 60. Ronaldo Lemos usa a expressão “petróleo” para expressar o valor dos dados pessoais na economia da informação, ou *data driven economy*, em que vivemos (LEMOS, Ronaldo. *Ou a sociedade acompanha internet ou a democracia começa a ficar em xeque*. Disponível em <https://blogdomorris.blogfolha.uol.com.br/2014/04/08/ou-sociedade-acompanha-internet-ou-democracia-comeca-a-ficar-em-xeque/>, acesso em 29. 11. 20). Conhecido artigo publicado na revista *The Economist*, publicado em 06. 05. 2017, que foi também sua capa, intitulado “*The world’s most valuable resource is no longer oil, but data*”, referiu-se aos dados pessoais como *new oil* – Disponível em <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em 29. 11. 20.

13 MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor**, vol. 20, n. 79, jul. -set. 2011, p. 45-82.

14 FACCHINI NETO, Eugênio; DEMOLINER, Karine Silva. Direito à privacidade na era digital – uma releitura do art. XII da Declaração Universal dos Direitos Humanos (DUDH) na sociedade do espetáculo. **Revista Internacional Consinter de Direito**. Ano V, n. IX, 2º Semestre 2019, p. 134.

15 ROSENVALD, Nelson. Prefácio. In: PINHO, Anna Carolina (Coord.). **Discussões sobre Direito na Era Digital**. Rio de Janeiro: G/Z Editora, 2021, p. IX.

16 “[V]ivemos em um mundo em que o real e o virtual não se distinguem mais. / Entretanto, não existem ‘almoços grátis’. Era preciso pagar a conta de todas essas benesses propiciadas pela Internet. Vinte anos atrás, cogitava-se a cobrança pelo uso da rede e também pelo envio de e-mails, à semelhança de uma carta tradicional. (...) Em vez de pagar-se exclusivamente com moeda, por que não pagar parte do preço com dados pessoais? / Pedem-se dados pessoais nos caixas das lojas e das farmácias. Em cada acesso à Internet, registra-se quem está acessando, em que local se encontra, quanto tempo permaneceu e o que visualizou, com quem conversou e de quem se comprou, como pagou e se gostou. Basta analisar todos esses dados em larga escala por meio de algoritmos com inteligência artificial e o resultado obtido se torna um ativo de elevado valor. / Além disso, a esfera do debate público modificou-se substancialmente. O conforto do lar e o suposto anonimato trouxeram à tona uma série de preconceitos e ódios então velados no seio da sociedade, por meio de discussões irracionais na Internet, e esse fato tem sido muito explorado de forma deletéria pelo tratamento de dados pessoais e da inteligência artificial em termos de mensuração das opiniões das pessoas” - TO-

o tratamento indiscriminado de dados pessoais e a divulgação não autorizada de conteúdos íntimos por terceiros”<sup>17</sup>.

Essa coleta e tratamento de dados tem um valor econômico incomensurável, pois permite o direcionamento de publicidade adequada e personalizada a cada perfil. Mas não são apenas os agentes econômicos que se utilizam dos dados pessoais como relevantíssimo ativo empresarial. No âmbito do poder público, os dados pessoais também são cruciais para a formulação e implementação de boa parte das políticas públicas<sup>18</sup>, pois sua estruturação e implementação não são possíveis sem o conhecimento do perfil da população e suas demandas<sup>19</sup>.

O risco, porém, é de a sociedade ficar passivamente acostumada com essa coleta incessante de dados pessoais, a ponto de posteriormente sentir-se impotente para fazer respeitar a fronteira que deve existir entre as esferas públicas e privada, como aparentemente ocorreu na China<sup>20</sup>.

Este item focará, porém, o que está ocorrendo no plano da economia digital, onde, segundo Shoshana Zuboff, “seis declarações assentaram o alicerce para o projeto mais amplo do capitalismo de vigilância”<sup>21</sup> (ou sociedade da vigilância<sup>22</sup>):

- 
- MASEVICIUS FILHOS, Eduardo. Prefácio. In: PINHO, Anna Carolina (Coord.). **Discussões sobre Direito na Era Digital**. Rio de Janeiro: G/Z Editora, 2021, p. XVI.
- 17 TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. **Pensar**, Fortaleza, v. 22, n. 1, p. 108-146, jan./abr. 2017, p. 141.
- 18 Além disso, “permanecem, latentes e plausíveis, porém, as hipóteses de rastreamento e controle invisível por parte do governo como perigo potencial para um futuro, que inclusive pode tomar proporções trágicas caso sociedades totalitárias tenham acesso às tecnologias necessárias” —mas não só por elas, já que o sistema Echelon de vigilância (rede de rastreamento global de telecomunicações) teria sido formado por países que compõem sólidas democracias modernas, como os Estados Unidos, Inglaterra, Canadá, Austrália e Nova Zelândia — nestes termos, DÓNEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. rev. e atual. São Paulo: Thomson Reuters Brasil/Revista dos Tribunais, 2019, p. 37/38 e n. r. 26.
- 19 MENEZES, Joyceane Bezerra de; COLAÇO, Hian Silva. Quando a Lei Geral de Proteção de Dados não se aplica? In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais – e suas repercussões no Direito Brasileiro**. 2. Ed. São Paulo: Thomson Reuters Brasil/Revista dos Tribunais, 2020, p. 158.
- 20 “Na China não há nenhum momento da vida cotidiana que não esteja submetido à observação. Cada clique, cada compra, cada contato, cada atividade nas redes sociais, são controlados. Quem atravessa no sinal vermelho, quem tem contato com críticos do regime e quem coloca comentários críticos nas redes sociais perde pontos. A vida, então, pode chegar a se tornar muito perigosa. Pelo contrário, quem compra pela Internet alimentos saudáveis e lê jornais que apoiam o regime ganha pontos. Quem tem pontuação suficiente obtém um visto de viagem e créditos baratos. Pelo contrário, quem cai abaixo de um determinado número de pontos pode perder seu trabalho. Na China essa vigilância social é possível porque ocorre uma irrestrita troca de dados entre os fornecedores da Internet e de telefonia celular e as autoridades. Praticamente não existe a proteção de dados. No vocabulário dos chineses não há o termo “esfera privada” BYUNG-CHUL HAN. **O coronavírus de hoje e o mundo de amanhã, segundo o filósofo Byung-Chul Han**. Entrevista concedida pelo filósofo sul-coreano Byung-Chul Han ao jornal EL PAÍS, em 22. 03. 2020. Disponível em <https://brasil.elpais.com/ideas/2020-03-22/o-coronavirus-de-hoje-e-o-mundo-de-amanha-segundo-o-filosofo-byung-chul-han.html>, acesso em 20. 01. 2022.
- 21 Ou economia da vigilância, para significar o fenômeno em que estamos imersos, em que o cidadão se torna um mero espectador passivo do fluxo de suas informações pessoais, como adverte ZUBOFF, Shoshana. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. **Journal of Information Technology**, 4 abr. 2015, p. 75/ 89, p. 79, disponível em [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2594754](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754) acesso em 20. 12. 2020. No mesmo sentido, adverte Frank Pasquale que a coleta dos dados pessoais, tanto por governos quanto por poderosos agentes econômicos, permite a criação do que ele chama de *one way mirror*, ou seja, uma situação em que eles podem tudo saber a respeito dos cidadãos/consumidores, sem que esses sequer saibam que estão sendo minuciosamente observados. Esse monitoramento constante, envolvendo cada ação individual (mesmo fora de transações formais, envolvendo simples manifestações de interesse na rede), leva ao chamado *capitalismo de vigilância*, uma economia que passou a se alimentar substancialmente dos dados pessoais para se desenvolver - PASQUALE, Frank. **The black box society: the secret algorithms that control money and information**. Harvard: Harvard University Press, 2015, p. 9.
- 22 A expressão *sociedade da vigilância* aparece no título do livro de LACE, Susanne. **The glass consumer: life in a surveillance society**. Bristol: Policy Press, 2005. A autora refere que todos nos tornamos “consumidores de vidro”, uma vez que os outros sabem tanto

1. Nós reivindicamos a experiência humana como matéria-prima gratuita para se pegar. Com base nessa reivindicação, podemos ignorar considerações de direitos, interesses, consciência ou entendimento dos indivíduos.
2. Com base na nossa reivindicação, afirmamos o direito de pegar a experiência do indivíduo para convertê-la em dados comportamentais.
3. Nosso direito de pegar, baseado na nossa reivindicação de matéria-prima gratuita, nos confere o direito de possuir os dados comportamentais derivados da experiência humana.
4. Nossos direitos de pegar e possuir nos conferem o direito de saber o que o conteúdo dos dados revela.
5. Nossos direitos de pegar, possuir e saber nos conferem o direito de decidir como usamos o nosso conhecimento.
6. Nossos direitos de pegar, possuir, saber e decidir nos conferem nossos direitos às condições que preservam nossos direitos de pegar, possuir, saber e decidir.<sup>23</sup>

Essa economia baseada na coleta e tratamento de dados alterou a clássica concepção de privacidade, originalmente concebida como o direito de ser deixado só (*to be let alone*, na conhecida fórmula divulgada por Warren e Brandeis no longínquo ano de 1890), de se resguardar da intromissão alheia, cuja tutela se implementava a partir de uma lógica proprietária: assim como o proprietário tinha o direito de afastar terceiros do gozo dos bens que compunham seu patrimônio, também tinha o direito de manter o resto da sociedade afastada do conhecimento de aspectos de sua vida privada. Cuidava-se de “perspectiva negativa e estática da privacidade. A mudança conceitual passou a envolver o direito ao controle dos dados pessoais”, em “perspectiva positiva, dinâmica e, mais importante, extrapatrimonial”. Agora, a construção da identidade e o desenvolvimento da personalidade “passa a depender da forma pela qual o sujeito é revelado a partir do tratamento de seus dados”<sup>24</sup>.

---

sobre nós que praticamente podem nos ver através de nós, como se fôssemos de vidro, já que nossas vidas cotidianas são gravadas, analisadas e monitoradas de inúmeras maneiras (p. 1). Já a expressão *Estado de Vigilância* é utilizada para identificar “uma forma de contaminação da democracia caracterizada pela intrusão dos governos e das corporações na liberdade e na privacidade de terceiros, sejam estes atores públicos ou privados” – nesses termos, MOLINARO, Carlos Alberto; SARLET, Ingo Wolfgang. Sociedade em rede, internet e estado de vigilância: algumas aproximações. Revista *AJURIS*, v. 40, n. 132, dez. 2012, p. 65.

23 ZUBOFF, Shoshana. **A era do capitalismo de vigilância**. A luta por um futuro humano na nova fronteira do poder. Trad. de George Schlesinger. Rio de Janeiro: Intrínseca, 2020, p. 210/211. À fl. 19 da mesma obra, Zuboff refere que a aglutinação dos dados reunidos sobre qualquer pessoa permite um conhecimento sobre ela que habilita prever “o que um determinado indivíduo faria agora, daqui a pouco e mais tarde. Por fim, esses produtos de predições são comercializados num novo tipo de mercado para predições comportamentais que chamo de *mercados de comportamentos futuros*. Os capitalistas de vigilância têm acumulado uma riqueza enorme a partir dessas operações comerciais, uma vez que muitas companhias estão ávidas para apostar no nosso comportamento futuro”.

24 TERRA, Aline de Miranda Valverde; CASTRO, Diana Paiva de. A responsabilidade do Poder Público no tratamento de dados pessoais: análise dos artigos 31 e 32 da LGPD. In: MULHOLLAND, Caitlin (Org.). **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago Ed., 2020, p. 240/241. Essa visão é inspirada na de Rodotà: comentando a evolução normativa europeia a partir da proteção da vida privada na Convenção de 1950 (que se limitava a proteger o “respeito à vida privada e familiar, seu domicílio

Com isso, a lógica do sigilo e a distinção entre as esferas pública e privada foram completamente alteradas, pois não só os dados sigilosos da esfera íntima passaram a ser protegidos, já que atualmente “todo dado pessoal passa a ser, *prima facie*, protegido, e toda operação de ‘tratamento’ de dados pessoais deve ser justificada” por enquadrar-se em alguma hipótese prevista na legislação protetiva dos dados. “Isso vale para dados pessoais que não sejam íntimos ou mesmo aos que são públicos. Trata-se de um regime jurídico voltado a regular toda e qualquer fase do fluxo e da circulação de dados pessoais na era da sociedade da informação”<sup>25</sup>.

A importância dos dados pessoais, mesmo que não pertinentes à esfera da intimidade, foi captada por importante e célebre decisão da Corte Constitucional alemã (*Bundesverfassungsgericht*), de 1983, envolvendo a análise da constitucionalidade da Lei de 25.03.82, que dispunha sobre o recenseamento da população, das profissões, das residências e dos locais de trabalho. Afirmou o tribunal que era irrelevante se as informações coletadas envolviam dados íntimos, privados ou públicos, pois qualquer que fossem, a partir do processamento eletrônico de tais dados era possível reconstruir um ‘perfil completo da personalidade’, o que acarretava potencial risco para os cidadãos. Afirmou-se que uma sociedade, “na qual os cidadãos não mais são capazes de saber quem sabe o que sobre eles, quando e em que situação”, seria contrária ao que identificou como um direito fundamental à autodeterminação informacional (ou informativa). Segundo o BVG, não mais existiriam dados insignificantes e que a atribuição de dados a uma esfera íntima não tem mais nenhum papel significativo<sup>26, 27</sup>.

---

e sua correspondência”) para a proteção conferida pela Carta de direitos Fundamentais da União Europeia, de 2000 (que garante também o “direito à proteção de dados pessoais” e prevê a efetivação de tal proteção através de uma autoridade independente), diz Rodotà que “a distinção entre o direito ao respeito da vida privada e familiar e o direito à proteção dos dados pessoais não é bizantina. O direito ao respeito da vida privada e familiar reflete, primeira e principalmente, um componente individualista: este poder basicamente consiste em impedir a interferência na vida privada e familiar de uma pessoa. Em outras palavras, é um tipo de proteção estático, negativo. Contrariamente, a proteção de dados estabelece regras sobre os mecanismos de processamento de dados (...) – *i. e.* é um tipo de proteção dinâmico, que segue o dado em todos os seus movimentos. Adicionalmente, a supervisão e outros poderes não são somente conferidos às pessoas interessadas (os sujeitos dos dados), mas são também entregues a uma autoridade independente. A proteção não é mais deixada somente aos sujeitos dos dados, uma vez que existe um órgão público permanente responsável por isso” - RODOTÀ, Stefano. **A vida na sociedade da vigilância** – a privacidade hoje. Organização, seleção e apresentação de Maria C. B. de Moraes. Trad.: Danilo Doneda e Luciana C. Doneda. Rio de Janeiro: Renovar, 2008, p. 17.

25 ABREU, Jacqueline de Souza. Tratamento de dados pessoais para segurança pública: contornos do regime jurídico pós-LGPD. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz; BIONI, Bruno Ricardo (Coord.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021, p. 588.

26 Sobre esse caso, imprescindível a leitura de MENDES, Laura Schertel. Autodeterminação informacional: origem e desenvolvimento conceitual na jurisprudência da Corte Constitucional alemã. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (Coord.). **Lei Geral de Proteção de Dados (Lei nº 13.709/2018)** – A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020, especialmente pp. 229 e 230. Essa visão doutrinária acabou repercutindo também na recente jurisprudência do STF, pois no julgamento da paradigmática ADI n. 6.387, julgada em 6 e 7 de maio de 2020, a Min. Carmen Lúcia, em seu voto concorrente, referiu que “não existem dados insignificantes” (no caso, tratava-se de nome, endereço e telefone – dados que há duas décadas atrás estavam disponíveis em todas as residências, através das listas telefônicas impressas – ou facilmente disponibilizadas pelo serviço de Informações, fornecido pela empresa oficial de telefonia...). Isso se deu, segundo a Ministra, em razão da “atual capacidade de processamento de dados, desde que cruzados com outras informações e compartilhados com pessoas ou entidades distintas”, o que permite que os dados ganhem novo valor e significado. Segundo ela, “a partir de técnicas de agregação e de tratamento, sua utilização pode-se dar para fins muito distintos dos expostos na coleta inicial”. E, no mesmo julgamento, o Min. Gilmar Mendes reforçou que o direito fundamental à proteção dos dados possui conteúdo mais alargado do que o direito à privacidade, já que não se restringe aos dados íntimos, estendendo-se, ao contrário, a todo e qualquer dado que possa conduzir à identificação de alguém.

27 É importante notar que após a paradigmática decisão da Corte Constitucional alemã de 1983, que reconheceu o direito funda-

Isso ocorre porque as principais decisões que impactam a vida das pessoas na sociedade, como concessão ou não de crédito, ou obtenção de vaga no emprego, que antes eram tomadas por seres humanos, agora quase sempre são delegadas para “sistemas automatizados, algoritmos de *ranking* e modelos de risco preditivo”<sup>28</sup>, a partir da análise dos mais variados dados encontráveis na rede.

E isso é preocupante, pois os dados pessoais “são nossos avatares com relação a tudo o que acontece conosco no mundo digital. Em outras palavras, os dados pessoais são a representação do que nós somos. Por meio deles, nossa vida é decidida em múltiplas esferas”<sup>29</sup>. A partir dos dados, forma-se uma espécie de “mosaico identitário”, proveniente não só dos dados que espontaneamente fornecemos para ter acesso a alguma informação ou aplicação, ou para fazer qualquer transação digital, mas também das ‘pegadas digitais’ (ou ‘sombras digitais’) que deixamos na rede, sejam imagens captadas em câmeras de vigilância, dados advindos das transações econômicas e bancárias, diagnósticos e prontuários médicos, histórico de compras, movimentações processuais, etc.<sup>30</sup>

Todas essas informações colhidas sobre cada um de nós, a partir desses dados que produzimos, consciente ou inconscientemente, na rede, são essenciais para esse novo modelo de negócios, baseado na exploração e monetização desses dados pessoais, cujo ulterior tratamento permitirá a criação de perfis, individuais

---

mental à autodeterminação informativa, uma segunda decisão igualmente importante foi proferida em 27. 02. 2008 pela mesma BVerfGE. Trata-se do caso *Online Durchsuehung*, que envolvia o controle de constitucionalidade do monitoramento *on-line* de sistemas informáticos por órgãos de segurança estatal. Nesse caso, “em vez de aplicar o direito à autodeterminação informativa (...), a Corte extraiu do direito geral à personalidade (art. 2, I, c/c art. 1, I, da Lei Fundamental alemã) um direito fundamental à garantia da confidencialidade e da integridade dos sistemas informáticos (...). Esse direito, que ficou conhecido na opinião pública alemã como ‘direito fundamental informático’ (*Computergrundrecht*), chama a atenção exatamente por se referir na sua designação à confidencialidade e à integridade dos sistemas, conceitos-chave que compõem a definição de segurança da informação. A inovação da decisão reside também no fato de que o objeto da proteção constitucional passa a ser o próprio sistema informático pessoal, e por consequência o indivíduo que o utiliza”. (...) “Não basta apenas garantir os direitos de acesso, correção e cancelamento de dados pelo titular, é preciso também garantir a confidencialidade, a integridade e a autenticidade dos sistemas informáticos, assegurar a confiança dos indivíduos nesses sistemas, bem como garantir a gestão de riscos de vazamento de informação” – Nesses termos, MENDES, Laura Schertel. Segurança da informação, proteção de dados pessoais e confiança: uma perspectiva comparada. In: GRUNDMAN, Stefan; MENDES, Gilmar; MARQUES, Claudia Lima, et al. (org.). **Direito privado, Constituição e fronteiras**: encontros da Associação Luso-Alemã de Juristas no Brasil. 2. ed. rev., atual. e ampl. São Paulo: Ed. Revista dos Tribunais, 2014, p. 276/277.

28 MEDON, Filipe. Decisões automatizadas: o necessário diálogo entre a Inteligência Artificial e a proteção de dados pessoais para a tutela de direitos fundamentais. In: TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (Coord.). **O Direito Civil na era da Inteligência Artificial**. São Paulo: Thomson Reuters Brasil/Revista dos Tribunais, 2020, p. 338. Segundo Frazão, “algoritmos preocupam tanto quando acertam como quando erram. Preocupam quando acertam, pois podem revelar aspectos íntimos da nossa personalidade (...). Preocupam quando erram, pois desconfiguram a nossa individualidade” - FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais – Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais – e suas repercussões no Direito Brasileiro**. 2. Ed. São Paulo: Thomson Reuters Brasil/Revista dos Tribunais, 2020, p. 34.

29 LEMOS, Ronaldo; BRANCO, Sérgio. *Privacy by Design*: conceito, fundamentos e aplicabilidade na LGPD. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz; BIONI, Bruno Ricardo (Coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021, p. 448.

30 RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – Lei 13. 709/2018. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz; BIONI, Bruno Ricardo (Coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021, p. 184/185.

e grupais, que otimizam a venda de espaços para publicidade<sup>31</sup>, além da venda dessas informações a parceiros comerciais<sup>32, 33</sup>.

Os perigos associados a esse *trade-off* entre benefícios que almejamos e informações pessoais que disponibilizamos são bem elucidadas por Joana Varon:

Por exemplo, ao fornecer o número do CPF para obter descontos nas farmácias, a lista de medicamentos associada a esse dado pode conter informações delicadas sobre nossa saúde. É possível que essas informações sejam utilizadas de maneira discriminatória por seguradoras de saúde, alterando o valor da franquia de acordo com o perfil. Da mesma forma, nosso histórico de compras *on-line* diz bastante sobre poder aquisitivo e preferências pessoais. Por meio dessas informações, é possível embasar o direcionamento de propagandas compatíveis com o nosso gosto, tentando-nos a comprar algo que não precisamos, bem como cobrar preços mais altos ou limitar o acesso ao crédito para determinados perfis. Dados sobre orientação sexual, em uma sociedade que ainda vive preconceitos contra a diversidade, também podem servir a práticas de segregação, restringindo, por exemplo, as oportunidades de trabalho.<sup>34</sup>

- 
- 31 A gigantesca coleta de dados, sua conexão e o tratamento que permite a identificação de perfis, conduziu à criação da chamada *publicidade direcionada*. Ou seja, permite-se identificar potenciais consumidores que frequentam determinados ambientes (websites), ou direcionar a publicidade especificamente a um público feminino, ou de terceira idade, ou de adolescentes, ou de pessoas que gostam de viagens, de culinária, etc. Essa nova forma de publicidade permitiu a redução dos seus custos, pois ela passou a ser direcionada exclusivamente ao consumidor interessado, tanto que o serviço de publicidade da Google – Google Ads, anteriormente conhecido como Google AdWords – prevê que a contraprestação somente será devida se o potencial consumidor clicar no correspondente anúncio. Sobre essas formas de publicidade e seus efeitos para a proteção de dados, v. BIONI, Bruno Ricardo. **Proteção de Dados Pessoais** – a função e os limites do consentimento. 2ª ed., rev., atual. e reform. Rio de Janeiro: Forense, 2020, p. 14/17. Não se há dúvidas de que se trata de uma atividade extraordinariamente lucrativa, considerando que a holding Alphabet (que abrange a Google e todas as companhias do grupo), em 2016, teve um faturamento superior a 90 bilhões de dólares, dos quais 87% originavam-se de publicidade – MATTIUZZO, Marcela. Business Models and Big Data: How Google uses your Personal Information. In: In: BRANCO, Sérgio; TEFFÉ, Chiara de (org.). **Privacidade em perspectivas**. Rio de Janeiro: Lumen Juris, 2018, p. 181.
- 32 TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados** – e suas repercussões no Direito Brasileiro. 2. ed. São Paulo: Ed. Revista dos Tribunais/Thompson Reuters Brasil, 2020, p. 290. Excelente estudo realizado pelo Ministério Público Federal nos informa que “empresas de tecnologia monitoram as atividades do consumidor quando conectado à internet – incluindo as pesquisas que ele fez, as páginas que ele visitou e o conteúdo consultado – com a finalidade de fornecer publicidade dirigida aos interesses individuais desse consumidor. (...) Os dados são tratados com o auxílio de métodos estatísticos e técnicas de inteligência artificial, com o fim de sintetizar hábitos, preferências pessoais e outros registros. A partir disso são criados perfis para cada usuário (*profiling*) que possibilitam o envio seletivo de mensagens publicitárias de um produto a seus potenciais compradores. Redes sociais *on-line* como o Facebook também realizam o tratamento de dados pessoais dos seus usuários. A rede social permite a seus usuários gerar um perfil público, alimentado por dados e informações pessoais, dispondo de ferramentas que permitem a interação com outros usuários afins ou não ao perfil publicado. A rede social é um intermediário que acumula informações pessoais sobre os usuários. Os clientes de redes sociais são aqueles que efetivamente contratam a rede social mediante retribuição, não os usuários, mas empresas que apresentam interesse na base de dados e na relação de usuários, para oferecer publicidade focada em grupos. As possibilidades oferecidas a uma pessoa são fechadas (encaixotadas) em torno de presunções realizadas por ferramentas de análise comportamental, guiando dessa forma suas escolhas futuras. A publicidade específica tem o efeito colateral de uniformizar padrões de comportamento, diminuindo o rol de escolhas apresentadas a uma pessoa. A elaboração de perfis pode levar à negativa de acesso a determinado bem ou serviço (negativa de acesso a site porque o consumidor acessou sites de proteção ao crédito), bem como preços diferentes a consumidores diversos conforme o seu perfil (*adaptive pricing*)” - Brasil. Ministério Público Federal. Câmara de Coordenação e Revisão, 3. **Sistema brasileiro de proteção e acesso a dados pessoais: análise de dispositivos da Lei de Acesso à Informação, da Lei de Identificação Civil, da Lei do Marco Civil da Internet e da Lei Nacional de Proteção de Dados** – Brasília : MPE, 2019. 85 p. – (Roteiro de Atuação ; v. 3), p. 58. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/ccr3/documentos-e-publicacoes/roteiros-de-atuacao/sistema-brasileiro-de-protecao-e-acesso-a-dados-pessoais-volume-3>, acesso em 19/12/2020.
- 33 Refere Frazão que “na seara consumerista, assim como na seara trabalhista, são inúmeros os riscos da utilização de tais dados para praticar toda sorte de discriminações e violações a consumidores, empregados e candidatos a emprego em processos de seleção ou recrutamento” – FRAZÃO, Ana. Nova LGPD: o tratamento dos dados pessoais sensíveis. *JOTA*, 26/09/2018, disponível em [https://www.jota.info/paywall?redirect\\_to=//www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018](https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018), acesso em 20/12/2020.
- 34 VARON, Joana. Entrevista concedida sobre o tema da Privacidade e dados pessoais, para a Revista **Panorama setorial da Internet**. N. 2, junho 2019, ano 11, p. 12. Joana é Diretora da *Coding Rights*.

A preocupação maior com a proteção dos dados sensíveis liga-se especialmente ao princípio da não discriminação<sup>35</sup> (embora também se procure aumentar a proteção à privacidade e à identidade<sup>36</sup>), objetivando-se evitar que a coleta de tais dados possa servir para tratamento discriminatório e lesivo. Tendo isso em vista, percebe-se que o valor a ser tutelado é o da igualdade material, e não o da privacidade propriamente dita.<sup>37</sup> A possibilidade de tratamento discriminatório em razão de aspectos relacionados a orientação sexual, religiosa, política, racial, filiação sindical, etc, não necessita de maiores explicações, à luz das experiências históricas de quase todos os países. Todavia, outros dados, mais triviais, podem se converter em dados sensíveis a partir do tratamento tecnológico alcançado pela chamada *Big Data*, que, como pontua Biondi, permite “correlacionar uma série de dados para prever comportamentos e acontecimentos”, exemplificando-se com o conhecido caso de uma loja de departamentos norte-americano que, através da coleta de dados da navegação pela internet das consumidoras, conseguiu identificar quais delas estariam grávidas, precisando, inclusive, seu período gestacional. O autor também refere estudo da Universidade de Cambridge mostrando que, a partir da análise de “curtidas” em uma rede social, foi possível criar um retrato fiel dos gostos e preferências dos usuários e suas próprias características, tendo logrado identificar com exatidão a porcentagem dos usuários homossexuais e heterossexuais, usuários brancos e negros, eleitores republicanos ou democratas<sup>38</sup>.

De fato, dados aparentemente irrelevantes, colhidos para uma determinada finalidade, podem ser conjugados com outros, tratados por algoritmos e inteligência artificial, permitindo a extração de novas informações totalmente descoladas da finalidade que originou sua coleta. Assim, dados considerados irrelevantes ou triviais como “idade, altura, nacionalidade, os locais de moradia e de trabalho podem server de insumo para correlações, predições e ranqueamentos acerca da personalidade do titular dos dados pessoais ou de determinados grupos sociais”<sup>39</sup>.

---

35 Apoiada em Rodotà, Ana Frazão refere que “a própria definição de dados pessoais sensíveis (...) está ligada muito mais à proteção da igualdade e da não discriminação do que propriamente à intimidade. Basta ver que a LGPD considera dado pessoal sensível qualquer dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” – FRAZÃO, Ana. Objetivos e alcance da lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados** – e suas repercussões no Direito Brasileiro. 2. ed. São Paulo: Ed. Revista dos Tribunais/Thompson Reuters Brasil, 2020, p. 105.

36 Essa é a chave de leitura proposta por Carlos Nelson Konder para explicar o destaque dado à proteção mais rigorosa aos dados sensíveis: proteção da privacidade, identidade e da não discriminação, como aspectos do direito da personalidade e da proteção da dignidade da pessoa humana – KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13. 709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados** – e suas repercussões no Direito Brasileiro. 2. ed. São Paulo: Ed. Revista dos Tribunais/Thompson Reuters Brasil, 2020, p. 442.

37 Como refere MULHOLLAND, Caitlin. Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (Lei 13. 709/2018). In: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (Coord.). **Responsabilidade Civil e Novas Tecnologias**. Indaiatuba: Ed. Foco, 2020, p. 110.

38 BIONI, Bruno Ricardo. **Proteção de Dados Pessoais** – a função e os limites do consentimento. 2ª ed., rev., atual. e reform. Rio de Janeiro: Forense, 2020, p. 84.

39 MENDES, Laura Schertel. Proteção de dados para além do consentimento: tendências de materialização. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz; BIONI, Bruno Ricardo (Coord.).

A localização física do consumidor, por exemplo, em vez de dado neutro, pode ser decisiva para “catalogá-lo” em determinada classe de pessoas, com potencial efeito discriminatório<sup>40</sup>.

O tratamento dos dados permite a construção de um perfil<sup>41</sup> (o “corpo eletrônico” da pessoa) e a inclusão do indivíduo em um grupo, com base em

---

**Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021, p. 82/83. Na mesma linha, Konder refere que “dados de localização geográfica, hábitos de compras, preferências de filmes e histórico de pesquisa podem parecer inofensivos isoladamente, mas um rápido tratamento em conjunto pode servir a identificar orientação religiosa, política e mesmo sexual” - KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13. 709/2018. In: TEPEĐINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados – e suas repercussões no Direito Brasileiro.** 2. ed. São Paulo: Ed. Revista dos Tribunais/Thompson Reuters Brasil, 2020, p. 451. Assim, “em verdade, qualquer dado pessoal, a depender do tratamento recebido, pode acabar revelando dado pessoal sensível, razão pela qual a classificação abstrata do dado se afigura reducionista e problemática” - TERRA, Aline de Miranda Valverde; CASTRO, Diana Paiva de. A responsabilidade do Poder Público no tratamento de dados pessoais: análise dos artigos 31 e 32 da LGPD. In: MULHOLLAND, Caitlin (Org.). **ALGPD e o novo marco normativo no Brasil.** Porto Alegre: Arquipelago Ed., 2020, p. 246.

<sup>40</sup> Em outro estudo, em co-autoria, tive a ocasião de descrever essa prática: “outra forma de discriminação injustificada é a prática de *weblining* que tem origem nas antigas práticas de seguradoras, que desenhavam linhas vermelhas – *redlining* – nos mapas das cidades para negar o acesso ao contrato de seguro, cancelá-lo ou vedar sua renovação em regiões de alto risco. (...) O *weblining* é a nova versão da técnica discriminatória, aplicada ao ciberespaço, à luz das técnicas de geolocalização, criando perfis especializados, no sentido de negar acesso a determinados bens e serviços, ou diferenciar preços a moradores de determinadas regiões, de acordo com sua condição financeira ou de determinada etnia” - COLOMBO, Cristiano; FACCHINI NETO, Eugênio. Decisões automatizadas em matéria de perfis e riscos algorítmicos: diálogos entre Brasil e Europa acerca dos direitos das vítimas de dano estético digital. In: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (Coord.). **Responsabilidade Civil e Novas Tecnologias.** Indaiatuba: Ed. Foco, 2020, p. 170. Sobre o *weblining*, v. HERNANDEZ, Gary A.; EDDY, Katherine; MUCHMORE, Joel. Insurance *weblining* and unfair discrimination in cyberspace. *Southern Methodist University Law Review.* Dallas, v. 54 (2001), p. 1953-1972. Em outro artigo, com a mesma parceria, ponderamos que “dados aparentemente ‘inocentes’, como alimentação em voos, manipulada para um determinado passageiro, pode revelar sua religião, bem como informações sobre alergias, podem indicar a presença de patologias. Tais dados, devidamente tratados, podem levar a um conhecimento iluminante sobre determinado sujeito, eventualmente sujeitando-o a exclusões discriminatórias” - COLOMBO, Cristiano; FACCHINI NETO, Eugênio. “Corpo eletrônico” como vítima de ofensas em matéria de tratamento de dados pessoais: reflexões acerca da responsabilidade civil por danos à luz da Lei Geral de Proteção de Dados pessoais brasileira e a viabilidade da aplicação da noção de dano estético ao mundo digital. In: ROSENVALD, Nelson; DRESCH, Rafael de Freitas Valle; WESENDONCK, Tula (Coord.). **Responsabilidade Civil: novos riscos.** Indaiatuba: Ed. Foco, 2019, p. 52/53.

<sup>41</sup> A concentração de inúmeros dados fragmentários sobre os gostos e atividades digitais de um indivíduo conduz a uma ‘metainformação’, capaz de permitir a categorização de tal indivíduo em determinado grupo de pessoas assemelhadas, prever as tendências de suas decisões futuras e manipular suas emoções no sentido de conduzi-lo a atuar de tal ou qual maneira. Sobre o tema do *profiling* e seus riscos, consulte-se as excelentes contribuições de BONNA, Alexandre Pereira. Dados pessoais, identidade virtual e a projeção da personalidade: “*profiling*”, estigmatização e responsabilidade civil. In: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (Coord.). **Responsabilidade Civil e Novas Tecnologias.** Indaiatuba: Ed. Foco, 2020, esp. p. 22/23. Esse autor aponta os riscos de estigmatização (identificado, pelo autor, como a divergência entre a identidade real e a virtual de uma pessoa, pois a técnica de *profiling* categoriza as pessoas em estantes, gostos e preferências que podem não corresponder à realidade, estigmatizando-a) a que estão sujeitos muitos dos usuários da internet: “por exemplo, uma pessoa que busca apenas música sertaneja, forró e brega, literatura e filmes populares, jamais receberá uma oferta de cursos ou de disponibilização de material sobre música clássica, literatura grega e filmes cult. Ou seja, embora qualquer ser humano possa, em tese, se interessar por tais estilos de música, literatura e filmes mais rebuscados qualitativamente, a prática mercadológica necessita agir de forma inteligente e certa diante do seu público alvo, motivo pelo qual o estigma criado serve como mola propulsora das plataformas digitais no momento de ofertar publicidade aos mais diferentes fornecedores de produtos e serviços.” Os estigmas criados pela técnica de *profiling* diminui “o leque de relações e contatos da pessoa com os mais diversos tipos de bens e serviços pagos ou gratuitos, tornando a rede menos democrática e mais discriminatória. Um outro exemplo, um sujeito que tem identidade virtual como ‘pobre/sem recursos financeiros’, sendo ou não de verdade, não receberá promoções de ingressos e viagens internacionais e/ou videoaulas de investimento financeiro (op. cit., p. 26/27). Características passadas do usuário, assim, acabam perpetuando o perfil pelo qual esse indivíduo se apresenta no mundo digital, dificultando sua mudança. Essa preocupação é universal, manifestada por todos os que atuam na área, como se vê do alerta levantado pelo Grupo de Trabalho 29 para Proteção de Dados, do Comitê Europeu de Proteção de Dados, em suas “ORIENTAÇÕES sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679”: “A definição de perfis é suscetível de perpetuar os estereótipos existentes e a segregação social. Pode igualmente amarrar as pessoas a uma categoria específica e limitá-las às respectivas preferências sugeridas, pondo assim em causa a sua liberdade para escolher, por exemplo, determinados produtos ou serviços” – disponível em [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=612053](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053), acesso em 29. 11. 21. O art. 4.º, ponto 4, do RGPD define a definição de perfis como “qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspectos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações” - GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS - Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679, adotadas em 3 de outubro de 2017, com a última redação revista e adotada em 6 de fevereiro de 2018 – Disponível em [https://www.cnpd.pt/home/rgpd/docs/wp260rev01\\_pt.pdf](https://www.cnpd.pt/home/rgpd/docs/wp260rev01_pt.pdf), acesso em 21/12/2021.



análises estatísticas, sendo que, muitas vezes, os caracteres do grupo não refletem as reais “características de uma pessoa concretamente considerada, gerando uma discriminação abusiva”<sup>42</sup>.

Assim, as decisões automatizadas, fundadas em métodos estatísticos para análise de grande volume de dados, entre os quais se busca estabelecer correlações, podem ter grande impacto sobre a autonomia, igualdade e personalidade de um indivíduo. Isto porque na sociedade digital, os dados pessoais constituem a principal, por vezes única, forma de representação das pessoas perante suas relações pessoais, perante a sociedade como um todo e até mesmo perante organismos estatais, podendo abrir ou fechar portas de oportunidade. Caso a representação esteja equivocada, seja por falha do algoritmo, seja pela incompleta ou equívoca base de dados em que se baseou, isso afeta tanto a forma como o indivíduo se percebe como também o modo como a sociedade o enxerga e o avalia. Caso feche oportunidades, isso representa uma restrição indevida à sua autonomia, limitando a sua liberdade de ação, suas escolhas econômicas e até mesmo existenciais. Também pode significar violação ao princípio da igualdade, na hipótese de que a classificação e seleção operada por algoritmos produza resultados desiguais para pessoas em situações semelhantes, afetando negativamente as suas oportunidades de vida na sociedade<sup>43</sup>.

De fato, “muito do que é coletado sobre os indivíduos não diz respeito somente à sua intimidade, mas também a aspectos públicos da sua vida que, quando reunidos, ganham nova dimensão, possibilitando a categorização dos usuários em determinados perfis”. Assim, a utilização dos dados deixa de se restringir apenas à questão da privacidade e passa necessariamente a envolver outras discussões, como o direito de não ser julgado ou categorizado para determinados fins ou com base em determinados critérios.<sup>44</sup> Isso tudo preocupa pois não se tem nem mesmo como avaliar o potencial danoso de algoritmos, cuja fórmula se ignora, bem como não se tem conhecimento da correção ou completude dos dados em que se baseiam, além do fato de trabalharem em cima de correlações que não correspondem a causalidades<sup>45</sup>.

---

42 MULHOLLAND, Caitlin. Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018). In: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (Coord.). **Responsabilidade Civil e Novas Tecnologias**. Indaiatuba: Ed. Foco, 2020, p. 116/117.

43 DONEDA, Danilo; MENDES, Laura Schertel; SOUZA, Carlos Affonso; ANDRADE, Norberto Nuno Gomes de. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. In: TEPEDINO, Gustavo; MENEZES, Joyceane Bezerra de (Coord.). **Autonomia privada, liberdade existencial e direitos fundamentais**. Belo Horizonte: Fórum, 2019, p. 98.

44 FRAZÃO, Ana. Plataformas digitais, *big data* e riscos para os direitos da personalidade. In: TEPEDINO, Gustavo; MENEZES, Joyceane Bezerra de (Coord.). **Autonomia privada, liberdade existencial e direitos fundamentais**. Belo Horizonte: Fórum, 2019, p. 340 e 341.

45 FRAZÃO, Ana. Plataformas digitais, *big data* e riscos para os direitos da personalidade. In: TEPEDINO, Gustavo; MENEZES, Joyceane Bezerra de (Coord.). **Autonomia privada, liberdade existencial e direitos fundamentais**. Belo Horizonte: Fórum, 2019, p. 343.

É hora de finalizar.

#### 4. CONSIDERAÇÕES FINAIS

O texto buscou evidenciar a civilização digital em que estamos inseridos, com todos os seus pontos positivos, mas também alertando para os riscos e perigos inerentes ao uso dessa nova tecnologia.

Passamos a viver em uma sociedade hiperconectada e migramos boa parte de nossas relações, sejam pessoais ou econômicas, para um mundo virtual. Enquanto no mundo real nossos percursos passam muitas vezes despercebidos, não deixando rastros ou testemunhos, no mundo virtual deixamos pegadas digitais que se tornam perenes. Nesse mundo projetamos uma sombra, reconstruída a partir dos dados que fornecemos e que são captados por incontáveis sensores. Esses dados esparsos – quiçá irrelevantes e isoladamente pouco identificadores – passaram a ser agrupados por meio de potentes algoritmos, que ajudam a construir nossos perfis (fenômeno conhecido como *profiling*, ou perfilização). E então, *voilà!* Conhecendo quem nós somos, do que gostamos, o que consumimos, o que fazemos, o que nos empolga, quais as nossas inclinações, fica bem mais fácil direcionar uma publicidade personalizada e despertar nossos impulsos.

Isso por vezes não tem efeitos tão preocupantes – resumidos a um maior consumismo. Mas como a acuidade desse perfil depende muito da qualidade e autenticidade dos dados coletados, por vezes ocorrem distorções que podem comprometer nossa verdadeira identidade. Ainda mais preocupante do que isso é a constatação da nossa inclusão em grupos de indivíduos que aparentemente possuem perfil semelhante – pela idade, etnia, tipo de trabalho, hábitos de consumo, localização, etc. E, por vezes, isso pode conduzir ao que é chamado de discriminação por associação, que pode acarretar uma série de problemas para os indivíduos ‘catalogados’ como membros de uma determinada categoria de pessoas. Se, por exemplo, alguém reside em um bairro de uma classe economicamente mais vulnerável e que, na média, possua um histórico de maior índice de inadimplência, talvez lhe venha a ser negado algum crédito, ou sua disponibilização a uma taxa de juros mais elevado, por ter o algoritmo previsto um risco maior de inadimplência, ainda que aquele cidadão, individualmente, seja um ‘bom pagador’.

Por outro lado, outro problema reside em que os dados coletados no passado irão definir o perfil de alguém e talvez colocá-lo em um certo ‘gueto’, do qual será difícil sair futuramente. Como se exemplificou no texto, se alguém, no passado, gostava de música de gosto mais popular e consumia outros produtos ou serviços típicos de pessoas de classe economicamente mais simples, dificilmente receberá informações sobre promoções de passagens aéreas internacionais ou de cursos sobre investimentos, pois o algoritmo concluirá que esses serviços não

combinam com o perfil daquele indivíduo. Se do ponto de vista estatístico essa ‘conclusão’ é acertada, do ponto de vista daquele preciso indivíduo, poderá estar equivocada, retirando deste algumas oportunidades. A média, como na piada - se alguém ganha 2 e outro ganha 10, dir-se-á que, na média, ambos ganham 6 -, nem sempre fornece uma orientação satisfatória, pois pode estar estatisticamente correta, mas individualmente equivocada.

Ou seja, na sociedade digital, governada por algoritmos simplificadores, que trabalham em cima de correlações e não necessariamente de causalidades, corre-se o risco de simplificações exageradas, de comprometimento da autonomia da pessoa, além de riscos de discriminações as mais diversas.

As inequívocas vantagens dessa tecnologia que nos envolve cada vez mais, em termos de maior racionalidade, agilidade, celeridade, em termos macro, não devem servir de desculpa para não nos preocuparmos com os problemas inerentes às aplicações de tal tecnologia na esfera micro, na busca de soluções satisfatórias, ou ao menos paliativas.

## REFERÊNCIAS BIBLIOGRÁFICAS

ABREU, Jacqueline de Souza. Tratamento de dados pessoais para segurança pública: contornos do regime jurídico pós-LGPD. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz; BIONI, Bruno Ricardo (Coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

BALKIN, Jack M. Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation. *Yale Law School: Faculty Scholarship Series*, n. 5160, 2018. Disponível em [https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=6159&context=fss\\_papers](https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=6159&context=fss_papers). Acesso em 22/10/2022.

BARROSO, Luís Roberto. Revolução tecnológica, crise da democracia e mudança climática: limites do direito num mundo em transformação. **Revista Estudos Institucionais**, v. 5, p. 1262-1313, set./dez. 2019.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais – a função e os limites do consentimento**. 2ª ed., rev., atual. e reform. Rio de Janeiro: Forense, 2020.

BONNA, Alexandre Pereira. Dados pessoais, identidade virtual e a projeção da personalidade: “*profiling*”, estigmatização e responsabilidade civil. In: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (Coord.). **Responsabilidade Civil e Novas Tecnologias**. Indaiatuba: Ed. Foco, 2020.

BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 3. **Sistema brasileiro de proteção e acesso a dados pessoais**: análise de dispositivos da Lei de Acesso à Informação, da Lei de Identificação Civil, da Lei do Marco Civil da Internet e da Lei Nacional de Proteção de Dados – Brasília : MPF, 2019. 85 p. – (Roteiro de Atuação; v. 3), p. 58. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/ccr3/documentos-e-publicacoes/roteiros-de-atuacao/sistema-brasileiro-de-protecao-e-acesso-a-dados-pessoais-volume-3>, acesso em 19/12/2020.

BYUNG-CHUL HAN. **O coronavírus de hoje e o mundo de amanhã, segundo o filósofo Byung-Chul Han**. Entrevista concedida pelo filósofo sul-coreano Byung-Chul Han ao jornal EL PAÍS, em 22.03.2020. Disponível em <https://brasil.elpais.com/ideas/2020-03-22/o-coronavirus-de-hoje-e-o-mundo-de-amanha-segundo-o-filosofo-byung-chul-han.html>, acesso em 20.01.2022.

COLOMBO, Cristiano; FACCHINI NETO, Eugênio. “Corpo eletrônico” como vítima de ofensas em matéria de tratamento de dados pessoais: reflexões acerca da responsabilidade civil por danos à luz da Lei Geral de Proteção de Dados pessoais brasileira e a viabilidade da aplicação da noção de dano estético ao mundo digital. In: ROSENVALD, Nelson; DRESCH, Rafael de Freitas Valle; WESENDONCK, Tula

- (Coord.). **Responsabilidade Civil: novos riscos**. Indaiatuba: Ed. Foco, 2019.
- COLOMBO, Cristiano. FACCHINI NETO, Eugênio. Decisões automatizadas em matéria de perfis e riscos algorítmicos: diálogos entre Brasil e Europa acerca dos direitos das vítimas de dano estético digital. In: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (Coord.). **Responsabilidade Civil e Novas Tecnologias**. Indaiatuba: Ed. Foco, 2020.
- DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. rev. e atual. São Paulo: Thomson Reuters Brasil/Revista dos Tribunais, 2019.
- DONEDA, Danilo; MENDES, Laura Schertel; SOUZA, Carlos Affonso; ANDRADE, Norberto Nuno Gomes de. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. In: TEPEDINO, Gustavo; MENEZES, Joyceane Bezerra de (Coord.). **Autonomia privada, liberdade existencial e direitos fundamentais**. Belo Horizonte: Fórum, 2019.
- DRESCH, Rafael de Freitas Vale; FALEIROS JÚNIOR, José Luiz de Moura. Reflexões sobre a responsabilidade civil na Lei Geral de Proteção de Dados (Lei n. 13.709/2018). In: ROSENVALD, Nelson; DRESCH, Rafael de Freitas Valle; WESENDONCK, Tula (Coord.). **Responsabilidade Civil: novos riscos**. Indaiatuba: Ed. Foco, 2019.
- FACCHINI NETO, Eugênio; DEMOLINER, Karine Silva. Direito à privacidade na era digital – uma releitura do art. XII da Declaração Universal dos Direitos Humanos (DUDH) na sociedade do espetáculo. **Revista Internacional Consinter de Direito**. Ano V, n. IX, 2º Semestre 2019.
- FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. Privacidade e lei geral de proteção de dados pessoais. **Revista de Direito Brasileira**. Florianópolis, v. 23, n. 9, p. 284-301 |Mai./Ago. 2019.
- FLORIDI, Luciano. *The Fourth Revolution: how the infosphere is reshaping the human reality*. Oxford: Oxford University Press, 2014.
- FRAZÃO, Ana. Plataformas digitais, *big data* e riscos para os direitos da personalidade. In: TEPEDINO, Gustavo; MENEZES, Joyceane Bezerra de (Coord.). **Autonomia privada, liberdade existencial e direitos fundamentais**. Belo Horizonte: Fórum, 2019.
- FRAZÃO, Ana. Objetivos e alcance da lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados – e suas repercussões no Direito Brasileiro**. 2. ed. São Paulo: Ed. Revista dos Tribunais/Thompson Reuters Brasil, 2020.
- FRAZÃO, Ana. Nova LGPD: o tratamento dos dados pessoais sensíveis. **JOTA**, 26/09/2018, disponível em [https://www.jota.info/paywall?redirect\\_to=//www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018](https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018), acesso em 20/12/2020.
- FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais – Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais – e suas repercussões no Direito Brasileiro**. 2. Ed. São Paulo: Thomson Reuters Brasil/Revista dos Tribunais, 2020.
- HERNANDEZ, Gary A.; EDDY, Katherine; MUCHMORE, Joel. Insurance weblining and unfair discrimination in cyberspace. *Southern Methodist University Law Review*. Dallas, v. 54 (2001).
- HOFFMANN-RIEM, Wolfgang. **Teoria Geral do Direito Digital**. Transformação digital – desafios para o direito. Trad. Italo Fuhrmann. Rio de Janeiro: Forense, 2021.
- ISAAK, Jim; HANNA, MINA J. User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. **Computer**, vol. 51, no. 8, pp. 56-59, August 2018– Disponível em <https://ieeexplore.ieee.org/document/8436400>, acesso em 21/12/2020.
- KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados – e suas repercussões no Direito Brasileiro**. 2. ed. São Paulo: Ed. Revista dos Tribunais/Thompson Reuters Brasil, 2020.
- LEMOS, Ronaldo; BRANCO, Sérgio. *Privacy by Design: conceito, fundamentos e aplicabilidade na LGPD*. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz; BIONI, Bruno Ricardo (Coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

- LACE, Susanne. *The glass consumer: life in a surveillance society*. Bristol: Policy Press, 2005.
- LANEY, Doug, disponível em <http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf>. Acesso em 10.12.2019.
- LEMOS, Ronaldo. **Ou a sociedade acompanha internet ou a democracia começa a ficar em xeque**. Disponível em <https://blogdomorris.blogfolha.uol.com.br/2014/04/08/ou-sociedade-acompanha-internet-ou-democracia-comeca-a-ficar-em-xeque/>, acesso em 29.11.20).
- MAGRANI, Eduardo; OLIVEIRA, Renan Medeiros de. O Big Data somos nós: novas tecnologias e projetos de gerenciamento pessoal de dados. In: TEPEDINO, Gustavo et al. (Coord.). **Anais do VI Congresso do Instituto Brasileiro de Direito Civil**. Belo Horizonte: Fórum, 2019.
- MATTIUZZO, Marcela. Business Models and Big Data: How Google uses your Personal Information. In: In: BRANCO, Sérgio; TEFFÉ, Chiara de (org.). **Privacidade em perspectivas**. Rio de Janeiro: Lumen Juris, 2018.
- MEDON, Filipe. Decisões automatizadas: o necessário diálogo entre a Inteligência Artificial e a proteção de dados pessoais para a tutela de direitos fundamentais. In: TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (Coord.). **O Direito Civil na era da Inteligência Artificial**. São Paulo: Thompson Reuters Brasil/Revista dos Tribunais, 2020.
- MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor**, vol. 20, n. 79, jul.-set. 2011.
- MENDES, Laura Schertel. Autodeterminação informacional: origem e desenvolvimento conceitual na jurisprudência da Corte Constitucional alemã. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (Coord.). **Lei Geral de Proteção de Dados (Lei nº 13.709/2018) – A caminho da efetividade: contribuições para a implementação da LGPD**. São Paulo: Thomson Reuters Brasil, 2020.
- MENDES, Laura Schertel. Segurança da informação, proteção de dados pessoais e confiança: uma perspectiva comparada. In: GRUNDMAN, Stefan; MENDES, Gilmar; MARQUES, Claudia Lima, et al. (org.). **Direito privado, Constituição e fronteiras: encontros da Associação Luso-Alemã de Juristas no Brasil**. 2. ed. rev., atual. e ampl. São Paulo: Ed. Revista dos Tribunais, 2014.
- MENDES, Laura Schertel. Proteção de dados para além do consentimento: tendências de materialização. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz; BIONI, Bruno Ricardo (Coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.
- MENEZES, Joyceane Bezerra de; COLAÇO, Hian Silva. Quando a Lei Geral de Proteção de Dados não se aplica? In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais – e suas repercussões no Direito Brasileiro**. 2. Ed. São Paulo: Thomson Reuters Brasil/Revista dos Tribunais, 2020.
- MOLINARO, Carlos Alberto; SARLET, Ingo Wolfgang. Sociedade em rede, internet e estado de vigilância: algumas aproximações. *Revista AJURIS*, v. 40, n. 132, dez. 2012.
- MOREY, Timothy; KRAJECKI, Kristin. *Personalization, Data and Trust: The Role of Brand in a Data-Driven, Personalized, Experience Economy*. Disponível em <https://www.frogdesign.com/design-mind/personalization-data-trust-role-brand-data-driven-personalized-experience-economy>, acesso em 22/12/2020 (originariamente publicado no *Journal of Brand Strategy*, Summer 2016 (V. 5, n. 2, p. 178-185).
- MULHOLLAND, Caitlin. Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018). In: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (Coord.). **Responsabilidade Civil e Novas Tecnologias**. Indaiatuba: Ed. Foco, 2020.
- OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela, Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados – e suas repercussões no Direito Brasileiro**. 2. ed. São Paulo: Ed. Revista dos Tribunais/Thompson Reuters Brasil, 2020.
- PAESANI, Liliana Minardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil**. 4. Ed. São Paulo: Atlas, 2008.
- PASQUALE, Frank. *The black box society: the secret algorithms that control money and information*.

Harvard: Harvard University Press, 2015.

PFEIFFER, Roberto Augusto Castellanos. Digital Economy, Big Data and Competition Law. *Market and Competition Law Review* / volume iii / no. 1 / abril 2019.

RODOTÀ, Stefano. **A vida na sociedade da vigilância** – a privacidade hoje. Organização, seleção e apresentação de Maria C. B. de Moraes. Trad.: Danilo Doneda e Luciana C. Doneda. Rio de Janeiro: Renovar, 2008.

ROSENVOLD, Nelson. Prefácio. In: PINHO, Anna Carolina (Coord.). **Discussões sobre Direito na Era Digital**. Rio de Janeiro: G/Z Editora, 2021.

RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da Lei Geral de proteção de Dados (LGPD) – Lei 13.709/2018. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz; BIONI, Bruno Ricardo (Coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

SARLET, Gabrielle Bezerra Sales; MOLINARO, Carlos Alberto. Questões tecnológicas, éticas e normativas da proteção de dados pessoais na área da saúde em um contexto de *big data*. **Direitos Fundamentais & Justiça**, Porto Alegre, v. 13 (2019).

SCHWAB, Klaus. **A Quarta Revolução Industrial**. Trad. Daniel Moreira Miranda. Bauru/SP: EDIPRO, 2019.

TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. **Pensar**. Fortaleza, v. 22, n. 1, p. 108-146, jan.-abr. 2017.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados** – e suas repercussões no Direito Brasileiro. 2. ed. São Paulo: Ed. Revista dos Tribunais/Thompson Reuters Brasil, 2020.

TERRA, Aline de Miranda Valverde; CASTRO, Diana Paiva de. A responsabilidade do Poder Público no tratamento de dados pessoais: análise dos artigos 31 e 32 da LGPD. In: MULHOLLAND, Caitlin (Org.). **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago Ed., 2020.

THE ECONOMIST. **The world's most valuable resource is no longer oil, but data**. Ed. de 06/05/2017. Disponível em <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em 29.11.20.

TOMASEVICIUS FILHOS, Eduardo. Prefácio. In: PINHO, Anna Carolina (Coord.). **Discussões sobre Direito na Era Digital**. Rio de Janeiro: G/Z Editora, 2021.

UNIÃO EUROPEIA. GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS - Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679, adotadas em 3 de outubro de 2017, com a última redação revista e adotada em 6 de fevereiro de 2018 – Disponível em [https://www.cnpd.pt/home/rgpd/docs/wp260\\_rev01\\_pt.pdf](https://www.cnpd.pt/home/rgpd/docs/wp260_rev01_pt.pdf), acesso em 21/12/2021.

VARON, Joana. Entrevista concedida sobre o tema da Privacidade e dados pessoais, para a Revista **Panorama setorial da Internet**. N. 2, junho 2019, ano 11.

ZUBOFF, Shoshana. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, 4 abr. 2015, p. 75/89, p. 79, disponível em [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2594754](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754) acesso em 20.12.2020.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**. A luta por um futuro humano na nova fronteira do poder. Trad. de George Schlesinger. Rio de Janeiro: Intrínseca, 2020.