

DADOS MÉDICOS E BIOMÉDICOS NO CAPITALISMO DE VIGILÂNCIA: ALERTAS DO PASSADO, NOVOS RISCOS E DESAFIOS DA PROTEÇÃO DE DADOS SENSÍVEIS

RECEBIDO EM:	17.5.2026
APROVADO EM:	1º.7.2026

Irene Nohara

 <https://orcid.org/0000-0003-4465-5802>
Universidade Presbiteriana Mackenzie, São Paulo
São Paulo, SP, Brasil
E-mail: irene.nohara@uol.com.br

Joseph Rodrigo Amorim Picazio

 <https://orcid.org/0000-0002-6948-239X>
Universidade Presbiteriana Mackenzie, São Paulo
São Paulo, SP, Brasil
E-mail: josephamorim16@gmail.com

Silvio Gabriel Serrano Nunes

 <https://orcid.org/0000-0001-5565-0965>
Universidade Santo Amaro, São Paulo
São Paulo, SP, Brasil
E-mail: serrano.nunes@gmail.com



- IRENE NOHARA
- JOSEPH RODRIGO AMORIM PICAZIO
- SILVIO GABRIEL SERRANO NUNES

Para citar este artigo: NOHARA, I.; PICAZIO, J. R. A.; NUNES, S. G. S. Dados médicos e bio-médicos no capitalismo de vigilância: alertas do passado, novos riscos e desafios da proteção de dados sensíveis. *Revista Direito Mackenzie*, São Paulo, SP, v. 20, n. 2, e18716, 2026. <http://dx.doi.org/10.5935/2317-2622/direito-mackenzie.v20n218716>.

- **RESUMO:** O artigo tem por objeto examinar a coleta e o tratamento de dados médicos e biomédicos no contexto do capitalismo de vigilância. Objetiva-se abordar a proteção da privacidade de dados sensíveis em saúde, considerando os novos riscos decorrentes da circulação econômica e tecnológica desses dados. O estudo problematiza os limites da autodeterminação informativa e do consentimento do paciente diante da assimetria de poder existente. A pesquisa adota metodologia de análise qualitativa, de caráter jurídico-dogmático e crítico, com foco na LGPD, nas regulamentações do CFM e no levantamento de casos concretos de vazamento de dados. Aborda-se o sigilo profissional, a autonomia do paciente e a confiança necessária à prática médica, buscando-se extrair aprendizados da experiência totalitária, na qual a medicina foi instrumentalizada para fins políticos e ideológicos. Como resultado, conclui-se pela necessidade de governança de dados que equilibre inovação tecnológica com tutela de direitos individuais, agregando rastreabilidade e prestação de contas.
- **PALAVRAS-CHAVE:** Capitalismo de vigilância; proteção de dados; dados médicos.

MEDICAL AND BIOMEDICAL DATA IN SURVEILLANCE CAPITALISM: WARNINGS FROM THE PAST, NEW RISKS, AND CHALLENGES FOR THE PROTECTION OF SENSITIVE DATA

- **ABSTRACT:** The article aims to examine the collection and processing of medical and biomedical data in the context of surveillance capitalism. It seeks to address the protection of privacy regarding sensitive health data, considering the new risks arising from the economic and technological circulation of such data. The study problematizes the limits of informational self-determination and patient consent in light of existing power asymmetries. The research adopts a qualitative, legal-dogmatic, and critical analytical methodology, focusing on the Brazilian General Data Protection Law (LGPD), the regulations of the Federal Council of Medicine (CFM), and the survey of concrete cases of data breaches.



It addresses professional confidentiality, patient autonomy, and the trust required for medical practice, seeking to draw lessons from the totalitarian experience, in which medicine was instrumentalized for political and ideological purposes. As a result, it concludes that data governance is needed to balance technological innovation with the protection of individual rights, incorporating traceability and accountability.

■ **KEYWORDS:** Surveillance capitalism; data protection; medical data.

1. Introdução

A era digital inaugurou um novo paradigma de relações sociais e econômicas, marcado pela ubiquidade da tecnologia e pela crescente digitalização da vida cotidiana. Nesse contexto, a coleta, o armazenamento e o processamento de dados em massa tornaram-se elementos centrais da sociedade, impactando diversos aspectos da vida humana, desde as relações interpessoais até os modelos de negócios. Em particular, a área da saúde experimenta uma profunda transformação impulsionada pela tecnologia, com a digitalização de prontuários, o desenvolvimento de aplicativos médicos, o uso de inteligência artificial no diagnóstico e no tratamento de doenças e a crescente coleta de dados médicos e biomédicos por diversos atores, o que gera novos riscos.

Nesse ambiente, emerge o que Shoshana Zuboff denominou de “capitalismo de vigilância”, considerado um modelo de negócios que se alimenta da coleta massiva de dados, da análise preditiva e da monetização da atenção humana (Zuboff, 2019, p. 18). Os dados pessoais, inclusive aqueles relativos à saúde, são transformados em matéria-prima para a criação de perfis individuais, a predição de comportamentos e a influência de decisões. Essa lógica mercantil, aplicada aos dados médicos e biomédicos, gera uma série de preocupações éticas e jurídicas, especialmente no que tange à privacidade, à autonomia e à dignidade das pessoas.

Um dos principais desafios na era do capitalismo de vigilância é garantir a autodeterminação informativa dos indivíduos, ou seja, o direito de controlar o uso dos próprios dados pessoais. No contexto da saúde, a autodeterminação informativa reveste-se de especial importância, uma vez que os dados médicos e biomédicos revelam informações íntimas e sensíveis sobre a saúde física e mental das pessoas, com potencial para gerar discriminação, estigmatização e violação de direitos.



- IRENE NOHARA
- JOSEPH RODRIGO AMORIM PICAZIO
- SILVIO GABRIEL SERRANO NUNES

A tecnologia deixou de ser mero instrumento auxiliar das relações humanas para se converter em infraestrutura permanente de mediação da experiência cotidiana, sendo os dados pessoais transformados em insumo estratégico para a organização de serviços, para a definição de modelos de negócios, formulação de políticas públicas e construção de perfis comportamentais. Assim, a circulação massiva de informações, impulsionada por plataformas digitais, sistemas algorítmicos, inteligência artificial e dispositivos conectados, ampliou significativamente os riscos relacionados à privacidade, à autonomia individual, à discriminação e ao controle social, provocando novos riscos.

No campo da saúde, a transformação assume contornos especialmente sensíveis. A digitalização de prontuários médicos, a expansão da telemedicina, o crescimento de aplicativos de saúde, o uso de inteligência artificial em diagnósticos e tratamentos, a coleta de dados por novos dispositivos e a utilização de informações genéticas e biométricas revelam ambiente de crescente produção e circulação de dados médicos e biomédicos. Tais dados não dizem respeito apenas a aspectos cadastrais dos indivíduos, mas alcançam dimensões profundamente íntimas da pessoa humana. Por essa razão, sua apropriação e exploração econômica suscitam preocupações éticas.

A saúde, nesse ambiente, deixa de ser apenas a esfera de cuidado e proteção para se converter também em campo de extração informacional, classificação de riscos, direcionamento de produtos, diferenciação de consumidores e produção de assimetrias. A utilização econômica de dados de saúde desafia diretamente à autodeterminação informativa, compreendida como a possibilidade de o indivíduo conhecer, controlar e limitar o uso de suas próprias informações pessoais.

Conforme será abordado, em face da problematização, embora a proteção de dados tenha se desenvolvido em torno da ideia de consentimento, a realidade das relações em saúde revela que a manifestação formal de vontade, em face da vulnerabilidade, dependência técnica e necessidade concreta de acesso a serviços essenciais, não se estabelece, na prática, em condições ideais de autonomia/liberdade. O consentimento acaba sendo uma autorização meramente formal, praticamente obrigatória para se obter o almejado serviço ou tratamento, realizada em face de documentos extensos, linguagem técnica, urgência clínica ou mesmo da impossibilidade prática de recusa.

A limitação do consentimento é ainda mais evidente quando se considera a complexidade das relações entre seus atores, sejam eles hospitais, clínicas, laboratórios, públicos ou privados, operadoras de planos de saúde, seguradoras, empresas



farmacêuticas, plataformas digitais, desenvolvedores de aplicativos, pertencentes a uma cadeia de tratamento de dados médicos e biomédicos.

O ordenamento jurídico brasileiro reconhece especial relevância aos dados sensíveis por meio da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018. A LGPD estabelece parâmetros para o tratamento de dados pessoais e confere atenção diferenciada às informações relacionadas à saúde, devendo ser complementadas na sua aplicação com as normas editadas pelo Conselho Federal de Medicina, especialmente no que se refere aos deveres éticos decorrentes da relação médico-paciente. Trata-se de relação de confiança estruturada. Entretanto, a existência de normas jurídicas e deontológicas não elimina, por si só, os riscos produzidos por práticas sociais e econômicas orientadas pela maximização da extração de dados. Será defendida, então, como objetivo da presente reflexão, a necessidade de aprofundamento de uma governança de dados, que garanta melhor fiscalização, educação institucional e cultura de responsabilidade.

A notificação compulsória de doenças desempenha papel crucial na saúde pública, possibilitando a rápida identificação e contenção de surtos epidemiológicos. Esse sistema obriga profissionais de saúde a reportar casos específicos de enfermidades às autoridades sanitárias, permitindo medidas preventivas e de controle. Conceitualmente, tal prática é considerada uma legítima quebra do sigilo médico em nome do interesse público. No entanto, a forma como as informações são utilizadas pode levantar questões éticas e históricas delicadas.

A experiência do nazismo, conforme será analisado, constitui alerta extremo sobre a instrumentalização da medicina e dos dados de saúde para fins políticos, ideológicos e eugenistas, dada utilização de notificações compulsórias, registros médicos e classificações biomédicas em políticas de esterilização forçada e extermínio sistemático de pessoas tidas por deficientes, o que demonstra que dados de saúde, quando deslocados para uma lógica de controle, podem alimentar engrenagens de desumanização. O passado revela que a circulação de informações biomédicas não é neutra e que sua utilização depende das estruturas institucionais, políticas e econômicas em que se insere, sendo levantado alertas de Harari (2018, p. 94) sobre o maior potencial atual de riscos decorrentes da circulação atual.

A memória histórica objetiva advertir que a coleta de informações sensíveis exige limites, justificativas, mecanismos de controle das finalidades do uso e responsabilidade institucional. Diante do exposto, o presente artigo examina a coleta e o tratamento de dados médicos e biomédicos no contexto do capitalismo de vigilância, situando



- IRENE NOHARA
- JOSEPH RODRIGO AMORIM PICAZIO
- SILVIO GABRIEL SERRANO NUNES

o problema sob a perspectiva dos limites jurídicos ao poder econômico no manejo da tecnologia. Parte-se da hipótese de que os dados sensíveis em saúde, em razão de seu valor preditivo e de sua capacidade de revelar vulnerabilidades individuais e coletivas, tornaram-se objeto de crescente disputa, especialmente quando a proteção formal do consentimento se mostra insuficiente para enfrentar relações marcadas por dependência, opacidade técnica e concentração de poder informacional.

Assim, serão desdobrados os seguintes assuntos nas partes do artigo: natureza e sensibilidade dos dados médicos e biomédicos em face do capitalismo de vigilância e seus impactos na saúde; a advertência histórica com base no uso distorcido dos dados, o que levanta riscos no seu compartilhamento; a assimetria informacional existente no consentimento; a autodeterminação informativa na relação médico-paciente; e os riscos de vazamento, sendo então levantados os desafios para o desenvolvimento de uma governança de dados.

Metodologicamente, o estudo adota abordagem qualitativa, de caráter jurídico-dogmático e crítico. A análise parte do exame da legislação brasileira de proteção de dados, com especial atenção à LGPD, e dos atos normativos editados pelo Conselho Federal de Medicina (CFM). Também serão considerados casos concretos de vazamento e uso indevido de dados em saúde, a fim de demonstrar os riscos analisados. A pesquisa mobiliza a reflexão histórico-crítica sobre experiências totalitárias, com o propósito de iluminar a importância da confiança, da responsabilidade e dos limites ético-jurídicos no tratamento de informações biomédicas.

Ao final, pretende-se, como resultado, reforçar a importância do desenvolvimento de uma governança de dados capaz de equilibrar inovação tecnológica e tutela de direitos fundamentais, mediante mecanismos de rastreabilidade, responsabilização, transparência e prestação de contas, como contribuição para o enfrentamento de novos riscos e os desafios na proteção dos dados médicos e biomédicos.

2. A natureza e a sensibilidade dos dados médicos e biomédicos

Os dados médicos e biomédicos abrangem ampla gama de informações sobre a saúde do indivíduo, desde seu histórico clínico e resultados de exames até seus dados genéticos e imagens médicas. A Lei Geral de Proteção de Dados Pessoais (LGPD), em seu art. 5º, inciso II, define dados sensíveis como aqueles “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” (Brasil, 2018).

A sensibilidade dos dados reside no fato de que revelam informações íntimas sobre o indivíduo, podendo ser utilizados para discriminação, estigmatização e violação de direitos. No contexto do capitalismo de vigilância, a coleta e o uso indiscriminado desses dados podem comprometer a autonomia e a dignidade da pessoa humana, além de gerar riscos à sua saúde física e mental.

É importante destacar que, embora o tema “dados médicos e biomédicos”, do ponto de vista jurídico, possa, à primeira vista, sugerir complementaridade entre medicina e biomedicina, tais áreas, enquanto profissões, são diferentes. Todavia, esta pesquisa jurídica busca analisar a importância dos dados gerados por esses ramos, motivo pelo qual não se adentrará ao cerne da profissão, mas sim à questão da coleta e utilização dos dados relativos à saúde humana e na relação médico-paciente. Assim, é crucial compreender algumas nuances quanto à distinção e origem dos dados.

A distinção entre dados médicos e biomédicos reside principalmente na natureza e na finalidade da coleta. Dados médicos são aqueles obtidos diretamente do paciente durante o atendimento, como histórico clínico, sintomas, exames físicos e resultados de procedimentos diagnósticos. Já os biomédicos, embora também estejam relacionados à saúde humana, são gerados a partir da análise de material biológico em laboratório, como sangue, tecidos e fluidos corporais, visando pesquisas, diagnósticos e ao desenvolvimento de novas tecnologias e tratamentos.

A diferença é crucial para a compreensão da aplicação da LGPD e de normas do Conselho Federal de Medicina (CFM), pois afeta o tipo de consentimento necessário e as responsabilidades de cada profissional. Conforme o histórico estabelecido pelo Conselho Federal de Biomedicina (CFBM), a Biomedicina surgiu com um papel voltado à pesquisa científica e ao desenvolvimento nas ciências básicas e aplicadas à saúde, enquanto a Medicina tem seu foco histórico e normativo na assistência direta, diagnóstico e tratamento clínico. Enquanto o médico lida com dados médicos sensíveis no contexto clínico, o biomédico trabalha com dados biomédicos que, embora possam ser rastreados até um indivíduo, são utilizados primariamente para fins científicos e tecnológicos.

De forma objetiva, dados médicos constituem informações sobre a saúde de determinado paciente, enquanto dados biomédicos são informações coletadas a partir de seres vivos, como seres humanos, animais, plantas e microrganismos, para fins de

- IRENE NOHARA
- JOSEPH RODRIGO AMORIM PICAZIO
- SILVIO GABRIEL SERRANO NUNES

pesquisa, diagnóstico e tratamento médico. Eles podem incluir uma variedade de informações, desde as mais básicas até as mais complexas, como: *informações demográficas*: localização geográfica, etnia, idade, sexo; *histórico médico*: doenças preexistentes, alergias, medicações, cirurgias, vacinação; resultados de exames: exames de sangue, biópsias, testes genéticos; *sinais vitais*: temperatura corporal, pressão arterial, frequência cardíaca, frequência respiratória; *dados genéticos*: sequenciamento de DNA, informações sobre genes e cromossomos; *imagens médicas*: raio-x, tomografias computadorizadas, ressonâncias magnéticas, ultrassonografias; *dados de dispositivos médicos*: leituras de monitores cardíacos, dados de bombas de insulina, informações de marca-passos; entre outros.

A utilização pode ter fins variados, a exemplo de: *pesquisa médica*: para entender doenças, desenvolver novos tratamentos e medicamentos; *diagnóstico médico*: para auxiliar no diagnóstico de doenças e condições médicas; *tratamento médico*: para personalizar o tratamento de acordo com as necessidades individuais do paciente; *saúde pública*: para monitorar a saúde da população e prevenir surtos de doenças; e *desenvolvimento de tecnologias médicas*: para conceber novas tecnologias e dispositivos médicos.

No contexto do capitalismo de vigilância, a utilização de dados médicos e biomédicos para fins que vão além do cuidado com a saúde do paciente levanta diversas preocupações. Zuboff (2019, p. 612) descreve o sistema como uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita utilizada para práticas comerciais originadas da extração, previsão e vendas. Trata-se de matéria-prima que também pode se direcionar aos dados sensíveis sobre saúde, que tem potencial de serem explorados de maneiras prejudiciais aos indivíduos.

A crescente utilização de dados médicos e biomédicos levanta específicas preocupações sobre a privacidade e a autonomia dos indivíduos. Um dos problemas é a discriminação, seja ela social ou algorítmica, em que empresas podem usar dados de saúde para negar empregos, seguros ou empréstimos (Zuboff, 2019, p. 345). Outro problema é a negação de serviços, com planos de saúde aumentando preços ou negando cobertura com base em dados sensíveis, mesmo com a LGPD proibindo tal prática (Doneda, 2021, p. 154).

A manipulação e influência também são preocupantes, com dados biomédicos sendo usados para influenciar escolhas de estilo de vida e até decisões políticas (Zuboff, 2019, p. 448). Governos e empresas podem usar dados para monitoramento e controle, invadindo a privacidade e restringindo liberdades (Molinari; Sarlet, 2013). Por fim, a exploração comercial de dados médicos e biomédicos por empresas visa ao lucro com a venda dessas informações (Zuboff, 2019, p. 213).



3. Capitalismo de vigilância e impactos na saúde

O capitalismo de vigilância, cunhado por Shoshana Zuboff (2019), descreve um novo modelo econômico que se alimenta da coleta massiva de dados, da análise preditiva e da monetização da atenção humana. As empresas de tecnologia, e as que usam seus serviços, por meio de plataformas digitais e dispositivos conectados, coletam informações sobre as atividades dos usuários, preferências, emoções e interações sociais, construindo perfis detalhados utilizados para fins comerciais e políticos.

Zuboff (2019, p. 23) define o capitalismo de vigilância como “uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais ocultas de extração, previsão e vendas”. Essa matéria-prima é extraída de maneira contínua e sistemática, sem o conhecimento ou consentimento explícito dos indivíduos, configurando forma de “vigilância oculta”.

As implicações do capitalismo de vigilância são profundas e multifacetadas. A erosão da privacidade, a manipulação comportamental, a polarização política e a discriminação algorítmica são apenas alguns dos problemas que emergem nesse contexto. A vigilância constante e a perda de controle sobre os próprios dados geram sentimento de vulnerabilidade e incerteza, afetando na autodeterminação e no livre desenvolvimento da personalidade. O capitalismo de vigilância torna-se ainda mais preocupante e desafiador quando ultrapassa limites éticos e normativos relacionados a dados sensíveis, como os de saúde. Empresas que comercializam esses dados coletam informações sobre preferências, emoções, interações sociais e hábitos de consumo, construindo perfis detalhados utilizados para fins comerciais e políticos.

Dispositivos conectados coletam informações sobre nossas atividades *on-line*, preferências, emoções e interações sociais. As principais características do capitalismo de vigilância são: *coleta massiva de dados*: coleta indiscriminada de informações sobre os indivíduos, abrangendo dados de navegação, localização, interações sociais, hábitos de consumo, entre outros; *monitoramento constante*: rastreamento contínuo das atividades dos indivíduos, tanto no mundo *on-line* quanto *off-line*, por meio de diversas tecnologias, como *cookies*, rastreadores, reconhecimento facial e dispositivos inteligentes; *análise preditiva*: uso de algoritmos para analisar os dados coletados e prever o comportamento dos indivíduos, com o objetivo de personalizar a experiência do usuário, direcionar publicidade e influenciar decisões; e *monetização da informação*: transformação

- IRENE NOHARA
- JOSEPH RODRIGO AMORIM PICAZIO
- SILVIO GABRIEL SERRANO NUNES

dos dados em produto, vendidos para anunciantes, empresas de *marketing* e outros atores interessados em explorar o valor comercial da informação.

Nos últimos anos, o capitalismo de vigilância se expandiu para além do mundo *on-line*, com a proliferação de dispositivos inteligentes e a internet das coisas. A nova fase do capitalismo de vigilância se caracteriza pela coleta de dados em tempo real sobre as atividades dos indivíduos no mundo físico, como localização, movimentação, dados referentes à saúde, como frequência cardíaca, hábitos de consumo e interações sociais.

O modelo de capitalismo de vigilância também se relaciona com o Estado de Vigilância, 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 (Molinaro; Sarlet, 2013, p. 65). Por meio do monitoramento constante e da monetização e controle da experiência humana, a lógica, aplicada em diversos setores, e principalmente na saúde, tem consequências profundas para a privacidade dos indivíduos, levando à sua erosão progressiva.

A vigilância constante e oculta, caracterizada pela coleta de dados sem o conhecimento ou consentimento dos indivíduos, representa grave ameaça à privacidade, pois é invisível e gera sentimento de insegurança e vulnerabilidade, impactando a liberdade de expressão e o livre desenvolvimento da personalidade. “A vigilância oculta mina a confiança nas instituições e nas relações sociais, criando um clima de suspeita e medo” (Lyon, 2001, p. 78), e contribui para a erosão da esfera privada. A linha que separa o público do privado se torna cada vez mais tênue, e as pessoas se sentem expostas e monitoradas em diversos aspectos de suas vidas, desde as atividades *on-line* até as interações sociais e hábitos de consumo.

Além disso, o capitalismo de vigilância pode levar à discriminação e à exclusão social. Algoritmos e sistemas de inteligência artificial, alimentados por dados coletados indiscriminadamente ou enviesados podem reproduzir os vieses em suas decisões, com impactos negativos para grupos vulneráveis, perpetuando e ampliando as discriminações, inclusive em função da raça, gênero, orientação sexual, religião ou outros elementos.

Outra consequência preocupante é a manipulação comportamental. A análise preditiva e a personalização de conteúdo, com base nos dados coletados, podem ser utilizadas para influenciar as escolhas e o comportamento das pessoas, sem que elas tenham consciência de tal influência. Assim, “a manipulação comportamental fere a autonomia e a liberdade dos indivíduos, que têm suas decisões influenciadas por



algoritmos e técnicas de persuasão ocultas” (Barros, 2020, p. 123), comprometendo a capacidade de tomar decisões de forma consciente e informada.

O capitalismo de vigilância caracteriza-se pela coleta massiva de dados, inclusive os sensíveis, com o objetivo de criar perfis individuais e prever comportamentos com alto grau de previsibilidade. No âmbito da saúde, destacam-se riscos de discriminação, exclusão e manipulação, além da erosão da confiança na relação médico-paciente.

4. Prontuários, vigilância e exclusão: o nazismo como advertência histórica de proteção de dados sensíveis

Antes mesmo do hediondo projeto T4, que envolveu a eutanásia de deficientes físicos e mentais em hospitais, um outro lado da mesma moeda (Albuquerque, 2008, p. 50) foi sendo implementado em 1933, meses após Hitler chegar ao poder, quando o seu ministro do Interior Wilhelm Frick introduziu as primeiras normas de esterilização sob a alegação de a Alemanha estar sofrendo uma grave ameaça de *volkstod*, “morte do povo” alemão, por aqueles que tinham *lebensunwertes leben*, uma “vida indigna de ser vivida”, por suas deficiências físicas e mentais e deveriam sofrer compulsoriamente o procedimento da esterilização.

“Todos os médicos eram legalmente obrigados a relatar aos oficiais de saúde qualquer pessoa que encontrassem em sua prática ou em outro lugar que se enquadrasse em qualquer uma das categorias [...] para esterilização” e também a dar testemunho sobre tais assuntos, sem restrições, pelo princípio de confidencialidade médico-paciente (Lifton, 2017, p. 25).

Roberto Chacon de Albuquerque salienta que, com o advento da Lei de Prevenção de Doenças Hereditárias, de 14 de julho de 1933, o dever de notificar os casos de deficiência recaía não somente aos profissionais de saúde, que poderiam ser penalmente e administrativamente punidos, mas também sobre a população em geral, bem como os usos mais mesquinhos e abomináveis com tal dever imposto:

Não eram apenas os médicos e os enfermeiros que tinham o dever de denunciar a existência de um deficiente físico ou mental. Todos os cidadãos alemães tinham o dever de notificar as autoridades competentes da existência de pessoas que supostamente sofriam de doenças hereditárias. Familiares notificavam a existência de parentes deficientes para vingar-se ou para herdar bens



- IRENE NOHARA
- JOSEPH RODRIGO AMORIM PICAZIO
- SILVIO GABRIEL SERRANO NUNES

de toda espécie, bloqueando a linha sucessória. Qualquer paciente podia ser denunciado por seu próprio médico ou enfermeira, os quais eram passíveis de denúncia caso boicotassem o dever de notificação. O sigilo profissional caiu por terra, perdendo por completo o seu valor como mecanismo destinado a assegurar a confiança e a lealdade na relação do paciente com seu médico. A violação do dever de notificação podia dar ensejo a sanções penais e ao cancelamento da autorização para o exercício da profissão (Albuquerque, 2008, p. 45).

O Programa de Eutanásia T4, implementado pelo governo de Adolf Hitler entre 1939 e 1941, teve como objetivo a eliminação sistemática de pessoas consideradas “indignas de viver”, especialmente aquelas com deficiências físicas e transtornos mentais. Administrado a partir da *Tiergartenstraße 4*, em Berlim, esse programa marcou o início das políticas de extermínio nazistas, que mais tarde culminariam no Holocausto. Inicialmente voltado para pacientes internados em hospitais psiquiátricos e instituições de assistência, o programa rapidamente se expandiu, alcançando crianças, idosos e indivíduos com doenças hereditárias.

Foi o programa que resultou no extermínio de cerca de 70 mil seres humanos (Guerrens, 1994, p. 38), executados com injeções letais ou em câmaras de gás. As vítimas eram levadas diretamente para hospitais para sua execução. A notificação compulsória de doenças, que deveria ser um instrumento voltado à proteção da sociedade, foi distorcida pelo regime nazista para identificar e selecionar indivíduos que seriam submetidos à esterilização compulsória e à eutanásia forçada. Profissionais de saúde eram obrigados a informar ao governo sobre pacientes com determinadas condições, fornecendo base documental para sua execução. Com isso, um sistema originalmente criado para monitoramento epidemiológico foi transformado em mecanismo de eliminação de vidas consideradas “inúteis” pelo Estado totalitário.

O envolvimento de médicos e cientistas nesse processo levanta reflexões importantes sobre os limites éticos da atuação profissional e o perigo de instrumentalizar a medicina para fins políticos e ideológicos. Muitos profissionais participaram ativamente da seleção de vítimas, evidenciando como a ciência, quando desvinculada de princípios humanitários, pode ser utilizada como ferramenta de opressão. Esse episódio trágico e criminoso reforça a necessidade de salvaguardas que garantam a proteção dos direitos individuais e impeçam que informações médicas sejam usadas para fins discriminatórios, além de diretrizes eficientes de proteção de dados.



Após a Segunda Guerra Mundial, os horrores da esterilização compulsória de pessoas com deficiências do Projeto T4 e de outras atrocidades médicas vieram à tona nos julgamentos de Nuremberg. Como resposta, o Código de Nuremberg estabeleceu diretrizes fundamentais para a ética na pesquisa médica, incluindo o princípio do consentimento informado. Além disso, a experiência nazista reforçou a importância de que a notificação compulsória de doenças seja utilizada exclusivamente para fins de saúde pública, garantindo transparência e respeito à dignidade humana em sua aplicação. Trata-se de importante alerta histórico sobre o potencial destrutivo que pode ter o compartilhamento de dados em saúde quando não se respeitam os princípios basilares da proteção de dados.

Feitas tais considerações sobre as tristes lições do passado, legadas pelas sombras do regime nazista, são oportunas algumas considerações feitas por Yuval Harari sobre o potencial de dados biométricos e a criação de uma lógica ainda mais totalitária nos usos de dados de saúde, em um futuro já não muito remoto, pois:

o que já está começando a acontecer na medicina provavelmente ocorrerá em outros campos. A invenção decisiva é a do sensor biométrico, que as pessoas podem usar nos seus corpos ou dentro deles, e que converte processos biológicos em informação eletrônica que computadores podem armazenar e analisar. Se tiverem dados biométricos e capacidade computacional suficientes, sistemas de processamento de dados externos poderão intervir em todos os seus desejos, todas as suas decisões e opiniões. Poderão saber exatamente quem é você (Harari, 2018, p. 76).

Harari também alerta para o possível uso indevido da inteligência artificial (IA) e sua imensa capacidade de processar informações. Sob esse aspecto, tanto dados médicos e de saúde, como dados genéticos, poderiam ser requisitados compulsoriamente por autoridade central, encaminhando-nos assim para uma ditadura digital, que não apenas conheceria os indivíduos profundamente, mas também manipularia os sentimentos convenientes para a sua perpetuação, de tal modo que lograria um poder absoluto sobre seus subjugados, numa gradação imensamente maior que aquela exercida pela Alemanha nazista e sem nenhuma margem de resistência.

O risco mais grave está no fato de que algoritmos capazes de conhecer padrões biológicos, emocionais e comportamentais dos indivíduos podem permitir formas inéditas de dominação política e social. Regimes autoritários, munidos da combinação entre biotecnologia e tecnologia da informação, poderão, de acordo com Harari, não apenas

- IRENE NOHARA
- JOSEPH RODRIGO AMORIM PICAZIO
- SILVIO GABRIEL SERRANO NUNES

monitorar seus cidadãos com precisão superior à dos totalitarismos do passado, mas também influenciar desejos, afetos, medos e inclusive preferências políticas (Harari, 2018, p. 94).

Nessa hipótese, o controle não se limitaria à vigilância externa, pois alcançaria dimensões internas da subjetividade humana. A consequência seria a formação de “ditaduras digitais”, nas quais a resistência se tornaria extremamente difícil, uma vez que o poder político passaria a dispor de instrumentos para prever e manipular comportamentos. A preservação da democracia, portanto, dependeria de sua capacidade de se reinventar institucionalmente diante da nova convergência entre dados, biotecnologia e poder, nos dizeres de Harari (2018, p. 95), “ou a democracia se reinventa com sucesso numa forma radicalmente nova, ou os humanos acabarão vivendo ditaduras digitais”.

5. Assimetria informacional, consentimento para o tratamento de dados de saúde e paralelo entre os atos normativos de proteção

Um dos principais desafios éticos do capitalismo de vigilância é a assimetria informacional entre as empresas de tecnologia que usam tecnologias para coleta e tratamento de dados e os indivíduos. As empresas que atuam na área da saúde detêm conhecimento profundo sobre os dados que coletam, processam e utilizam, enquanto os indivíduos, em geral, têm pouca ou nenhuma informação sobre como seus dados são utilizados. A assimetria informacional coloca os indivíduos em posição de vulnerabilidade, pois eles não têm controle sobre o uso de suas informações e não podem tomar decisões informadas sobre o compartilhamento de seus dados.

Como destaca Danilo Doneda (2021, p. 45), “a assimetria de informação entre o titular dos dados e o controlador gera um desequilíbrio que dificulta o exercício da autonomia e do controle sobre os próprios dados”.

A Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece dez princípios para o tratamento de dados pessoais: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas. Em relação aos dados sensíveis, a LGPD exige o consentimento específico e informado do titular para o seu tratamento, exceto em algumas hipóteses previstas em lei, como o cumprimento de obrigação legal ou regulatória pelo controlador, a tutela da saúde, a realização de estudos por órgão de pesquisa e



o exercício regular de direitos em processo judicial, administrativo ou arbitral (art. 11, inciso II, alínea “a”).

O consentimento é um dos fundamentos para o tratamento de dados pessoais na LGPD, especialmente os sensíveis. O consentimento deve ser livre, informado e inequívoco, manifestado por escrito ou por outro meio que demonstre a vontade do titular. No caso de dados sensíveis médicos e biomédicos, o consentimento deve ser ainda mais claro e específico, informando ao titular sobre a finalidade do tratamento, os tipos de dados coletados, os riscos envolvidos, e seus direitos como titular dos dados. Doneda (2021) destaca a importância do consentimento como instrumento de autodeterminação informativa, permitindo ao indivíduo controlar o uso de seus dados pessoais.

No caso dos profissionais da saúde que atuam na área da medicina, estes também devem respeitar os regulamentos do Conselho Federal de Medicina (CFM). Embora não apresente explicitamente o termo “consentimento informativo de dados pessoais”, diversas normas abordam o consentimento do paciente em relação ao acesso e uso de suas informações de saúde, notadamente: o Código de Ética Médica (Resolução CFM nº 1.931/2009), que traz princípios gerais sobre o sigilo profissional e o consentimento do paciente em relação às informações de saúde; as resoluções sobre prontuário médico (Resolução CFM nº 1.821/2007 e Resolução CFM nº 2.217/2018), que garantem o direito do paciente de acessar suas informações e receber explicações, o que implicitamente exige seu consentimento para o uso desses dados; e a Resolução CFM nº 2.217/2018, que regulamenta a telemedicina, reforça a necessidade de garantir o acesso do paciente às informações e a segurança dos dados, o que implica a obtenção do consentimento para o tratamento dos dados em ambiente virtual.

Desse modo, para melhor contextualização, é possível analisar a consonância da Lei Geral de Proteção de Dados com as Resoluções Normativas do Conselho Federal de Medicina. Todavia, enquanto a LGPD versa exclusivamente sobre a proteção de dados, as Resoluções do CFM versam sobre a conduta profissional médica.

A previsão da LGPD quanto ao princípio da finalidade, inscrita no art. 6º, inciso I, estabelece que o tratamento de dados deve ocorrer para propósitos legítimos, específicos, explícitos e informados ao titular, vedado o uso posterior incompatível com tais finalidades. Esse comando encontra correspondência nas normas do Conselho Federal de Medicina (CFM) relativas ao prontuário médico, especialmente na Resolução CFM nº 1.638/2002, segundo a qual as informações devem ser coletadas para finalidades específicas, vinculadas à assistência à saúde do paciente. A Resolução CFM nº

- IRENE NOHARA
- JOSEPH RODRIGO AMORIM PICAZIO
- SILVIO GABRIEL SERRANO NUNES

2.217/2018, ao tratar da telemedicina, também reforça essa lógica ao determinar que dados e informações sobre a saúde do paciente teleassistido sejam armazenados em prontuário clínico eletrônico, preservando a vinculação entre coleta, registro e finalidade assistencial.

Quanto ao princípio da necessidade, o art. 6º, inciso III, da LGPD limita o tratamento ao mínimo indispensável para a realização de suas finalidades, exigindo pertinência, proporcionalidade e não excessividade dos dados coletados. A diretriz se aproxima da orientação constante da Resolução CFM nº 1.638/2002, segundo a qual as informações registradas no prontuário devem ser estritamente necessárias ao atendimento do paciente. O paralelo revela que, tanto no regime geral de proteção de dados quanto na disciplina ética da atividade médica, a coleta de informações de saúde não pode ser ilimitada ou meramente conveniente, devendo estar funcionalmente conectada à prestação adequada do cuidado médico.

No tema do consentimento e do sigilo profissional, a LGPD prevê, no art. 7º, que o tratamento de dados pessoais pode ocorrer mediante consentimento do titular, além de assegurar, no art. 9º, o direito de acesso facilitado a informações claras e adequadas sobre o tratamento realizado. As resoluções do CFM convergem com essa lógica ao estabelecerem, no Código de Ética Médica, a vedação à revelação de fatos conhecidos pelo médico em razão do exercício profissional, exceto por motivo justo, dever legal ou consentimento escrito do paciente. Além disso, a Resolução CFM nº 1.821/2007 assegura ao paciente, ou a seu representante legal, o direito de acesso ao prontuário e às explicações necessárias à sua compreensão.

Por fim, há correspondência relevante entre a segurança dos dados e os direitos do titular previstos na LGPD e as normas do CFM relativas à documentação médica. O art. 46 da LGPD impõe aos agentes de tratamento o dever de adotar medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados, perdas, alterações ou tratamentos ilícitos. Em paralelo, a Resolução CFM nº 2.299/2021 exige, para a emissão de documentos médicos por tecnologias digitais, assinatura digital com certificação adequada pela ICP-Brasil, garantindo validade legal, autenticidade, confiabilidade, autoria e não repúdio. Do mesmo modo, os direitos previstos nos artigos 18 a 22 da LGPD, preveem acesso, retificação, exclusão, anonimização, bloqueio e portabilidade, dialogando, pois, com as Resoluções CFM nº 1.821/2007 e CFM nº 1.638/2002, que reconhecem o direito de acesso do paciente ao prontuário e afirmam



que as informações nele contidas pertencem ao paciente, devendo ser preservadas a integridade e a confidencialidade.

É importante frisar que a LGPD se sobrepõe às normas do CFM em caso de conflito, e que os profissionais de saúde devem estar atentos aos dois parâmetros normativos para garantir a proteção dos dados dos pacientes.

6. Relação médico-paciente e autodeterminação informativa

A autodeterminação informativa compreende o direito de controlar o uso dos próprios dados pessoais. Mesmo com leis como a Lei Geral de Proteção de Dados Pessoais (LGPD), o exercício desse direito é desafiado por fatores como a assimetria de poder. Indivíduos que procuram o sistema de saúde, seja ele público ou particular, na grande maioria dos casos, já o fazem por uma necessidade, de maior ou menor urgência. A gravidade ou complexidade do caso sempre estará sujeita às circunstâncias e orientações médicas, fundamentadas em análises e exames biomédicos aos quais o paciente precisa se submeter para cuidar de uma enfermidade ou manter sua saúde em dia.

O fato é que o paciente tem pouco ou quase nenhum poder de barganha frente aos médicos, hospitais ou laboratórios que coletam seus dados. As políticas de privacidade são longas, complexas e difíceis de entender, e os usuários raramente têm opções reais de escolha. O consentimento, muitas vezes, se resume a “pegar ou largar”, isto é, “aceitar ou recusar”. A concordância para o uso de dados é uma condição para a utilização de serviços, que, no caso de saúde, nem é uma opção, tendo em vista a essencialidade da prestação do serviço médico, seja ele presencial ou por meio de plataformas digitais. A própria natureza da saúde impõe situação de “pegar e aceitar” na qual o paciente apenas se submete em face da necessidade.

Outras obscuridades que podem afetar a manutenção da confiança médico-paciente ou mesmo com a instituição hospitalar são a falta de transparência, controle e rastreamento de dados por dispositivos de saúde monitorados, que rastreiam os usuários sem seu conhecimento ou consentimento, utilizando cookies e pixels de rastreamento. Também é algo problemático o compartilhamento de dados com terceiros sem que os usuários tenham clareza sobre com quem seus dados são compartilhados e para quais fins e as dificuldades de exercer os direitos assegurados na LGPD, como o direito de acesso, retificação e exclusão de dados.



- IRENE NOHARA
- JOSEPH RODRIGO AMORIM PICAZIO
- SILVIO GABRIEL SERRANO NUNES

Milhares de médicos e outros profissionais da saúde permitem que seus dados e os de seus pacientes trafeguem entre plataformas integradas. Com o grande fluxo de troca de informações no ambiente digital, muitos profissionais da saúde buscam sistemas que sejam capazes de se comunicar entre si, chamados de sistemas com interoperabilidade. Esse é um conceito muito válido, porém, existe uma linha tênue entre o que pode ou não ser comunicado e a finalidade do uso da informação.

A interoperabilidade só faz sentido se beneficiar o paciente, que, muitas vezes, é encantado pela arquitetura das plataformas de serviços para coleta de dados, as quais são projetadas para incentivar o compartilhamento de dados e o uso contínuo dos serviços, utilizando técnicas de *design* persuasivo.

Outro aspecto a ser considerado é o “efeito rede”. Katz e Shapiro (1985, p. 424) definem o efeito rede como “a interdependência da demanda, em que o benefício de um consumidor ao adotar um bem aumenta com o número de outros consumidores que também o adotam”, ou seja, quanto mais pessoas usam uma plataforma, mais valiosos se tornam os dados coletados, criando um ciclo que reforça o poder das grandes empresas de tecnologia.

Lacunas na LGPD ainda não abordam todos os aspectos do capitalismo de vigilância, como o uso de dados para fins de inferência e a manipulação comportamental, e a dificuldade de fiscalização e aplicação da lei. A fiscalização e a aplicação da LGPD ainda são um desafio especialmente em relação às grandes empresas de tecnologia que oferecem sistemas de coleta de dados. O baixo investimento em campanhas de conscientização e educação também é um gargalo a ser enfrentado. Isso se reflete no senso comum de muitas pessoas que não têm consciência dos riscos do compartilhamento de dados e da importância da privacidade.

Os desafios para a proteção de dados na era do capitalismo de vigilância carecem de educação digital e literacia em dados, que são ferramentas essenciais para empoderar os indivíduos neste contexto. A educação digital deve ser prioridade para preparar as pessoas para os desafios da era digital, incluindo a proteção da privacidade e o uso responsável das tecnologias (Levy, 2010, p. 15). É fundamental que os cidadãos compreendam como seus dados são coletados, processados e utilizados, nos setores da saúde pública e privada, para que possam tomar decisões informadas sobre o compartilhamento de suas informações e manter a salvo a relação de confiança com as instituições de saúde, hospitais, clínicas e, principalmente, na relação médico-paciente.



A autodeterminação informativa é um direito fundamental na era digital, mas enfrenta limites significativos no contexto do capitalismo de vigilância. É necessário fortalecer a LGPD e outras leis de proteção de dados, promover a transparência e o controle sobre o uso de dados, e investir em educação e conscientização sobre direitos digitais e segurança da informação.

7. Invasões *hacker* e vazamento dos dados de saúde

Uma das principais consequências do capitalismo de vigilância é a perda de controle sobre os próprios dados. As pessoas se tornam “objetos de conhecimento” (Zuboff, 2019, p. 21), tendo seus dados coletados, analisados e utilizados por empresas e governos sem seu conhecimento e/ou controle. A perda de controle gera um sentimento de vulnerabilidade e incerteza, afetando a autonomia e o livre desenvolvimento da personalidade. A situação de incerteza se agrava pelos riscos que tais dados podem gerar quando desviados de sua finalidade ou criminosamente utilizados para fins ilegais.

Os dados sensíveis relativos à saúde têm sido alvo constante de criminosos devido a seu alto valor no mercado negro. Vazamentos e roubos de dados podem ocorrer por diversos fatores, como falhas de segurança em sistemas de informação, ataques cibernéticos, negligência de funcionários e venda ilegal de dados. As consequências de vazamentos e roubos de dados médicos e biomédicos podem gerar graves consequências para os indivíduos, incluindo discriminação, estigmatização, perda de oportunidades, danos financeiros e emocionais.

Em âmbito público, um dos casos mais emblemáticos aconteceu em 2021, quando o site do Ministério da Saúde (www.saude.gov.br/) sofreu um ataque *hacker* na madrugada de 10 de dezembro de 2021 e saiu do ar. Todos os portais da pasta, como o ConecteSUS e o Portal Covid, também foram afetados e ficaram sem possibilidade de acesso.

O portal sofreu um *ransomware*, ataque caracterizado pela paralisação do sistema, seguido de um pedido de resgate para liberação. Diante da situação, empresas e agências atingidas devem tomar a difícil decisão sobre pagar ou não os hackers para remover a interrupção (Porto, 2021).

Na ocasião, o grupo de *hackers* *Lapsus\$ Group* assumiu a autoria do ataque cibernético afirmando que 50 *terabytes* de informações tinham sido retirados do sistema e



- IRENE NOHARA
- JOSEPH RODRIGO AMORIM PICAZIO
- SILVIO GABRIEL SERRANO NUNES

estavam em posse do grupo. “Nos contate caso queiram o retorno dos dados”, dizia a mensagem enviada pelos *hackers*. Vale ressaltar que o aplicativo Conecte SUS ficou sem acesso por 13 dias, impossibilitando o acesso ao comprovante de vacinação, e o sistema de dados da pasta só foi restabelecido depois de mais de um mês fora do ar.

Esse não foi o único caso: o banco de dados do Sistema Único de Saúde brasileiro vem sofrendo constantes tentativas de invasão. Em 17 de maio de 2022, o Ministério da Saúde divulgou que as plataformas Conecte SUS, e-SUS Notifica e SI-PNI ficariam fora do ar após uma tentativa de invasão. Íntegra do comunicado:

[...] o Ministério da Saúde informa que as plataformas Conecte SUS, e-SUS Notifica e SI-PNI se encontram em manutenção corretiva, com previsão de retorno para às 16h. O Departamento de Informática do SUS (Datasus) identificou nessa segunda-feira (16) uma tentativa de acesso indevido e para resguardar as informações, os acessos foram suspensos até que toda a análise seja realizada. Vale ressaltar que a manutenção não causou impacto nos dados das plataformas (Silva, 2022, *on-line*).

Os acontecimentos demonstram um outro lado do capitalismo de vigilância, além do sequestro de dados que, por vezes, busca abastecer o mercado obscuro da *dark web*, parte da internet oculta e não indexada por mecanismos de busca comuns. Desafiando o Estado a garantir segurança informacional e cumprir o papel fundamental na proteção da privacidade informacional de dados sensíveis, “o Estado tem o dever de proteger a privacidade dos cidadãos, garantindo o controle sobre seus dados pessoais e prevenindo abusos por parte de empresas e governos” (Lemos, 2017, p. 56).

Ataques podem ter diferentes objetivos, notadamente o roubo de dados, para causar interrupção de serviços, com extorsão, sequestrando dados e exigindo resgate para a liberação, e vandalismo, com dano e/ou destruição de dados e sistemas. Os riscos são comuns também no ambiente de saúde privado e podem comprometer dados sensíveis de pacientes, conforme notificação enviada em 2020 pelo Procon-SP ao Hospital Albert Einstein para que explicasse o vazamento de lista que dava acesso a informações pessoais e médicas de pacientes testados, diagnosticados e internados por Covid-19.

Segundo notícia publicada pelo jornal *O GLOBO*, em 26 de novembro de 2020, um erro de um funcionário do Hospital Albert Einstein, em São Paulo, expôs os dados de 16 milhões de brasileiros com suspeita ou confirmação de Covid-19. As senhas que



davam acesso às informações privadas dessas pessoas ficaram disponíveis na internet por cerca de um mês, o que tornou públicos dados como endereço, telefone e condições de saúde (O Globo, 2020). Em nota, o Hospital Albert Einstein afirmou que o funcionário foi demitido da instituição por ter infringido normas internas de proteção e segurança de dados. O hospital disse também que, assim que tomou conhecimento do fato, removeu as informações da internet e comunicou o caso ao Ministério da Saúde.

Esse não é um caso isolado. Outro exemplo foi o vazamento de dados do Conselho Regional de Medicina do Estado de São Paulo (Cremesp). O Cremesp e a Prefeitura de São Paulo são investigados por possível vazamento de informações confidenciais de médicos que realizaram abortos legais. O Ministério Público Federal (MPF) instaurou um inquérito para investigar o Conselho Regional de Medicina de São Paulo e a Prefeitura de São Paulo por possível vazamento de informações confidenciais de médicos que realizaram abortos legais no estado. A Secretaria Municipal da Saúde é alvo da investigação por suspeita de ter copiado e compartilhado prontuários médicos com o Cremesp. Em nota, o Cremesp respondeu que:

O Cremesp respeita o direito da mulher ao aborto legal em casos de vítimas de crime sexual. Ressaltamos que o Conselho é uma autarquia federal que tem a prerrogativa de fiscalizar o exercício ético da Medicina em qualquer instituição hospitalar no Estado de São Paulo. O Cremesp está apurando os fatos que se encontram em sigilo nos termos da Lei. É lamentável que informações que não correspondem à realidade sejam veiculadas na sociedade, afirmou em nota, na época (Koyama, 2024, on-line).

Nesse caso, os dados de médicos que realizaram abortos legais, incluindo seus nomes e informações sobre os procedimentos realizados, também foram vazados. Os médicos vêm sofrendo perseguição após o vazamento dos dados. Esses são apenas alguns exemplos de vazamentos de dados médicos.

É importante destacar que o problema é global e afeta tanto instituições públicas quanto privadas. O combate ao crime cibernético e a proteção de dados em um mundo cada vez mais interconectado exigem a cooperação entre estados nacionais e atores internacionais. A cooperação é essencial para a criação de acordos, troca de informações, realização de investigações conjuntas e harmonização de legislações.

- IRENE NOHARA
- JOSEPH RODRIGO AMORIM PICAZIO
- SILVIO GABRIEL SERRANO NUNES

8. Desafios para saúde pública e privada e a governança de dados

A Lei Geral de Proteção de Dados (LGPD) representa um marco legal para a proteção de dados no Brasil, trazendo nova perspectiva para o tratamento da informação e os direitos dos titulares de dados (Schwartz, 2020, p. 34). A lei prevê a possibilidade de tratamento de dados sensíveis para fins de pesquisa e saúde pública, desde que respeitados requisitos específicos, como a relevância para o progresso científico e tecnológico e que sejam observados os padrões éticos reconhecidos pela comunidade científica.

Para fins de saúde pública, o tratamento de dados sensíveis deve ser realizado por órgão de pesquisa em saúde pública, com a finalidade de prevenção, monitoramento e controle de doenças e agravos à saúde. A LGPD deixa explícito que o intuito principal da proteção de dados é proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Todavia, a cultura de proteção de dados ainda é incipiente no Brasil, o que exige esforço conjunto de empresas, governo e sociedade civil para garantir a efetividade da LGPD (Mendes, 2021, p. 67). Os riscos inerentes ao capitalismo de vigilância e a lógica expansiva das indústrias relacionadas ao setor de saúde por dados preditivos apresentam desafio ao cumprimento das normas, regulações e conceitos éticos. A venda de dados médicos e desvios de finalidade podem ocorrer por diversos fatores, desde desvios intencionais motivados pelo ganho financeiro até por motivos pessoais com intuito de retaliação contra instituições e hospitais.

Com efeito, a Lei Geral de Proteção de Dados impõe obrigações a todos os atores do tratamento de dados. No caso dos médicos que atuam na cadeia de coleta e abastecimento de dados sensíveis do paciente, estes têm o duplo dever profissional de também observar e seguir as resoluções do Conselho Federal de Medicina (CFM). Cabe registrar que a Resolução nº 2.299/2021, que regulamenta, disciplina e normatiza a emissão de documentos médicos eletrônicos, descreve, em seu artigo 3º, que:

Os dados dos pacientes devem trafegar na rede mundial de computadores (internet) com infraestrutura, gerenciamento de riscos e os requisitos obrigatórios para assegurar registro digital apropriado e seguro, obedecendo às normas do CFM pertinentes à guarda, ao manuseio, à integridade, à veracidade, à confidencialidade, à privacidade e à garantia do sigilo profissional



das informações. § 2º Deve ser assegurado cumprimento integral à Lei Geral de Proteção de Dados (LGPD) (Brasil. 2021).

Ainda, na exposição de motivos dessa resolução, é informado que, em face da ausência de regulamentação específica para a emissão de documentos eletrônicos por meio de ferramentas tecnológicas, pacientes e profissionais de saúde são colocados em risco, pois não há garantia de que as plataformas de prescrição eletrônica sigam padrões avançados de segurança da informação e privacidade de dados sensíveis (como os da LGPD), nem de que garantam o equilíbrio nas relações comerciais, além dos regramentos éticos existentes no CFM e nos demais órgãos responsáveis.

O desenvolvimento de tecnologias que promovam a privacidade é outro caminho importante para enfrentar os desafios do capitalismo de vigilância. A criptografia, o *blockchain*, a privacidade diferencial e outras soluções podem ajudar a proteger os dados pessoais e a limitar o poder das empresas de tecnologia. Expõe Schneier (2015, p. 212) que “a tecnologia pode ser uma aliada na proteção da privacidade, desde que seja desenvolvida e utilizada de forma ética e responsável”.

A segurança da informação é crucial para a proteção de dados sensíveis médicos e biomédicos. As instituições que coletam e tratam esses dados devem adotar medidas técnicas e organizacionais adequadas para garantir sua confidencialidade, integridade e disponibilidade. As medidas incluem a criptografia de dados, a autenticação multifator, o controle de acesso, a realização de auditorias de segurança e a implementação de planos de continuidade de negócios.

Nesse cenário, a governança de dados se apresenta como ferramenta essencial para proteger os dados médicos e biomédicos. Ela envolve conjunto de práticas, processos e políticas que visam a garantir a disponibilidade, integridade, confidencialidade e segurança dessas informações. Doneda (2021, p. 237) destaca que “a governança de dados é fundamental para garantir que os dados pessoais sejam tratados de forma ética e responsável, em conformidade com a LGPD”.

Dentre os principais benefícios da governança de dados, destacam-se: minimizar o risco de vazamentos ao implementar medidas de segurança, como criptografia, controle de acesso e auditorias, reduzindo a vulnerabilidade a ataques cibernéticos e de vazamentos de dados, na proteção às informações sensíveis de pacientes; promoção do uso ético dos dados, a partir da definição de políticas claras e transparentes sobre a coleta, armazenamento, uso e compartilhamento de dados, garantindo que sejam

- IRENE NOHARA
- JOSEPH RODRIGO AMORIM PICAZIO
- SILVIO GABRIEL SERRANO NUNES

utilizados apenas para fins legítimos e com o consentimento informado dos pacientes; fortalecimento da confiança dos pacientes, a partir do compromisso com a proteção de dados e a privacidade, essencial para a relação médico-paciente e a adesão aos tratamentos; melhor cumprimento da LGPD, evitando sanções e penalidades, e promovendo a conformidade legal; e incentivo à inovação responsável, pois a governança de dados permite o uso deles para pesquisa e inovação, garantindo a proteção da privacidade e o desenvolvimento ético de novas tecnologias na saúde.

9. Conclusão

A análise desenvolvida ao longo do artigo permite concluir que dados médicos e biomédicos integram as preocupações contemporâneas sobre possíveis violações à proteção de dados pessoais, sobretudo no contexto do capitalismo de vigilância. Por essa razão, deve-se ter um olhar específico que recaia sobre sua coleta e tratamento, demandando o estabelecimento de limites jurídicos, éticos e institucionais mais rigorosos. O capitalismo de vigilância agrava a questão ao transformar os dados médicos e biomédicos em dados economicamente aproveitáveis e insumos de valor estratégico para informações de distintos atores, que se beneficiam de modelos preditivos, desenvolvimento de produtos e estratégias de mercado.

Um dos principais alertas do presente artigo consiste na insuficiência do consentimento como fundamento isolado de legitimação do tratamento de dados médicos e biomédicos. Embora o consentimento livre e informado continue a desempenhar papel relevante na proteção da autonomia do paciente, ele não resolve as assimetrias das relações de saúde, dado que o paciente frequentemente se encontra em situação de necessidade, dependência técnica e vulnerabilidade, o que limita sua capacidade real de negociação, tornando, portanto, o consentimento praticamente obrigatório para a utilização dos serviços necessários. Além disso, a complexidade dos sistemas digitais, das políticas de privacidade e das cadeias de compartilhamento de dados compromete a compreensão efetiva sobre o destino e os usos futuros das informações fornecidas.

Outro ponto focado foi o perigo de abuso dos dados inseridos via notificações compulsórias. A memória histórica das experiências totalitárias examinadas no artigo reforça a gravidade do tema. O uso de dados médicos pelo regime nazista em políticas de esterilização forçada, segregação e extermínio demonstra que informações de saúde podem ser instrumentalizadas quando deslocadas da ética do cuidado para a lógica de



vigilância, controle e exclusão. A referência histórica cumpre a função crítica de recordar que bases de dados sensíveis, quando submetidas a poderes sem controle, têm potencial de produzir violações extremas a direitos.

O passado, nesse aspecto, opera como advertência em face da naturalização da coleta e do compartilhamento de informações biomédicas. Tal advertência ganha atualidade diante das reflexões de Yuval Harari (2018, p. 76) sobre sensores biométricos, inteligência artificial e capacidade computacional, pois, se no passado registros médicos foram usados por regimes autoritários para classificar, excluir e eliminar pessoas, hoje a concentração de dados médicos, genéticos e biométricos pode inaugurar formas ainda mais intensas de vigilância. O risco já não se limita ao conhecimento sobre o corpo e a saúde, mas alcança a possibilidade de interferência sobre desejos, decisões e emoções (Nohara; Martins, 2023, p. 2016). Assim, a requisição compulsória de dados sensíveis, quando submetida a estruturas centralizadas e opacas, sujeitas inclusive a vazamentos, pode converter a proteção da saúde em instrumento de controle comportamental e de dominação social.

A notificação compulsória de doenças ilustra, portanto, a tensão permanente entre interesse público e proteção individual, sendo legítima e necessária em contextos de vigilância epidemiológica, prevenção de surtos e proteção coletiva da saúde; contudo, sua legitimidade depende da vinculação estrita a finalidades públicas, da proporcionalidade das medidas adotadas, da preservação do sigilo, sempre que possível, e da vedação de usos distorcidos.

Ademais, depreende-se que a relação médico-paciente deve ser pautada pela confiança mútua. O paciente deve se sentir à vontade para compartilhar informações e dúvidas com o médico, sem medo de julgamentos, e o médico, seguindo os princípios do Código de Ética, deve buscar o melhor relacionamento com o paciente e garantir a maior autonomia da vontade. A autonomia deve se estender a todas as práticas da relação interpessoal, principalmente quando da tomada e coleta de informações pessoais íntimas e sua inclusão em sistemas de dados.

A necessidade do tratamento das enfermidades do paciente não pode justificar a falta ou a precariedade de tratamento dos dados sensíveis, sob pena de o paciente se ver obrigado a mentir ou omitir dados relevantes a seu tratamento, em face do medo de exposição, discriminação ou prejuízo social ou econômico, em caso de vazamento, extravio ou *hacking* de dados sensíveis. Para além da ética médica, é necessário, então, compreender que a proteção de dados sensíveis médicos e biomédicos na era do

- IRENE NOHARA
- JOSEPH RODRIGO AMORIM PICAZIO
- SILVIO GABRIEL SERRANO NUNES

capitalismo de vigilância é um desafio complexo que demanda a atuação conjunta, numa governança que envolva o Estado, as empresas e a sociedade civil.

A pesquisa também reforçou que a proteção de dados em saúde exige uma articulação entre a Lei Geral de Proteção de Dados Pessoais (LGPD) e os deveres éticos da medicina. A LGPD fornece base normativa ao reconhecer a especificidade dos dados sensíveis e ao estabelecer princípios como finalidade, adequação, necessidade, transparência, segurança, prevenção e responsabilização, já os atos normativos editados pelo Conselho Federal de Medicina (CFM) expostos reforçam a centralidade do sigilo, da confiança, da autonomia e do consentimento no exercício ético da atividade médica.

Contudo, a proteção adequada dos dados médicos e biomédicos demanda mais do que declarações formais de conformidade, sendo imprescindível o reforço das políticas de governança que assegurem rastreabilidade dos acessos, limitação de finalidades, minimização e anonimização de dados, avaliação de riscos, controle sobre compartilhamentos, segurança informacional, transparência compreensível e responsabilização em caso de vazamento ou uso indevido.

Em síntese, o artigo enfatiza que a proteção de dados médicos e biomédicos no capitalismo de vigilância constitui desafio jurídico central da contemporaneidade. Ela envolve a defesa da privacidade, mas também ultrapassa tal dimensão, alcançando a autonomia, o reequilíbrio, a confiança institucional, a ética médica, o estímulo à educação digital, a saúde pública e, sobretudo, os limites ao poder econômico.

A principal conclusão, portanto, é que dados sensíveis em saúde não podem ser tratados como simples recurso informacional disponível à exploração técnica ou mercadológica. Sua utilização deve permanecer vinculada a finalidades legítimas, controláveis e compatíveis com a dignidade da pessoa humana, sendo relevante criar uma estrutura de governança de dados apta a limitar inferências discriminatórias e construir estruturas institucionais capazes de submeter o poder tecnológico aos fins de cuidado próprios da seara médica.

A construção de uma governança adequada para tais dados exige, por conseguinte, uma combinação de normas, instituições, práticas profissionais e cultura democrática. A LGPD e as normas ético-profissionais do CFM oferecem fundamentos relevantes, mas sua eficácia depende de implementação concreta, fiscalização, transparência e responsabilização, a partir da compreensão da proteção de dados médicos e biomédicos como condição de construção de confiança social, de legitimidade institucional e da proteção humana em virtude das novas formas de vigilância econômica e tecnológica.



REFERÊNCIAS

ALBUQUERQUE, R. C. de. A Lei de prevenção de doenças hereditárias e o programa de eutanásia durante a segunda guerra mundial. *Revista CEJ*, p. 43-51, v. 12, n. 40, 2008.

BRASIL. Conselho Federal de Medicina. Resolução CFM nº 2.299, de 19 de outubro de 2021. Regula, disciplina e normatiza a emissão de documentos médicos eletrônicos. *Diário Oficial da União*, Brasília, DF, 26 out. 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*, Brasília, DF, 15 ago. 2018.

BRASIL. Conselho Federal de Medicina. Resolução CFM nº 2.299, de 30 de setembro de 2021. Regula, disciplina e normatiza a emissão de documentos médicos eletrônicos. Brasília, DF: Conselho Federal de Medicina, 2021. Disponível em: <https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2021/2299>. Acesso em: 23 set. 2024.

BRASIL. Conselho Federal de Medicina. Resolução CFM nº 2.217, de 27 de setembro de 2018. Define e regulamenta a telemedicina como forma de prestação de serviços médicos mediados por tecnologias. *Diário Oficial da União*, Brasília, DF, 01 out. 2018.

BRASIL. Conselho Federal de Medicina. Resolução CFM nº 1.931, de 17 de setembro de 2009. Aprova o Código de Ética Médica. *Diário Oficial da União*, Brasília, DF, 24 set. 2009.

BRASIL. Conselho Federal de Medicina. Resolução CFM nº 1.821, de 22 de novembro de 2007. Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde. *Diário Oficial da União*, Brasília, DF, 29 nov. 2007.

BARROS, A. P. de. *O direito à privacidade na era digital*. São Paulo: Atlas, 2020.

BIONI, B. O estado de exceção digital: vigilância, privacidade e os desafios da proteção de dados no Brasil. *Revista Brasileira de Direitos Fundamentais & Justiça*, v. 16, n. 2, 2020.

CONSELHO FEDERAL DE BIOMEDICINA. CFBM *História da Biomedicina*. Brasília: CFBM, [s. d.]. Disponível em: <https://cfbm.gov.br/o-que-fazemos/historia-da-biomedicina/>. Acesso em: 21 ago. 2026.

DONEDA, D. *Proteção de dados pessoais: a função e os limites do consentimento*. São Paulo: Thomson Reuters Brasil, 2021.

GERRENS, U. *Medizinisches ethos und theologische ethik: die positionen von Karl Bonhoeffer und Dietrich Bonhoeffer in den Auseinandersetzungen um Zwangssterilisation und 'Euthanasie' im Nationalsozialismus*. München: Oldenbourg, 1994.

HARARI, Y. N. *21 lições para o século 21*. São Paulo: Companhia das Letras, 2018.

KATZ, M. L.; SHAPIRO, C. Network externalities, competition, and compatibility. *The American Economic Review*, v. 75, n. 3, p. 424-440, 1985.

KOYAMA, N. MPF investiga atuação do Cremesp contra médicos que realizaram aborto legal no Hospital Vila Nova Cachoeirinha, em SP. *G1*, São Paulo, 21 nov. 2024. Disponível em: <https://g1.globo.com/sp/sao-paulo/noticia/2024/11/21/mpf-investiga-atuacao-do-cremesp-contra-medicos-que-realizaram-aborto-legal-no-hospital-vila-nova-cachoeirinha-em-sp.ghtml>. Acesso em: 30 nov. 2024.



- IRENE NOHARA
- JOSEPH RODRIGO AMORIM PICAZIO
- SILVIO GABRIEL SERRANO NUNES

LEITE, I. *Moraes dá 5 dias para prefeitura e governo de SP responderem se passaram dados de pacientes de aborto legal ao Cremesp*. g1, São Paulo, 3 dez. 2024. Disponível em: <https://g1.globo.com/sp/sao-paulo/noticia/2024/12/03/moraes-da-5-dias-para-prefeitura-e-governo-de-sp-responderem-se-passaram-dados-de-pacientes-de-aborto-legal-ao-cremesp.ghtml>. Acesso em: 8 dez. 2024.

LEMONS, R. *O direito no século XXI*. São Paulo: Revista dos Tribunais, 2017.

LEVY, P. *O que é o virtual?* São Paulo: Editora 34, 2010.

LIFTON, R. J. *The nazi doctors: medical killing and the psychology of genocide*. New York: Basic Books, 2017.

LIMA, C. R. P. de. *Autoridade Nacional de Proteção de Dados e a efetividade da Lei Geral de Proteção de Dados*. São Paulo: Almedina, 2020.

LYON, D. *A sociedade de vigilância*. Rio de Janeiro: Editora FGV, 2001.

MEIRELES, A. V. Algoritmos e autonomia: relações de poder e resistência no capitalismo de vigilância. *Opinião Pública*, Campinas, v. 27, n. 1, p. 28-50, jan./abr. 2021.

MENDES, L. S. Dados pessoais e discriminação algorítmica: perspectivas para a proteção de grupos vulneráveis. *Revista de Direito, Estado e Telecomunicações*, v. 13, n. 1, 2021.

MOLINARO, C. A.; SARLET, I. W. Sociedade em rede, internet e estado de vigilância: algumas aproximações. *Revista da AJURIS*, [S. l.], v. 40, n. 132, 2013. Disponível em: <https://revistadaajuris.ajuris.org.br/index.php/REVAJURIS/article/view/249>. Acesso em: 16 set. 2026.

NOHARA, I. P.; MARTINS, F. M. G. Desafio ético de regulação de tecnologias que influenciam comportamentos. In: NOHARA, I. P.; CHIARELLO DE SOUZA PINTO, F. (coord.); SOARES, E. da S.; TIZZO, L. G. L.; NOBEMASSA, M. T. (org.). *Governança da regulação e o poder econômico*. São Paulo: Dialética, 2023.

O GLOBO. Funcionário do Einstein vaza dados do Ministério da Saúde e expõe 16 milhões de pacientes com Covid-19. *O GLOBO*, Rio de Janeiro, 26 nov. 2020. Disponível em: <https://oglobo.globo.com/brasil/funcionario-do-einstein-vaza-dados-do-ministerio-da-saude-expoe-16-milhoes-de-pacientes-com-covid-19-24766745>. Acesso em: 8 dez. 2024.

PECK PINHEIRO, P. *Direito digital*. São Paulo: Saraiva Educação, 2019.

PORTO, D. Após ataque ao site da Saúde, PF abre inquérito e confirma sistema comprometido. *CNN Brasil*, São Paulo, 10 dez. 2021. Disponível em: <https://www.cnnbrasil.com.br/nacional/apos-ataque-pf-abre-inquerito-e-confirma-sistema-comprometido/>. Acesso em: 8 dez. 2024.

PROCON-SP. Procon-SP notifica Hospital Albert Einstein. *Procon-SP*, São Paulo, 30 nov. 2020. Disponível em: <https://www.procon.sp.gov.br/procon-sp-notifica-hospital-albert-einstein/> [URL inválido removido]. Acesso em: 8 dez. 2024.

SCHNEIER, B. *Data and Goliath: the hidden battles to collect your data and control your world*. Nova York: W. W. Norton & Company, 2015.

SCHWARTZ, C. *Lei Geral de Proteção de Dados Pessoais comentada*. São Paulo: Revista dos Tribunais, 2020.



SILVA, B. *Ministério da Saúde identifica tentativa de ataque cibernético em sistemas*. Security Leaders, 17 maio 2022. Disponível em: <https://securityleaders.com.br/ministerio-da-saude-identifica-nova-tentativa-de-ataque-cibernetico-em-sistemas/>. Acesso em: 23 set. 2024.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). *Jornal Oficial da União Europeia*, L 119/1, 2016.

ZUBOFF, S. *A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder*. Rio de Janeiro: Intrínseca, 2019.

Irene Nohara

Livre-docente em Direito Administrativo (2012, USP). Doutora (2006) e mestra (2002) em Direito do Estado pela Faculdade de Direito da USP, onde se graduou (1999) pela área de direito público. Professora-pesquisadora do Programa de Pós-Graduação *Stricto Sensu* em Direito Político e Econômico da Universidade Presbiteriana Mackenzie (UPM), onde leciona na Graduação. Advogada Pa-racerista e Árbitra. Suas pesquisas concentram-se no direito público, com enfoque na governança regulatória, em função da análise da conformidade (*compliance*) de atos de regulação e de autorregulação das organizações, a partir da matriz de riscos, com interpretação e aplicação do Direito em pa-râmetros de razoabilidade e eficiência, no sopesamento de interesses em conflito, contidos em novas modelagens de parcerias em infraestrutura e serviços, incluindo licitação, celebração e execução dos respectivos contratos administrativos diante dos desafios das novas tecnologias. Integra a linha de pesquisa o Poder Econômico e Seus Limites Jurídicos do Programa de Pós-Graduação em Direito Po-lítico e Econômico do Mackenzie.

Universidade Presbiteriana Mackenzie, São Paulo

São Paulo, SP, Brasil

E-mail: irene.nohara@uol.com.br

Joseph Rodrigo Amorim Picazio

Doutorando em Direito Político e Econômico pela Universidade Presbiteriana Mackenzie (UPM), com bolsa da Capes. Mestre em Direito da Sociedade da Informação pelo Centro Universitário das Faculdades Metropolitanas Unidas (FMU). Linhas de pesquisa: Decisão Jurídica e Monopólio do Esta-do, Cidadania e Controle Social no Estado Democrático de Direito e Efetividade Jurisdicional Estatal. Especialista com dupla titulação em LL.M. (Master of Laws) em Proteção de Dados: LGPD e GDPR, em um curso binacional oferecido pela Fundação Escola Superior do Ministério Público (FMP) do Rio Grande do Sul, em parceria com o Centro de Investigação de Direito Privado (CIDP) da Faculdade de Direito da Universidade de Lisboa (Portugal/União Europeia). Graduado em Direito pelo Centro Uni-versitário das Faculdades Metropolitanas Unidas (FMU). Membro do grupo de pesquisa Estado e Eco-nomia no Brasil, vinculado à linha de pesquisa Poder Econômico e Seus Limites Jurídicos do PPGDPE da Universidade Presbiteriana Mackenzie (UPM). Autor do livro: *Inteligência Artificial e seus Impactos nos Direitos Sociais: um panorama da convergência e dos desafios da IA para a efetividade dos direitos e garantias fundamentais*. Integrante do Cadastro Nacional e Internacional de Avaliadores do Conselho Nacional de Pesquisa e Pós-Graduação em Direito (Conpedi). Membro do grupo de pesquisa Periódicos e Sucupira, responsável pelo acompanhamento e lançamento de dados da produção científica do

- IRENE NOHARA
- JOSEPH RODRIGO AMORIM PICAZIO
- SILVIO GABRIEL SERRANO NUNES

Programa de Pós-Graduação em Direito Político e Econômico (PPGDPE) da Universidade Presbiteriana Mackenzie. Advogado, pesquisador, palestrante e integrante da equipe editorial da *Revista APG Mackenzie - Educação Emancipatória*.

Universidade Presbiteriana Mackenzie, São Paulo

São Paulo, SP, Brasil

E-mail: josephamorim16@gmail.com

Silvio Gabriel Serrano Nunes

Bacharel (2007), licenciado (2009), mestre (2011) e doutor (2017) em Filosofia pela Universidade de São Paulo (USP) com bolsa outorgada pelo Programa Institucional de Bolsas de Doutorado Sanduíche no Exterior - PDSE/Capes para estágio na Université Paris Panthéon - Sorbonne (processo de n. 99999.002829/2015-00) sob a supervisão do professor doutor Bertrand Binoche para o período de maio a dezembro de 2015. Bacharel em Direito pela Pontifícia Universidade Católica de São Paulo (PUC-SP/2003), advogado (2004) e especialista em Direito Administrativo pela Faculdade Autônoma de Direito de São Paulo (Fadisp/2008). Foi professor do Mestrado Interdisciplinar em Ciências Humanas (Unisa/2021-2024). É professor do Mestrado Acadêmico em Direito Médico da Universidade Santo Amaro (Unisa), desde 2021. Atua nas áreas de Filosofia Política e Direito Constitucional e Direito Administrativo. Foi professor contratado da PUC/Campinas - Pós-graduação *Lato Sensu* Especialização em Direito Constitucional (segundo semestre de 2024). Pesquisa a questão do Direito de Resistência e a Reforma Protestante nas origens do Estado Moderno e seus desdobramentos, com ênfase na tradição do Constitucionalismo Calvinista e seu legado em institutos contemporâneos de Direito Público como o Controle Jurisdicional da Administração Pública, o Controle de Constitucionalidade das Leis e o conceito de Leis Fundamentais. Outro ponto relevante na pesquisa consiste na análise das questões sobre a participação das mulheres no poder político, uma discussão frequente nos tratados políticos dos calvinistas no século XVI. Foi professor de Direito Constitucional, Direito Administrativo, Ciência Política e Filosofia Jurídica na Universidade Nove de Julho (2017-2019). Docente da Escola Superior de Gestão e Contas Públicas do Tribunal de Contas do Município de São Paulo dos Cursos de Pós-Graduação: Especialização em Gestão e Controle Externo das Contas Públicas, Especialização em Direito Público Municipal, Aperfeiçoamento em Formação Política do Estado e Especialização em Formação do Estado: Ética e Filosofia Política, Especialização em Políticas Públicas, Especialização em Direito Administrativo. Coordenador Científico de Pós-Graduações na Escola Superior de Gestão e Contas Públicas do Tribunal de Contas do Município de São Paulo. Professor de História do Direito da Escola Brasileira de Direito (Ebradi). Pesquisador do Instituto Brasileiro de Contas Públicas (IBContas). Professor convidado do Curso de Pós-Graduação *Lato Sensu* em Direito Constitucional - Cogae/PUC-SP. Paralelamente às atividades regulares de pesquisa em Filosofia Política e Direito Público mencionadas, estuda: Segunda República, Guerra Civil Espanhola, Ditadura Franquista, o processo de transição democrática da Espanha e sua repercussão na redemocratização do Brasil, Constituição Espanhola de 1978 e sua influência na Constituição Brasileira de 1988.

Universidade Santo Amaro, São Paulo

São Paulo, SP, Brasil

E-mail: serrano.nunes@gmail.com

Equipe editorial

Editor Acadêmico Felipe Chiarello de Souza Pinto

Editor Executivo Marco Antonio Loschiavo Leme de Barros



Produção editorial

Coordenação Editorial Andréia Ferreira Cominetti

Preparação de texto Mônica de Aguiar Rocha

Diagramação Libro Comunicação

Revisão Vera Ayres

Estagiária editorial Luiza da Silva Oliveira

