Luiza Loureiro Coutinho

Riscos em Sistemas de *Inteligência Artificial*

definição, tipologias, correlações, principiologia, responsabilidade civil e regulação

2024

EDITORA JusPODIVM

www.editorajuspodivm.com.br

Capítulo 2

AS MATRIZES DE RISCO DA INTELIGÊNCIA ARTIFICIAL À LUZ DO MAPEAMENTO DE SUA BASE AXIOLÓGICA

Na Sociedade Informacional, os dados desempenham papel fundamental na tomada de decisões, nos modelos de negócio e na criação de valor. A Internet impulsionou a ascensão da Economia de Dados, do *Big Data* e dos avanços em Inteligência Artificial, que anunciam não só a nova era da computação, mas uma desvalorização profunda de axiomas constitucionais. Outrossim, a IoAI automatizou funções e hoje monitora a vida cotidiana de modo onipresente. Tais ferramentas propiciam mudanças sofisticadas no comportamento individual e coletivo, mormente de grupos vulneráveis e suscetíveis a influências externas, como consumidores e eleitores[1]. Demandam ainda um alto custo social face à erosão da confiança nas instituições democráticas, à falta de controle sobre os próprios dados[2] e à resultante perda de autonomia.

Nos Estados Unidos da América, o centro de pesquisas *Berkman Klein Center for Internet & Society*[3], da Universidade de Harvard, realizou,

1. MANHEIN, Karl M.; KAPLAN, Lyric. Artificial Intelligence: risks to privacy and democracy (October 25, 2018). *21 Yale Journal of Law and Technolog,* v.106 (2019), Loyola Law School, Los Angeles Legal Studies Research Paper n. 2018-37. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3273016. Acesso em: 19.05.2023.

2. "O sucesso das definições de privacidade baseadas no princípio do *control of information about oneself* se explica justamente pelo fato de que elas colocavam em evidência a novidade representada pela atribuição aos interessados de um poder autônomo de controle. De fato, apesar das críticas as quais foram submetidas, são justamente essas definições que correspondem melhor à técnica usada pelas leis sobre proteção de dados, que ofereceram uma versão dinâmica dos poderes de controle sobre as informações através da previsão de um direito de acesso." (RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Maria Celina Bodin de Moraes (org.). Tradução de Danilo Doneda e Luciana Doneda. Rio de Janeiro: Renovar, 2008, p. 46-47).

3. BERKMAN KLEIN CENTER FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY. *Principled Artificial Intelligence*: mapping consensus in ethical and rights-based approaches to principles for AI. Harvard

no início de 2020, o mapeamento de 36 documentos internacionais para verificar o consenso sobre os princípios da Inteligência Artificial. Além de outros interesses setoriais, foi revelado crescente consenso da comunidade internacional a respeito de oito princípios: (i) *accountability*; (ii) privacidade; (iii) segurança e proteção; (iv) transparência e explicabilidade; (v) justiça, equidade e não discriminação; (vi) controle humano das tecnologias de Inteligência Artificial; (vii) responsabilidade profissional; e (viii) promoção de valores humanos frente aos riscos apresentados por sistemas de IA.

Após aludida base axiológica ter sido discutida no Japão pela primeira vez em 2017, durante a *AI Network Society Conference MIC*[4], os tópicos foram levados a debates mais pungentes junto à Comissão Europeia de Princípios da IA, centrados no ser humano e visando um projeto de diretrizes de P&D de IA para discussões internacionais e o *Draft AI Utilization Principles* (em síntese, um rascunho de princípios para o uso desses modelos).

Foi estabelecido, em 2019, pela OCDE um arcabouço principiológico para pesquisa, desenvolvimento, implantação e uso de sistemas de Inteligência Artificial[5]: a) crescimento inclusivo, desenvolvimento sustentável e bem-estar, com alusão à privacidade, à autonomia e à proteção de dados pessoais; b) valores centrados no ser humano, justiça e equidade; c) transparência e explicabilidade; d) proteção, segurança e robustez; d) *accountability*.

Os princípios de Inteligência Artificial, delineados pela OCDE, dedicam-se a como os os agentes de IA devem moldar a abordagem regulatória centrada no ser humano. Percebido o *OECD AI Principles* como instrumento jurídico, os princípios representam aspiração comum dos países aderentes. Além de fixar base axiológica mundialmente replicada, também define orientações para políticas públicas sobre IA, como a continuidade nos investimentos em P&D de aplicações éticas de IA, a promoção de ecossistema digital compatível com seus distintos tipos, a capacitação humana, a transição do mercado de trabalho e a cooperação internacional.

Publications, Ethics and Governance of AI, 2020. Disponível em: https://cyber.harvard.edu/publication/2020/principled-ai. Acesso em: 08.03.2023.

4. ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. Japan's AI Utilization Guidelines: an initiative for implementing the OECD AI Principles. Disponível em: https://oecd.ai/en/wonk/japans-ai-utilization-guidelines-an-initiative-for-implementing-the-oecd-ai-principles. Acesso em: 18.03.2023.

5. ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *OECD AI PRINCIPLES*, 2019. Disponível em: https://oecd.ai/en/ai-principles. Acesso em: 18.03.2023.

> Os princípios são, portanto, normas que atribuem fundamento a outras normas, por indicarem fins a serem promovidos, sem, no entanto, preverem o meio para a sua realização. Eles apresentam (...) alto grau de indeterminação, não no sentido de mera vagueza, (...) mas no sentido específico de não enumerarem exaustivamente os fatos em presença dos quais produzem a consequência jurídica ou de demandarem a concretização por outra norma, de modos diversos e alternativos[6].

Todavia, não basta que sejam positivados os princípios da IA, é preciso concretude para que se transmutem em direitos com máxima exequibilidade por seus titulares, sob pena do agravamento de justificadas inquietações dos especialistas em IA e das implicações lesivas decorrentes do desenvolvimento e uso de modelos de IA na Sociedade da Vigilância. Assim, esforços regulatórios devem ser exercidos para amparar esse sustentáculo principiológico.

São distintas as matrizes de riscos da Inteligência Artificial conforme a tipologia do modelo de IA, as etapas de desenvolvimento e seus níveis de autonomia, entre outros fatores. Em uma abordagem regulatória antropocêntrica, definir a parametrificação axiológica para a P&D de IA é listar, minimamente, os valores a se proteger prioritariamente. Nesse diapasão, suas matrizes de risco devem se alicerçar nesses princípios. Com vistas ao mapeamento do consenso internacional sobre os princípios da IA, corroborado pelo guia orientativo europeu *OCDE Princípios da IA*, serão abordadas, neste capítulo, as matrizes de risco da IA a partir de um estudo pragmático sobre a importância e os perigos da violação desses pilares axiológicos.

Com relação a tipologias de IA, as matrizes de risco devem ser baseadas em diferentes categorias de sistemas de Inteligência Artificial, aspectos já estudados no capítulo precedente. Cada tipo de IA tem suas próprias características e riscos específicos, que, após classificado, permite a identificação e gradação do risco, a ser demonstrado no capítulo subsequente. Desse modo, as matrizes de risco são ferramentas úteis a avaliar os perigos associados aos modelos de IA e garantir que sejam desenvolvidos e usados de maneira ética, confiável e responsável.

Ao apontar ubiquidade, opacidade, poder de persuasão e influência comportamental propiciados por modelos de IA, será este estudo capaz de demonstrar o quão substancial é a calibragem de riscos de sistemas de IA

6. ÁVILA, Humberto. *Teoria dos princípios*: da definição à aplicação dos princípios jurídicos. 18.ed. São Paulo: Malheiros, 2018, p. 155.

segundo um elenco de matrizes centrado na dignidade humana e fixado sob a égide dos princípios da IA reconhecidos internacionalmente, com o fim de regular adequadamente o regime de responsabilidade civil por danos causados pela IA.

Os princípios da Inteligência Artificial são, então, o assentado caminho sobre o qual as matrizes de riscos serão a seguir explanadas de forma ilustrada por diversificados sistemas de IA e suas repercussões jurídicas na sociedade brasileira e na realidade estrangeira, tendo como destino a gradação dos riscos conforme as diferentes tipologias de tecnologias de IA.

2.1 Privacidade: o controle de dados pessoais como forma de exercício de poder sobre o consumidor de produtos e serviços dotados de IA

Sob a perspectiva grega clássica, a concepção de privacidade e intimidade afigurava-se como condição de privação de vida voltada à satisfação de necessidades básicas, desprovida da liberdade política própria de espaços públicos. Tal entendimento diverge, frontalmente, da visão individualista própria da modernidade, como o direito de ser deixado em paz (*the right to be left alone*), liberto de interferências externas em escolhas existenciais[7]. O paradigma do "zero-relacionamento" como noção hodierna de privacidade surge como a quintessência da ausência de comunicação, mantendo a esfera particular do indivíduo em seu pleno gozo[8].

Em verdade, a privacidade molda-se conforme suas bases culturais, sociais e políticas, razão pela qual deve ser compreendida como uma compreensão cultural induzida no tempo e espaço. Nesse sentido, assume contornos variados a depender do dinamismo das experiências normativas em diferentes lugares do mundo, tornando-se conceito ajustável a particularidades de cada ordenamento jurídico. Sob a ótica da legalidade constitucional, visa-se atender tanto ao perfil estrutural (como é) quanto ao funcional (para que serve)[9] dos fenômenos jurídicos.

Essa ideia de privacidade marcou a história da sociedade burguesa estadunidense com a publicação de Samuel Warren e Louis Brandeis inti-

7. DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: fundamentos da Lei Geral de Proteção de Dados. São Paulo: Thomson Reuters, 2020, p. 18. *E-book*.

8. ROBL FILHO, Ilton Norberto. *Direito, intimidade e vida privada*: paradoxos jurídicos e sociais na sociedade pós-moralista e hipermoderna. Curitiba: Juruá, 2010, p. 57.

9. PERLINGIERI, Pietro. *Perfis do Direito Civil*: introdução ao Direito Civil Constitucional. 23.ed. Rio de Janeiro: Renovar, 2002, p. 94.

tulada "The right to privacy", veiculada em 1890 pela *Harvard Law Review*. Apreensivos com os efeitos jurídicos das tecnologias da época – embora limitados se comparados às atuais –, foram pioneiros ao abordar privacidade associada à inviolabilidade da personalidade (*inviolate personality*), referendando precedente judicial do "direito a ser deixado só", trazido pelo magistrado Thomas McIntyre Cooley[10].

Malgrado alçada a privacidade a um prisma de personalização do direito, a matriz da despatrimonialização não estava assentada. O *right to privacy* ainda possuía um componente individualista, não integrado à solidarização, com um forte viés proprietário entre as situações jurídicas patrimoniais. Enquanto dever geral de abstenção ligado à burguesia e ao apogeu do liberalismo clássico – na segunda metade do século XIX –, exsurge como privilégio adquirido por determinado grupo, em oposição a uma demanda natural inerente a cada indivíduo[11].

Somente em meados do século seguinte à publicação de Warren e Brandeis positivou-se a privacidade no art. 8º da Convenção Europeia de Direitos Humanos[12], o qual prevê o direito à vida privada e familiar e o respeito ao asilo inviolável, às correspondências e aos dados pessoais. Por um ângulo mais abrangente, o art. 12 da Declaração Universal de Direitos Humanos[13], proclamada pela Assembleia Geral das Nações Unidas em dezembro de 1948, também resguarda o indivíduo de intervenções arbitrárias em sua privacidade, família, casa e correspondência, além de salvaguardar seu nome, honra e imagem.

---

10. WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*, v.4, n.5, 1890, p. 193-220.

11. DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: fundamentos da Lei Geral de Proteção de Dados. São Paulo: Thomson Reuters, 2020, p. 23. *E-book*.

12. "Artigo 8º (Direito ao respeito pela vida privada e familiar). 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros." (ORGANIZAÇÃO DOS ESTADOS AMERICANOS – OEA. Convenção Europeia de Direitos Humanos. Disponível em: https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=536&lID=4. Acesso em: 21.05.2023).

13. "Artigo 12. Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques." (FUNDO DAS NAÇÕES UNIDAS PARA A INFÂNCIA – UNICEF. Declaração Universal dos Direitos Humanos. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 21.05.2023).

Já em 1960, emergiu inaugural vislumbre da internet por meio de um projeto militar desenvolvido nos Estados Unidos da América. Nas duas décadas seguintes, a internet passou a ser usada em grandes centros de ensino para troca de informações entre seus pesquisadores, via correspondência eletrônica (*e-mail*). E nos anos 1990, a contar do marco inventivo da *World Wide Web* (WWW) por Tim Berners-Lee, os primeiros provedores disponibilizaram acesso à internet para o usuário comum, dando início à difusão de seu uso residencial[14].

Conduzindo no mesmo sentido da conjuntura internacional, a ordem jurídica brasileira consolidou a inviolabilidade da privacidade e da intimidade como um direito fundamental, contemplando-o no inciso X do artigo 5º da Constituição da República de 1988 (CRFB), não sendo considerado um valor meramente individual, mas elemento essencial ao funcionamento do Estado Democrático de Direito e ao livre desenvolvimento da personalidade.

Com o progressivo fluxo informacional na internet, mais traiçoeiros que as formas clássicas de invasão da privacidade, hoje os métodos de intromissão são objeto de controle na palma das mãos dos infratores e sem qualquer conhecimento – e muito menos expresso e prévio consentimento – da pessoa atingida, sendo extraídos seus dados "sem que a lesão cause uma deformidade aparente ou determine um confronto entre o agressor e a vítima"[15].

De acordo com Danilo Doneda, autor-referência sobre privacidade e proteção de dados no Brasil – a quem se presta, aqui, homenagem póstuma – a tecnologia, em confluência com as transformações no tecido social, engendrou o contexto de correlação entre informação pessoal e privacidade. O domínio informacional sempre constituiu elemento de poder no seio da sociedade, entretanto, a intensificação do fluxo de da-

14. "Já na década de 1970, Alvin Tofler apontou o surgimento de uma sociedade derivada da informação, de maneira que a ´sociedade da informação´ seria conduzida por dois relógios, sendo um relógio analógico e outro digital (...) enquanto o relógio analógico é regido pelo ´tempo físico´ – que corresponde às 24 horas do dia e 7 dias por semana e ao nosso cotidiano usual –, o relógio virtual é regido pelo ´tempo virtual´, ou seja, é um tempo que pode ser relativizado, podendo exceder os limites usuais de um dia, já que as ações podem se acumular e se realizar de forma simultânea nesse espaço-tempo (...) a sociedade da informação, que vive no mundo físico e no digital, exige que cada vez mais seus participantes executem mais tarefas, acessem mais informações, rompendo os limites de fusos horários e distâncias físicas; ações que devem ser executadas num tempo paralelo, ou seja, digital." (PINHEIRO, Patrícia Peck. *Direito Digital.* 7.ed. São Paulo: Saraiva Educação, 2021, p. 18. *E-book*).

15. DOTTI, René Ariel. Tutela jurídica da privacidade. In: DOTTI, René Ariel *et al* (org.). *Estudos em homenagem ao professor Washington de Barros Monteiro*. São Paulo: Saraiva, 1982, p. 336.

dos propiciada por Tecnologias da Informação e Comunicação (TICs)[16] e aumento de suas fontes e destinatários, influenciaram quantitativa e qualitativamente as balizas do equilíbrio entre poder, informação e controle[17]. Tal implica em identificar a nova estrutura de poder relativa a essa arquitetura informacional.

Nas últimas décadas, a centralidade da privacidade em pautas jurídicas de interesse social, em especial no universo da hiperexposição, acarretou substanciais alterações em sua concepção. Com efeito, Rodotá questiona se existe espaço para reinvenção afirmativa, ou se uma abordagem defensiva seria a única opção possível e conclui que "os dois objetivos não devem ser separados"[18]. A privacidade não mais se restringe à estrutura "pessoa-informação-segredo", típica do paradigma do *zero relationship*; muito pelo contrário, é verificada a sua reestruturação calcada no eixo "pessoa-informação-circulação-controle".

Para Foucault, em "Vigiar e Punir", são necessários às mutações vários processos que lhe armam uma base, de "modificação no jogo das pressões econômicas, de uma elevação geral do nível de vida, de um vigoroso crescimento demográfico, de uma multiplicação das riquezas e das propriedades e da necessidade de segurança que é uma consequência disso"[19]. A proteção de dados pessoais – cujas raízes se entrelaçam ao direito à privacidade e, em geral, ao fortalecimento dos direitos individuais – estruturou-se, com maior autonomia, quando o processamento de dados passou a representar um fator de risco à sociedade[20]. A privacidade e a tecnologia estabeleceram relação de interdependência ante a aptidão permanente desta de controle,

16. Embora não haja definição universal de Tecnologias da Informação e Comunicação (TICs), o termo tem sido usado para se referir a dispositivos, aplicativos e sistemas que combinados permitem a pessoas e grupos (pessoas jurídicas de direito público ou privado, agências sem fins lucrativos e até organizações criminosas) interagir no mundo digital por meio de uma infraestrutura tecnológica e de seus componentes (acesso à internet, *softwares* e *hardwares*, computação na nuvem, códigos de barra, etc.), que se servem de mecanismos e funcionalidades que otimizam o tratamento dessas informações em diversos segmentos da economia movida a dados.

17. DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: fundamentos da Lei Geral de Proteção de Dados. São Paulo: Thomson Reuters, 2020, p. 26. *E-book*.

18. RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Maria Celina Bodin de Moraes (org.). Tradução de Danilo Doneda e Luciana Doneda. Rio de Janeiro: Renovar, 2008, p. 81.

19. FOUCAULT, Michel. *Vigiar e punir*. Tradução de Raquel Ramalhete. 42.ed. Petrópolis: Ed. Vozes, 2014, p. 72.

20. DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno Ricardo (coord.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021, p. 22.

direto ou indireto, das informações de todos os cidadãos, segundo sustenta Lessig[21].

Um das pioneiras demonstrações legislativas sobre a importância da relação intrínseca entre privacidade e proteção de dados revelou-se na Lei nº 12.965/2014, o Marco Civil da Internet, quando, em seu art. 3º, arrola, no inciso II, entre os princípios da disciplina do uso da internet no Brasil, a proteção da privacidade e, no inciso seguinte, a de dados pessoais, "na forma da lei" (a Lei nº 13.709/2018). Fundou sua base hermenêutica sobre três princípios – neutralidade da rede, privacidade e liberdade de expressão –, representando iniciativa original a regular os conflitos de interesses oriundos da economia de dados. No campo da privacidade, positivou direitos essenciais ao usuário da rede voltados à autodeterminação informativa[22].

O Marco Civil da Internet (MCI) afigura relevante ponto de partida aos debates sobre proteção de dados pessoais no Brasil e, consequentemente, aos primórdios vislumbres sobre regulação da Inteligência Artificial no país. Malgrado não seja especificamente direcionado à regulação da IA, nas disposições preliminares, alguns dos fundamentos (art. 2º), princípios (art. 3º), objetivos (art. 4º), conceitos (art. 5º) e diretrizes devem ser aplicados a tecnologias de IA, garantindo as bases para que seja desenvolvida e usada de forma ética e responsável.

O Parlamento Europeu, ao elucidar sobre os princípios da Inteligência Artificial[23], fez incluir o respeito à privacidade e à integridade dos dados, que podem ser comprometidos pelo uso de sistemas de IA severamente, sendo a prevenção de danos um comando a se seguir. Outrossim, a governança de dados é fundamental à qualidade, adequação e integridade dos dados, que devem ser significativos ao domínio no qual o sistema inteligente será implantado, além de estar disponíveis estritamente a pessoas autorizadas e ser processados atendendo a protocolos específicos de acesso que estabeleçam finalidades e limites precisos ao seu uso.

Consoante à posição consolidada pela Academia de Inteligência Artificial de Pequim (China), sua pesquisa e desenvolvimento, de modo confiável, devem ter como objetivo fulcral servir à humanidade e estar em conformidade com valores fundamentais e interesses sociais. Destarte, a

21. LESSIG, Lawrence. The architecture of privacy. *Vanderbilt Entertainment Law and Practice*. Nashville, v.1, n.1, p.56-65, jan./1999.

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

23. ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *OECD AI PRINCIPLES*, 2019. Disponível em: https://oecd.ai/en/ai-principles. Acesso em: 18.03.2023.

China salvaguarda a dignidade humana e seus consectários, privacidade, liberdade e autonomia durante todo o ciclo de vida da IA e faz crucial que os profissionais envolvidos, nesse ciclo, sejam treinados e incentivados a considerar os impactos sociais e éticos de suas ações, cumprindo diretrizes rigorosas, controladas e centradas na proteção de direitos[24].

À vista da assimetria informacional e de poder entre os titulares de dados pessoais e os agentes de tratamento, apreende-se o deslocamento da inviolabilidade da vida privada rumo à consolidação de um direito fundamental à proteção de dados pessoais e da dimensão coletiva da privacidade[25]. Pasquale[26] leciona que o fenômeno do *one way mirror* é uma das faces do capitalismo movido a dados, eis que um agente sabe tudo sobre o outro e sobre ele o outro nada sabe. Sendo a privacidade e a proteção de dados pessoais direitos fundamentais ligados umbilicalmente, necessitam como base transparência, governança e sindicabilidade de dados.

> Não seria exagero dizer que, na atualidade, todos os aspectos da vida humana, tanto em sua dimensão individual, como em sua dimensão coletiva, são direta ou indiretamente afetados pela coleta e pelo tratamento de dados. Daí a necessidade de um sistema protetivo que, longe de se preocupar apenas com a tutela da privacidade em um sentido mais clássico, vinculado à intimidade, possa compreender a proteção de dados vinculada á autodeterminação informativa e a direitos fundamentais da mais alta importância, tais como a liberdade, a igualdade e a própria cidadania. (...). Logo, longe de se restringir apenas à economia, as discussões sobre o tratamento de dados apresentam importantes consequências também para a política, a sociedade e as próprias dimensões existenciais dos cidadãos, que passam a sofrer riscos cada vez mais graves conforme avança o capitalismo movido a dados[27].

Mais interessantes que os dados de titular único são o volume, a variedade e a massiva coleta permanente de dados de uma vultosa diversidade de

---

24 CORTIZ, Diogo; BURLE, Caroline. *Mapeamento de princípios de inteligência artificial*. São Paulo: Núcleo de Informação e Coordenação do Ponto BR – NIC.BR, 2020, p. 7. Disponível em: https://acervo.ceweb.br/acervos/conteudo/8d5a37ce-dfa2-47c2-90e1-7a008ec9e051. Acesso em: 12.05.2023.

25. KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. *Revisão de decisões automatizadas na Lei Geral de Proteção de Dados Pessoais*. Tese (Doutorado em Direito Civil). Faculdade de Direito da Universidade do Estado do Rio de Janeiro (UERJ). Rio de Janeiro, 2022, p. 49-51.

26. PASQUALE, Frank. *The black box society*: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015, p. 9-10. *E-book*.

27. FRAZÃO, Ana. Propósitos, desafios e parâmetros gerais dos programas de *compliance* e das políticas de proteção de dados. In: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (coord.). *Compliance e políticas de proteção de dados*. São Paulo: Revista dos Tribunais, 2021, p. 34-35. *E-book*.

pessoas que, agrupados, minerados e analisados podem influenciar escolhas e até manobrar a opinião pública, produzindo efeitos desconcertantes ao plano existencial individual e à democracia em geral. Diferente do regime disciplinar, "não são *corpos e energias* que são explorados, mas *informações e dados* (...) em capitalismo de vigilância e degrada seres humanos (...) em *animais de consumo e dados*"[28].

Se os dados movem a economia, o seu controle deve ser enxergado como exercício de poder, mormente sobre os sujeitos de direitos mais vulneráveis nessa dinâmica de forças, os consumidores de produtos e serviços dotados de IA, frente a uma sociedade que traça o seu perfil, conhece os seus anseios e lhe sugere, de modo invisível, comportamentos e ideologias. "*Ser agarrado conceitualmente* pelo que se sobrepõe faz com que este se abra naquele. O poder absoluto não necessita de violência (...) está baseado em uma submissão *livre*"[29].

2.1.1 Modelos de negócios na Sociedade Informacional: uma proposta de privacy by design *para desenvolvimento, implementação e uso de IA*

De acordo com a *Harvard Business Review*, um modelo de negócios pode ser referido como "um termo de arte". Para Michael Lewis, na obra "The New, New Thing", as pessoas sentem que podem reconhecer quando o veem, todavia, não conseguem traçar uma definição. O modelo de negócios voltado à internet atrai milhões de acessos ao conteúdo de um *website* e depois vende a fornecedores e comerciantes a chance de anunciar em suas páginas virtuais. Faz-se, como constata Peter Drucker em sua "teoria do negócio", de 1994, suposições sobre como a empresa é paga, malgrado não tenha mencionado o termo "modelo de negócios"[30].

A nova era digital induz o surgimento de modelos de negócios jamais imaginados na era analógica, tanto em vista dos bens e serviços transacionados (marcadamente os intangíveis e de fácil reprodução) quanto em termos de alcance. Exemplo emblemático de sucesso é o das plataformas digitais, entendidas como modelos de negócio que fornecem meios à interação de, ao menos, dois polos, agregando-os, mantendo-os em contato

28. HAN, Byung-Chul. *Infocracia*: digitalização e a crise da democracia. Tradução de Gabriel Salvi Philipson. Petrópolis – RJ: Editora Vozes, 2022, p. 7.

29. HAN, Byung-Chul. *O que é poder?* Tradução de Gabriel Salvi Philipson. Petrópolis – RJ: Editora Vozes, 2019, p. 118.

30. OVANS, Andrea. *What is a business model?* Harvard Business Review, 2015. Disponível em: https://hbr.org/2015/01/what-is-a-business-model. Acesso em: 21.03.2023.

mútuo e criando *networks* escaláveis e com efeitos de rede, em um ambiente globalizado que demanda hiperconexões.

Ante a disparidade de poder entre os modelos de negócios e seus usuários, o horizonte de incertezas e ignorância digital requer mecanismos mais eficazes de tutela da privacidade. É premente proteger o titular de dados pessoais de pressões indesejadas, interferências externas (e até subliminares) e abusos de direito e poder. O titular de dados pessoais é o protagonista nesse cenário, é ele quem deve conduzir a narrativa da proteção de suas próprias informações.

"O comércio de dados pessoais como modelo de negócios está sendo cada vez mais exportado para (...) [a] sociedade da vigilância[31], ou capitalismo de vigilância"[32], transformando cidadãos em usuários. Num Estado Democrático de Direito, não é aceitável que um sistema econômico seja alicerçado sobre a burla de valores fundamentais, como, por exemplo, o rebaixamento da privacidade do usuário como moeda de troca ao acesso liberado de todas as funcionalidades de um sistema de Inteligência Artificial.

Todavia, a realidade é que, no mundo das *smarthouses* (casas inteligentes), ao acordar, o cidadão desliga o despertador em seu *smartwatch* (relógio inteligente) e verifica as horas. E não apenas elas, mas também batimentos cardíacos, pressão arterial, temperatura corporal, controle de calorias, qualidade do sono (a média de horas dormidas e os índices de sono leve e profundo) e outros dados pessoais de saúde dispostos na base de dados desse único *wearable* (tecnologia vestível)[33]. Após se levantar, pede ao assistente virtual que abra as cortinas, ligue a TV, informe as notícias ou toque uma música, e assim começa o dia do nada *smartperson* (pessoa

---

31. "A técnica digital da informação faz com que a comunicação vire vigilância. Quanto mais geramos dados, quanto mais intensivamente nos comunicamos, mais a vigilância fica eficiente. (...) Paradoxalmente, é o sentimento de liberdade que assegura a dominação (...) *as pessoas estão aprisionadas nas informações* (...). O presídio digital é transparente. A loja modelo da Apple em Nova Iorque é um cubo de vidro." (HAN, Byung-Chul. *Infocracia*: digitalização e a crise da democracia. Tradução de Gabriel Salvi Philipson. Petrópolis – RJ: Editora Vozes, 2022, p. 13-15).

32. VÉLIZ, CARISSA. *Privacidade é poder*: por que e como você deveria retomar o controle de seus dados. Tradução de Samuel Oliveira. 1.ed. São Paulo: Editora Contracorrente, 2021, p. 23.

33. "O *quantified self* também referencia essa crença. O corpo é equipado com sensores que registram dados automaticamente. São medidos a temperatura corporal, os níveis de glicose no sangue, a ingestão e o consumo de calorias, os deslocamentos ou os níveis de gordura corporal. (...) o desempenho e a eficiência (...) [e]stados de ânimo, sensações e atividades cotidianas também são registrados. O desempenho corporal e mental deve ser melhorado através da autoaferição e do autocontrole. (...) O lema do *quantified self* é: *Self knowledge through numbers* (autoconhecimento através dos números)." (HAN, Byung-Chul. *Psicopolítica*: o neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte: Âyiné, 2020, p. 83-84).

inteligente), pois, a cada comando, seus dados foram, contratualmente, coletados[34].

No universo da Internet das Coisas, em tradução do anglicano *Internet of Things* (IoT), bilhões de dispositivos físicos coletam, armazenam e compartilham dados pessoais, através da interação entre objetos cotidianos conectados à internet e equipados com sensores que captam aspectos do mundo real, como temperatura, umidade e movimento, enviando informações a empresas que as mineram e usam em seus modelos de negócios[35]. Passar o aspirador de pó em casa pode repercutir em risco à intimidade, como noticiado pelo jornal *Dailymail*: um robô aspirador *iRobot Roomba* fotografou momentos íntimos de uma mulher enquanto estava no banheiro de sua casa, sem que ela notasse, e as imagens foram compartilhadas nas redes sociais *Discord* e *Facebook*, segundo averiguado pelo *MIT Technology Review*[36].

Outro caso inusitado de captura de imagens privadas envolveu os veículos da marca Tesla com várias câmeras instaladas externamente, que objetivam garantir sua dirigibilidade e autonomia. Todavia, as imagens foram usadas para propósito diverso, tendo seus funcionários compartilhado, via sistema interno de troca de mensagens, vídeos de clientes nus abrindo e fechando seus veículos dentro da garagem interna de suas residências, inclusive de seu CEO, Elon Musk, entre outras capturas de imagens, desde acidentes a cenas da vida privada[37].

Ambas são hipóteses de vazamento de dados pessoais por humanos, porém acessados via aplicações de Inteligência Artificial. Destarte, Rodotà,

---

34. "No presídio digital como zona de bem-estar *smart* não se ergue nenhuma oposição contra o regime dominante. O *Like* exclui toda revolução. (...) O poder disciplinar repressivo dá lugar a um poder *smart*, que não dá ordens, mas *sussurra*, que não comanda, mas *nudge*, (...) *dá um toque* com meios sutis para controlar o comportamento. *Vigiar e punir*, características do regime disciplinar de Foucault, dão lugar a *motivar e otimizar*. (...) Os *followers* participam assim de uma *eucaristia digital*. Mídias sociais se assemelham a uma igreja: *Like é amém. Compartilhar é comunicação. Consumo é redenção.* (...) Consumo e identidade se tornam a mesma coisa. A identidade é, ela própria, uma mercadoria. *Big Data* e inteligência artificial constituem uma *lupa digital* que explora o inconsciente (...). *Mídia é dominação.* (...) *soberano é quem dispõe das informações em rede*." (HAN, Byung-Chul. HAN, BYUNG-CHUL. *Infocracia*: digitalização e a crise da democracia. Tradução de Gabriel Salvi Philipson. Petrópolis – RJ: Editora Vozes, 2022, p. 16-24).

35. MAGRANI, Eduardo. *A internet das coisas*. Rio de Janeiro: FGV Editora, 2018, p. 44.

36. DAILYMAIL. Robot vacuum cleaner took photos of woman on the toilet… and the images ended up being shared on Facebook. Disponível em: https://www.dailymail.co.uk/news/article-11562599/Robot-vacuum-cleaner-took-photos-woman-toilet-images-ended-Facebook.html. Acesso em: 26.05.2023.

37. THE TELEGRAPH. Tesla workers shared footage of naked customers taken from vehicles' cameras. Disponível em: https://www.telegraph.co.uk/world-news/2023/04/06/tesla-elon-musk-workers-videos-naked-customers/. Acesso em: 26.05.2023.

ao tracejar "o primeiro paradoxo da privacidade", assevera que "a tecnologia ajuda a moldar uma esfera privada mais rica, porém mais frágil, cada vez mais exposta a ameaças: daí deriva a necessidade do fortalecimento contínuo de sua proteção jurídica, da ampliação das fronteiras do direito à privacidade"[38].

> Lawrence Lessig faz uma comparação (...) em seu artigo "Privacy as property", publicado em 2002 (...) a Amazon mudou, no ano 2000, sua política de privacidade, de modo que os dados pessoais dos usuários, que não seriam cedidos a terceiro até então, poderiam passar a sê-lo – inclusive com efeito retroativo. Em sua defesa, a Amazon alegou que estava escrito na política de privacidade que ela poderia ser alterada a qualquer momento. Assim foi feito, e os consumidores estavam avisados. Então, Lessig compara essa situação à seguinte hipótese: imagina que você tenha deixado seu carro estacionado em um *shopping center* e recebeu um comprovante do estacionamento, (...) [com] as garantias e as limitações de responsabilidade estabelecidas pela empresa (...) [e] ressalva idêntica àquela da Amazon: "A política de uso do *shopping* pode ser alterada a qualquer tempo". Assim, ao voltar para buscar seu carro, e sendo incapaz de encontrá-lo, você é informado pelo funcionário do *shopping center* que, enquanto fazia compras, a política de uso do estacionamento havia de fato sido alterada (...) o administrador do estacionamento passava a ter o direito de vender o carro a terceiros, e essa era a razão por que ele não estava mais lá. Embora absurda, a história ilustra de modo claro como acabamos nos preocupando menos com nossos bens imateriais do que com os físicos[39].

Adicionalmente, Carissa Véliz alerta, na obra "Privacidade é poder", sobre os *cookies* sonoros, que permitem aos dispositivos instalados em

---

38. Rodotá afirma a existência de três paradoxos da privacidade – o primeiro no qual a esfera privada se enriquece com as novas tecnologias, mas que também a colocam em risco; o segundo no qual são categorizados certos dados pessoais como sensíveis, todavia sem natural vocação ao sigilo; e o terceiro no qual aponta a incongruência entre o simultâneo fomento ao desenvolvimento de leis para a tutela de dados pessoais e a difusão de leis sobre o acesso à informação. Identifica ainda o autor a existência de quatro tendências ao ambiente no qual se opera a noção de privacidade, sintetizando-as da seguinte forma: 1ª) do direito a ser deixado só ao de manter controle sobre os próprios dados pessoais; 2ª) da tutela da privacidade ao direito à autodeterminação informativa; 3ª) da privacidade a não discriminação; 4ª) do sigilo ao controle das informações que lhe digam respeito. (RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Maria Celina Bodin de Moraes (org.). Tradução de Danilo Doneda e Luciana Doneda. Rio de Janeiro: Renovar, 2008, p. 95-98).

39. LEMOS, Ronaldo; BRANCO, Sérgio. *Privacy by design*: conceito, fundamentos e aplicabilidade na LGPD. In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno Ricardo (coord.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021, p. 447-458.

celulares – em especial aqueles que, por desatenção do usuário, sejam mantidos com a regra de configuração-padrão de rastreamento por localização ativado – o cruzamento de dados sobre hábitos de consumo, opiniões e rotina do usuário. "O dia inteiro você foi rastreado pelos (...) serviços de localização disponíveis para que possa receber notícias locais, o clima local ou outras informações semelhantes (...). A publicidade baseada em localização é um negócio estimado em US$ 21 bilhões"[40].

Os *cookies*[41], como regulados no Brasil, sem impor aos sites ter que fornecer a opção aos titulares de dados de pronta recusa à sua captação, infringem o sétimo fundamento de *privacy by design*. Ensina Ann Cavoukian sobre a centralização regulatória da privacidade em confidencialidade, integridade e segurança dos dados pessoais em garantia de seus titulares, cabendo aos desenvolvedores oferecerem aos usuários, prioritariamente, opções amigáveis de configurações dos *cookies*, por serem notórias ferramentas que auxiliam na formação do perfil psicográfico do usuário a partir da coleta e do processamento de seus dados de navegação.

Na sociedade capitalista nada é verdadeiramente gratuito. No regime do Capitalismo de Vigilância[42], numa economia movida a dados, a afirmação de gratuidade de determinados modelos de negócios é inegavelmente enganosa, frente ao pagamento indireto efetuado pelo titular ao conceder, às vezes voluntariamente, o acesso aos seus dados pessoais para obter, em contrapartida, produto ou serviço, sob pena de, havendo recusa, ser digitalmente excluído[43]. Até que ponto é juridicamente livre a emissão

40. VÉLIZ, CARISSA. *Privacidade é poder*: por que e como você deveria retomar o controle de seus dados. Tradução de Samuel Oliveira. 1.ed. São Paulo: Editora Contracorrente, 2021, p. 43-44.

41. "*Cookies* são arquivos criados por *sites* que você acessa [que] salvam informações de navegação para facilitar sua experiência *online*. Com os *cookies*, os sites podem manter seu *login*, lembrar suas preferências do *site* e fornecer conteúdo relevante localmente. Há dois tipos de *cookies*: *cookies* primários: criados pelo site que você acessa [e o] site é mostrado na barra de endereços; *cookies* de terceiros: criados por outros sites que têm uma parte do conteúdo mostrado na página, como anúncios ou imagens." Ajustando as configurações do Chrome às exigências do usuário, é possível bloquear todos os *cookies*, apenas os *cookies* de um site específico ou excluir os *cookies* sempre logo após fechar o Chrome. (GOOGLE CHROME. Central de ajuda: remover, permitir e gerenciar *cookies* no Chrome. Disponível em: https://support.google.com/chrome/answer/95647?hl=pt-BR&co=GENIE.Platform%3DDesktop. Acesso em: 27.05.2023).

42. Shoshana Zuboff, sobre as implicações das Tecnologias da Informação e da Comunicação (TICs) na era do Capitalismo de Vigilância, delineia três leis: (i) tudo o que pode ser automatizado será automatizado; (ii) tudo o que pode ser informatizado será informatizado; (iii) todos os aplicativos digitais que puderem ser usados para vigilância e controle serão usados para tais fins. (ZUBOFF, Shoshana. *The age of surveillance capitalism*: the fight for a human future at the new frontier of power. New York: Publicaffairs, 2019. *E-book*).

43. UNIVERSITY OF SOUTHERN CALIFORNIA. USC NEWS. 'Free' apps may not be so free after all: they take a big toll on your phone. Disponível em: https://news.usc.edu/79081/beware-of-an-ads-hidden-cost-

de vontade do titular de dados pessoais quando não estiver plenamente informado sobre a tipologia da IA com a qual se depara e seus riscos?

Nick Srnicek[44], ao estudar a *data driven economy*, cunhou a expressão "Capitalismo de Plataforma", em sua obra homônima, cujo desenrolar se compromete a demonstrar como emergiram os correntes modelos de negócios marcados pela exploração de dados pessoais dos usuários disponíveis em plataformas digitais e seus desdobramentos microeconômicos, além de discutir as projeções da dinâmica plataformizada. O Capitalismo de Plataforma centra-se em modelos de negócio que exploram grandes conjuntos de dados pessoais, gerando poder informacional e econômico àquelas empresas que detêm maior variedade e volume de dados.

Do reconhecimento do regime jurídico de bancos de dados, cadastros de consumidores e congêneres como de caráter público[45] até as aprimoradas técnicas de mineração de textos e dados[46], novas dimensões da privacidade necessitaram ser reavaliadas ante o novo cenário de riscos e danos no Capitalismo de Plataforma. A fusão e a mineração lhes conferem real poder! "Enquanto isolados, os conjuntos de dados individuais dispersos na rede em milhares de servidores podem fornecer *insights* limitados de informações, mas tal limitação pode ser resolvida por um processo de fusão de dados, que mescla, analisa, organiza e correlaciona"[47].

Algoritmos de perfilização analisam dados para criar perfis que direcionam conteúdo personalizado ao usuário. Assim, as plataformas exibem anúncios, recomendam conteúdo, sugerem conexões com outras pessoas e manipulam o *feed* do usuário. Quanto mais dados são compartilhados, mais detalhado o *profiling* é e também o seu poder de assédio e manipulação.

---

s-in-free-mobile-apps/. Acesso em: 26.05.2023.

44. SRNICEK, Nick. *Platform capitalism*. Cambridge: Polity Press, 2017, p. 39.

45. Veja o disposto na Lei nº 8.078/1990 (CDC), Art. 43. (...). "§4°. Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público."

46. Sobre a mineração de dados, veja o art. 4º, VIII, do PL nº 2.338/2023 (BRASIL. SENADO FEDERAL. Projeto de Lei nº 2.338, de 2023. Atividade Legislativa, 2023. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233?_gl=1*1qw7sar*_ga*ODQ3Nzg0NDY2LjE2MjQ2M-zc4Mzg.*_ga_CW3ZH25XMK*MTY4NDE2Mjk0My4yLjAuMTY4NDE2Mjk0My4wLjAuMA. Acesso em: 28.05.2023).

47. MARRAFON, Marco Aurélio; COUTINHO, Luiza Leite Cabral Loureiro. Princípio da privacidade por *design*: fundamentos e efetividade regulatória na garantia do direito à proteção de dados. *Revista Eletrônica Direito e Política*, Programa de Pós-Graduação *Stricto Sensu* em Ciência Jurídica da UNIVALI, Itajaí, v.15, n.3, 3º quadrimestre de 2020.

> As plataformas foram adquirindo relevância conforme a internet se popularizava, principalmente a partir dos anos 2000 (...) com a explosão do compartilhamento nas chamadas redes P2P (*peer-to-peer*). O sucesso da cultura do compartilhamento foi reconhecido pelo mercado que buscou operar a capitalização desse modelo. (...) Em 2003 é lançado o LinkedIn. Em 2004, o Orkut é inaugurado em janeiro e o Facebook em fevereiro. O Youtube foi criado em 2005 e o Twitter nasceu em 2006. O êxito dessas plataformas incentivou a proliferação de modelos de negócios baseados na intermediação entre ofertantes e demandantes de serviços e mercadorias. O Airbnb surgiu em 2008 e o Uber no ano seguinte. (...) Em outubro de 2008 o Spotify inicia (...). Em 2011, o Netflix já contava com 23 milhões de assinantes apenas nos Estados Unidos. O Instagram começa a operar em 2010 e é adquirido pelo Facebook em 2012. O Waze é lançado em 2008 e adquirido pelo Google em 2013[48].

Reconhece-se que as concepções de privacidade têm sido diariamente – sem hipérbole na expressão – vilipendiadas. A privacidade informacional (*informational privacy*)[49] abarca o direito ao autodomínio sobre o fluxo dos próprios dados, aplicando-se de modo equânime tanto às informações de foro íntimo como às que compartilhamos com outros em confiança. A privacidade decisória (*decisional privacy*), por sua vez, consubstancia o direito de empreender livres escolhas e deliberar sobre elas sem devassa, interferência, intromissão e/ou escrutínio alheio. Já a comportamental (*behavioral privacy*) engendra ser possível agir em consonância com a própria vontade, inteiramente liberto de observações indesejadas e da ingerência de terceiros. A física (*physical privacy*), por fim, abrange um escopo mais amplo, incorporando o direito ao esquecimento e a proteção jurídica contra mandado ilegal de busca e apreensão[50].

Devem ser cegamente confiáveis os supostos propósitos legítimos e os fins informados sobre o tratamento de dados pessoais de bilhões de

48. SOUZA, Joyce; AVELINO, Rodolfo; SILVEIRA, Sérgio Amadeu (Org.). *A sociedade de controle*: manipulação e modulação nas redes digitais. São Paulo: Hedra, 2018, p. 32-33.

49. Segundo o cofundador do *Data Privacy Brasil*, Dr. Bruno Ricardo Bioni, se, por um lado, a tecnologia pode ser invasiva à privacidade informacional, por outro "pode ser uma ferramenta para a proteção dos dados pessoais, tal como propõem as denominadas *Privacy Enhancing Technologies* (PETs)", cuja compreensão como tecnologias que reforçam a privacidade denota a grande abrangência de "guarda-chuva" da terminologia, sendo capaz de abarcar toda tecnologia amigável à e promotora da privacidade. (BIONI, Bruno Ricardo. *Proteção de dados pessoais*. Rio de Janeiro: Forense, 2020, p. 176. *E-book*).

50. CASTELLITTO, Anita L. Allen. *Understanding privacy*: the basics. Disponível em: https://www.law.upenn.edu/cf/faculty/aallen/workingpapers/pli2007.pdf. Acesso em: 26.05.2023.