

Problematizando o direito à privacidade e à proteção de dados pessoais em face da vigilância biométrica

Maria Fernanda Battaglin Loureiro¹; João Víctor Vieira Carneiro²

Recibido: 14 de mayo de 2020 / Aceptado: 13 de julio de 2020 [Open peer reviews](#)

Resumo. A aceleração tecnológica do capitalismo digital tem como um de seus elementos a ênfase na coleta de dados — em especial, dados pessoais — como matéria-prima para a operação de algoritmos computacionais. Em meio a tal fenômeno, percebe-se uma crescente coleta de informações referentes a características corporais humanas por meio de tecnologias biométricas como o reconhecimento facial. Neste contexto, o presente artigo busca analisar o fenômeno da digitalização do corpo humano, pelo referencial teórico dos estudos de vigilância e da biopolítica. Observa-se uma objetificação do corpo pelas tecnologias biométricas, fenômeno este que serve aos interesses de Estado, como a segurança pública, bem como à lógica do mercado de comodificação de informações pessoais. Com este percurso teórico, passa-se a uma breve análise de dois casos judiciais que envolvem o metrô de São Paulo, que consistiram no uso intrusivo de reconhecimento facial de seus usuários para fins publicitários e de segurança pública. O exame dos casos possibilita a demonstração da necessidade de instrumentos jurídicos de proteção aos dados pessoais, bem como os limites de uma tutela puramente jurídica fundada na privacidade.

Palavras-chave: biopolítica; capitalismo de vigilância; corpo humano; direito; reconhecimento facial.

[en] Questioning the right to privacy and data protection in light of biometric surveillance

Abstract. One of the elements of technological acceleration in digital capitalism is the emphasis on data collection – in particular, personal data – as raw material for the operation of computational algorithms. In the midst of this phenomenon, there is a growing collection of information regarding human body characteristics, gathered by biometric technologies such as facial recognition. In this context, this article seeks to analyze the phenomenon of digitalization of the human body, using the theoretical framework of surveillance studies and biopolitics. There is a noticeable objectification of the body by biometric technologies, a phenomenon that serves the interests of the State, such as public security, as well as the logic of the market for the commodification of personal information. With this theoretical path, a brief analysis of two judicial cases involving the São Paulo subway is carried out, which consisted of the intrusive use of facial recognition of its users for advertising and public security purposes. The examination of these cases makes it possible to demonstrate the need for legal instruments to protect personal data, as well as the limits of a purely legal protection based on privacy.

Keywords: biopolitics; facial recognition; human body; law; surveillance capitalism.

Sumário. 1. Carne e informação: o que é o corpo da biometria? 2. Corpo objeto: da surveillance à biopolítica. 3. Capitalismo de vigilância e segurança pública: violação da privacidade no metrô de São Paulo? 4. Considerações finais. 5. Referências.

Cómo citar: Battaglin Loureiro, M. F.; Vieira Carneiro, J. V. (2020). Problematizando o direito à privacidade e à proteção de dados pes-soais em face da vigilância biométrica. *Teknokultura. Revista de Cultura Digital y Movimientos Sociales*, 17(2), 205-213.

1. Carne e informação: o que é o corpo da biometria?

“O que interessa é tornar visível – e, sobretudo, tornar-se visível”. É assim que Paula Sibilia (2019) se refere ao comportamento contemporâneo de parcela considerável da população mundial perante as tecnologias e as redes sociais. O trabalho dessa autora

perpassa pela investigação sobre como o meio digital é capaz de redefinir as noções de privacidade, ética e propriedade (Sibilia, 2019, p. 268). Ela apresenta uma redefinição da intimidade, que passa a ser transmutada em extimidade, representando a transformação do espaço de ocultação do ser em verdadeiro palco para a exibição de si.

¹ Universidade Federal do Paraná (Brasil).
E-mail: battaglinloureiro@gmail.com

² Universidade Federal do Paraná (Brasil).
E-mail: joaovvieira@gmail.com

Essa é uma perspectiva extremamente importante, sobretudo, no que diz respeito aos estudos críticos dos usos que vêm sendo conferidos a determinados aparatos tecnológicos – em especial, as redes sociais — e como isso afeta a própria constituição das subjetividades. Muito embora as reflexões da autora estejam diretamente conectadas com a perspectiva do uso “recreativo” das tecnologias, a forma como ela problematiza o conceito de intimidade e o percebe como extimidade, por exemplo, pode ser um recurso bastante contundente para se questionar um outro uso que vem sendo conferido a recursos como as tecnologias biométricas.

Esse tipo de tecnologia se desenvolve por meio da captura de dados pessoais extraídos dos corpos. Para melhor compreendê-la, destacamos a definição de biometria apresentada por Arun Ross e Anil Jain:

Biometria é a ciência de estabelecer a identidade de uma pessoa com base nos atributos físicos (por exemplo, impressões digitais, face, geometria da mão e da íris) ou comportamentais (por exemplo, dinâmica do caminhar, assinatura e teclado) associados a um indivíduo. Um sistema biométrico típico usa sensores projetados adequadamente para capturar a característica biométrica de uma pessoa e a compara com as informações armazenadas em um banco de dados para estabelecer a identidade. Um sistema biométrico pode operar em dois modos distintos: no modo de verificação, o sistema confirma ou nega uma identidade reivindicada, enquanto no modo de identificação determina a identidade de um indivíduo. (Ross e Jain, 2015, p. 289, tradução nossa).

A aplicação da biometria é genericamente dividida em quatro categorias. A primeira se refere ao controle de acesso a dados, como o reconhecimento facial para o desbloqueio de um smartphone. A segunda é o controle de acesso a áreas ou materiais, como a abertura de uma porta por meio de um sensor de impressões digitais. A terceira diz respeito à validação de uma alegada identidade em face de credenciais já cadastradas; é o caso do controle de fronteiras nacionais. A quarta é o registro ou identificação de indivíduos cuja identidade precisa ser estabelecida por meios biométricos, mormente utilizando bases de dados distribuídas ou centralizadas – os casos mais recorrentes são as aplicações militares e de *law enforcement* (Day, 2015).

Segundo Marianne Díaz (2018), os quatro requisitos básicos para a configuração de um identificador biométrico são: (i) a colecionabilidade, ou a possibilidade de ser medido; (ii) a universalidade, ou a existência em todas as pessoas do elemento mensurável; (iii) a unicidade, ou a noção de que os elementos universais são distintivos de cada pessoa individualmente; (iv) a permanência do elemento no tempo, ou a certeza de que o elemento não será perdido ou substantivamente alterado com o passar do tempo.

David Lyon (2008) sustenta que a atratividade da biometria está no fato de que a identificação pode ser realizada a partir de características possuídas por praticamente todos os humanos, com baixo risco de erro. De acordo com ele, as funções do uso da biometria são (i) a verificação/autenticação (essa pessoa é quem diz ser?) e (ii) a identificação (quem é essa pessoa?).

A definição e os aspectos técnicos da biometria permitem visualizar a sua abrangência. Há uma multiplicidade de usos que pode ser conferido a essa espécie de dado, que, por ser extraído de elementos corporais únicos e específicos de cada pessoa são tratados pela legislação brasileira como dado sensível. Repetindo o marco regulatório europeu (*General Data Protection Regulation*), a lei brasileira, Lei Geral de Proteção de Dados (LGPD), reproduz a necessidade de se conferir uma proteção especial a essa categoria de dado.

A questão é que, contemporaneamente, a opção pelo uso da biometria como recurso de identificação que proporciona maior segurança (como uma espécie de valor supremo) e prevenção de fraudes pode ser interpretada como uma das formas de materialização da passagem da intimidade para a extimidade, tratada por Sibilia. Aquilo que era exclusivo do ser, pois parte de seu corpo, passa a ser detalhadamente conhecido por máquinas e armazenado em bancos de dados. O que era próprio do corpo é descoberto por meio de leituras tecnológicas que, mesmo sem deixar uma marca explícita, obriga-nos a torná-lo visível. É o que nos promete segurança, mas entrega vigilância.

Trata-se da passagem de uma percepção do corpo-físico para o corpo-informação. A ideia de que o corpo humano passa por um processo de digitalização ou datificação recebe tratamentos distintos. O fenômeno da tradução do corpo em arquivo de dados se intensifica no capitalismo tecnocientífico, porquanto o corpo passa cada vez mais a ser visto como um conjunto de dados digitais e genéticos (Corrêa, 2006; Santos, 2003). Com isso, os limites entre o corpo-físico e o corpo-informação não podem mais ser tomados como certos (Van der Ploeg, 2012). Acerca dessa relação discorre Carvalho (2018), para quem o conceito de ‘informação’ permite estabelecer uma analogia entre máquina e organismo:

Os esquemas operatórios ou modos de funcionamento das máquinas e dos organismos são equivalentes e podem ser intercambiados entre si. Eles podem porque tanto a máquina quanto o organismo são referidos a um termo comum que os definem e os colocam em relação de equivalência; a noção de processamento de informação ou sistema cibernético. (Carvalho, 2018, p. 99).

As concepções sobre o corpo estão sempre sujeitas a mudanças – as diferentes formas de compreendê-lo possuem repercussões no campo de estudo das ciências, da filosofia e da religião, por exemplo. De modo geral, porém, pode-se dizer que a noção de corpo se determina pelos conhecimentos e linguagens disponíveis, bem como pelas maneiras práticas como o manuseamos e o tratamos. Conforme defende van der Ploeg (2012), é necessário considerar que a adaptação de nossa existência física à condição digital é uma mudança em termos ontológicos, não se restringindo a meras representações.

A possibilidade de se ler o corpo por meio da biometria revela um caráter bastante interessante a respeito dele: geralmente não conseguimos definir com precisão se é coisa ou se é pessoa (Edelman, 2009). O corpo da biometria corresponde ao objeto de uma gestão de securitização de identidades; nesta perspectiva, o corpo não mente, mas concebe uma verdade objetiva e não

ambígua, sem a necessidade de comunicação para a determinação das identidades (Aas, 2006). O corpo, como afirma Rodotà (2008), torna-se uma senha, e os elementos corporais estão crescentemente sendo usados não apenas como forma de identificação ou verificação, mas também como instrumento de classificação.

A partir dessa perspectiva, surgem conceitos buscando definir este corpo que passa por um processo de digitalização. O termo “corps statistique” é trabalhado por Rouvroy e Berns (2009) como o corpo que evacua as dimensões “física” e “linguística” que caracterizam a particularidade do corpo subjetivo; nem a experiência física do corpo, nem a narrativa auto biográfica do sujeito são mais “autorizadas” ou “autoritativas”, no sentido de que seu “autor” possuiria a “autoridade” necessária para controlar sua inteligibilidade e interpretação (Rouvroy e Berns, 2009, pp. 173-174).

A noção apresentada por esses autores é fundamental para a compreensão do fenômeno que pretendemos problematizar. De fato, a digitalização do corpo traz consigo a automática exclusão dos aspectos subjetivos do ente observado. A pessoa humana torna-se mera “pessoa-fonte” dos dados coletados, o que confere uma aparente contradição entre sua proteção ético-jurídica e, por outro lado, a transformação do corpo em uma fonte de conteúdos biológicos e informacionais (Corrêa, 2010). O corpo humano é “scaneado”, interpretado enquanto sistema de processamento de informação, sendo ao mesmo tempo, carne e informação (Lemos, 2013, p. 180).

É o que Torrano e Barrinuevo (2016) denominam “políticas extrativistas sobre o corpo”: é empreendida uma captura biométrica dos dados que se encontram na superfície do corpo humano. O uso do termo “superfície” por parte desses autores transmite uma ideia essencial para a compreensão crítica do fenômeno, uma vez que os aspectos constitutivos da identidade humana são reduzidos a aspectos meramente físicos. É a partir desses pontos que pretendemos inserir a questão da *surveillance* que vem se sobrepondo aos corpos-objeto, para, posteriormente, explorar alguns dos problemas jurídicos que podem ser suscitados, em específico, quando assistimos à implementação de câmeras capazes de realizar o reconhecimento facial – uma das expressões do uso da biometria – em espaços públicos, motivadas por ações de mercado e de segurança pública.

2. Corpo objeto: da *surveillance* à biopolítica

O debate acerca das concepções possíveis sobre o corpo é extremamente vasto e rico, como decorrência das suas múltiplas abordagens, pois diz respeito à forma como experienciamos o mundo. Apesar de relevante, não pretendemos adentrar às profundezas dessa questão, partimos do seguinte: ao se fazer predominar uma visão objetiva do corpo, retirando o seu aspecto existencial/sacro, ele se torna objeto. Se nossos corpos são meros objetos vivos, é mais fácil conduzi-los, gerenciá-los e torná-los lucrativos, e é esta constatação que torna relevantes as práticas de vigilância.

No campo do Direito, abre-se espaço para uma infinidade de interlocuções que transitam pela própria concepção sobre o que é o corpo, caminhando em direção às dúvidas sobre quem pode dizer quais são os limites para a utilização dos dados extraídos desses corpos.

Um dos pontos suscitados por Zuboff (2020b) diz respeito aos legitimados e aos responsáveis pela regulação desses temas, o que, tradicionalmente, faz-se por meio de instrumentos normativos. De acordo com a autora estadunidense, dois grupos batalham intensamente na definição desses papéis. De um lado está a indústria da tecnologia, que se compreende como legitimada a promover sua autorregulação, tendo em vista que uma regulação externa poderia ser altamente custosa e contraproducente. De outro lado, estão os militantes das liberdades civis, que entendem que o poder acumulado pelas empresas gerenciadoras de dados significa verdadeira ameaça às liberdades individuais.

Essa disputa faz sentido porque a manipulação dos dados pessoais assumiu uma posição de altíssima relevância no capitalismo contemporâneo. E quanto mais íntima, maior o valor econômico da informação extraída do corpo e vida das pessoas (Harcourt, 2014). O que está por trás disso é quem poderá manipular e como poderão ser gerenciados e utilizados os dados pessoais, genericamente, e os biométricos, especificamente. De acordo com Zuboff (2020b), a dificuldade em concretizar uma regulação jurídica da matéria que favoreça a proteção das pessoas existe há mais de duas décadas; e para ela, por ora, há um lado vencedor, uma nova lógica econômica que ela chama de *surveillance capitalism*.

Para compreendermos melhor esse ponto, destacamos que a *surveillance* pode ser compreendida, grosso modo, como vigilância. Sobre esse conceito, evidenciamos as palavras da pesquisadora Fernanda Bruno (2013):

Atividades de vigilância para indivíduos ou populações humanas envolvem, de modo geral, três elementos centrais: observação, conhecimento e intervenção. A observação pode ser efetuada de diferentes modos (visual, mecânico, eletrônico, digital) e implica a inspeção regular, sistemática e focalizada de indivíduos, populações, informações ou processos comportamentais, corporais, psíquicos, sociais, entre outros. Ela deve, ainda, permitir a produção de conhecimento sobre os vigiados, o que pode ser formalizado de diversas formas (extração de padrões, regularidades ou cadeias causais, por exemplo). Ou seja, as informações apreendidas pela observação devem ser convertidas em conhecimento a respeito daqueles sob vigilância, de modo a permitir agir sobre suas escolhas, subjetividades, comportamentos. Aí reside o terceiro e último elemento. Nem a observação nem o conhecimento que dela derivam se caracterizam se não houver a perspectiva de intervir sobre os indivíduos ou populações em foco (Bruno, 2013, p. 18).

Um modo de abordar a noção de *surveillance* é a retomada, a título de referência, da análise foucaultiana do panóptico de Jeremy Bentham para explicar fenômenos contemporâneos. Tal referência é um ponto de

partida teórico para a problematização da *surveillance*, ainda que a aplicabilidade do conceito como modelo de análise na atualidade seja alvo de controvérsia nos estudos de vigilância (Haggerty, 2006). A abordagem sobre o panóptico conecta-se intimamente com os processos disciplinares, e Michel Foucault (1999) destaca a descoberta do corpo como objeto e alvo de poder. É na ‘época clássica’ (séculos XVII e XVIII) que assistimos à docilização desses corpos, adestrados para se tornarem obedientes e habilidosos; nesse sentido, “é dócil um corpo que pode ser submetido, que pode ser utilizado, que pode ser transformado e aperfeiçoado” (Foucault, 1999, p. 163). Essa incidência disciplinar do poder sobre o corpo implicaria em analisá-lo minuciosamente, nas mais diminutas condutas e nos mais meticulosos gestos, reconduzindo-os ao processo de produtividade e obediência. A permanência dessas relações indicadas por Foucault nos remetem à exacerbação das minúcias corporais alcançadas pelas tecnologias biométricas.

O ambiente do panóptico é utilizado por Foucault como uma ‘figura arquitetural’, onde “basta então colocar um vigia na torre central, e em cada cela trancar um louco, um doente, um condenado, um operário ou um escolar” (Foucault, 1999, pp. 223). O panóptico permite o exercício do poder hierárquico e anônimo sobre os indivíduos de tal sorte que leva o indivíduo “a um estado consciente e permanente de visibilidade” que assegura o funcionamento automático do poder (Foucault, 1999, p. 224). O efeito é uma vigilância permanente que promove o engajamento do próprio indivíduo na correção de seu corpo.

Uma das características mais notáveis do panóptico e das instituições disciplinares é que a disciplina se restringia a grupos limitados de indivíduos. É aí que reside uma das mais significativas diferenças em relação às sociedades contemporâneas. Sob esse aspecto, entendemos, novamente, que o avanço tecnológico foi fundamental para tornar isso possível: a *surveillance* e a biopolítica atuam em nível populacional. Por isso, buscamos os ensinamentos de Gilles Deleuze (1992), ao tratar das sociedades de controle, e do próprio Michel Foucault (2005), ao tratar da biopolítica, modelos que se sobrepõem às sociedades disciplinares, mas não as substituem.

Nas sociedades de controle, “os indivíduos tornam-se ‘dividuais’, divisíveis, e as massas tornaram-se amostras, dados, mercados ou ‘bancos’” (Deleuze, 1992, p. 222). Se a sociedade disciplinar tem a produção do indivíduo docilizado como elemento fundamental, na sociedade de controle o poder circulará de forma difusa, por meio de cada indivíduo (Luz, 2018). Como aponta Ayse Ceyhan (2012), a *surveillance* contemporânea é marcada por processos ocultos e silenciosos embutidos na malha social, e portanto torna-se difícil que indivíduos e sociedade estejam cientes da existência e finalidades desses processos.

Outra análise importante, feita por Foucault, trata da emergência da biopolítica, deslocando-se a noção de corpo-máquina para a de corpo-espécie. Ambas as tecnologias de poder, para Foucault (2009), têm como objetivo dominar os processos vitais. Para ele, os dispo-

sitivos de segurança da biopolítica diferem das medidas disciplinares clássicas, pois, uma vez que estas dependem diretamente da coerção, aqueles não intervêm diretamente no “jogo”, mas moldam as suas regras (Ceyhan, 2012).

Ao agregar a temática da tecnologia aos estudos a respeito do poder e da *surveillance*, Rouvroy e Berns (2013) trabalham com o conceito de *gouvernementalité algorithmique*. Esta leitura percebe que práticas estatísticas anteriores são remodeladas e conferem espaço a novas formas de controle, visando à produção de modelos que permitam ‘conduzir as condutas’ das pessoas em sociedade. A virtualização do *milieu* foucaultiano reforça a *surveillance* como um dispositivo orientado a práticas de governamentalidade, o qual busca alcançar o máximo de eficiência para a regulação dos corpos e das espécies (Ceyhan, 2012, p. 40).

A conexão entre todos esses temas fica evidente quando percebemos que o detentor do poder de armazenar, manipular e operar os dados é o capital privado da vigilância, que em última análise é regido por um sistema de autorregulação, conforme afirma Zuboff (2020b). Essa perspectiva da autorregulação vai ao encontro das teorizações de Foucault (2008) acerca da governamentalidade neoliberal, marcada pela inclusão do elemento econômico como limitador da ação do Estado, que se insere em uma relação simbólica com o mercado (Foucault, 2004).

Na esteira dos ensinamentos de Foucault e seguindo a perspectiva neoliberal da auto-responsabilização, do capital humano e do ‘cada um por si’, segundo Zuboff (2020a), nos iludimos com a gratuidade dos novos serviços virtuais, sem percebermos que, na verdade, eles imprimem um custo real a cada pessoa que se associa a algum site, rede social, e-commerce. Converte a lição do hacktivista Julian Assange (2013) acerca de serviços online como Google e Facebook: se você não é o cliente de tais provedores, você é o produto a ser vendido – sobretudo por meio da venda de dados pessoais a empresas publicitárias.

A lógica subjacente a estes serviços deixa a entender uma suposta escolha racional entre permitir ou não o uso de dados pessoais. A preservação ou a perda da privacidade é portanto visualizada como uma transação comercial, e a cada vez que cedemos nossa intimidade, aprofundamos e naturalizamos mais estes regimes, reforçando uma narrativa de que a privacidade não teria valor (Hull, 2015). De modo semelhante, Zuboff (2020b), argumenta que a eficácia desses e outros sistemas de vigilância e controle (públicos ou privados) depende das partes de nós mesmos das quais já desistimos ou que nos foram roubadas de modo oculto.

Diante disso, entendemos que a lição de Sibilía (2019) sobre a transição da intimidade para extimidade se encontra com a de Zuboff (2020b) de que a privacidade é pública. Frente ao *surveillance* capitalism, que se apropria das novas tecnologias, originalmente pensadas como instrumentos de guerra (Crary, 2014), é um desafio defender a privacidade como um bem coletivo, ligado aos valores da autonomia humana e da autodeterminação das pessoas, os quais nos acostumamos a atrelar à qualidade democrática das sociedades (Zuboff, 2020b).

3. Capitalismo de vigilância e segurança pública: violação da privacidade no metrô de São Paulo?

Em meio a tão ubíqua vigilância, dizer que a intimidade se tornou extimidade ou que a privacidade se tornou pública é, sem dúvidas, uma afirmação desconfortável, principalmente ao se pensar em termos jurídicos. Na América Latina, especialmente, constata-se uma complicada demora na regulamentação de sistemas de vigilância e segurança, o que demanda maiores esforços na problematização de tais tecnologias. O ambiente legislativo brasileiro, por exemplo, não parece dar muita importância ao crescente uso de circuitos fechados de televisão (CCTV) em espaços públicos nos últimos anos, como aponta um estudo de Firmino, Kanashiro, Bruno, Evangelista e Nascimento (2013).

Com a realização da Copa do Mundo FIFA de 2014 e as Olimpíadas de 2016 em território brasileiro, o país pôde também observar um aumento expressivo na utilização de tecnologias de monitoramento por autoridades públicas (Vicente, 2016). Na Copa de 2014, por exemplo, foram implementados doze Centros Integrados de Comando e Controle (Ciccs), um para cada cidade anfitriã de jogos da competição. O legado da Copa se estendeu, todavia: após o fim do evento, todavia, o governo federal veio a inaugurar novos centros em todas as capitais de estados do país, contando com modernas tecnologias de controle e segurança (Cardoso, 2018).

O governo federal brasileiro tem realizado repetidas iniciativas legislativas e regulatórias com o fim de centralizar as bases de dados biométricos públicas do país. Em 2008, o Tribunal Superior Eleitoral (TSE) iniciou o programa de cadastramento biométrico, com a finalidade de coletar esses dados para fins de verificação de identidade nas atividades eleitorais; deste modo, a disponibilização de impressões digitais passou a ser requisito para o legítimo exercício do voto. Logo, a finalidade eleitoral foi flexibilizada e a base de dados passou a ser compartilhada com serviços de proteção ao crédito e autoridades de segurança pública. A aprovação da Lei de Identificação Civil Nacional (13.444/2017) passou a permitir compartilhamentos problemáticos entre bases de dados biométricos de identificação civil e bases de dados destinadas à persecução criminal (Corrêa, 2019).

Tratam-se, claro, de casos em que não se utilizou sistemas de reconhecimento facial, mas tecnologias de monitoramento por câmeras e coleta de impressões digitais. Contudo, observa-se uma grande expansão no uso do reconhecimento facial no Brasil – um consultor desta área afirma ser possível observar taxas de crescimento de 20% a 30% por ano nesse nicho do mercado brasileiro (Sistemas de reconhecimento, 2019). Como um modo de ilustrar esse fenômeno, as duas situações que pretendemos explorar dizem respeito à utilização de dados biométricos em sistemas de segurança do metrô de São Paulo. No primeiro caso, para a promoção de propagandas direcionadas; no segundo, para fins de modernização do sistema de segurança pública.

3.1. O sistema de “Portas Digitais Interativas” e sua repercussão jurídica

Partimos para a análise da primeira das situações que envolve o metrô de São Paulo. Um dos casos que escolhemos abordar e sobre o qual faremos um panorama breve é o do projeto “Portas Digitais Interativas”, criado em meados de 2018, que visava à instalação de câmeras com leitores faciais nas portas dos vagões dos trens da Linha 4. O objetivo do projeto era realizar uma pesquisa sobre o padrão dos usuários do sistema, a partir da captura das emoções manifestadas em seus rostos, para que se pudesse direcionar as propagandas mais adequadas (Soprana, 2018).

O próprio objetivo, como adiantamos acima, é controverso e nos reporta a uma previsão de Jonathan Crary (2014): as mais inovadoras técnicas de vigilância e análise de dados utilizados por agências de inteligência se tornaram também indispensáveis às estratégias de marketing de grandes empresas. Portanto, além de as tecnologias de reconhecimento facial atenderem a demandas de vigilância e redução do aparato estatal, os seus usos impulsionam a lucratividade de negócios.

Os responsáveis pelo projeto não entenderam necessário informar às pessoas de que seriam filmadas, e alegaram desejar apenas melhorias em sua política de publicidade e propaganda dentro dos vagões. Ainda assim, sob a visão de alguns operadores do direito, a investida da concessionária e da empresa parceira configurou a violação de uma série de direitos, o que deu ensejo ao ajuizamento de uma Ação Civil Pública em face da Concessionária da Linha 4 do Metrô de São Paulo (ViaQuatro).

Tal ação foi ajuizada pelo Instituto Brasileiro de Defesa do Consumidor (Idec, 2018), com auxílio do LAVITS (Rede Latino-Americana de Estudos de Vigilância) e de pesquisadoras da Universidade de São Paulo. A finalidade da ação era a cessação da coleta dos dados biométricos dos passageiros com o desligamento das câmeras de reconhecimento facial. Questionava-se, pela via da proteção ao direito do consumidor, a captura compulsória e indistinta dos dados biométricos dos usuários do metrô de São Paulo, em flagrante violação ao direito à privacidade (Idec, 2018).

Inicialmente, trabalharam com dispositivos da Constituição da República, destacando-se o direito fundamental à proteção da intimidade, vida privada, honra e imagem das pessoas (art. 5º, X, CF). Também citou-se o Código Civil, Código de Defesa do Consumidor, Lei de Acesso à Informação e Marco Civil da Internet. Saliêntamos que no momento da propositura de tal ação, a Lei Geral de Proteção de Dados Pessoais (LGPD) estava com sua eficácia comprometida por estar em *vacatio legis*, e sua aplicação segue impedida até hoje.

A magistrada de primeiro grau, ainda que em decisão não definitiva, foi favorável ao pleito do IDEC, obrigando a concessionária a interromper a captação de imagens e outros dados, sob pena de multa diária. Levou em consideração a proteção à intimidade e à vida privada, e afirmou ainda que a finalidade da coleta de tratamento não é clara o bastante, em especial considerando o caráter público do serviço (T.J.S.P., 2018, p. 330).

A Ação Civil Pública mencionada foi ajuizada em agosto de 2018 e, quase dois anos depois, ainda aguardava uma decisão definitiva, muito embora estivesse respaldada por uma decisão provisória favorável. Nesse período, outros programas de utilização de sistemas de reconhecimento facial já entraram em funcionamento. Citamos como exemplos as câmeras nas ruas de cidades como o Rio de Janeiro e Salvador, instaladas e testadas no período do carnaval de 2019. No caso de Salvador, o recém-implantado sistema de reconhecimento facial da Secretaria de Segurança Pública baiana detectou um criminoso foragido que, fantasiado em meio à multidão, pretendia participar de um bloco de carnaval (Santos, 2019). Já o governo carioca, para o carnaval do mesmo ano, contratou um serviço de “câmeras inteligentes” de uma empresa que já fora multada por coleta e venda ilegal de dados pessoais (Kawaguti, 2019).

3.2. O sistema de monitoramento da Companhia do Metropolitano de São Paulo

Mesmo com a ação judicial acima abordada, não demorou para que o metrô paulistano voltasse a ser o centro de polêmicas. Dessa vez, a questão diz respeito à adoção do sistema de câmeras de reconhecimento facial nas linhas 1, 2 e 3 do metrô. A Companhia do Metropolitano de São Paulo (Metrô), operadora dessas linhas, publicou em julho de 2019 um edital de licitação, visando à contratação de um sistema de monitoração eletrônica de seus usuários. Os requisitos de tal sistema incluíam a operação integrada com sistemas externos semelhantes, bem como o armazenamento de imagens pessoais e o carregamento de dados internos e externos. No final de outubro, foi homologada a adjudicação do objeto do contrato ao Consórcio Engie, Ineo e Johnson; irredimidas, empresas concorrentes interporam recurso, ao qual foi negado provimento (Companhia do Metropolitano de São Paulo, 2020).

Tendo em vista tal notícia, a Defensoria Pública do Estado de São Paulo, a Defensoria Pública da União, o Instituto Brasileiro de Defesa do Consumidor (IDEC), o Coletivo Intervozes e o Artigo 19 Brasil ajuizaram em fevereiro de 2020 uma Ação Autônoma de Produção Antecipada de Provas. O processo no Tribunal de Justiça de São Paulo teve como propósito impor à concessionária do metrô dever de produzir prova acerca do alcance, finalidade, cautelas e delimitação de banco de dados do sistema, com base na potencial violação de direitos dos usuários (T.J.S.P., 2020). Ainda levou-se em consideração a legislação federal e local sobre a defesa de consumidores e usuários de serviços públicos.

Os autores da ação também questionaram o tratamento de dados dos menores de idade que utilizam o metrô, com base no Estatuto da Criança e do Adolescente (Lei n.º 8.069, Art. 100, V). O direito à privacidade previsto no Estatuto coaduna com as previsões da LGPD, que estabelece que o tratamento de dados de crianças e adolescentes somente poderá ser realizado por meio de consentimento expresso do representante legal (Art. 14, §4º). Nesse sentido, sustentam que o modo de operação previsto para o sistema não faria qualquer distinção

entre crianças e adolescentes e adultos, resultando em grande potencial lesivo (T.J.S.P., 2020).

Por essas e outras razões, os autores da ação concluíram sua petição inicial com o pedido de esclarecimentos, por parte do Metrô, sobre: (i) confiabilidade e eficiência do sistema; (ii) impacto sobre a proteção de dados e todos os seus pormenores, (iii) banco de dados a ser utilizado, (iv) como se obteria consentimento de responsáveis por crianças e adolescentes; (v) como será realizada a anonimização e armazenamento dos dados; (vi) impacto financeiro de eventuais falhas do sistema e a provisão orçamentária para os próximos vinte anos; (vii) governança do banco de dados e o compartilhamento deles; e (viii) motivação pública do procedimento licitatório.

Dos subseqüentes esclarecimentos prestados pela defesa do Metrô, sublinhamos alguns pontos relevantes para a nossa análise. O representante do Metrô alegou que o objetivo principal da contratação seria a modernização do sistema de segurança por monitoramento de câmeras então existente (T.J.S.P., 2020). A defesa afirmou também que a finalidade da coleta e tratamento dos dados seria a “melhoria da qualidade dos serviços”, bem como a promoção da segurança pública e investigação de infrações penais.

Deste modo, o Metrô buscou amparo legal na própria LGPD, cuja aplicação é afastada no uso de dados feito exclusivamente para fins de segurança pública e de investigação de infrações penais (Art. 4º, III). A defesa ignorou a argumentação dos autores da ação sobre a baixa confiabilidade de sistemas similares, em especial quanto a questões raciais e de gênero. Nesse sentido, destacamos o estudo realizado por Lynch (2018), no qual concluiu que sistemas de reconhecimento facial tendem a ser mais precisos na identificação de homens brancos.

Com a manifestação da defesa, que não juntou aos autos os relatórios requeridos, os autores da ação solicitaram o arquivamento do processo. Isto não significa, todavia, um fracasso desta tentativa de intervenção, como pareceria à primeira vista: deve-se lembrar que a ação tinha como objeto apenas a obtenção de tais provas. A ausência delas, de modo quase irônico, serve como comprovação dos argumentos da petição inicial: a implementação do sistema de vigilância ocorreria de modo inconsequente e despreocupado com suas repercussões em direitos fundamentais.

É possível encontrar outros exemplos desse recorrente descaso com a segurança dos dados armazenados. Em novembro de 2019, uma vulnerabilidade extremamente trivial no site da concessionária ViaQuatro – apresentada no primeiro caso judicial abordado acima – levou ao vazamento de dados pessoais de milhares de usuários dos bicicletários das estações de metrô de São Paulo (Demartini, 2019).

3.3. Capitalismo de vigilância e tutelas jurídicas da privacidade: alguns apontamentos

Na prática, mesmo que tenhamos leis de privacidade, elas não se mostram suficientes para lidar, por si só, com os problemas atuais. Nesse sentido, Zuboff (2020b)

compreende que o vazio deixado pela falta de renovação dos paradigmas jurídicos ameaça a manutenção de padrões de respeito à privacidade, uma vez que é o capitalismo de vigilância que na sua própria velocidade refaz a sociedade.

A aposta da autora é na perspectiva da coletivização do Direito e na aliança entre legisladores e cidadãos engajados no questionamento do capitalismo de vigilância (Zuboff, 2020a). Mas importa compreendermos que não há fronteiras para o capitalismo de vigilância e que nem mesmo o Direito passa imune: é também contaminado, imprimindo o seu valor em leis e manifestações judiciais (Brown, 2017).

Vários desafios são trazidos à seara jurídica pelo avanço das práticas de vigilância. O direito não consegue lidar com a aceleração do desenvolvimento tecnológico, buscando estabilidade e segurança. As normas que versam sobre privacidade e proteção de dados são mormente nacionais ou regionais, ao passo que o fluxo de dados é globalizado; em outros termos, o princípio jurídico da territorialidade é problemático no que tange à privacidade (Weber, 2012). Esses limites encontram, outrossim, outro obstáculo: a dificuldade de legislar sobre a matéria, pois normas com teor técnico, ou especializadas demais, podem tornar-se obsoletas rapidamente com a ascensão de novas tecnologias, enquanto normas abstratas demais podem configurar um empecilho para a efetivação destes novos direitos.

Em que pesem tais constatações, reforçamos que é fundamental reconhecer que a tutela jurídica da privacidade e da proteção de dados pessoais precisa ser aprofundada. Boehme-Neßler (2016) afirma que o objetivo da proteção jurídica de dados pessoais é assegurar a dignidade humana e o livre desenvolvimento da personalidade, dado que a privacidade mostra-se uma necessidade antropológica e psicológica. Ele assegura que a incerteza de uma pessoa em relação ao que outros sabem sobre ela configura um limite à sua autonomia: a sensação de ser sempre vigiado é uma forma de embotar a formação de opinião e de pensamento.

As teorizações de Deleuze sobre a sociedade de controle e as de Foucault sobre a biopolítica evidenciam a complexidade do terreno sobre o qual se dá o debate sobre a vigilância em escala populacional e são substrato interessante para a enfrentar essas questões e compreender de que modo os elementos sociais como um todo, nos quais o direito se inclui, encontram-se plasmados por questões econômicas e de controle. A comodificação das partes corporais digitalizadas como fonte de lucro e objeto de segurança pública são a concretização disso. Por isso, somente um olhar crítico sobre a privacidade nos permitiria perceber que ela, nos seus moldes tradicionais, está sitiada entre os interesses de Estado e a lógica do mercado (Gediel; Corrêa, 2008).

4. Considerações finais

A identificação por meio do uso de dados biométricos, certamente, teve uma transformação impressiva nas últimas décadas, especialmente, sob a perspectiva do de-

envolvimento tecnológico. A percepção de que se trata de um método capaz de reconhecer pessoas em massa se confirmou; porém, a sua confiabilidade vem sendo colocada em cheque em razão das falhas a que esses sistemas são suscetíveis, o que pode produzir danos a direitos fundamentais e personalíssimos.

Entendemos que a opção pelo uso da biometria como elemento identificador dos seres humanos é expressão da transformação de algo que era íntimo e se tornou étimo; o que era de cada ser – as medidas do seu próprio corpo –, agora é do mundo. Esse processo só foi possível em razão de um determinado fim aplicado às novas tecnologias e demonstra que é fundamental politizar os corpos da biometria. O que buscamos fazer com a inserção do debate sobre a *surveillance* e com o resgate muito sucinto de conceitos trabalhados por Michel Foucault, como biopolítica, dispositivo de segurança, governamentalidade neoliberal, e de Gilles Deleuze, como a sociedade de controle. Além disso, procuramos atualizar esses pontos e conceitos com a indicação de autores mais contemporâneos, mas que trabalham a partir desse mesmo marco teórico.

A partir disso, buscou-se aproximar essa questão do campo jurídico, por meio da apresentação de duas ações judiciais movidas contra a instalação de sistemas de reconhecimento facial no metrô de São Paulo. Tomamos essa situação como exemplar não apenas por ser voltada para o monitoramento da população, mas também por estar alinhada com lógicas de mercado e segurança pública. Daí a importância do resgate da razão presente na governamentalidade neoliberal apresentada por Rouvroy e Berns como ‘governamentalidade algorítmica’, que se aproxima, em alguma medida, daquilo que Zuboff denomina ‘capitalismo de vigilância’.

Como apontado previamente, o direito tem dificuldade em acompanhar a aceleração tecnológica, e o princípio da territorialidade é um empecilho para a eficácia da regulação nacional de fenômenos crescentemente globais. Percebem-se, todavia, alguns casos que podem inspirar novas iniciativas legislativas: a cidade de San Francisco, por exemplo, foi a primeira nos Estados Unidos a aprovar uma lei banindo em seu território as tecnologias de reconhecimento facial (Conger, 2019). No caso brasileiro, os esforços dos legisladores não parecem andar em tal caminho, e o país tem ainda como um obstáculo a demora para a entrada em vigor da Lei Geral de Proteção de Dados.

As situações que motivaram essas e outras ações judiciais escancaram a conexão entre vigilância, capitalismo e controle. A análise dos casos demonstra que os instrumentos jurídicos de tutela à privacidade, conquanto não bastantes como ferramenta única de combate à vigilância, servem como importante forma de contestação e garantia de direitos. Neste sentido, a proteção jurídica dos dados pessoais almeja a tutela de direitos fundamentais e personalíssimos, partindo do ponto de vista segundo o qual a privacidade é uma necessidade psicológica e antropológica. A via jurídica não exclui, portanto, outras formas de resistência e ativismo contra as atividades de vigilância, mas configura um importante meio para que esse debate se insira nas instituições.

5. Referências

- Aas, K. F. (2006). 'The body does not lie': Identity, risk and trust in technoculture. *Crime, media, culture*, 2(2), 143-158. <https://doi.org/10.1177/1741659006065401>.
- Assange, J. (2013). *Cyberpunks: liberdade e o futuro da internet*. São Paulo: Boitempo Editorial.
- Boehme-Neßler, V. (2016). Privacy: a matter of democracy. Why democracy needs privacy and data protection. *International Data Privacy Law*, 6(3), 222-229. <https://doi.org/10.1093/idpl/ipw007>.
- Brown, W. (2017). Neoliberalism and the economization of rights. Em *Critical theory in critical times* (P. Deutscher e C. Lafonte, pp. 91-116). Nova York: Columbia University Press. <https://doi.org/10.7312/columbia/9780231181518.003.0005>.
- Cardoso, B. (2018). Estado, tecnologias de segurança e normatividade neoliberal. Em *Tecnopolíticas da vigilância: perspectivas da margem* (F. Bruno, B. Cardoso, M. Kanashiro, L. Guilhon e L. Melgaço, pp. 91-105). São Paulo: Boitempo.
- Carvalho, J. D. (2018). Sistema cibernético e sistema biótico: duas visões da relação entre máquina e organismo. Em *Bioteχνologias e regulações: desafios contemporâneos* (I. Domingues, pp. 91-112). Belo Horizonte: Editora da UFMG.
- Ceyhan, A. (2012). Surveillance as biopower. Em *Routledge Handbook of Surveillance Studies* (K. Ball, K. D. Haggerty, D. Lyon, pp. 38-45). Nova York: Routledge.
- Companhia do Metropolitan de São Paulo (2020, 6 fevereiro). *Parecer JUC/CLN nº 097/2020*. Recuperado de <https://bit.ly/2Cm1sK8>.
- Conger, K. (2019, 14 maio). San Francisco bans facial recognition technology. *The New York Times*. Recuperado de <https://nyti.ms/2VG3Zr9>.
- Corrêa, A. E. (2006). O corpo digitalizado: um novo objeto para o direito. *Revista da Faculdade de Direito UFPR*, 44(1), 77-94. <http://dx.doi.org/10.5380/rfdufr.v44i0.9416>.
- Corrêa, A. E. (2010). *O corpo digitalizado: bancos de dados genéticos e sua regulação jurídica*. Florianópolis: Conceito Editorial.
- Corrêa, A. E. (2019, 18 fevereiro). Lei de proteção de dados e a identificação nacional: há antinomias? *ARPEN Brasil*. Recuperado de <http://www.arpenbrasil.org.br/artigo.php?id=318>.
- Crary, J. (2014). *24/7: capitalismo e os fins do sono*. São Paulo: Cosac Naify.
- Day, D. (2015). Biometric Applications: Overview. Em *Encyclopedia of Biometrics* (S. Z. Li e A. K. Jain, pp. 169-174). Boston: Springer. https://doi.org/10.1007/978-1-4899-7488-4_20.
- Deleuze, G. (1992). *Conversações*. Rio de Janeiro: Editora 34.
- Demartini, F. (2019, 27 novembro). Site da ViaQuatro vaza dados de 10 mil usuários da Linha 4 do Metrô de SP. *Canaltech*. Recuperado de <https://canaltech.com.br/T7AYZ>.
- Díaz, M. (2018). *El Cuerpo como Dato*. Santiago de Chile: Derechos Digitales. Recuperado de https://www.derechosdigitales.org/wp-content/uploads/cuerpo_DATO.pdf.
- Edelman, B. (2009). *Ni chose ni personne: le corps humain en question*. Paris: Hermann Éditeurs.
- Firmino, R. J., Kanashiro, M., Bruno, F., Evangelista, R., e Nascimento, L. (2013). Fear, security, and the spread of CCTV in Brazilian cities: legislation, debate, and the market. *Journal of urban technology*, 20(3), 65-84. <https://doi.org/10.1080/10630732.2013.809221>.
- Foucault, M. (1999). *Vigiar e Punir: nascimento da prisão*. Petrópolis: Vozes.
- Foucault, M. (2004). *Sécurité, Territoire, Population*. Paris: Gallimard.
- Foucault, M. (2005). *Em defesa da sociedade*. São Paulo: Martins Fontes.
- Foucault, M. (2008). *Nascimento da Biopolítica*. São Paulo: Martins Fontes.
- Foucault, M. (2009). *História da Sexualidade* (Vol. 1). São Paulo: Graal.
- Gediel, J. A. P. e Corrêa, A. E. (2008). Proteção jurídica de dados pessoais: a intimidade sitiada entre o estado e o mercado. *Revista da Faculdade de Direito UFPR*, 47(1), 141-153. <http://dx.doi.org/10.5380/rfdufr.v47i0.15738>.
- Haggerty, K. D. (2006). Tear down the walls: on demolishing the panopticon. Em *Theorizing surveillance: the panopticon and beyond* (D. Lyon, pp. 23-45). Cullompton: Willan Publishing.
- Harcourt, B. E. (2014). *Governing, exchanging, securing: Big Data and the production of digital knowledge*. Columbia Public Law Research Paper (14-390). Recuperado de <https://ssrn.com/abstract=2443515>.
- Hull, G. (2015). Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data. *Ethics and Information Technology*, 17(2), 89-101. <https://doi.org/10.2139/ssrn.2533057>.
- Instituto Brasileiro de Defesa do Consumidor. (2018, 31 agosto). *Idec vai à Justiça contra coleta de emoções de usuários do metrô de SP*. Recuperado de <https://idec.org.br/noticia/idec-vai-justica-contra-coleta-de-emocoes-de-usuarios-do-metro-de-sp>.
- Kawaguti, L. (2019, 24 janeiro). Câmera inteligente no RJ terá sistema da Oi, multada por violar privacidade. *UOL Notícias*. Recuperado de <https://noticias.uol.com.br/cotidiano/ultimas-noticias/2019/01/24/cameras-monitoramento-carnaval-rio.htm>.
- Lemos, A. (2013). *Cibercultura: tecnologia e vida social na cultura contemporânea*. Porto Alegre: Sulina.
- Luz, P. H. M. (2018). Disciplina, controle e informação: contribuições para um estudo do panorama societário atual. Em *Propedêutica humanística em foco* (A. G. B. Pozzobon, B. Neves e P. H. M. Luz, pp. 231-253). Porto Alegre: Editora Fi.
- Lyon, D. (2008). Biometrics, identification and surveillance. *Bioethics*, 22(9), 499-508. <https://doi.org/10.1111/j.1467-8519.2008.00697.x>.
- Lynch, J. (2018). *Face Off: law enforcement use of face recognition technology*. San Francisco: Electronic Frontier Foundation. Recuperado de <https://www.eff.org/files/2018/02/15/face-off-report-1b.pdf>.
- Rodotà, S. (2008). *A vida na sociedade da vigilância: a privacidade hoje*. São Paulo: Renovar.
- Ross, A. e Jain, A. K. (2015). Biometrics, Overview. Em *Encyclopedia of Biometrics* (S. Z. Li e A. K. Jain, pp. 289-294). Boston: Springer. https://doi.org/10.1007/978-1-4899-7488-4_182.
- Rouvroy, A. e Berns, T. (2013). Gouvernamentalité algorithmique et perspectives d'émancipation: le disparate comme condition d'individuation par la relation?. *Réseaux*, 177(1), 163-196. <https://doi.org/10.3917/res.177.0163>.
- Rouvroy, A. e Berns, T. (2009). Le corps statistique. *La pensée et les hommes*, 74(1), 173-194.

- Santos, A. (2019, 03 março). Câmeras de reconhecimento facial acham criminoso no Carnaval de Salvador. *UOL Notícias*. Recuperado de <https://noticias.uol.com.br/cotidiano/ultimas-noticias/2019/03/05/cameras-de-reconhecimento-facial-acham-criminoso-no-carnaval-de-salvador.htm>.
- Santos, L. G. (2003). *Politizar as novas tecnologias: o impacto sócio-técnico da informação digital e genética*. São Paulo: Editora 34.
- Sibilia, P. (2019). *O show do eu: a intimidade como espetáculo*. Rio de Janeiro: Nova Fronteira.
- Sistemas de reconhecimento facial crescem no Brasil (2019, 29 março). *Uol Notícias*. Recuperado de <https://www.uol.com.br/tilt/noticias/redacao/2019/03/29/sistemas-de-reconhecimento-facial-crescem-no-brasil.htm>.
- Soprana, P. (2018, 31 agosto). Concessionária é alvo de processo por leitura facial no metrô de SP. *Folha de S. Paulo*. Recuperado de <https://folha.com/3qr14acu>.
- Torrano, M. A. e Barrionuevo, L. (2016). Políticas extractivistas sobre el cuerpo: SIBIOS y el Derecho a a identificación y la privacidad. *Crítica y Resistencias: revista de conflictos sociales latinoamericanos*, 2(1), 127-149.
- T.J.S.P. (2020). *Ação Antecipada de Produção de Provas No. 1006616-14.2020.8.26.0053*. Recuperado de <https://esaj.tjsp.jus.br/>
- T.J.S.P. (2018). *Ação Civil Pública No. 1090663-42.2018.8.26.0100*. Recuperado de <https://esaj.tjsp.jus.br/>.
- Van der Ploeg, I. (2012). The body as data in the age of information. Em *Routledge Handbook of Surveillance Studies* (K. Ball, K. D. Haggerty e D. Lyon, pp. 176-183). New York: Routledge.
- Vicente, J. P. (2016, 27 julho). Como as Olimpíadas ajudaram o Brasil a aumentar seu aparato de vigilância social. *VICE Brasil*. Recuperado de https://www.vice.com/pt_br/article/3dp8wy/como-o-brasil-aprimorou-seu-aparato-de-vigilancia-social-para-as-olimpiadas.
- Weber, R. H. (2012). How Does Privacy Change in the Age of the Internet?. Em *Internet and Surveillance: The Challenges of Web 2.0 and Social Media* (A. Albrechtslund, K. Boersma e C. Fuchs, pp. 273-295). New York: Routledge.
- Zuboff, S. (2020a, 4 maio). Nuovi capitalismi (della sorveglianza). *Formiche*. Recuperado de https://formiche.net/files/2017/07/Formiche158_abbonati.pdf.
- Zuboff, S. (2020b, 24 janeiro), You are now remotely controlled: Surveillance capitalists control the science and the scientists, the secrets and the truth. *The New York Times*. Recuperado de <https://nyti.ms/2sXbT2d>.