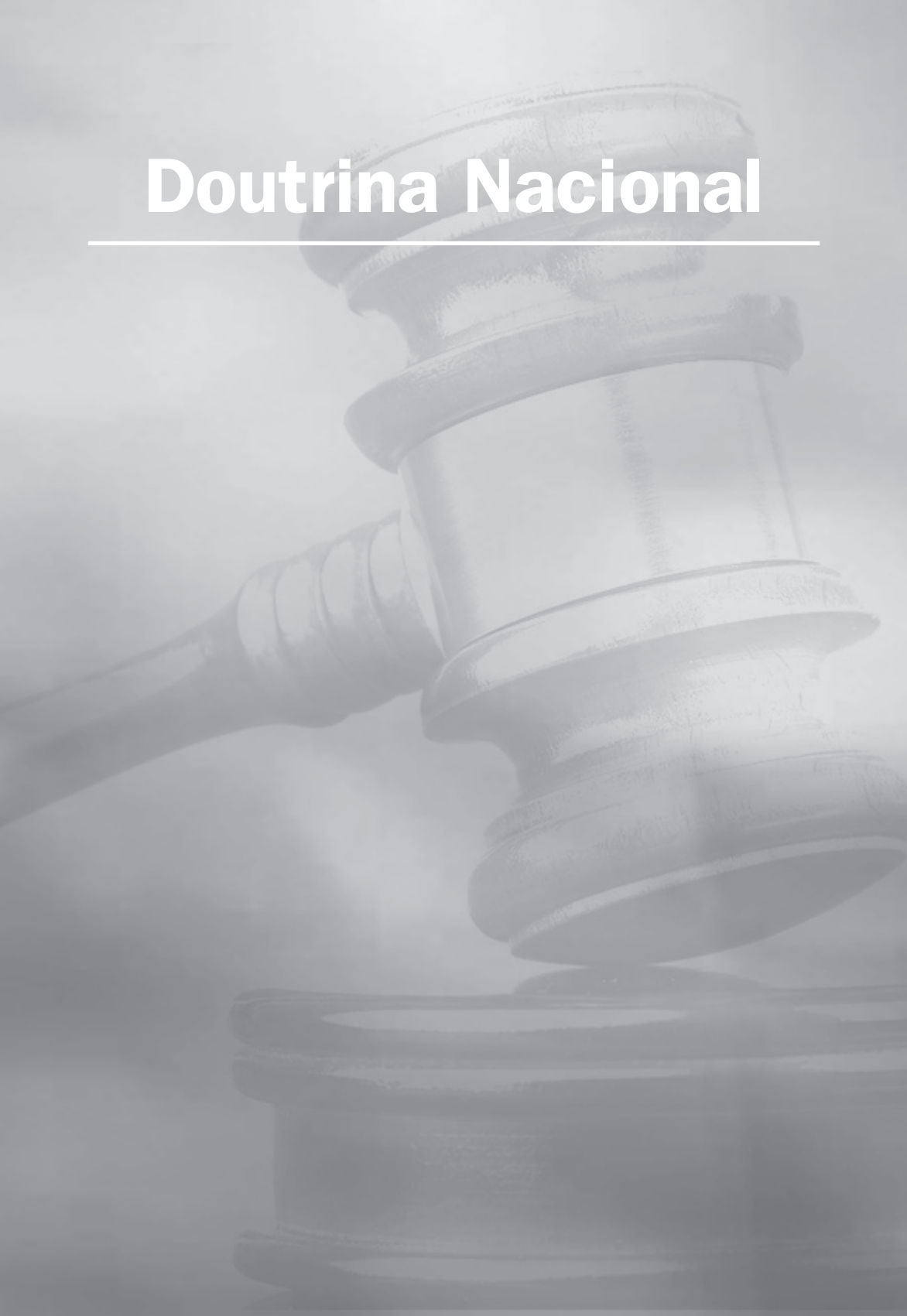
Doutrina Nacional



TECNOLOGIAS DE PERFILAMENTO E DADOS AGREGADOS DE GEOLOCALIZAÇÃO NO COMBATE À COVID-19 NO BRASIL: UMA ANÁLISE DOS RISCOS INDIVIDUAIS E COLETIVOS À LUZ DA LGPD

Diego Carvalho Machado

Mestre e Doutorando em Direito Civil pela Universidade do Estado do Rio de Janeiro – UERJ. *CyberBRICS Scholar*. Foi *Research Fellow* no *Centre for Law, Technology and Society* da Universidade de Ottawa. Pesquisador do Centro de Direito, Internet e Sociedade do IDP (CEDIS/IDP). Professor. Advogado.

Laura Schertel Mendes

Professora Adjunta de Direito Civil da Universidade de Brasília – UnB e do Instituto Brasiliense de Direito Público – IDP. Doutora *summa cum laude* em Direito Privado pela Universidade Humboldt de Berlim, sendo publicada sua tese sobre proteção de dados na Alemanha. Mestre em Direito, Estado e Constituição pela Universidade de Brasília – UnB. Compõe o Conselho Diretor da Associação Luso-Alemã de Juristas – DLJV-Berlim e do Instituto Brasileiro de Política e Direito do Consumidor – Brasilcon. Coordenadora do Centro de Direito, Internet e Sociedade do IDP – CEDIS/IDP.

Resumo: O presente trabalho visa analisar os riscos à privacidade e à proteção de dados pessoais – nas suas dimensões individual e coletiva – gerados pelo perfilamento baseado no uso de dados agregados de geolocalização de dispositivos móveis, buscando investigar a existência de parâmetros normativos encontrados na Lei Geral de Proteção de Dados (LGPD) aplicáveis aos riscos identificados. Para tanto, o artigo propõe as seguintes questões de pesquisa: (i) quais riscos aos direitos fundamentais à privacidade e à proteção de dados pessoais tecnologias de perfilamento baseadas no uso de dados agregados de geolocalização de dispositivos móveis geram nos níveis individual e coletivo na luta contra a pandemia de COVID-19 no Brasil? (ii) a LGPD prevê parâmetros normativos aplicáveis a fim de lidar com esses riscos, em especial a grupos criados a partir de sistemas algorítmicos? Na sociedade orientada por dados, o perfilamento automatizado tem importante função na infraestrutura da informação e da comunicação preponderante da computação preemptiva (*preemptive computing*). Neste contexto, dá-se a afirmação da dimensão coletiva dos direitos à privacidade e à proteção de dados pessoais. Os riscos detectados a ambos direitos, inclusive no âmbito coletivo ou de grupo, são o de reidentificação dos usuários de dispositivos móveis por ataques inferenciais (*membership inference attacks*) e de desvirtuamento de função e finalidade originária do tratamento dos dados. A fim de lidar com tais riscos, sugere-se uma interpretação sistemática de parâmetros normativos da LGPD, que tratam de perfilamento automatizado e de relatório de impacto à proteção de dados pessoais.

Palavras-chave: Perfilamento; dados de geolocalização; COVID-19; riscos individuais e coletivos; privacidade de grupo.

1 Introdução

Países em todo globo enfrentam uma das mais graves emergências sanitárias da humanidade devido à pandemia de COVID-19, causada pelo vírus SARS-CoV-2. A um só tempo, se viu os surtos de contágio se espalharem por toda parte numa impressionante progressão geométrica e o profuso compartilhamento e fluxo de dados em escala internacional sem precedentes.[1] Após as epidemias dos vírus Ebola e Zika entre 2015 e 2016, criou-se certo consenso de que o acesso amplo e rápido de informações[2] durante uma crise de alcance planetário seria essencial para a comunidade de pesquisadores que produz conhecimento científico relevante para orientar a tomada de decisões de governos e autoridades sanitárias no enfrentamento de epidemias. Ao lado disso, contudo, emergem algumas preocupações relacionadas ao respeito a direitos e liberdades – notadamente os direitos à privacidade e à proteção dos dados pessoais – de indivíduos e grupos cujos dados são tratados não apenas por entidades governamentais e pesquisadores, mas também por atores do mercado.

No atual contexto em que a pandemia acentua a relevância do acesso e da circulação de dados, não se deve entender que o direito à proteção dos dados pessoais, bem como o direito à privacidade, sejam obstáculos ao tratamento de informações necessárias para a adoção de ações e políticas de controle epidemiológico pelas autoridades de saúde pública. Como salientado por órgãos como

[1] ROCHA, Roberto. The data-driven pandemic: Information sharing with COVID-19 is 'unprecedented'. *CBC*, 2020. Disponível em: https://www.cbc.ca/news/canada/coronavirus-date-information-sharing-1.5500709. Acesso em: 25 jun. 2020. *Vide* ainda: RIOS, Rafael S.; ZHENG, Kenneth I.; ZHENG, Ming-Hua. Data sharing during COVID-19 pandemic: what to take away. *Expert Review of Gastroenterology & Hepatology*, 2020. Disponível em: https://www.tandfonline.com/doi/full/10.1080/17474124.2020.1815533. Acesso em: 27 ago. 2020; LOTEMPIO, Jonathan *et al*. We Can Do Better: Lessons Learned on Data Sharing in COVID-19 Pandemic Can Inform Future Outbreak Preparedness and Response. *Science & Diplomacy*, v. 9, n. 2, jun. 2020, p. 2-3. Disponível em: https://www.sciencediplomacy.org/article/2020/we-can-do-betterlessons-learned-data-sharing-in-covid-19-pandemic-can-inform-future. Acesso em: 27 ago. 2020.

[2] DYE, Christopher *et al*. Data sharing in public health emergencies: a call to researchers. *Bulletin of the World Health Organization*, v. 94, p. 158, 2016. Disponível em: https://www.who.int/bulletin/volumes/94/3/16-170860.pdf. Acesso em: 25 jun. 2020.

o *European Data Protection Board*[3] e o *Global Privacy Assembly*,[4] não há incompatibilidade entre o interesse público de promoção da saúde coletiva no combate ao novo coronavírus e tais direitos. A exemplo do Regulamento n. 2016/679 (GDPR), da União Europeia, as legislações de proteção de dados de diversos países são suficientemente flexíveis para autorizar o lícito tratamento de dados pessoais no atual cenário,[5] não descuidando, concomitantemente, de indispensáveis garantias e salvaguardas mesmo em face de circunstâncias excepcionais.

Entre os países afetados que possuem regime geral de proteção de dados instituído por lei, o Brasil parece ocupar uma posição peculiar. No país mais populoso da América do Sul e o primeiro a confirmar casos de COVID-19,[6] a lei que regula a atividade de tratamento de dados pessoais (Lei n. 13.709/2018 – LGPD) está, em sua maior parte, em período de *vacatio legis*.[7] A duração deste período, entretanto, foi lançada num baralhado jogo de prorrogações e emendas no efervescente processo legislativo do parlamento nacional durante a instalada situação de emergência sanitária[8]. Tendo em vista outros fatores, como os estágios de

[3] EUROPEAN DATA PROTECTION BOARD. *Statement on the processing of personal data in the context of the COVID-19 outbreak*. Disponível em: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf. Acesso em: 30 jul. 2020.

[4] GLOBAL PRIVACY ASSEMBLY. *GPA COVID-19 Response Repository*. Disponível em: https://globalprivacyassembly.org/covid19/. Acesso em: 30 jul. 2020.

[5] GDPR, art. 6º, 1, *d* e *e*. O considerando n. 46 do regulamento europeu é expresso quanto à licitude, para fins de controle epidemiológico, do tratamento de dados pessoais necessários para proteger interesses vitais do titular ou de terceiro e para realizar atividade desempenhada no interesse público: "The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters" UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 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*, Estrasburgo, 04/05/2016. Disponível em: https://op.europa.eu/s/oe9q. Acesso em: 28 ago. 2020).

[6] CORONAVIRUS in Latin America: What governments are doing to stop the spread. *Global Americans,* 26 mar. 2020. Disponível em: https://theglobalamericans.org/2020/03/coronavirus-in-latin-america/. Acesso em: 30 jul. 2020.

[7] Quando da redação do presente artigo, a LGPD, em sua maior parte, ainda se encontrava em período de *vacatio legis*, isto é, com sua eficácia suspensa. Na data de 26 de agosto de 2020, o Senado votou a Medida Provisória 959/2020, mas com a retirada do texto que postergava a entrada em vigor da LGPD. A referida casa legislativa publicou nota afirmando que a entrada em vigor não é imediata, mas da sanção da Medida Provisória pelo Presidente da República. SENADO FEDERAL. *Nota de esclarecimento – Vigência da LGPD*. Disponível em: https://www12.senado.leg.br/assessoria-de-imprensa/notas/nota-de-esclarecimento-vigencia-da-lgpd. Acesso em: 03 set. 2020.

[8] A respeito desta discussão, confira a seguinte síntese: BELLI, Luca; ZINGALES, Nicolo. *Brazilian Data Protection under Covid-19:* Legal Certainty is the Main Casualty. Disponível em: https://blogdroiteuropeen.

desenvolvimento da pandemia, adiante abordado, e o tempo que será necessário ao desenvolvimento de vacina e imunização da população brasileira, acredita-se provável a entrada em vigor da LGPD em alguma das fases da pandemia causada pelo novo coronavírus.

Para o combate à COVID-19 no Brasil, o uso de dados agregados[9] de geolocalização de usuários de telefones celulares, modelos analíticos e sistemas algorítmicos construídos a partir do tratamento de dados de mobilidade disponibilizados de forma agregada por provedores de serviço de telefonia móvel tem se constituído um dos principais recursos tecnológicos a orientar as políticas de saúde pública adotadas nas diversas esferas de governo. Como se demonstrará oportunamente, haja vista a técnica em que estão alicerçadas as tais formas de tratamento de dados, tem-se, na verdade, o emprego de *tecnologias de perfilamento* para municiar a tomada de decisões em meio à situação emergencial.

Adota-se o seguinte conceito de *perfilamento*:

> Perfilamento é uma técnica de tratamento (parcialmente) automatizado de dados pessoais e/ou não pessoais, que visa a produção de conhecimento por meio da inferência de correlações de dados na forma de perfis que podem ser posteriormente aplicados como base para a tomada de decisão.
>
> Um perfil é um conjunto de dados correlacionados que representa um sujeito (individual ou coletivo).
>
> A construção de perfis é o processo de descoberta de padrões desconhecidos entre dados em grandes bases de dados que podem ser usados para criar perfis. A aplicação de perfis é o processo de identificação e representação de um indivíduo ou grupo específico como

com/2020/07/03/brazilian-data-protection-under-covid-19-legal-certainty-is-the-main-casualty-by-luca-belli-and-nicolo-zingales/. Acesso em: 23 jul. 2020.

9 Define-se agregação de dados, de acordo com o extinto Grupo de Trabalho do Artigo 29, da seguinte maneira: "Aggregation and K-anonymity techniques aim to prevent a data subject from being singled out by grouping them with, at least, k other individuals. To achieve this, the attribute values are generalized to an extent such that each individual shares the same value. For example, by lowering the granularity of a location from a city to a country a higher number of data subjects are included. Individual dates of birth can be generalized into a range of dates, or grouped by month or year. Other numerical attributes (e.g. salaries, weight, height, or the dose of a medicine) can be generalized by interval values (*e.g.* salary €20,000 – €30,000). These methods may be used when the correlation of punctual values of attributes may create quasi-identifiers" (ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 5/2014 on Anonymisation techniques. Bruxelas: [s.n.], 2014. p. 16. Disponível em: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Acesso em: 28 jul. 2020).

> adequado a um perfil, e de tomada de alguma forma de decisão com base nessa identificação ou representação.[10]

Diante dos usos de tais tecnologias no contexto brasileiro, o presente trabalho tem por objetivos (i) analisar os riscos impostos aos direitos à proteção de dados pessoais e à privacidade, nas dimensões individual e coletiva, e (ii) investigar a existência de parâmetros normativos encontrados na LGPD aplicáveis aos riscos identificados. Para tanto, propõe-se as seguintes questões de pesquisa: (i) quais riscos aos direitos fundamentais à privacidade e à proteção de dados pessoais tecnologias de perfilamento baseadas no uso de dados agregados de geolocalização de dispositivos móveis geram nos níveis individual e coletivo na luta contra a pandemia de COVID-19 no Brasil?; (ii) A LGPD prevê parâmetros normativos aplicáveis a fim de lidar com esses riscos, em especial a grupos criados a partir de sistemas algorítmicos?

O artigo está estruturado em três partes. Primeiramente, será discutido por que os dados de localização e mobilidade são úteis para a definição de políticas e tomada de decisão por autoridades sanitárias para enfrentar a disseminação do vírus SARS-CoV-2, e as tecnologias de perfilamento utilizadas no Brasil. Em seguida, a segunda parte cuida de distinguir os direitos à proteção de dados pessoais e à privacidade, ressaltando não apenas as ameaças que o perfilamento automatizado gera a tais direitos, como também a dimensão coletiva de ambos. Por fim, a terceira parte é destinada a identificar os riscos ensejados por tecnologias de perfilamento que processam dados agregados de geolocalização, e analisar os possíveis parâmetros normativos da LGPD a essas operações de tratamento no cenário brasileiro.

[10] BOSCO, Francesca *et al*. Profiling technologies and fundamental rights: an introduction. *In*: CREEMERS, Niklas *et al*. *Profiling Technologies in Practice:* Applications and Impact on Fundamental Rights and Values. Oisterwijk: Wolf Legal Publishers, 2017. p. 9. Tradução livre de: "Profiling is a technique of (partly) automated processing of personal and/or non-personal data, aimed at producing knowledge by inferring correlations from data in the form of profiles that can subsequently be applied as a basis for decision-making.

A profile is a set of correlated data that represents a (individual or collective) subject.

Constructing profiles is the process of discovering unknown patterns between data in large data sets that can be used to create profiles. Applying profiles is the process of identifying and representing a specific individual or group as fitting a profile and of taking some form of decision based on this identification or representation". *Vide* também: HILDEBRANDT, Mireille. Defining Profiling: A New Type of Knowledge? *In*: GUTWIRTH, Serge; HILDEBRANDT, Mireille (Ed.). *Profiling the European Citizen*. New York: Springer, 2008. p. 17-45.

2 Tratamento de dados de localização e tecnologias de perfilamento durante a pandemia de COVID-19 no Brasil

A coleta de dados de geolocalização de telefones celulares e seu uso como *proxy* para analisar a mobilidade dos usuários se tornou bastante difundida,[11] notadamente com o surgimento dos *smartphones* e inúmeros aplicativos móveis.[12] Trata-se de dados que "contêm a localização aproximada de indivíduos e pode ser usada para reconstruir os movimentos das pessoas no espaço e no tempo".[13] Ao campo da epidemiologia isso não passou despercebido. Ao contrário, há pesquisadores que professam a importância dos dados de aparelhos celulares (e outros *proxies* de localização) para elaboração de modelos epidemiológicos, os quais dependem, segundo afirmam, da captura precisa dos movimentos populacionais para entender e reproduzir a propagação no espaço de uma epidemia de doença infectocontagiosa.[14] Quais dados de localização e de processos de mobilidade são relevantes, no entanto, é resposta que se obtém a partir do tipo de doença objeto de estudo.

De acordo com Michele Tizzoni e outros, "[p]ara infecções direta e rapidamente transmitidas, a movimentação de indivíduos representa o principal meio de transmissão espacial".[15] Constatado que a COVID-19 tem essas mesmas características de contágio rápido e direto entre pessoas,[16] o emprego de dados sobre a localização de dispositivos de telefonia móvel para conhecer padrões de mobilidade de indivíduos e grupos é proposto por um grupo de pesquisadores de diversos países. Para eles, é crítico o acesso a esses dados durante todo o ciclo de vida da pandemia para a tomada de decisões em matéria de saúde pública e avaliação das intervenções.[17] Perquirindo sobre o valor e contribuição dos

[11] Para uma melhor compreensão os dados de geolocalização, as formas de coleta e quem os acessa, *vide*: GRAY, Stacey. A Closer Look at Location Data: Privacy and Pandemics. *Future of Privacy Forum*, 2020. Disponível em: https://fpf.org/2020/03/25/a-closer-look-at-location-data-privacy-and-pandemics/. Acesso em: 20 abr. 2020.

[12] DE MONTJOYE, Yves-Alexandre *et al*. Unique in the Crowd: The privacy bounds of human mobility. *Scientific Reports*, v. 3, p. 1-5, 2013, p. 1.

[13] DE MONTJOYE, Yves-Alexandre *et al*. *Op. cit.*, p. 1. Tradução livre de: "contains the approximate whereabouts of individuals and can be used to reconstruct individuals' movements across space and time".

[14] TIZZONI, Michele *et al*. On the Use of Human Mobility Proxies for Modeling Epidemics. *PLoS Computational Biology*, v. 10, n. 7, p. 1-15, jul. 2014, p. 1.

[15] TIZZONI, Michele *et al*. *Op. cit.*, p. 1. Tradução livre de: "[f]or rapid directly transmitted infections, daily movements of individuals represent the main mean of spatial transmission".

[16] WORLD HEALTH ORGANIZATION. *Q & A: How is COVID-19 transmitted?* Disponível em: https://www.who.int/news-room/q-a-detail/q-a-how-is-covid-19-transmitted. Acesso em: 25 jul. 2020.

[17] "Decision-making and evaluation or such interventions during all stages of the pandemic life cycle require specific, reliable, and timely data not only about infections but also about human behavior, especially mobility and physical copresence. We argue that mobile phone data, when used properly and carefully,

dados móveis para os esforços analíticos voltados ao controle da pandemia de COVID-19, os pesquisadores argumentam que existem quatro áreas em que o uso desses dados pelas autoridades de saúde pública é relevante.

Inicialmente, importa ventilar questões de conscientização situacional a fim de promover melhor compreensão da dinamicidade do ambiente da pandemia. Os dados de telefones celulares são potencialmente úteis para fornecer estimativas populacionais anteriormente indisponíveis e informações de mobilidade para que os entes envolvidos em todos os setores entendam melhor as tendências e distribuição geográfica das infecções de SARS-CoV-2. Em segundo lugar, as questões sobre causa e efeito direcionam à identificação dos principais mecanismos e resultados da implementação de diferentes medidas para conter a propagação do COVID-19. São perguntas cujas respostas visam estabelecer quais variáveis fazem diferença para um problema e se outros problemas podem ser causados. Em terceiro lugar, a análise preditiva se propõe a delimitar a probabilidade de resultados futuros e pode, por exemplo, aproveitar a contagem e dados quantitativos de grupos populacionais em tempo real e dados de mobilidade para habilitar recursos preditivos e permitir a avaliação de riscos, necessidades e oportunidades futuras. Por fim, tem-se as avaliações de impacto, que visam determinar quais, se e como as várias intervenções afetam a disseminação do COVID-19. Para tanto, dados são necessários para identificar seja os obstáculos que impedem a realização de certos objetivos, seja o êxito de intervenções específicas.[18]

As formas e utilidades da análise de dados de mobilidade são direcionadas e adequadas conforme as fases da pandemia, as quais totalizam seis: (i) investigação, (ii) reconhecimento, (iii) iniciação, (iv) aceleração, (v) desaceleração e (vi) preparação. Durante a fase de aceleração, o grupo de pesquisadores defende que dados agregados de localização de dispositivos móveis são importantes para

represents a critical arsenal of tools for supporting public health actions across early-, middle-, and late-stage phases of the COVID-19 pandemic" (OLIVER, Nuria *et al*. Mobile phone data for informing public health actions across the COVID-19 pandemic life cycle. *Science Advances*, v. 6, n. 23, p. 1–7, 2020, p. 1). Em estudo sobre o uso de tecnologias digitais, analítica de dados e dados de telefones celulares durante a epidemia de Ebola no oeste do continente africano, Sean McDonald colocou em dúvida utilidade desses dados para melhora da resposta dos sistemas de saúde pública: "The assumption that open and interoperable data will lead to better health response is untested, as is the assumption that mobile network data records measurably improve health system response efforts. There are fewer questions about whether access to large datasets that are typically subject to commercial, privacy, and governmental restriction, is valuable. Opening health information systems and mobile network data implicitly reduces dependence and decentralizes response capacity – which may improve outcomes, but it may also substantially complicate the already significant challenges involved in creating a coordinated, cohesive response" (MCDONALD, Sean M. Ebola: A Big Data Disaster - Privacy, Property, and the Law of Disaster Experimentation. *The Centre for Internet and Society*, n. 2016.01, 2016. p. 12).

[18] OLIVER, Nuria *et al*. Mobile phone data for informing public health actions across the COVID-19 pandemic life cycle. *Science Advances*, v. 6, n. 23, p. 1-7, 2020, p. 1-2.

avaliar a eficácia das políticas adotadas mediante o monitoramento da mobilidade entre as cidades e regiões afetadas, bem como para construir acurados modelos epidemiológicos capazes de explicar e antecipar a disseminação da doença.[19] Já nas fases de desaceleração e preparação, por sua vez, o continuado acompanhamento da situação epidêmica é crucial para lidar com as novas ondas de contágio do novo coronavírus. Para isso, mapas de mobilidade em tempo real e mapas de calor serão relevantes para a compreensão de como a suspensão e o restabelecimento de várias medidas adotadas se traduzem em comportamentos dos cidadãos, especialmente a fim de encontrar a combinação ótima de medidas no momento certo e para equilibrar essas restrições com ações de retomada de atividades econômicas.[20] Ainda, com o declínio da curva epidemiológica, sustenta-se que dados de dispositivos móveis serão úteis para testes *post hoc* (post hoc *analysis*) do impacto das intervenções implementadas na progressão da doença e análises de custo-benefício das quarentenas e restrições de locomoção.[21]

Isto posto, percebe-se que modelos analíticos com tratamento de dados de localização agregados, isto é, modelos de mobilidade baseados em estatísticas agregadas[22] têm sido indicados pela comunidade científica como recurso muito importante a auxiliar as autoridades competentes na elaboração e execução de políticas de controle epidemiológico. Em outras palavras, o que se está preconizando é o uso de *tecnologias de perfilamento* com o processamento de dados de localização de usuários de dispositivos móveis para se enfrentar a pandemia em curso.

Perfilamento é, como já visto, uma técnica de tratamento automatizado de dados pessoais e dados não-pessoais, cujo objetivo é a produção de conhecimento mediante a inferência de correlações de dados na forma de perfis, os quais, ao ser aplicados, servem de lastro para a tomada de decisão. Os modelos analíticos de mobilidade que usam dados agregados de geolocalização são fundados nessa técnica, construídos a partir da extração de perfis de grupo com seus padrões de deslocamento por algoritmos de mineração de dados[23] para ulterior aplicação e tomada de decisão.

---

19 OLIVER, Nuria *et al*. *Op. cit.*, p. 2.

20 OLIVER, Nuria *et al*. *Op. cit.*, p. 2.

21 OLIVER, Nuria *et al*. *Op. cit.*, p. 2.

22 Pesquisa na área da ciência da computação aponta para a viabilidade e eficiência desses modelos: PYRGELIS, A.; DE CRISTOFARO, E.; ROSS, G. J. Privacy-friendly mobility analytics using aggregate location data. *GIS: Proceedings of the ACM International Symposium on Advances in Geographic Information Systems*, n. 1, 2016. Disponível em: https://arxiv.org/pdf/1609.06582.pdf. Acesso em: 27 jul. 2020.

23 A mineração de dados (*data mining*) é, no contexto do perfilamento, um dos passos do "descobrimento de conhecimento em base de dados" (*knowledge discovery in databases* – KDD), sendo este definido como "the non-trivial process of identifying valid, novel, potentially useful, and ultimately understandable patterns in data". Pode-se entender a mineração de dados como "a step in the KDD process consisting of

No Brasil, as principais tecnologias de dados utilizadas pelas autoridades públicas e sanitárias baseiam-se em técnicas de perfilamento e tratamento de dados de mobilidade. Nesta direção, para a mensuração de cumprimento de políticas de isolamento/distanciamento social, provedores de telefonia celular criaram mapas de calor e índice de isolamento social a fim de auxiliar governos municipais, estaduais e federal na estruturação de suas estratégias.[24] Há que se ressaltar que a divulgação e tratamento de dados agregados de localização de usuários de telefone celular tem fundamento legal no art. 72, §2º, da Lei n. 9.472, de 16 de julho de 1997 (Lei Geral de Telecomunicações).[25] Surgiram também algumas propostas de modelos para previsão de novos focos de transmissão do vírus no território brasileiro, consideradas diferentes regiões e populações.[26]

3 Tecnologias de perfilamento e possíveis ameaças aos direitos à privacidade e à proteção de dados pessoais

Antes de cuidar dos específicos riscos originados do tratamento de dados agregados de localização por tecnologias de perfilamento empregadas no contexto de emergência sanitária, importa compreender e diferenciar as noções de privacidade e de proteção de dados pessoais e o que se tutela em cada um desses direitos. Conforme se sustenta neste trabalho, são dois direitos autônomos, apesar das interseções existentes entre um e outro. A bem da verdade, não é nova a discussão doutrinária sobre a discriminação de ambas ideias, fruto de um longo processo de clivagem conceitual.[27] Considerado, todavia, o cenário jurídico brasileiro atual, a importância do entendimento e afirmação da autonomia dogmática

applying data analysis and discovery algorithms that, under acceptable computational efficiency limitations, produce a particular enumeration of patterns over the data" (FAYYAD, U.; PIATETSKY-SHAPIRO, G.; SMYTH, P. Knowledge Discovery and Data Mining: Towards a Unifying Framework. *KDD-96 Proceedings*, p. 82-88, 1997, p. 83).

[24] CONVERGÊNCIA DIGITAL. *Dispara número de estados e municípios que usam dados celulares na Covid-19*. Disponível em: https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=53617&sid=8. Acesso em: 29 jul. 2020.

[25] O art. 72, §2º, da Lei Geral de Telecomunicações dispõe: "A prestadora poderá divulgar a terceiros informações agregadas sobre o uso de seus serviços, desde que elas não permitam a identificação, direta ou indireta, do usuário, ou a violação de sua intimidade".

[26] Entre as iniciativas encontra-se: GRUPO MAVE. *Previsão de curto prazo nos estados brasileiros*. Disponível em: https://covid-19.procc.fiocruz.br/prediction/. Acesso em: 28 jul. 2020; PEIXOTO, Pedro S. *et al*. Potential dissemination of epidemics based on Brazilian mobile geolocation data. Part I: Population dynamics and future spreading of infection in the states of São Paulo and Rio de Janeiro during the pandemic of COVID-19. *medRxiv*, April, 2020. Disponível em: https://www.medrxiv.org/content/10.1101/2020.04.07.20056739v1.full.pdf. Acesso em 28 jul. 2020 [artigo não submetido à revisão por pares].

[27] Cf. FUSTER, Gloria González. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Londres-Heildelberg-Nova Iorque: Springer, 2014.

de ambos direitos foi recentemente destacada em pronunciamentos judiciais do Supremo Tribunal Federal, que, em sede de jurisdição constitucional, versaram sobre o tema.

Em razão da propositura das Ações Diretas de Inconstitucionalidade n. 6387, 6388, 6389, 6390 e 6393, em face da Medida Provisória 954/2020, a Suprema Corte teve, pela primeira vez, a oportunidade de se manifestar sobre o direito fundamental à proteção de dados pessoais e a autonomia de sua tutela constitucional no sistema jurídico nacional. No ensejo da apreciação plenária das ações constitucionais, em seu voto o Ministro Gilmar Mendes consignou que o julgamento suscitara:

> [...] a oportunidade e o dever de o Supremo Tribunal Federal aprofundar a identificação, na ordem constitucional brasileira, de um direito fundamental à proteção de dados pessoais, a fim de estabelecer de forma clara o âmbito de proteção e os limites constitucionais à intervenção estatal sobre essa garantia individual.[28]

O tema foi igualmente abordado na Ação de Descumprimento de Preceito Fundamental n. 695, em que se discute a constitucionalidade do compartilhamento de dados dos mais de 76 milhões de brasileiros que possuem Carteira Nacional de Habilitação (CNH) pelo Serviço Federal de Processamento de Dados com a Agência Brasileira de Inteligência. Uma vez mais terá a Corte Suprema ocasião para apreciar a temática da proteção de dados pessoais tendo por pano de fundo a atividade de tratamento de dados pelo poder público.

Além da distinção conceitual, com significativas repercussões de cunho dogmático, há que se identificar as possíveis ameaças que o perfilamento automatizado gera a ambos direitos fundamentais na sociedade orientada por dados. Como será visto, as invisibilidades da computação preemptiva[29] (*preemptive computing*) e as decisões tomadas de forma automatizada com base em tecnologias de perfilamento dão ensejo a desafios de ordem individual e coletiva, o que dá novos matizes para a afirmação da dimensão coletiva da proteção de dados, da ideia de "privacidade de grupo" (*group privacy*) e sua proteção jurídica. Somente com a compreensão das ameaças possíveis aos direitos à privacidade e à proteção de

[28] BRASIL. Supremo Tribunal Federal (Tribunal Pleno). *Ações Diretas de Inconstitucionalidade n. 6387, 6388, 6389, 6390 e 6393/DF*. Relatora: Ministra Rosa Weber, 07 de maio de 2020.

[29] "Um tipo de computação que combina análise preditiva com intervenções computacionais destinadas a substituir a ação humana, atendê-la ou anulá-la antes que o humano tenha a chance de formar uma intenção consciente" (HILDEBRANDT, Mireille. *Smart Technologies and The End(s) of Law*. Cheltenham-Northampton: Edward Elgar, 2015. p. 263).

dados pessoais, é que se pode, então, passar ao nível mais concreto da apreciação de riscos do uso de tecnologias de perfilamento com dados de geolocalização para fazer frente à pandemia do novo coronavírus no Brasil.

3.1 Sobre privacidade e proteção de dados pessoais: diferenciando dois conceitos

No marco do Estado de Direito e no curso do desenvolvimento dos seus modelos orientados à limitação e legitimação do poder, o Estado Democrático de Direito se caracteriza como aquele que se empenha em assegurar aos seus cidadãos o exercício efetivo dos direitos e liberdades fundamentais, independentemente da dimensão ou natureza destes, se civis, políticos, econômicos, sociais ou culturais.[30] Para esse fim, elaborou-se nos quadrantes das democracias constitucionais, segundo Serge Gutwirth e Paul De Hert, dois tipos de instrumentos jurídicos que são complementares entre si e funcionalizados pelos mesmos fins de "controle e limitação do poder":[31] instrumentos de opacidade e instrumentos de transparência.

Em síntese, os instrumentos de opacidade desempenham importante papel na proteção dos indivíduos contra a interferência estatal e de entes privados em sua esfera de liberdade pessoal e autonomia.[32] Já os instrumentos de transparência, por sua vez, consistem em mecanismos que limitam o poder mediante formas de controle exercidas pelos próprios cidadãos, entes coletivos e inclusive outros órgãos estatais; estes instrumentos têm em comum a busca pela garantia de transparência na tomada de decisão governamental e de atores privados, sendo este um verdadeiro pressuposto para a governança responsável.[33] Defendem

[30] MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo G. *Curso de direito constitucional*. 3. ed. São Paulo: Saraiva, 2008. p. 149.

[31] DE HERT, Paul; GUTWIRTH, Serge. Privacy, data protection and law enforcement: opacity of the individual and transparency of power. *In*: CLAES, Erik; GUTWIRTH, Serge; DUFF, Antony (Org.). *Privacy and the Criminal Law*. Antwerpen-Oxford: Intersentia, 2006. p. 66. *Vide* também: DE HERT, Paul; GUTWIRTH, Serge. Regulating Profiling in a Democratic Constitutional State. *In*: HILDEBRANDT, Mireille; GUTWIRTH, Serge (Ed.). *Profiling the European Citizen:* Cross-disciplinary Perspectives. [S.l.]: Springer, 2008. p. 275 *et seq*.

[32] DE HERT, Paul; GUTWIRTH, Serge. Privacy, data protection and law enforcement: opacity of the individual and transparency of power. *In*: CLAES, Erik; GUTWIRTH, Serge; DUFF, Antony (Org.). *Privacy and the Criminal Law*. Antwerpen-Oxford: Intersentia, 2006. p. 67-69.

[33] DE HERT, Paul; GUTWIRTH, Serge. *Op. cit.*, p. 69-70. Os autores destacam as diferenças entre os dois tipos de instrumentos: "The tools of opacity are quite different in nature from the tools of transparency. Opacity tools embody normative choices about the limits of power; transparency tools come into play after these normative choices have been made in order still to channel the normatively accepted exercise of power. While the latter are thus directed toward the control and channelling of legitimate uses of power, the former are protecting the citizens against illegitimate and excessive uses of power. The latter do take into account that the temptations of abuse of power are huge, and empower citizens and whatchdogs to

os autores que as leis e regulações de proteção de dados pessoais consiste, majoritariamente, em instrumentos de transparência, enquanto a tutela da privacidade, de outro lado, pertence aos instrumentos de opacidade.[34] Ou seja, por este ângulo, o direito à proteção de dados pessoais e suas estruturas regulatórias se vale, especialmente, de instrumentos de transparência para controle do exercício de atividade lícita (de tratamento de dados pessoais) que, devido a existência de assimetrias de poder, deve ser fiscalizada – pelos próprios titulares dos dados e outras entidades – para se coibir abusos. De outro lado, também num contexto de relações de poder, o direito à privacidade e sua disciplina se moldam, preponderantemente, como anteparo contra interferências adversas sobre sua liberdade e autonomia e meio que possibilita a construção da identidade pessoal.[35]

A distinção acima adota, segundo Lorenzo Dalla Corte, um critério teleológico para estremar privacidade e proteção de dados pessoais.[36] Contudo, além deste, há parcela da doutrina que utiliza o critério da natureza ou perfil do direito para traçar linha distintiva entre ambos conceitos, sendo o primeiro de natureza substantiva e o segundo de perfil procedimental. De acordo com Lorenzo Dalla Corte, os direitos substantivos são criados para proteger e defender interesses considerados importantes, enquanto os direitos de caráter procedimental aparecem em um estágio posterior, estabelecendo as condições mediante as quais esses direitos substantivos são implementados.[37] Tendo em vista que a proteção de dados pessoais tem por *télos* que a inspira proteger as pessoas contra injustificado e abusivo de tratamento e circulação de aspectos de sua personalidade,[38] aponta-se ter esse direito um caráter prevalentemente procedimental, em que prescreve-se procedimentos e métodos a ser observados durante todo o ciclo de vida da informação pessoal. Tais procedimentos e formas, uma vez observados,

have and eye even on the legitimate use of power: they put counter powers into place" (DE HERT, Paul; GUTWIRTH, Serge. *Op. cit.*, p. 70).

[34] DE HERT, Paul; GUTWIRTH, Serge. *Op. cit.*, p. 78.

[35] É importante ressaltar que, na visão dos autores, o direito à privacidade não possui tão somente uma função negativa, como se apenas liberdade negativa fosse; possui também uma função positiva, uma vez que é indispensável para o processo de construção da identidade e participação na vida pública (DE HERT, Paul; GUTWIRTH, Serge. *Op. cit.*, p. 72-73).

[36] CORTE, Lorenzo Dalla. A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection. *In*: HALLINAN, D. *et al*. (Ed.). *Data Protection and Privacy:* Data Protection and Democracy. Oxford: Hart Publishing, 2020. p. 41.

[37] CORTE, Lorenzo Dalla. A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection. *In*: HALLINAN, D. *et al*. (Ed.). *Data Protection and Privacy:* Data Protection and Democracy. Oxford: Hart Publishing, 2020. p. 41. Tradução livre de: "[s]ubstantive rights are created to protect and uphold interests considered important, while procedural rights appear at a later stage, setting the conditions through which those substantive rights are implemented".

[38] ZANFIR, Gabriela. Forgetting About Consent. Why The Focus Should Be On "Suitable Safeguards" in Data Protection Law. *In*: GUTWIRTH, Serge; LEENES, Ronald; DE HERT, Paul. (Ed.). *Reloading Data Protection Law:* Multidisciplinary Insights and Contemporary Challenges. London: Springer, 2008. p. 245.

promovem uma série de direitos e liberdades fundamentais, a exemplo do direito à privacidade – que possui caráter eminentemente substancial.[39] [40] Apesar de o fim último do direito fundamental à proteção de dados pessoais ser a tutela da pessoa humana, esse direito visa garantir a operação de mecanismos indispensáveis à efetiva proteção contra o ilegítimo e injustificado tratamento de dados pessoais. Daí Gabriela Zanfir utilizar a inusual expressão "um direito que protege a proteção",[41] para descrever o perfil procedimental do direito à proteção de dados pessoais.

A este respeito, importa consignar que tanto a doutrina como a legislação mais atual em tema de proteção de dados pessoais chamam a atenção para a relevante função que o instituto das *salvaguardas* recebe no sistema de proteção de dados e na tutela de direitos e liberdades fundamentais. A exprimir o perfil procedimental do direito à proteção de dados, pode se definir salvaguardas como "o conjunto de prerrogativas concedidas ao titular dos dados, para que o próprio objeto procedimental de proteção de dados pessoais seja tutelado".[42] No Regulamento Geral de Proteção de Dados da União Europeia (GDPR)[43] e na Diretiva n. 2016/680 do Parlamento Europeu e do Conselho,[44] há expressa previsão a respeito. Também a LGPD, no ordenamento jurídico nacional, alude às salvaguardas, ainda que de forma tímida, nos arts. 5º, XVII, 38, parágrafo único, 48, §2º, 50, §2º, I, "d".[45]

---

[39] Cf. HERT, Paul De; GUTWIRTH, Serge. Privacy, data protection and law enforcement: opacity of the individual and transparency of power. In: CLAES, Erik; GUTWIRTH, Serge; DUFF, Antony (Orgs.). *Privacy and the Criminal Law*. Antwerpen-Oxford: Intersentia, 2006. p. 77-78; ZANFIR, Gabriela. *Op. cit.*, p. 245-246; QUELLE, Claudia. Privacy, Proceduralism and Self-Regulation in Data Protection Law. *Teoria Critica Della Regolazione Sociale,* v. 1, n. 14, p. 89–106, 2017; CORTE, Lorenzo Dalla. A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection. In: HALLINAN, Dara et al. (Eds.). *Data Protection and Privacy:* Data Protection and Democracy. Oxford: Hart Publishing, 2020. p. 27-58

[40] Nesse sentido, leis de proteção de dados como a GDPR e a LGPD, que instituem a avaliação de impacto de proteção de dados pessoais se voltam à identificação e minoração de riscos a *direitos e liberdades fundamentais*. Sobre o assunto, assim entendeu o extinto Grupo de Trabalho de Proteção de Dados do Artigo 29: "the reference to "the rights and freedoms" of data subjects primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion" (ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*. Bruxelas: [s.n.], 2017. p. 6.

[41] ZANFIR, Gabriela. *Op. cit.*, p. 245.

[42] ZANFIR, Gabriela. *Op. cit.*, p. 246-247. Tradução livre de: "the bundle of prerogatives accorded to the data subject so that the procedural object of protecting personal data is protected itself".

[43] Por exemplo: arts. 6º, 4, "e", 9º, 2, "g" e "i", 22, 2, "b", 3 e 4.

[44] Por exemplo: art. 11, 2. A diretiva em questão é relativa à proteção das pessoas naturais no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados.

[45] O instituto aparece fortemente presente no tema do relatório de impacto à proteção de dados pessoais.

O papel das salvaguardas para a efetivação do direito fundamental à proteção de dados pessoais encontra suas bases em pelo menos três razões, para além da natureza preponderantemente procedimental do direito. Em primeiro lugar, o direito à proteção de dados pessoais não tem por característica ser proibitivo, isto é, ele não proíbe, por padrão, a circulação de informações pessoais e a atividade de tratamento de dados[46] – o que seria decerto irreal no atual contexto da economia digital. Em segundo lugar, com o ocaso da centralidade do tradicional modelo calcado no consentimento do titular (*notice and consent*) como o pilar da proteção de dados pessoais,[47] as salvaguardas apropriadas se tornam, nas palavras de Gabriela Zanfir, a nova "pedra angular"[48] da proteção de dados pessoais. A terceira razão se encontra no fato de a disciplina da proteção de dados, no Brasil inclusive, ser voltada à proteção das pessoas naturais contra riscos a direitos fundamentais gerados pela atividade de tratamento de informação pessoal. Em não podendo se eliminar os riscos graves, medidas adequadas para sua minoração devem ser implementadas.

Quanto à busca por entender a natureza substancial da privacidade – sobre o que é importante tecer algumas considerações, apesar dos limites deste trabalho – ao invés de vincular esta a noções com o direito de ser deixado só, sigilo ou controle, alinha-se ao referencial teórico de um número crescente de estudiosos e filósofos do direito que associam a privacidade e sua tutela jurídica[49] à identidade pessoal.[50] Segue essa linha de pensamento Mireille Hildebrandt, teórica do direito que concebe a privacidade como um elemento crucial para a construção da identidade. Com base no conceito de Philip Agre e Marc Rotenberg, ela define

[46] Sobre o assunto: cf. DE HERT, Paul; GUTWIRTH, Serge. Privacy, data protection and law enforcement: opacity of the individual and transparency of power. *In*: CLAES, Erik; GUTWIRTH, Serge; DUFF, Antony (Org.). *Privacy and the Criminal Law*. Antwerpen-Oxford: Intersentia, 2006. p. 77-78; GONZÁLEZ FUSTER, Glória; GUTWIRTH, Serge. Opening up personal data protection: A conceptual controversy. *Computer Law and Security Review*, v. 29, n. 5, p. 531-539, 2013.

[47] Entre outros *vide*: ZANFIR, Gabriela. Forgetting About Consent. Why The Focus Should Be On "Suitable Safeguards" in Data Protection Law. *In*: GUTWIRTH, Serge; LEENES, Ronald; DE HERT, Paul. (Ed.). *Reloading Data Protection Law*: Multidisciplinary Insights and Contemporary Challenges. London: Springer, 2008. p. 237-257; MANTELERO, Alessandro. The future of consumer data protection in the E.U. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics. *Computer Law and Security Review*, v. 30, n. 6, p. 643-660, 2014; SCHERMER, Bart W.; CUSTERS, Bart; VAN DER HOF, Simone. The crisis of consent: How stronger legal protection may lead to weaker consent in data protection. *Ethics and Information Technology*, v. 16, n. 2, p. 171–182, 2014.

[48] ZANFIR, Gabriela. *Op. cit.*, p. 246.

[49] Portanto, trata-se de uma abordagem baseada em direitos.

[50] Entre outros, cf. COHEN, Julie E. *Configuring the Networked Self*: Law, Code, and the Play of Everyday Practice. New Haven: Yale University Press, 2012. p. 107-152; FLORIDI, Luciano. The ontological interpretation of informational privacy. *Ethics and Information Technology*, v. 7, n. 4, p. 185–200, 2005; FLORIDI, Luciano. Four challenges for a theory of informational privacy. *Ethics and Information Technology*, v. 8, n. 3, p. 109-119, 2006.

privacidade "como liberdade de restrições irrazoáveis à construção da própria identidade".[51]

Nesta conceituação, uma textura aberta e fluida é intencionalmente dada à privacidade. Rejeita-se a alegação de que seja necessário delinear uma definição estrita do que é privacidade, que se baseia no método cartesiano proposto por estudiosos como David Archard,[52] que afirmam que "uma definição deve ser capaz de unificar diferentes reivindicações ao direito à privacidade, no sentido de que compartilham uma característica comum significativa e substantiva".[53] Isso significa que, para conceituar a privacidade, não se deve ignorar sua complexidade e a pluralidade de aspectos a ela relacionados. Assim, autonomia, dignidade, sigilo, anonimato e integridade corporal — para listar algumas ideias ou valores relacionados à privacidade — devem ser vistos como facetas da privacidade que, em última análise, também estão relacionadas entre si como possuidoras da mesma "semelhança de família".[54]

Além da contribuição de Agre e Rotenberg, a abordagem teórica de Irvin Altman desempenha um papel central nessa concepção de privacidade como liberdade de restrições irrazoáveis à construção da própria identidade. Em seu trabalho, o psicólogo Altman também propõe tanto a privacidade quanto a identidade como noções emaranhadas, definindo a primeira em termos de "negociações de limite" (*boundary negotiations*) ou "controle seletivo de acesso ao *self* ou ao seu grupo".[55] A identidade pessoal não é uma condição estática ou um dado estado humano; consiste em um processo de construção que percorre a vida de uma pessoa, levando em consideração o outro, os grupos e suas interações sociais. Nesse sentido, a privacidade é tomada como "um processo dialético em mudança".[56]

---

[51] HILDEBRANDT, Mireille. *Smart Technologies and The End(s) of Law*. Cheltenham-Northampton: Edward Elgar, 2015. p. 80. Tradução livre de: "as freedom from unreasonable constraints on the construction of one's own identity".

[52] ARCHARD, David. The Value of Privacy. *In*: CLAES, E.; DUFF, A.; GUTWIRTH, S. (Ed.). *Privacy and the Criminal Law*. Antwerpen-Oxford: Intersentia, 2006. p. 13-32.

[53] HILDEBRANDT, Mireille. Privacy and Identity. *In*: CLAES, E.; DUFF, A.; GUTWIRTH, S. (Ed.). *Privacy and the Criminal Law*. Antwerpen-Oxford: Intersentia, 2006. p. 44. Tradução livre de: "a definition should be able to cohere different claims to the right of privacy in the sense that they share a common significant and substantive feature".

[54] HILDEBRANDT, Mireille. *Op. cit.,* p. 45. Sobre a concepção de Wittgenstein de "semelhanças de família", WITTGENSTEIN, Ludwig. *Investigações filosóficas* – Edição bilíngue alemão/português. Trad. João José R. L. de Almeida. Campinas: Unicamp, 2017. p. 62 *et seq*. Entre os estudiosos da privacidade, essa noção de Wittgenstein é usada por Daniel Solove em sua teoria pragmatista da privacidade: SOLOVE, Daniel. J. *Understanding Privacy*. Cambridge; London: Harvard University Press, 2008. p. 42-44.

[55] ALTMAN, Irwin. Privacy: A Conceptual Analysis. *Environment and Behavior*, v. 8, n. 1, p. 7-29, 1976, p. 8. Traduação livre de: "selective control of access to the self or to one's group".

[56] ALTMAN, Irwin. Privacy: A Conceptual Analysis. *Environment and Behavior*, v. 8, n. 1, p. 7-29, 1976, p. 12. Tradução livre de: "a shifting dialectic process". Na sua visão, "[p]rivacy is a continually changing

Existem dois aspectos da identidade aos quais deve-se atentar: identidade-*idem* ("mesmidade") e identidade-*ipse* ("ipseidade"). Sob o ponto de vista de Paul Ricoeur da *identidade narrativa*, enquanto o primeiro se refere ao senso de permanência no tempo e na semelhança,[57] o segundo aspecto trata da mutabilidade e da ideia de alteridade, o núcleo mutável da personalidade,[58] que, no entanto, apresenta algum tipo de conservação específica do *self*. Como explica Hildebrandt, identidade-*idem* e identidade-*ipse* são dois lados diferentes de uma única moeda. A "mesmidade" tem a ver com a criação de um conjunto de atributos capazes de individualizar uma pessoa dentro de uma coletividade, "concerne à identificação a partir da perspectiva de uma terceira pessoa, pressupõe objetificação".[59] O outro lado da moeda, que é a *ipseidade*, está associado à "construção da identidade pessoal a partir da perspectiva da primeira pessoa"[60] que inevitavelmente ocorre entre outras pessoas. Para sintetizar o que a identidade pessoal significa, Hildebrandt postula:

> O *self* vive no nexo de dois aspectos da identidade, que nunca são dados: a identidade do *self* (ipse) deve ser afirmada *em face dos outros*, e o self deve ser afirmado como sendo o *mesmo* (idem) *ao longo do tempo*. A continuidade desse self relacional implica que a autobiografia de si mesmo é continuamente reescrita em confronto com o fluxo de novos eventos que moldam a percepção de si mesmo, do mundo e dos outros.[61]

Dado o fato de que a identidade pessoal surge incessantemente do processo de autoconstrução que uma pessoa enfrenta na vida em sociedade, é concebível defender que existe um componente de indeterminação que constitui cada

process which reflexes a momentary ideal level of interpersonal contact, which can range from wanting to be accessible to others, to wanting to be alone" (ALTMAN, Irwin. *Op. cit.*, p. 12).

57 Cf. HILDEBRANDT, Mireille. Privacy as protection of the incomputable self: From agnostic to agonistic machine learning. *Theoretical Inquiries in Law*, v. 20, n. 1, p. 83–121, 2019, p. 87; RICOEUR, Paul. *O si-mesmo como outro*. São Paulo: Martins Fontes, 2014. p. 115-116.

58 RICOEUR, Paul. *Op. cit.,* p. XIII.

59 HILDEBRANDT, Mireille. Privacy and Identity. *In*: CLAES, E.; DUFF, A.; GUTWIRTH, S. (Ed.). *Privacy and the Criminal Law*. Antwerpen-Oxford: Intersentia, 2006. p. 51. Tradução livre de: "[i]t concerns identification from the perspective of a third person, it presumes objectification".

60 HILDEBRANDT, Mireille. *Op. cit.*, p. 51. Tradução livre de: "the construction of self-identity from the perspective of the first person".

61 HILDEBRANDT, Mireille. *Op. cit.*, p. 51-52. *Vide* também: HILDEBRANDT, Mireille. *Smart Technologies and The End(s) of Law*. Cheltenham-Northampton: Edward Elgar, 2015. p. 81-82. Tradução livre de: "The self lives at the nexus of two aspects of identity, that are never given: identity of the self (ipse) has to be claimed versus others, and the self has to be claimed as being the same (idem) over the course of time. The continuity of this relational self implies that the autobiography of the self is continuously re-written in confrontation with the flow of new events that shape one's perception of self, world and others".

indivíduo como pessoa humana.[62] Essa característica do *self*, na verdade, tem um grande impacto sobre como o direito à privacidade deve desempenhar seu papel nas sociedades hoje hiperconectadas e orientadas por dados, ou no que é chamado mundo *onlife*.[63]

Em um mundo em que se reivindica que tudo é suscetível de ser "datificado" em linguagem de máquina por computação ubíqua e tecnologias digitais baseadas em analítica de dados e sistemas algorítmicos de aprendizado de máquina,[64] as infraestruturas de informação e comunicação dependem cada vez mais do "Espaço Big Data", é dizer, o "heterogêneo, descentrado e distribuído espaço-tempo em que quantidades exponenciais de dados são armazenadas e processadas, enquanto o acesso é distribuído e a exatidão dependente de uma série de fatores invisíveis".[65] Nesse sentido, as tecnologias atuais ou aplicações tecnológicas que estão sendo desenvolvidas ou utilizadas, como reconhecimento facial, Internet das Coisas, *smart grids*, carros autônomos, assistentes pessoais virtuais e robótica, contam com o denominado "Espaço Big Data".[66]

No mundo *onlife,* uma predominante infraestrutura da informação e comunicação está emergindo e ela prospera na computação preemptiva (*preemptive computing*). A criação do novo paradigma só é possível por meio de uso de técnicas de perfilamento (automatizado), o que significa que é uma componente básica da

---

[62] Para explicar essa indeterminação da construção da identidade pessoal, Hildebrandt desenvolve a ideia de *dupla contingência*, *vide* HILDEBRANDT, Mireille. Privacy as protection of the incomputable self: From agnostic to agonistic machine learning. *Theoretical Inquiries in Law*, v. 20, n. 1, p. 83-121, 2019, p. 88

[63] A expressão "mundo *onlife*" pretende se referir mais precisamente a como a implementação e a adoção de tecnologias digitais afetam a condição humana. Isso conduziu a quatro grandes transformações: "i. the blurring of the distinction between reality and virtuality; ii. the blurring of the distinctions between human, machine and nature; iii. the reversal from information scarcity to information abundance; and iv. the shift from the primacy of entities to the primacy of interactions" (FLORIDI, Luciano (Ed.). *The Onlife Manifesto: Being Human in a Hyperconnected Era*. Heidelberg-London-New York-Dordrecht: Springer, 2015. p. 7).

[64] Cf. CUKIER, Kenneth; MAYER-SCHÖNBERGER, Viktor. *Big Data:* A Revolution That Will Transform How We Live, Work, and Think. Boston: Houghton Mifflin Harcourt, 2013. p. 73-97.

[65] HILDEBRANDT, Mireille. *Smart Technologies and The End(s) of Law*. Cheltenham-Northampton: Edward Elgar, 2015. p. 261. Tradução livre de: "heterogeneous, decentred, distributed timespace where exponential amounts of data are stored and processed, while access is distributed and accuracy is contingent upon a number of mostly invisible factors".

[66] Nas palavras de Hildebrandt, o "Espaço Big Data" é o *inconsciente digital* do qual depende a infraestrutura da computação preemptiva da sociedade orientada por dados: "Big Data Space extends our minds with a digital unconscious that is largely beyond the reach of our conscious mind. This digital unconscious is not owned by any one person and cannot be controlled by any one organization. It has been created by individuals, enterprises, governments and machines, and is rapidly becoming the backbone of our education, scientific research, economic ecosystem, government administration and our critical infrastructures. It enables data-driven agency in software, embedded systems and robotics, and will increasingly turn human agency itself into a new hybrid that is partly data-driven. The onlife world that we now inhabit is data-driven and feeds on a distributed, heterogeneous, digital unconscious" (HILDEBRANDT, Mireille. *Op. cit.*, p. 45). As principais características do "Big Data Space" são: difusão, hiperconectividade, interface intuitiva, complexidade oculta e adaptação proativa contínua, com base em mecanismos de *feedback* e conscientização do contexto.

criação de conhecimento por meio de análises preditivas e algoritmos de aprendizado de máquina incorporados em *softwares* executados no *hardware* do ambiente físico.[67] De acordo com essa perspectiva, uma vez que os seres humanos estão sendo perfilados de maneira contínua, invisível e inconsciente por sistemas que tomam decisões sobre suas vidas automaticamente com base em conhecimento inferencial, a proteção da privacidade deve garantir à pessoa humana o papel participativo na codeterminação da maneira como é lida e representada.[68]

3.2 Perfilamento automatizado e ameaças possíveis ao indivíduo e à coletividade: a afirmação da dimensão coletiva dos direitos à privacidade e à proteção de dados

"Tecnologia não é boa nem má; bem como não é neutra".[69] Essa afirmação de Melvin Kranzberg concita, brevemente, ao afastamento tanto do determinismo tecnológico quanto da visão instrumentalista da neutralidade dos artefatos tecnológicos. Assim, impõe-se analisar as tecnologias de perfilamento no cenário brasileiro e o tratamento de dados de localização agregados de maneira empírica, que considera os seus efetivos usos e contexto sociocultural vigente, partindo de um ângulo pós-fenomenológico.[70]

De acordo com o que foi dito anteriormente sobre as tecnologias de perfilamento, nas etapas de construção do perfil e de aplicação, não há a restrição da atuação sobre indivíduos, mas também há o alcance – principalmente –

[67] Basta considerar as noções de *computação ubíqua* e *internet das coisas* para se entender como o ambiente físico também se torna um *hardware* em que funcionam programas com tratamento intensivo e automatizado de dados. A ubiquidade computacional antevista por Mark Weiser no início da década de 1990 do século passado, em que computadores integrariam ambientes físicos invisivelmente, se realiza com a *internet* dos dias atuais, que não apenas conecta computadores permitindo a comunicação entre pessoas mundo afora, mas compõe um ecossistema que vai se formando por objetos interconectados em rede e estruturados em sistemas de inteligência artificial, impulsionados por técnicas de análise de grandes dados e serviços de computação em nuvem, a fim de oferecer utilidades personalizadas e em tempo real ao(s) usuário(s). Segundo Weiser, a computação ubíqua (*ubiquitous computing*) "has as its goal the nonintrusive availability of computers throughout the physical environment, virtually, if not effectively, invisible to the user" (WEISER, Mark. Ubiquitous computing. *Computer*, [s.l.], v. 26, n. 10, p. 72, out. 1993).

[68] HILDEBRANDT, Mireille. *Op. cit.*, p. 102-103.

[69] KRANZBERG, Melvin. Technology and History: "Kranzberg's Laws". *Johns Hopkins University Press*, v. 27, n. 3, p. 544-560, 1986, p. 545.

[70] Cf. COHEN, Julie E. Affording Fundamental Rights: A Provocation Inspired by Mireille Hildebrandt. *Critical Analysis of Law*, v. 4, n. 1, p. 78–90, 2017, p. 79 *et seq.*; IHDE, Don. Technology and the lifeworld: from garden to earth. Bloomington-Indianapolis: Indiana University Press, 1990.

sobre grupos,[71] sendo inclusive o perfilamento de grupo (*group profiling*) um crucial método de classificação algorítmica[72] presente no perfilamento automatizado.[73] Isso significa que a elaboração computacional de perfis mediante a mineração de padrões e correlações de dados não são apenas relacionados a pessoas naturais identificadas ou identificáveis (perfis personalizados[74]), mas também a tipos ou características comportamentais referentes a grupos (comunidades ou categorias[75]). Com isso, tem-se que tecnologias que usam técnicas de perfilamento e as aplicam são capazes de tratar dados que não possuem *prima facie* caráter pessoal por identificar grupos ou coletividades. É o que se dá, por exemplo, em aplicações que visam segmentar grupo de consumidores por certas preferências de consumo para fornecer publicidade direcionada,[76] discriminar preços com base

[71] MANTELERO, Alessandro. Responsabilità e rischio nel Reg. UE 2016/679. *Le Nuove Leggi Civili Commentate*, v. XL, n. 1, p. 144-164, 2017, p. 146.

[72] Sobre a expressão "classificação algorítmica", v. MITTELSTADT, Brent. From Individual to Group Privacy in Big Data Analytics. *Philosophy and Technology*, v. 30, n. 4, p. 475-494, 2017.

[73] FIDIS. *Descriptive analysis and inventory of profiling practices*. Disponível em: http://www.fidis.net/resources/fidis-deliverables/profiling/int-d72000/doc/4/. Acesso em: 16 jul. 2020. *Vide*, também: HILDEBRANDT, Mireille. Defining Profiling: A New Type of Knowledge? *In*: GUTWIRTH, Serge; HILDEBRANDT, Mireille (Ed.). *Profiling the European Citizen:* Cross-Disciplinary Perspectives. New York: Springer, 2008. p. 20.

[74] Perfis personalizados são aqueles em que há mineração de dados de sujeito individualizado. (HILDEBRANDT, Mireille. *Op. cit.*, p. 22). Não se deve entender, entretanto, que isso significa que perfis personalizados envolvem, necessariamente, o tratamento de dados pessoais. Segundo Wim Schreurs e outros, é possível que tais perfis sejam alimentados por dados anonimizados (SCHREURS, Wim *et al*. *Cogitas Ergo Sum:* The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector. *In*: GUTWIRTH, Serge; HILDEBRANDT, Mireille (Ed.). *Profiling the European Citizen:* Cross-Disciplinary Perspectives. New York: Springer, 2008. p. 249).

[75] O perfilamento de grupo pode versar sobre *comunidades* ou *categorias*. As primeiras são grupos que preexistem ao processo de mineração de dados realizado para traçar as correlações e padrões e, assim, identificar características comuns aos membros do grupo (*v. g.,* grupo étnico, trabalhadores de uma empresa). As categorias, por sua vez, são constituídas uma vez estabelecidas as correlações por algoritmos de mineração de dados que identificam atributos comuns (*v.g.*, pessoas que gostam de certo alimento possuem QI mais elevado): "[t]he category is usually called a group and the set of attributes are called the group's profile". Acertadamente, resume a autora sobre o perfilamento de grupo: "Group profiling can concern both communities (existing groups) and categories (e.g., all people with blue eyes). In the case of categories, the members of the group did not necessarily form a community when the process was initiated; in the case of communities the members of the group already formed a community (however unstructured). The fact that profiling may establish categories as sharing certain attributes may in fact lead to community building, if the members of such a category become aware of the profile they share. The fact that data controllers may tar- get the members of a category in a certain way – without them being aware of this – may of course impact their behaviour as members of this category" (HILDEBRANDT, Mireille. Defining Profiling: A New Type of Knowledge? *In*: GUTWIRTH, Serge; HILDEBRANDT, Mireille (Ed.). *Profiling the European Citizen:* Cross-Disciplinary Perspectives. New York: Springer, 2008. p. 20).

[76] SPENCER, Shaun B. Privacy and Predictive Analytics in E-Commerce. *New England Law Review*, v. 49, n. January 2015, p. 629-647, jan. 2015, p. 636-637.

em zona geográfica,[77] ou descobrir, a partir do reconhecimento de padrões de mobilidade de grupos, futuros focos de surto de doenças infectocontagiosas.[78]

Uma novidade que o perfilamento automatizado traz ao nível coletivo é a criação algorítmica de *categorias*, ou de *grupos ad hoc*.[79] Diferentemente das comunidades, grupos previamente existentes à operação de algoritmos no processo de "descoberta de conhecimento em base de dados" (*knowledge discovery in databases*), as categorias consistem em agrupamentos fluídos que surgem a partir do processamento e mineração de grandes volumes de dados. A característica central desse tipo de grupo é ser "definido remotamente mediante tratamento de dados, de modo que os membros do grupo não são necessariamente conscientes de pertencerem a ele".[80] [81]

O fenômeno tem impulsionado uma inovadora tomada de posição epistemológica[82] a respeito da noção de grupo, para além de teorias sociológicas

[77] Conforme noticiado na imprensa norte-americana, lojas de *e-commerce* praticam discriminação de preço conforme o *ZIP code* de consumidores: VALENTINO-DEVRIES, Jennifer; SINGER-VINE, Jeremy Singer-Vine; SOLTANI, Ashkan. Websites Vary Prices, Deals Based on Users' Information. *The Wall Street Journal*. Disponível em: https://www.wsj.com/articles/SB10001424127887323777204578189391813881534. Acesso em: 19 jul. 2020; HOWE, Neil. A Special Price Just For You. *Forbes*. Disponível em: https://www.forbes.com/sites/neilhowe/2017/11/17/a-special-price-just-for-you/#11e3c39290b3. Acesso em: 19 jul. 2020.

[78] TAYLOR, Linnet. Safety in Numbers? Group Privacy and Big Data Analytics in the Developing World. *In*: TAYLOR, Linnet; FLORIDI, Luciano; SLOOT, Bart van der (Ed.). *Group Privacy:* New Challenges of Data Technologies. Dordrecht: Springer, 2017. p. 22.

[79] Cf. MITTELSTADT, Brent. From Individual to Group Privacy in Big Data Analytics. *Philosophy and Technology*, v. 30, n. 4, p. 475–494, 2017, p. 479-480; WACHTER, Sandra. Affinity Profiling and Discrimination by Association in Online Behavioural Advertising. *Berkeley Technology Law Journal*, v. 35, n. 2, 2020, p. 56-57 (no prelo).

[80] TAYLOR, Linnet. *Op. cit.*, p. 15. Tradução livre de: "defined remotely by processing data, so that the group's members are not necessarily aware that they belong to it".

[81] O jornalismo investigativo do *The Intercept Brasil* reportou caso que revela nítido exemplo de grupo *ad hoc* criado por análise de dados agregados (localização, faixa etária, gênero, entre outros), dos quais as pessoas compreendidas na classificação – algumas identificadas pela reportagem – não tinham consciência. Em processamento realizado a partir de dados comercializados pela Vivo, provedora de telefonia móvel, criou-se um certo perfil de pessoas categorizado como "famílias populares": "Na planilha vendida em 2017 ao governo do Espírito Santo, Rocha não é exatamente Rocha. É um indivíduo não identificado, homem, idade entre 50 e 59 anos, que vive em Domingos Martins, cidade de 33 mil habitantes, e vai esporadicamente a Santa Maria de Jetibá, que tem 40 mil. Pertence à classe B e é classificado como integrante de "famílias populares", uma categoria criada pelo estudo para definir a típica família brasileira de classe média". (...) "Esses dados são 'anonimizados', jura a empresa, e organizados nos chamados 'clusters comportamentais', que agrupam as pessoas segundo suas características sociodemográficas – onde vivem, quanto ganham e como consomem" (DIAS, Tatiane. Vigiar e lucrar. *The Intercept Brasil*, 13 abr. 2020. Disponível em: https://theintercept.com/2020/04/13/vivo-venda-localizacao-anonima/. Acesso em: 26 jul. 2020).

[82] Entre outros, cf. TAYLOR, Linnet. Safety in Numbers? Group Privacy and Big Data Analytics in the Developing World. *In*: TAYLOR, Linnet; FLORIDI, Luciano; SLOOT, Bart van der (Ed.). *Group Privacy:* New Challenges of Data Technologies. Dordrecht: Springer, 2017. p. 15; MANTELERO, Alessandro. From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era. *In*: TAYLOR, Linnet; FLORIDI, Luciano; SLOOT, Bart van der (Ed.). *Group Privacy:* New Challenges of Data Technologies. Dordrecht: Springer, 2017. p. 144; SUH, Jennifer J. *et al*. Distinguishing Group Privacy From

tradicionais,[83] e revigorado a discussão sobre a dimensão coletiva tanto do direito à privacidade – por muitos já denominada de *privacidade de grupo*[84] – como do direito à proteção de dados pessoais, de maneira a reconhecer a necessidade de tutela jurídica a interesses de cunho transindividual no âmbito de proteção desses direitos.

Quanto à privacidade, em termos conceituais é importante salientar que (i) no processo de construção da identidade, os grupos e coletividades a que a pessoa pertence são relevantes para se dizer como esta é representada, ainda que por agentes artificiais;[85] e (ii) no caso das categorias ou grupos *ad hoc*, estes são imperfeitos reflexos dos indivíduos nele contidos, moldados pela leitura dos dados processados pelo sistema algorítmico. Nesse sentido, Brent Mittelstadt defende que o agrupamento *ad hoc* "propicia maneiras imprevistas de visualizer e inferior informações sobre o indivíduo", de modo que a "classificação algorítmica deve, portanto, ser considerada uma ameaça à capacidade dos titulares dos dados moldar e controlar a própria identidade".[86] Isto é, de acordo com o conceito de Mireille Hildebrandt abordado na seção anterior, o agrupamento algorítmico pode vir a configurar uma interferência irrazoável na construção da própria identidade.

Personal Privacy. *Proceedings of the ACM on Human-Computer Interaction*, v. 2, n. CSCW, p. 1-22, nov. 2018, p. 3-4.

83 Mantelero leciona que as teorias individualista e orgânica conformam uma perspectiva de análise tradicional sobre o conceito de grupo. O autor italiano ressalta que: "[t]hese theories, although different, are both based on members' awareness of being part of a group and on the social dimension of the group as a network of relationships among its members". Afirma, ainda, que: "the traditional approach to group privacy considers groups that are based on stable and socially recognized relationships between individuals, although they can be informal in nature (e.g. love affairs, priest-penitent relationships) or last only for a certain time (e.g. marital relationships, association)" (MANTELERO, Alessandro. From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era. *In*: TAYLOR, Linnet; FLORIDI, Luciano; SLOOT, Bart van der (Ed.). *Group Privacy:* New Challenges of Data Technologies. Dordrecht: Springer, 2017. p. 144.

84 Por todos, vide: MANTELERO, Alessandro. *Op. cit.*, p. 140-144. Ressalte-se, porém, que o autor defende o uso do conceito de "privacidade coletiva" (*collective privacy*). Sobre a privacidade de grupo sob a ótica tradicional: WESTIN, Alan F. *Privacy and Freedom.* New York: Atheneum, 1967. p. 42 *et seq.*; BLOUSTEIN, Edward. J. Group Privacy: A Right to Huddle. *In*: BLOUSTEIN, Edward. *Individual and Group Privacy*. New York: Routledge, 2017. p. 123-186.

85 Um agente é uma entidade que age, que faz algo. Para que haja *ação* (*agency*), porém, não é necessário que certo ente tenha uma mente. Partindo dessa premissa, reconhece-se a ação de agentes artificiais, tais como aqueles baseados em algoritmos determinísticos, em aprendizado de máquina, e, inclusive, em sistemas multiagentes. Seguindo, uma vez mais, a contribuição de Hildebrandt, "[t]he crucial and most elementary characteristic of agency is the capability of an entity to sense its environment and to act upon it. The most important step from deterministic to other types of agent is an agent's capability to learn from the combination of action and perception and thus to improve its performance in relation to the goals it aims to reach" (HILDEBRANDT, Mireille. *Smart Technologies and The End(s) of Law*. Cheltenham-Northampton: Edward Elgar, 2015. p. 30).

86 MITTELSTADT, Brent. From Individual to Group Privacy in Big Data Analytics. *Philosophy and Technology*, v. 30, n. 4, p. 475-494, 2017, p. 480. Tradução livre de: "provides unanticipated ways of viewing and inferring information about the individual" e "[a]lgorithmic classification must therefore be considered a threat to data subjects' capacity to shape and control identity".

A partir disso, aliás, há que se dizer que a dimensão de grupo passa também a integrar o significado de privacidade por guardar conexão da mesma "semelhança de família" com demais facetas desta noção.

Nessa ordem de ideias, a tutela da privacidade deve compreender a proteção de interesses coletivos, que não se confundem com o somatório daqueles dos indivíduos que integram o grupo, apesar da sua característica fluidez e de, no mais das vezes, faltar consciência aos membros sobre sua constituição[87]. Dessa tutela de ordem substancial, pode-se também, por derivação lógica, tecer as linhas da dimensão coletiva da proteção de dados pessoais. O perfil procedimental desse direito se coaduna com a imposição de métodos e procedimentos durante o tratamento de dados para proteger a privacidade de grupo (*v.g.,* salvaguardas para o fornecimento de informações significativas e relevantes sobre a lógica do tratamento automatizado de dados e a contestabilidade de decisão automatizada) e, como instrumento de transparência, controlar atividade de processamento algorítmico de dados em face de abusos e assimetrias de poder. Seria este reconhecimento uma forma de "expansão do poder coletivo"[88] a que Stefano Rodotà aludiu, na década de 1990, em alerta sobre a dimensão coletiva da proteção de dados pessoais.

As ameaças que a implementação de técnicas de perfilamento gera aos direitos à privacidade e à proteção de dados pessoais perpassa ambos aspectos individual e coletivo. Dentre as situações de perigo a estes direitos fundamentais pode-se elencar os processos de "normalização" (*normalisation*) e de "customização" (*customisation*), e discriminação de grupo e intervenção direta.

A espontânea "normalização" é efeito do constante monitoramento e coleta de dados pessoais por atores do mercado que processam e usam essas informações de formas que os titulares dos dados desconhecem. O pouco (ou nenhum) controle ou participação das decisões que são tomadas a seu respeito leva os indivíduos a temer que os dados tratados sejam usados em seu prejuízo, temor que pode modelar o comportamento individual a ponto de se ajustar a

[87] MANTELERO, Alessandro. From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era. *In*: TAYLOR, Linnet; FLORIDI, Luciano; SLOOT, Bart van der (Ed.). *Group Privacy:* New Challenges of Data Technologies. Dordrecht: Springer, 2017. p. 146-147; SUH, Jennifer J. et al. Distinguishing Group Privacy From Personal Privacy. *Proceedings of the ACM on Human-Computer Interaction*, v. 2, n. CSCW, p. 1–22, nov. 2018, p. 3-4. Mantelero aventa o seguinte exemplo sobre escore de crédito: "An example in this sense is provided by credit scoring models based on big data, which predict the credit risks of individuals that live in a small geographic area. These individuals are classified according to their social context in a way that bears no relationship to their individual conditions, but is based on the aggregate score of the area" (MANTELERO, Alessandro. *Op. cit.*, p. 147).

[88] RODOTÀ, Stefano. *Tecnologie e diritti.* Bolonha: Il Mulino, 1995. p. 38.

certo perfil.[89] Já a "customização", a seu turno, é engendrada pela publicidade direcionada e fornecimento de produtos e serviços de modo personalizado com base em sistemas algorítmicos que antecipam as preferências e vontades dos consumidores mediante análises preditivas.[90] Neste caso, porém, a pessoa pode agir sem sequer ter certeza de que se conduz de acordo com seus próprios desejos, vontades e predileções.

O direito à proteção de dados pessoais se vê, então, ameaçado de violação porque a invisibilidade e inconsciência em relação às operações de tratamento de dados pessoais, somadas à ordinária opacidade dos sistemas algorítmicos (*black boxes*) que movimentam as técnicas de perfilamento, tiram dos titulares dos dados a capacidade de uso de mecanismos de controle do tratamento automatizado de suas informações e contestação das decisões que afetam seus direitos e interesses. Quanto ao prisma da privacidade, esta também pode ser violada porque o processo de construção da identidade passa a sofrer interferências de agentes artificiais que podem atuar com base numa equívoca representação da pessoa. Aliás, é falha a própria pressuposição de que a complexidade humana e a indeterminação da identidade pode ser capturada, "datificada" e representada por sistemas algorítmicos.[91]

A discriminação com base na identificação de grupo é uma possibilidade com gravíssimas consequências. Ainda que os dados objeto de tratamento e as inferências resultantes da construção e aplicação de perfil sejam dados reputados anonimizados, não referentes a pessoas naturais identificadas ou identificáveis, é possível agir, com base no conhecimento extraído da base de dados, sobre grupos identificados e determinados por algoritmos. Em nível coletivo, já se sabe que atos discriminatórios e de persecução estatal são passíveis de ser direcionados a grupos e pessoas a ele pertencentes, de maneira que a individualização de um titular de dados tem pouca relevância nesse tipo de contexto. No genocídio de Ruanda, em 1994, o extermínio de minorias étnicas de forma sistemática e organizada tinha suporte na informação sobre grupo étnico das pessoas. Isso foi viabilizado pela decisão do governo pós-colonial de incluir a classificação de

[89] Cf. SOLOVE, Daniel J. *The digital person:* technology and privacy in the information age. New York: New York University, 2004. p. 39, 50-51.

[90] HILDEBRANDT, Mireille. Profiling and Identity of the European Citizen. In: HILDEBRANDT, Mireille; GUTWIRTH, Serge (Ed.). *Profiling the european citizen:* Cross-Disciplinary Perspectives. New York: Springer, 2008. p. 307.

[91] HAO, Karen. AI can't predict how a child's life will turn out even with a ton of data. *MIT Technology Review,* 02 abr. 2020. Disponível em: https://www.technologyreview.com/2020/04/02/998478/ai-machine-learning-social-outcome-prediction-study/#Echobox=1585941290. Acesso em: 30 jul. 2020.

grupo étnico nos documentos de identidade.[92] Muito embora modelos analíticos já tenham sido implementados de forma benéfica em cenários emergenciais e de desastre humanitário para informar política de combate epidemiológico – como no Haiti, após o terremoto de 2010[93] –, de outro lado, considera-se a ameaça de danos e lesão a direitos de grupos vulneráveis da população pelo uso de informações demográficas por tais modelos.[94]

4 Analítica de dados de geolocalização no combate à COVID-19 e riscos: a LGPD oferece parâmetros aplicáveis?

O tratamento de dados agregados de localização de celulares durante a pandemia não possui serventia para autoridades sanitárias apenas nas fases de iniciação e de aceleração de um surto de contágio do novo coronavírus,[95] mas, como já visto anteriormente, em todo ciclo de vida da pandemia de COVID-19. Essa é uma importante constatação para fins de análise de risco do processamento desses dados no contexto brasileiro, visto que, dadas a circunstâncias incertas até o desenvolvimento de vacina eficaz e imunização populacional, a duração da pandemia há de perdurar por longos meses. Levando em consideração especialmente ambos os direitos à privacidade e à proteção de dados pessoais, a avaliação sobre os riscos em causa deve atentar para a LGPD e sua estrutura regulatória,

[92] RAHMAN, Zara. Dangerous Data: The Role of Data Collection in Genocides. *The Engine Room*, 2016. Disponível em: https://www.theengineroom.org/dangerous-data-the-role-of-data-collection-in-genocides/. Acesso em: 22 jul. 2020.

[93] Pesquisadores utilizaram dados de localização de dispositivos móveis para monitorar o deslocamento populacional da capital e, assim, ajudar na tomada de medidas de contenção do surto de cólera (BENGTSSON, L. *et al*. Improved response to disasters and outbreaks by tracking population movements with mobile phone network data: A post-earthquake geospatial study in Haiti. *PLoS Medicine*, v. 8, n. 8, p. 1-7, 2011).

[94] SANDVIK, Kristin; RAYMOND, Nathaniel. Beyond the Protective Effect: Towards a Theory of Harm for Information Communication Technologies in Mass Atrocity Response. *Genocide Studies and Prevention*, v. 11, n. 1, p. 9–24, 2017, p. 10. Os autores utilizam o conceito de *informação demograficamente identificável*, que significa "either individual and/or aggregated data points that allow inferences to be drawn that enable the classification, identification, and/or tracking of both named and/or unnamed individuals, groups of individuals, and/or multiple groups of individuals according to ethnicity, economic class, religion, gender, age, health condition, location, occupation, and/or other demographically defining factors" (SANDVIK, Kristin; RAYMOND, Nathaniel. *Op. cit.*, p. 10-11).

[95] Ao tempo da redação deste trabalho, o Brasil ainda se encontra na fase de aceleração: Cf. BRASIL tem recorde de casos diários de Covid-19, mais de 65 mil. *Folha de São Paulo,* 22. jul. 2020. Disponível em: https://www1.folha.uol.com.br/equilibrioesaude/2020/07/brasil-tem-recorde-de-casos-diarios-de-covid-19-mais-de-65-mil.shtml. Acesso em: 22 jul. 2020.

independente da já confusa projeção sobre a entrada em vigor da lei,[96] que muito provavelmente se dará em algum dos estágios da emergência sanitária.[97]

A LGPD, à semelhança do Regulamento n. 2016/679, da União Europeia (GDPR), visa regular a atividade de tratamento de dados pessoais por agentes públicos ou privados e, assim, promover o direito à proteção de dados pessoais, em primeiro lugar, bem como outros direitos e liberdades fundamentais na sociedade orientada por dados, a exemplo do direito à privacidade. A abordagem de uma e outra legislação é voltada a regular os riscos que a atividade de tratamento de dados ocasiona aos titulares de tais posições jurídicas, seja em nível individual, seja no campo coletivo[98] – como se pretende demonstrar –, o que, vale ressaltar, induziu os legisladores a preferir um modelo de responsabilidade voltado à prevenção do dano.[99] Daí a necessidade de, além de identificar os riscos advenientes do uso de tecnologias de perfilamento para o tratamento de dados agregados de geolocalização, investigar se há na LGPD parâmetros aplicáveis a fim de lidar com esses riscos, mitigando-os. É o que se faz abaixo.

4.1 Delineamento dos riscos

A noção de risco adotada neste trabalho, em linha de harmonia aos contornos da LGPD, não se reduz aos ditos riscos de conformidade com a lei, isto

[96] Para um apropriado resumo, *vide*: BELLI, Luca; ZINGALES, Nicolo. *Brazilian Data Protection under Covid-19:* Legal Certainty is the Main Casualty. Disponível em: https://blogdroiteuropeen.com/2020/07/03/brazilian-data-protection-under-covid-19-legal-certainty-is-the-main-casualty-by-luca-belli-and-nicolo-zingales/. Acesso em: 23 jul. 2020.

[97] Como salientado na nota de rodapé nº 7, após votação da Medida Provisória 959/2020 pelo Senado Federal, que retirou do texto dispositivo que postergava a entrada em vigor da LGPD, esta casa legislativa entendeu que o vigor teria início a partir da sanção presidencial. Esta, por sua vez, se deu no dia 17 de setembro de 2020. Deste modo, o vigor da LGPD iniciou no dia 18 de setembro de 2020. Cf. NAKAGAWA, Liliane. LGPD: Bolsonaro sanciona e lei começa a valer nesta sexta-feira. *Olhar Digital*, 17 set. 2020. Disponível em: https://olhardigital.com.br/noticia/lgpd-bolsonaro-sanciona-e-lei-comeca-a-valer-nesta-sexta-feira/107251. Acesso em: 25 set. 2020.

[98] No tocante à LGPD, cf. DONEDA, Danilo; MENDES, Laura Schertel. Um perfil da nova Lei Geral de Proteção de Dados brasileira. *In*: BELLI, Luca; CAVALLI, Olga (Org.). *Governança e Regulações da Internet na América Latina*. Rio de Janeiro: FGV Direito Rio, 2018. p. 318. Sobre a orientação ao risco da GDPR, afirma Mantelero: "L'approccio incentrato sul rischio costituisce, infatti, uno dei punti cardine del nuovo Regolamento UE 2016/679 ed induce il legislatore a prediligere un modello di responsabilità volto alla prevenzione del danno. Danno che, rispetto alle capacità d'indagine offerte dagli algoritmi che elaborano grandi quantità di informazioni, non si limita ai tradizionali aspetti concernenti la sicurezza dei dati, né alla sola dimensione individuale, bensì riguarda anche gli effetti collettivi dell'uso dei dati, da cui possono conseguire diversi profili di pregiudizio, quale ad esempio la violazione del principio di non discriminazione" (MANTELERO, Alessandro. Responsabilità e rischio nel Reg. UE 2016/679. *Le Nuove Leggi Civili Commentate*, v. XL, n. 1, p. 144-164, 2017, p. 146-147).

[99] MANTELERO, Alessandro. Responsabilità e rischio nel Reg. UE 2016/679. *Le Nuove Leggi Civili Commentate*, v. XL, n. 1, p. 144–164, 2017, p. 146.

é, riscos de *compliance*,[100] ou numa ideia centrada apenas em possíveis danos decorrentes de incidentes de segurança,[101] mas alcança também os riscos de violação e lesão a direitos e liberdades fundamentais.[102] Desta sorte, sob essa perspectiva identificam-se ao menos dois riscos associados ao tratamento de dados agregados de geolocalização no atual contexto brasileiro: (i) a reidentificação dos usuários de dispositivos móveis, e consequentes adversos desdobramentos possíveis; e (ii) o desvirtuamento da função e da finalidade atribuídas na origem aos dados no combate à emergência sanitária de COVID-19.

4.1.1 Reidentificação

A reidentificação dos usuários de dispositivos móveis é um risco que, não obstante minorado pela agregação de dados de localização,[103] não é eliminado. Este é o primeiro risco e que consigo traz desdobramentos. Os cientistas da computação Pyergelis, Troncoso e De Cristofaro apontam que a elaboração de modelos de mobilidade com esse tipo de dado coletado por certo período de tempo é sujeito a ameaça capaz de, por inferência, reconhecer a contribuição de uma

[100] Sobre a noção no âmbito da GDPR, *vide*: GELLERT, Raphaël. Understanding the notion of risk in the General Data Protection Regulation. *Computer Law and Security Review*, v. 34, n. 2, p. 279–288, 2018, p. 282.

[101] Em mais uma leitura da GDPR, de utilidade comparativa à LGPD, *vide*: MANTELERO, Alessandro. Responsabilità e rischio nel Reg. UE 2016/679. *Le Nuove Leggi Civili Commentate*, v. XL, n. 1, p. 144-164, 2017, p. 156.

[102] A preocupação da LGPD "direitos e liberdades fundamentais" é expressa e recorrente no seu texto legal. É o que se constata da leitura dos arts. 5º, XVII, 7º, IX, 10, II, 11, II, "g". Assim empregado o conceito de risco, compatibiliza-se ao "modelo *ex ante*" de aplicação da LGPD: "A grande inovação que a LGPD operou no ordenamento jurídico brasileiro pode ser compreendida na instituição de um modelo *ex ante* de proteção de dados, baseado no conceito de que não existem mais dados irrelevantes diante do processamento eletrônico e ubíquo de dados na sociedade da informação. Os dados pessoais são projeções diretas da personalidade e como tal devem ser considerados. Assim, qualquer tratamento de dados, por influenciar na representação da pessoa na sociedade, pode afetar a sua personalidade e, portanto, tem o potencial de violar os seus direitos fundamentais" (MENDES, Laura Schertel. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. *In*: SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscila (Coord.). *Lei Geral de Proteção de Dados* – Caderno Especial. São Paulo: Revista dos Tribunais, 2019. p. 45).

[103] Pyergelis, Troncoso e De Cristofaro qualificam a agregação de dados como uma defesa de privacidade ("privacy defense") (PYRGELIS, Apostolos; TRONCOSO, Carmela; DE CRISTOFARO, Emiliano. What Does The Crowd Say About You? Evaluating Aggregation-based Location Privacy. *Proceedings on Privacy Enhancing Technologies*, v. 2017, n. 4, p. 156–176, 2017, p. 156). No mesmo sentido: PYRGELIS, Apostolos; TRONCOSO, Carmela; DE CRISTOFARO, Emiliano. Measuring Membership Privacy on Aggregate Location Time-Series. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, v. 2, n. 4, 2020, p. 1. O antigo Grupo de Trabalho do Artigo 29, predecessor do atual *European Data Protection Board*, considerou a agregação de dados uma técnica de anonimização (ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 5/2014 on Anonymisation techniques. Bruxelas: [s. n.], 2014. p. 8-9. Disponível em: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Acesso em: 28 jul. 2020).

pessoa na formação de um agregado de geolocalização, possuindo o adversário dados auxiliares. O ataque, denominado *membership inference attack* (MIA),[104] possui significativas implicações, conforme destacam os autores: (i) o só fato de se concluir que os dados de alguém faz parte de um agregado pode constituir informação sensível; e (ii) esse tipo de ataque é um primeiro passo para ulteriores inferências que visam obter informações adicionais sobre indivíduos, tais como seu perfil de mobilidade e/ou suas trajetórias a partir dos dados agregados.[105] Concluiu-se na pesquisa que a variação (*variance*) da localização ao longo do tempo é um aspecto dominante para facilitar a inferência. De modo geral, afirmam que "alta mobilidade e diversidade, regularidade e singularidade dos padrões de movimentação, bem como a dispersão da localização, estão entre os fatores que contribuem para o sucesso do ataque".[106]

Em tempos de emergência sanitária desencadeada pela pandemia do novo coronavírus, o conhecimento de que uma pessoa (identificada ou identificável) faz parte de um grupo ligado a local onde há casos ou surtos de contágio é informação bastante para gerar risco de discriminação ilícita, decorrente tanto de falsa categorização como da verdadeira categorização (*false categorization threat* e *true categorization threat*)[107] do titular dos dados a tal grupo. Ademais, a realidade tem mostrado que a discriminação pode advir não apenas da assunção da probabilidade de certo indivíduo estar infectado pelo agente viral, como também de outros aspectos sensíveis que podem ser associados, tais como etnia e orientação sexual.

Disso, aliás, tem-se exemplos concretos. No início do mês de maio, na Coreia do Sul, após o país controlar a primeira onda do surto de COVID-19, o Centro de Controle e Prevenção de Doenças sul-coreano rastreou quase 30 casos de infecção conectados a distrito da comunidade LGBTQ situado na capital. Isso repercutiu na imprensa do país, que viu surgir grande afluxo de atos e discursos

[104] Segundo Paul Irolla, "[t]he Membership Inference Attack is the process of determining whether a sample comes from the training dataset of a trained ML model or not. [...] [I]n the case where samples are linked to a person, such as medical or financial data, inferring whether samples come from the training dataset of the ML model constitutes a privacy threat" (IROLLA, Paul. *Demystifying the Membership Inference Attack*. Disponível em: https://medium.com/disaitek/demystifying-the-membership-inference-attack-e33e510a0c39. Acesso em: 27 jul. 2020).

[105] PYRGELIS, Apostolos; TRONCOSO, Carmela; DE CRISTOFARO, Emiliano. Measuring Membership Privacy on Aggregate Location Time-Series. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, v. 2, n. 4, 2020, p. 1.

[106] PYRGELIS, Apostolos; TRONCOSO, Carmela; DE CRISTOFARO, Emiliano. *Op. cit.*, p. 2. Tradução livre de: "high mobility and diversity, regularity and uniqueness of moving patterns, as well as location sparsity, are among the factors that contribute to the success of the attack".

[107] Sobre esse tipo de ameaça por categorização em grupo: SUH, Jennifer J. *et al*. Distinguishing Group Privacy From Personal Privacy. *Proceedings of the ACM on Human-Computer Interaction*, v. 2, n. CSCW, p. 1–22, nov. 2018, p. 4.

preconceituosos direcionados a homossexuais.[108] Nos Estados Unidos, foram reportados casos de discriminação contra pessoas de origem latina por trabalharem em fábricas de embalagem de carne, setor este cujos locais de trabalho foram confirmados como foco de milhares de casos de COVID-19.[109]

4.1.2 Desvirtuamento da função e da finalidade

Outro risco vinculado ao uso de modelos analíticos baseados em dados agregados de geolocalização é o desvirtuamento da função e da finalidade a que originalmente destinados os dados no enfrentamento da pandemia. A considerar a dimensão coletiva dos direitos fundamentais à privacidade e à proteção de dados pessoais, a concretização desse risco pode desaguar em discriminação de grupos – incluídos entre estes agrupamentos as categorias ou grupos *ad hoc*[110] – e restrições a outros direitos fundamentais tais como liberdade de locomoção devido à determinação e execução de medidas de quarentena.[111] Durante a atual emergência sanitária, muito embora diversos países tenham utilizado dados de localização para monitorar e executar quarentenas em nível individual,[112] nada obsta que estas sejam aplicadas a grupos.[113]

---

[108] KIM, Nemo. South Korea struggles to contain new outbreak amid anti-gay backlash. *The Guardian*, 11 mai. 2020. Disponível em: https://amp.theguardian.com/world/2020/may/11/south-korea-struggles-to-contain-new-outbreak-amid-anti-lgbt-backlash?_twitter_impression=true. Acesso em: 26 jul. 2020. Segue o depoimento de uma pessoa sobre os fatos: "I admit it was a huge mistake to visit the gay district when the corona situation was not fully over", Lee Youngwu, a gay man in his 30s, told the Guardian. "But visiting the area is the only time when I can be myself and hang out with others similar to me. During the week, I have to pretend to like women". "My credit card company told me that they passed on my payment information in the district to the authorities. I feel so trapped and hunted down. If I get tested, my company will most likely find out I'm gay. I'll lose my job and face a public humiliation. I feel as if my whole life is about to collapse. I have never felt suicidal before and never thought I would, but I am feeling suicidal now".

[109] GABBATT, Adam. Latino workers face discrimination over spread of coronavirus in meat plants. *The Guardian*, 22 mai. 2020. Disponível em: https://www.theguardian.com/world/2020/may/25/latino-workers-coronavirus-discrimination-meat-plants. Acesso em: 27 jul. 2020.

[110] Sobre a possibilidade de ações discriminatórias sobre grupos, em profunda análise no contexto da publicidade comportamental *online*, cf. WACHTER, Sandra. Affinity Profiling and Discrimination by Association in Online Behavioural Advertising. *Berkeley Technology Law Journal*, v. 35, n. 2, 2020, p. 55-57 (no prelo).

[111] Cf. TAYLOR, Linnet. Safety in Numbers? Group Privacy and Big Data Analytics in the Developing World. In: TAYLOR, Linnet; FLORIDI, Luciano; SLOOT, Bart van der (Eds.). *Group Privacy:* New Challenges of Data Technologies. Dordrecht: Springer, 2017. p. 24-25.

[112] PRIVACY INTERNATIONAL. *Quarantine enforcement and Covid-19*. Disponível em: https://privacyinternational.org/examples/quarantine-enforcement-and-covid-19. Acesso em: 28 jul. 2020.

[113] Na *Turning Point Model State Public Health Act*, a Seção 5-108 dispõe sobre hipóteses de autorização da quarentena e isolamento: "A state or local public health agency may isolate or quarantine an individual or group of individuals pursuant to rules or regulations promulgated by the state public health agency consistent with the provisions of this Section" (THE TURNING POINT PUBLIC HEALTH STATUTE MODERNIZATION COLLABORATIVE. *The Model State Public Health Act*. Disponível em: https://law.asu.

Dentre os alvos de possível violação do princípio da não discriminação estão migrantes, cujos padrões de deslocamento podem ser precisados em tempo real.[114] Por motivos semelhantes, o corrompimento da função e propósito iniciais pode igualmente desembocar em perseguição a participantes de protestos[115] e adversários de grupo político que esteja no poder, violando liberdades públicas de expressão e de reunião, por exemplo.

4.2 Parâmetros normativos aplicáveis da LGPD

Apesar de a LGPD, regulando a atividade de tratamento de dados pessoais, possuir uma perspectiva eminentemente individual de tutela – como, aliás, tradicionalmente se desenvolveu o direito de proteção de dados –, existem elementos normativos que apontam para a acomodação em sua estrutura da dimensão coletiva da privacidade e da proteção de dados pessoais e o cuidado com os riscos que o tratamento de dados gera tanto a interesses individuais como interesses de ordem coletiva, o que é imprescindível para oferecer diretrizes e soluções ao caso do uso de dados agregados de geolocalização por tecnologias de perfilamento para o combate à pandemia de COVID-19.

edu/sites/default/files/multimedia/faculty-research/centers/phlp/turning-point-model-act.pdf. Acesso em: 28 jul. 2020).

[114] Linnet Taylor explica como esses riscos a migrantes atingem o nível coletivo: "The risk attached to such practices is not the uncovering of individual identity. Digital traces from the phones migrants carry with them may be traceable to registered SIM cards in their countries of origin, but in fact names and addresses at the place of origin would not be important in comparison to the ability to track the movement of the group. Unwanted migrants may be caught on an individual basis, but are resisted by receiving states on the group level. For example, if a group of people carrying mobile phones are attempting to cross the Mediterranean and enter the EU, they can be tracked in real time by anyone with access to the data. The data will also show their place of origin via the phone's record of their original network provider, and (if it is a smart phone) will show the networks they have connected to along the way, making it possible to identify whether they have taken an overland route and are therefore likely to be undocumented. The phone data thus conveys how many people are moving, where they come from, and the route they have taken. The value of this information is its potential to identify where a group is on its way, and to understand whether this is likely to be a group which might be able to claim asylum and which would include minors and highly vulnerable people (for example Syrians fleeing violence), or whether it is likely to be a group of economic migrants" (TAYLOR, Linnet. Safety in Numbers? Group Privacy and Big Data Analytics in the Developing World. *In*: TAYLOR, Linnet; FLORIDI, Luciano; SLOOT, Bart van der (Ed.). *Group Privacy:* New Challenges of Data Technologies. Dordrecht: Springer, 2017. p. 22).

[115] Numa demonstração do que é o risco do desvirtuamento da função e finalidade de instrumentos implementados para lidar com a pandemia de COVID-19, em Minnesota, nos Estados Unidos, o comissário de segurança pública afirmou, em coletiva de imprensa, que as autoridades policiais fariam rastreamento de contato com as pessoas presas durante protestos: ''"It's contact tracing of who are they associated with, what platforms are they advocating for, and we have seen things like white supremacists who have posted things on platforms about coming to Minnesota," Harrington said. "We are checking to see, do the folks that we have made arrests on, are they connected to those platforms?"' (NG, Alfred. Contact tracers concerned police tracking protesters will hurt COVID-19 aid. *CNet,* 01 jun. 2020. Disponível em: https://www.cnet.com/news/contact-tracers-concerned-police-tracking-protesters-will-hurt-covid-19-aid/. Acesso em: 27 jul. 2020).

Primeiramente, deve se atentar para a abertura do texto legislativo à noção de *proteção de dados desde a concepção* (*data protection by design*), o que se faz a partir (i) da prescrição aos agentes de tratamento do dever de adoção de medidas de segurança adequadas à proteção de dados "desde a fase de concepção do produto ou do serviço até a sua execução",[116] e (ii) pela consagração do princípio da prevenção, que estabelece que o tratamento de dados pessoais deve ser acompanhado (ou nele incorporado) mecanismos de prevenção de danos, isto é, atenuação de riscos.[117] O preceito tem significado mais profundo do que uma recomendação de cunho técnico de ser preferível considerar aspectos de proteção de dados desde o estágio inicial do processo de desenvolvimento de produtos e serviços ao invés de fazer adaptações posteriores.[118] Proteção de dados desde a concepção significa, na verdade, um imperativo de incorporação dos preceitos do sistema jurídico de proteção de dados pessoais nas infraestruturas de informação e comunicação em que se operam os fluxos de dados, em especial infraestrutura da computação preemptiva (*preemptive computing*), integrada pelas tecnologias de perfilamento e analítica de dados.[119]

Assim, não há como conter a regulação da atividade de tratamento de dados pessoais tão somente na seara dos interesses individuais. Stefano Rodotà, ao fim do século passado, se apercebeu do alcance para além do indivíduo que o tratamento de dados pessoais ensejava na nova infraestrutura da informação:

> É necessário valorar diretamente a posição e o significado da nova 'infraestrutura informativa'. [...] Estamos diante de questões que, pela complexidade dos meios empregados e o número de sujeitos interessados, podem ser corretamente colocadas apenas em chave de interesses coletivos.

[116] LGPD, art. 46, §2º.

[117] Neste sentido: DONEDA, Danilo; MENDES, Laura Schertel. Um perfil da nova Lei Geral de Proteção de Dados brasileira. *In*: BELLI, Luca; CAVALLI, Olga (Org.). *Governança e Regulações da Internet na América Latina*. Rio de Janeiro: FGV Direito Rio, 2018. p. 316.

[118] Numa vertente técnica dos conceitos de *data protection by design* e *privacy by design*: "The principle 'Privacy/data protection by design' is based on the insight that building in privacy features from the beginning of the design process is preferable over the attempt to adapt a product or service at a later stage. The involvement in the design process supports the consideration of the full lifecycle of the data and its usage" (DANEZIS, George *et al*. *Privacy and Data Protection By Design* – From Policy to Engineering. [S.l.]: ENISA, 2015. p. 11. Disponível em: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design. Acesso em: 20 mai. 2020).

[119] A proteção de dados desde a concepção deve ser lida como uma expressão do que Hildebrandt chama de "proteção jurídica desde a concepção" (*legal protection by design*). Segundo a autora: "The point of departure is the task of articulating compatibility with a legal norm into an architecture, protocol, standard, hardware configuration, operating system, App or grid" (HILDEBRANDT, Mireille. *Smart Technologies and The End(s) of Law*. Cheltenham-Northampton: Edward Elgar, 2015. p. 218).

> [...]
>
> Se o fim a se alcançar é aquele da realização do melhor uso possível de um dos mais importantes recursos de base da sociedade do futuro, a via a se seguir é aquela que, coerentemente às indicações das análises precedentes, conduz à expansão do poder coletivo.[120]

Em segundo lugar, há que se considerar o regramento da lei de proteção de dados brasileira sobre a construção e a aplicação de perfis. As poucas disposições legais com as quais a LGPD regula diretamente a implementação de técnicas de perfilamento automatizado (LGPD, arts. 12, §2º[121] e 20[122]) aparentam, numa primeira leitura, incompatíveis com o movimento de expansão normativa à dimensão coletiva sustentada acima. No entanto, a reflexão cuidadosa aponta para certa porosidade do texto legal a interesses de grupos devido ao próprio funcionamento da técnica de perfilamento automatizado e da finalidade da LGPD em proteger direitos e liberdades fundamentais da pessoa humana frente às tecnologias digitais que a utilizam, desenvolvidas com os avanços da analítica de dados e dos sistemas algorítmicos de tratamento intensivo de informações.

Os arts. 12, §2º e 20, respectivamente, têm por objeto as fases de *criação* do perfil e de sua *aplicação*, sendo esta base para tomada de decisão automatizada.[123] [124] Enquanto aquele primeiro dispositivo alude à "formação de perfil

[120] RODOTÀ, Stefano. *Tecnologie e diritti.* Bolonha: Il Mulino, 1995. p. 36, 38. Tradução livre de: "È necessario valutare direttamente la posizione e il significato della nuova 'infrastruttura informativa'. [...] Siamo di fronte a questioni che, per il complesso di mezzi impiegati ed il numero di soggetti interessati, possano esse correttamente impostate soltante in chiave di interessi collettivi. [...] Se il fine da raggiungere e quello di realizzare la miglior utilizzazione possibile di una delle più importanti risorse di base della società del futuro, la via da seguire è quella che, coerentemente alle indicazioni dell'analisi precedenti, conduce all'espansione del potere collettivo".

[121] "Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. [...] §2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada".

[122] "Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. [...]".

[123] Sobre o tema, no contexto do direito europeu: cf. BRKAN, Maja. Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International Journal of Law and Information Technology*, v. 27, n. 2, p. 91–121, 2019, p. 96-97.

[124] A respeito da noção de decisão automatizada, é válido fazer alguns esclarecimentos. A atividade de tratamento automatizado de dados pessoais ou mesmo não pessoais pode ou não desaguar em efetiva tomada de decisão automatizada (cf. KAMARINOU, Dimitra; MILLARD, Christopher; SINGH, Jatinder. Machine Learning with Personal Data. *In:* LEENES, Ronald *et al. Data Protection and Privacy:* The Age of the Intelligent

comportamental", o segundo se refere textualmente a "definir o seu perfil":[125] duas diferentes etapas. Com isso, a LGPD visa estabelecer uma regulação jurídica aplicável ao processo complexo de que, havendo operações de tratamento de dados pessoais, o perfilamento automatizado é parte integrante.

A lei e seu regime geral incide antes da *construção* do perfil, quando esta fase é precedida da *coleta* de dados de caráter pessoal (*v. g.*, nome, endereço, número de telefone e dados de geolocalização de usuário de telefone celular). Duas possibilidades se abrem ao controlador que tenha o propósito de usar perfilamento automatizado em sua atividade e *criar* perfis: (i) processar dados pessoais para deles obter como *output* modelos estatísticos ou perfis personalizados[126] (*v.g.*, padrões de velocidade e deslocamento de proprietário de carro semiautônomo identificados pelo *software* embutido no veículo); ou (ii) anonimizar as informações pessoais para então processá-las e minerá-las para formar modelos estatísticos ou perfis personalizados[127] ou de grupo (*group profiling*[128]) – *v.g.*, modelos preditivos de mobilidade populacional baseado em dados agregados de localização de usuários de telefone celular.

O intérprete deve se atentar ao fato de que o art. 12, §2º, não é aplicável à situação (i) acima, uma vez que os dados pessoais objeto de tratamento durante a etapa de formação de perfis personalizados já ensejam a aplicação do regime geral de proteção de dados. O texto normativo é aplicável na situação da alternativa (ii), visto que cuida de uma particularidade do assunto versado no *caput* da disposição legal. Significa isso dizer que, dados a princípio anonimizados – portanto, qualificados preliminarmente como dados não pessoais – se utilizados para "formação de perfil comportamental *de determinada pessoa, se identificada*" hão de ser considerados dados pessoais para fins de aplicação da LGPD.

Machines. Oxford: Hart Publishing, 2017, p. 95). É o que ocorre em áreas, por exemplo, como análise de risco de crédito, *high-frequency trading* no mercado financeiro, e análise para identificação de fraude fiscal. Em termos conceituais, tomada de decisão automatizada pode ser entendida como aquela realizada sem intervenção humana (BRKAN, Maja. *Op. cit.*, p. 93), ou, ainda, "a habilidade de realizar decisões por meios tecnológicos sem o envolvimento humano" (ARTICLE 29 WORKING PARTY. *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679*. Brussels: [s.n.], p. 8).

[125] Nesse ponto reside uma das críticas que podem ser feitas à redação do art. 20, *caput*. É incorreto falar em "decisões destinadas a definir o seu perfil". Como já visto, no tratamento de dados em que há emprego de perfilamento automatizado, a tomada de decisão se dá após a construção do perfil e com suporte na sua aplicação a indivíduo ou grupo.

[126] Sobre esse tipo de perfil vide nota de rodapé nº 74.

[127] É possível que esse tipo de perfil seja construído a partir de dados anonimizados (SCHREURS, Wim *et al*. *Cogitas Ergo Sum:* The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector. *In*: GUTWIRTH, Serge; HILDEBRANDT, Mireille (Ed.). *Profiling the European Citizen:* Cross-Disciplinary Perspectives. New York: Springer, 2008. p. 249).

[128] *Vide* nota de rodapé nº 75 e o item 3.2.

A parte final do dispositivo colocada em destaque parece sugerir que o imperativo legal é destinado a reger a elaboração perfis personalizados apenas, reputando pessoais os dados usados para sua formação. Essa interpretação, entretanto, afasta do âmbito de aplicação da lei tipos de classificação algorítmica de grupo, as quais são amplamente utilizadas por agentes de tratamento e geram significativos impactos na vida de indivíduos que são representados como pertencentes a um certo grupo (comunidades ou categorias) – o que, aliás, se dá com o tratamento de dados agregados de geolocalização de usuários de *smartphone*, conforme defendido neste *paper*. A interpretação sistemática desse dispositivo, que considera os fundamentos da lei, seus princípios, a fim de se garantir a aplicação de certos direitos, deveres de transparência e salvaguardas em dimensão coletiva, parece ser a única consistente com a proteção e promoção de direitos e liberdades fundamentais.[129]

Ademais, a regulação do perfilamento automatizado na fase da *aplicação* de perfil e tomada de decisão do art. 20, consagra no §1º um ponto visível de abertura à dimensão coletiva da proteção de dados e da privacidade. Ao determinar que o controlador possui o dever de informar, sob requerimento, de forma clara e adequada "a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada", a LGPD abre espaço para que explicações em nível de grupo, como quando implementada técnica de perfilamento de grupo (*group profiling*) para a tomada de decisão automatizada, sejam fornecidas a titulares de dados. Cumpre ressaltar que no campo da ciência da computação há propostas de sistemas de explicabilidade em vários níveis, com maior ou menor granularidade.[130]

[129] Jef Auloos e René Mahieu defendem haver importante dimensão coletiva do direito de acesso na GPDR: "Access rights are often used collectively to pursue social justice goals that go beyond data protection and privacy. In light of how they empower individuals to obtain fine-grained information about the data infrastructures that surround and have an impact on them, access rights can be very valuable in pursuing (social) justice goals. Information from access rights may be used to seek inferences, data and metadata about prediction and training data which can reveal how systems function and affect individuals/society. This information may be compiled to shine light on the functioning of a model, or compared across individuals, demographics or applications so as to reveal potential discriminatory practices. Access rights might also be able to shine light on where models come from, which actors were involved in training and building them, and when. This can be important in a wide variety of circumstances, not in the least to lay bare and scrutinise the 'manipulative potential of algorithmic processes', the importance of which has recently been confirmed by the Council of Europe. The OpenSchufa; Uber, and FairTube, cases provide evident illustrations of how crowd-sourcing access rights can be used to achieve social justice aims" (AULOOS, Jef; MAHIEU, René. *Recognising and Enabling the Collective Dimension of the GDPR and the Right of Access*. Disponível em: https://osf.io/preprints/lawarxiv/b5dwm. Acesso em: 03 set. 2020).

[130] Nessa direção, cf. RAMAMURTHY, Karthikeyan N. *et al*. *Model Agnostic Multilevel Explanations*. p. 1-21, 2020. Disponível em: https://arxiv.org/pdf/2003.06005.pdf. Acesso em: 03 set. 2020.

Em terceiro lugar, a LGPD prevê a realização de relatório de impacto à proteção de dados pessoais[131] (RIPDP) pelo controlador nas hipóteses em que o tratamento de dados pessoais ocasione riscos (mais graves) a direitos e liberdades fundamentais. Não obstante a lei não disciplinar os requisitos do RIPDP, deixando sua regulamentação a cargo da Autoridade Nacional de Proteção de Dados (ANPD),[132] pode-se deduzir do sistema brasileiro de proteção de dados pessoais alguns de seus contornos como instrumento para avaliação de riscos e impactos gerados pelo tratamento de dados pessoais por sistemas algorítmicos. Em vista dos limites do presente trabalho, indica-se duas características apenas: (i) ato resultante de procedimento iterativo; e (ii) instrumento de proteção e promoção de direitos dos titulares de dados.

O RIPDP deve ser visto como resultado de ato complexo, antecedente à implementação da atividade de tratamento de dados, que reflete o estado da dinâmica avaliação de riscos causados pelo tratamento de dados pessoais sob investigação, apreciadas e estabelecidas as medidas e salvaguardas apropriadas à mitigação dos riscos a direitos e liberdades divisados. O procedimento do qual o relatório é produto tem caráter *iterativo*,[133] ou seja, não se exaure num ato único, mas é revisitado múltiplas vezes, enquanto não cessa a própria atividade de tratamento de dados que cria riscos a indivíduos e grupos. Assim, a avaliação de impacto à proteção de dados pessoais compartilha da dinamicidade própria dos avanços tecnológicos e os seus (novos) riscos.

Além disso, o RIPDP se insere na sistema de proteção de dados pessoais como um poderoso instrumento para proteger e promover direitos dos titulares, visto que a metodologia de avaliação de impacto da implementação de um sistema algorítmico há de desincumbir-se de encargo justificativo – próprio à ideia de *accountability* –, que posteriormente poderá ser base para o cumprimento de direitos dos titulares (*v.g.*, direito ao acesso, à informação, à explicação), informando

[131] O art. 5º, XVII, da LGPD define relatório de impacto à proteção de dados pessoais como "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco".

[132] LGPD, art. 55-J, XIII.

[133] Nessa direção, em relação ao direito europeu de proteção de dados pessoais: cf. KAMINSKI, Margot E.; MALGIERI, Giancarlo. Multi-layered explanations from algorithmic impact assessments in the GDPR. *FAT*2020 – Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency,* p. 68-79, 2020, p. 72; ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is* "likely to result in a high risk" *for the purposes of Regulation 2016/679*. Bruxelas: [s.n.], 2017. p. 16. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236. Acesso em: 28 jul. 2020; KLOZA, Dariusz *et al*. Towards a method for data protection impact assessment: Making sense of GDPR requirements. *d.pia.lab*, Policy Brief n. 1, 2019, p. 2. Disponível em: https://cris.vub.be/files/48091346/dpialab_pb2019_1_final.pdf. Acesso em: 21 set. 2020.

o controlador, por exemplo, de "critérios" e *categorias* resultantes de perfilamento de grupo aplicado em certa decisão automatizada. É nesse ponto que a dimensão coletiva ou de grupos do direito à proteção de dados pessoais tem expressão, em fina sintonia com o que se afirmou anteriormente sobre a aplicação de perfis e o art. 20, §1º, da LGPD. Ao propor um modelo de explicações multicamadas ou multinível (*multilayered explanations*) a partir da avaliação de impacto à proteção de dados, Kaminski e Malgieri afirmam que a descrição da atividade de tratamento de dados de sistema algorítmico a ser feita numa análise de impacto pode se dar em diversos níveis:

> Na verdade, a descrição do tratamento algorítmico de dados, incluindo fundamentos e critérios, pode muito bem ser especificada tanto no nível do grupo quanto no nível individual: a descrição das categorias de dados e sua pertinência, do procedimento de construção do perfil e sua relevância e uso, dos efeitos e salvaguardas, podem ser baseadas em grupos de indivíduos semelhantes afetados por essa decisão automatizada ou mesmo em um único titular de dados específico que está fazendo uma solicitação de explicação.[134]

Dessa forma, exigir a avaliação de impacto à proteção de dados a entes públicos ou privados responsáveis pela construção e/ou aplicação de modelos de mobilidade baseados no uso de dados agregados de geolocalização teria a função de demonstrar a justificação, entre outros aspectos, da relevância, adequação e pertinência de categorias ou grupos *ad hoc* e das salvaguardas implementadas na dimensão coletiva.[135] Cumpre destacar que salvaguardas apropriadas podem desempenhar o importante papel de atenuar o risco de desvirtuamento de função e finalidade do uso dos dados agregados de localização durante a situação de emergência sanitária. Para tanto é imperativo a estipulação das salvaguardas de *proibição de uso dos dados para fins outros que não o de enfrentamento da pandemia de COVID-19* e o seu *apagamento uma vez encerrada a situação de*

[134] KAMINSKI, Margot E.; MALGIERI, Giancarlo. Multi-layered explanations from algorithmic impact assessments in the GDPR. *FAT*2020 – Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency,* p. 68-79, 2020, p. 76-77. Tradução livre de: "Indeed, the description of algorithmic processing, including rationales and criteria, might well be specified on both a group level and on individual level: the description of data categories and their pertinence, of the profile-building procedure and its relevance and use, of effects and safeguards can be based on groups of similar individuals affected by that automated decision or even on a single specific data subject who is making an explanation request".

[135] Mais sobre a importância da avaliação de risco em relação à "privacidade coletiva": MANTELERO, Alessandro. From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era. *In*: TAYLOR, Linnet; FLORIDI, Luciano; SLOOT, Bart van der (Ed.). *Group Privacy: New Challenges of Data Technologies*. Dordrecht: Springer, 2017. p. 150 *et seq*.

emergência, além das *justificações da relevância, adequação e pertinência de categorias ou grupos* ad hoc.

Por fim, atenção merece o risco de reidentificação citado. Considerada a agregação de dados uma técnica de anonimização, a postura, a princípio, que poder-se-ia adotar seria a de sustentar a impertinência dos usos em questão ao âmbito de aplicação material da LGPD. Contudo, para além dos aspectos da dimensão coletiva da proteção de dados pessoais a que se deu destaque acima, o ataque inferencial MIA mostra que há possibilidade de reidentificação de indivíduos cujos dados de localização foram tratados para posterior agregação e treinamento de modelos analíticos de mobilidade. Nesse sentido, a LGPD estabelece no art. 12, *caput*, ser lei aplicável quando o processo de anonimização ao qual foram submetidos os dados pessoais for revertido, "utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido". Significa dizer que, para ser efetivamente anonimizado, o dado não pode ter associação com pessoa natural identificada ou identificável de forma permanente e irreversível,[136] não apenas em relação ao próprio agente de tratamento que aplica a técnica, mas também a qualquer outra pessoa.[137]

Para a lei brasileira, porém, não basta a simples possibilidade de superação da anonimização para se concluir pela ineficácia da técnica e, por consequência, o caráter pessoal da informação objeto de tratamento. É necessário nessa avaliação do risco de reidentificação do tratamento de dados agregados de geolocalização a observância o critério dos "meios e esforços razoáveis". Trata-se de critério que depende de aspectos objetivos e contextuais, uma vez que busca ser balizado por fatores como custos e tempo de trabalho exigidos para a reidentificação, o estado da arte da tecnologia existente no período de duração do tratamento e os riscos de falhas técnicas, por exemplo.[138]

[136] Neste particular, a LGPD prescreve: "Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido". *Vide* também: MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor:* linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 57-58.

[137] A assertiva está em linha com a concepção ampla da noção de dado pessoal e a corrente *objetiva* ou *absoluta*. A respeito das abordagens *relativa* e *objetiva* do conceito de dado pessoal, cf. BORGESIUS, Frederik Zuiderveen. Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation. *Computer Law and Security Review*, v. 32, n. 2, p. 256–271, 2016, p. 8-9; SPINDLER, Gerald; SCHMECHEL, Philipp. Personal Data and Encryption in the European General Data Protection Regulation. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, v. 7, p. 163-177, 2016, p. 165; PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, v. 10, n. 1, p. 40–81, 2018, p. 46, 64.

[138] É o que dispõe o art. 12, §1º, da LGPD: "A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios".

Ainda que se considere que os ataques inferenciais atualmente configuram meios e exijam esforços não razoáveis para identificar titulares de dados, agentes que tratam dados de geolocalização agregados devem adotar as medidas de segurança e defesas apropriadas para atenuar o risco. Chama-se atenção, ressoando as conclusões de Pyrgelis, Troncoso e De Cristofaro que, em relação a dados agregados de localização, não há uma única estratégia bastante de proteção contra MIAs que preserve em nível ótimo a utilidade da análise dos dados agregados; há diferentes medidas que funcionam melhor para diferentes aplicações analíticas.[139]

5 Considerações finais

Eventos da envergadura da pandemia atualmente vivenciada causam marcas na sociedade e nas instituições, senão indeléveis, permanentes o bastante para impactar sistemas de direitos e garantias – arrefecendo-os por vezes – e se fazer sentidas mesmo após mais de uma década. Os atos terroristas de 2001 foram, muito provavelmente, os últimos eventos históricos com repercussões tão significativas quanto duradouras sobre o campo da proteção de dados pessoais e da tutela da privacidade na era digital. A pandemia de COVID-19 e seus efeitos nas relações sociais e no uso das tecnologias de dados podem ter análogas consequências sobre os direitos à proteção de dados pessoais e à privacidade, haja vista os riscos de lesão a tais direitos. A democracias constitucionais como a brasileira cabe o redobrado cuidado e atitude preventiva.

O prevalecente uso no Brasil de tecnologias de perfilamento alimentadas pelo processamento de dados agregados de geolocalização de dispositivos móveis para combater a COVID-19 pode gerar riscos de reidentificação dos usuários de telefones celulares por ataques inferenciais (MIA) e de desvirtuamento de função e finalidade originária do tratamento dos dados. Sem prejuízo da sua utilidade prática, é preciso se atentar que ambos têm possíveis desdobramentos lesivos ao direito à proteção de dados pessoais, à tutela da privacidade e ao princípio da não discriminação, tocando as dimensões individual e coletiva. Esta última, aliás, tem sua afirmação no ordenamento jurídico brasileiro resultante de construção teórica e dogmática que parte da distinção entre o direito à proteção de dados pessoais e o direito à privacidade, e encontra expressão na estrutura regulatória e respectivos instrumentos da LGPD. Muito embora esta tenha uma tônica voltada ao indivíduo,

[139] PYRGELIS, Apostolos; TRONCOSO, Carmela; DE CRISTOFARO, Emiliano. Measuring Membership Privacy on Aggregate Location Time-Series. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, v. 2, n. 4, 2020, p. 2-3.

pessoa natural identificada ou identificável, a lei possui elementos normativos que comportam interesses coletivos e sua tutela.

Assim, ainda que satisfatoriamente atenuado o risco de reidentificação dos usuários de telefone celular com as medidas de segurança e defesas computacionais pertinentes, abre-se ensejo a interpretação sistemática da LGPD, bem como do art. 72, §2º, da Lei Geral de Telecomunicações, que seja capaz de lidar com o risco de violação à privacidade de grupo. Para tanto há que se considerar como balizas hermenêuticas, primeiramente, a proteção de dados desde a concepção como imperativo de incorporação dos preceitos do sistema jurídico de proteção de dados pessoais nas infraestruturas de informação e comunicação que suportam os fluxos de dados, em especial infraestrutura da computação preemptiva (*preemptive computing*), integrada pelas tecnologias de perfilamento e analítica de dados.

Em segundo lugar, o regramento incidente sobre técnicas de perfilamento automatizado deve alcançar tanto a formação de perfis (LGPD, art. 12, §2º) como sua aplicação para tomada de decisão automatizada (LGPD, art. 20). É dizer, para fins de aplicação da lei, são tidos por pessoais aqueles dados qualificados preliminarmente como dados não pessoais, se utilizados para "formação de perfil comportamental". Ademais, sendo a aplicação do perfil base para tomada de decisão automatizada, há que se entender admissível o exercício do direito à explicação a respeito dos critérios e lógica utilizada na dimensão de grupo. Por fim, há pertinência na aplicação de instrumentos como o RIPDP – que poderá dar substância ao cumprimento do dever de justificação/explicação –, bem como adequadas salvaguardas a entes públicos ou privados que lancem mão de tecnologias de perfilamento com o tratamento de dados agregados de geolocalização.

Abstract: The present work aims to analyze the risks to privacy and to the protection of personal data – in both their individual and collective dimensions – generated by profiling based on the use of mobile phone geolocation aggregated data, seeking to investigate the existence of legal parameters found in the Brazilian General Data Protection Regulation (LGPD) and applicable to the identified risks. For this purpose, the present work proposes the following research questions: (i) what risks to the fundamental rights to privacy and to the protection of personal does data profiling technologies based on the use of geolocation aggregated data from mobile devices generate at the individual and collective levels in the fight against the COVID-19 pandemic in Brazil? (ii) Does the LGPD provide normative parameters applicable in order to deal with these risks, in particular to groups created from algorithmic systems? In a data-driven society, automated profiling plays out an important role in the information and communication infrastructure of preemptive computing. In this context, the collective dimension of both the right to privacy and the right to the protection of personal data is affirmed. The identified risks to data protection and privacy, including at the collective or group level, are both re-identification of mobile phone users through inferencial attacks (membership inference attacks) and function creep of the data processing and its purpose. In order to deal with such risks, it is suggested a systematical

interpretation of LGPD legal parameters, regarding automated profiling and data protection impact assessments.

Keywords: Profiling; geolocation data; COVID-19; individual and collective risks; group privacy.

Referências

ALTMAN, Irwin. Privacy: A Conceptual Analysis. *Environment and Behavior*, v. 8, n. 1, p. 7-29, 1976.

ARCHARD, David. The Value of Privacy. *In*: CLAES, E.; DUFF, A.; GUTWIRTH, S. (Ed.). *Privacy and the Criminal Law*. Antwerpen-Oxford: Intersentia, 2006. p. 13-32.

ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 5/2014 on Anonymisation techniques*. Bruxelas: [s.n.], 2014. Disponível em: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Acesso em: 28 jul. 2020.

ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*. Bruxelas: [s.n.], 2017. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236. Acesso em: 28 jul. 2020.

ARTICLE 29 WORKING PARTY. *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679*. Brussels: [s.n.], 2018. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053. Acesso em: 31 ago. 2020.

AULOOS, Jef; MAHIEU, René. *Recognising and Enabling the Collective Dimension of the GDPR and the Right of Access*. Disponível em: https://osf.io/preprints/lawarxiv/b5dwm. Acesso em: 03 set. 2020.

BENGTSSON, L. *et al*. Improved response to disasters and outbreaks by tracking population movements with mobile phone network data: A post-earthquake geospatial study in Haiti. *PLoS Medicine*, v. 8, n. 8, p. 1-7, 2011.

BLOUSTEIN, Edward. J. Group Privacy: A Right to Huddle. *In*: BLOUSTEIN, Edward. *Individual and Group Privacy*. New York: Routledge, 2017. p. 123-186.

BOSCO, Francesca *et al*. Profiling technologies and fundamental rights: an introduction. In: CREEMERS, Niklas *et al*. *Profiling Technologies in Practice*: Applications and Impact on Fundamental Rights and Values. Oisterwijk: Wolf Legal Publishers, 2017. p. 9-20.

BRASIL tem recorde de casos diários de Covid-19, mais de 65 mil. *Folha de São Paulo*, 22. jul. 2020. Disponível em: https://www1.folha.uol.com.br/equilibrioesaude/2020/07/brasil-tem-recorde-de-casos-diarios-de-covid-19-mais-de-65-mil.shtml. Acesso em: 22 jul. 2020.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). *Ações Diretas de Inconstitucionalidade n. 6387, 6388, 6389, 6390 e 6393/DF*. Relatora: Ministra Rosa Weber, 07 de maio de 2020.

BRASIL. *Lei n. 9.472, de 16 de julho de 1997*. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9472.htm. Acesso em: 23 set. 2020.

BRASIL. *Lei n. 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 28 ago. 2020.

BRKAN, Maja. Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International Journal of Law and Information Technology*, v. 27, n. 2, p. 91-121, 2019.

COHEN, Julie E. *Configuring the Networked Self*: Law, Code, and the Play of Everyday Practice. New Haven: Yale University Press, 2012.

CORONAVIRUS in Latin America: What governments are doing to stop the spread. *Global Americans,* 26 mar. 2020. Disponível em: https://theglobalamericans.org/2020/03/coronavirus-in-latin-america/. Acesso em: 30 jul. 2020.

CORTE, Lorenzo Dalla. A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection. *In*: HALLINAN, D. *et al*. (Ed.). *Data Protection and Privacy:* Data Protection and Democracy. Oxford: Hart Publishing, 2020. p. 27–58.

CUKIER, Kenneth; MAYER-SCHÖNBERGER, Viktor. *Big Data:* A Revolution That Will Transform How We Live, Work, and Think. Boston: Houghton Mifflin Harcourt, 2013.

DANEZIS, George *et al*. *Privacy and Data Protection By Design* – From Policy to Engineering. [S.l.]: ENISA, 2015. Disponível em: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design. Acesso em: 20 maio 2020.

DE HERT, Paul; GUTWIRTH, Serge. Privacy, data protection and law enforcement: opacity of the individual and transparency of power. *In*: CLAES, Erik; GUTWIRTH, Serge; DUFF, Antony (Ed.). *Privacy and the Criminal Law*. Antwerpen-Oxford: Intersentia, 2006. p. 61-104.

DE HERT, Paul; GUTWIRTH, Serge. Regulating Profiling in a Democratic Constitutional State. *In*: HILDEBRANDT, Mireille; GUTWIRTH, Serge (Ed.). *Profiling the European Citizen:* Cross-disciplinary Perspectives. [S. l.]: Springer, 2008. p. 271-293.

DE MONTJOYE, Yves-Alexandre *et al*. Unique in the Crowd: The privacy bounds of human mobility. *Scientific Reports*, v. 3, p. 1-5, 2013.

DONEDA, Danilo; MENDES, Laura Schertel. Um perfil da nova Lei Geral de Proteção de Dados brasileira. *In*: BELLI, Luca; CAVALLI, Olga (Org.). *Governança e Regulações da Internet na América Latina*. Rio de Janeiro: FGV Direito Rio, 2018. p. 309-324.

DYE, Christopher *et al*. Data sharing in public health emergencies: a call to researchers. *Bulletin of the World Health Organization*, v. 94, p. 158, 2016. Disponível em: https://www.who.int/bulletin/volumes/94/3/16-170860.pdf. Acesso em: 25 jun. 2020.

EUROPEAN DATA PROTECTION BOARD. *Statement on the processing of personal data in the context of the COVID-19 outbreak*. Disponível em: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf. Acesso em: 30 jul. 2020.

FAYYAD, U.; PIATETSKY-SHAPIRO, G.; SMYTH, P. Knowledge Discovery and Data Mining: Towards a Unifying Framework. *KDD-96 Proceedings*, p. 82-88, 1997.

FIDIS. *Descriptive analysis and inventory of profiling practices*. Disponível em: http://www.fidis.net/resources/fidis-deliverables/profiling/int-d72000/doc/4/. Acesso em: 16 jul. 2020.

FLORIDI, Luciano. Four challenges for a theory of informational privacy. *Ethics and Information Technology*, v. 8, n. 3, p. 109-119, 2006.

FLORIDI, Luciano (Ed.). *The Onlife Manifesto:* Being Human in a Hyperconnected Era. Heidelberg-London-New York-Dordrecht: Springer, 2015.

FUSTER, Gloria González. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Londres-Heildelberg-Nova Iorque: Springer, 2014.

FUSTER, Gloria González; GUTWIRTH, Serge. Opening up personal data protection: A conceptual controversy. *Computer Law and Security Review*, v. 29, n. 5, p. 531–539, 2013.

GELLERT, Raphaël. Understanding the notion of risk in the General Data Protection Regulation. *Computer Law and Security Review*, v. 34, n. 2, p. 279-288, 2018.

GLOBAL PRIVACY ASSEMBLY. *GPA COVID-19 Response Repository*. Disponível em: https://globalprivacyassembly.org/covid19/. Acesso em: 30 jul. 2020.

GRAY, Stacey. A Closer Look at Location Data: Privacy and Pandemics. *Future of Privacy Forum*, 2020. Disponível em: https://fpf.org/2020/03/25/a-closer-look-at-location-data-privacy-and-pandemics/. Acesso em: 20 abr. 2020.

GRUPO MAVE. *Previsão de curto prazo nos estados brasileiro*s. Disponível em: https://covid-19.procc.fiocruz.br/prediction/. Acesso em: 28 jul. 2020.

HILDEBRANDT, Mireille. Defining Profiling: A New Type of Knowledge? *In*: GUTWIRTH, Serge; HILDEBRANDT, Mireille (Ed.). *Profiling the European Citizen:* Cross-Disciplinary Perspectives. New York: Springer, 2008. p. 17-45.

HILDEBRANDT, Mireille. Profiling and Identity of the European Citizen. In: HILDEBRANDT, Mireille; GUTWIRTH, Serge (Ed.). *Profiling the European Citizen:* Cross-Disciplinary Perspectives. New York: Springer, 2008. p. 303-343.

HILDEBRANDT, Mireille. *Smart Technologies and The End(s) of Law*. Cheltenham-Northampton: Edward Elgar, 2015.

HILDEBRANDT, Mireille. Privacy and Identity. *In*: CLAES, E.; DUFF, A.; GUTWIRTH, S. (Ed.). *Privacy and the Criminal Law*. Antwerpen-Oxford: Intersentia, 2006. p. 43–57.

HILDEBRANDT, Mireille. Privacy as protection of the incomputable self: From agnostic to agonistic machine learning. *Theoretical Inquiries in Law*, v. 20, n. 1, p. 83-121, 2019.

HOWE, Neil. A Special Price Just For You. *Forbes*. Disponível em: https://www.forbes.com/sites/neilhowe/2017/11/17/a-special-price-just-for-you/#11e3c39290b3. Acesso em: 19 jul. 2020.

IROLLA, Paul. *Demystifying the Membership Inference Attack*. Disponível em: https://medium.com/disaitek/demystifying-the-membership-inference-attack-e33e510a0c39. Acesso em: 27 jul. 2020.

KAMARINOU, Dimitra; MILLARD, Christopher; SINGH, Jatinder. Machine Learning with Personal Data. *In*: LEENES, Ronald *et al*. *Data Protection and Privacy*: The Age of the Intelligent Machines. Oxford: Hart Publishing, 2017. p. 89-114.

KAMINSKI, Margot E.; MALGIERI, Giancarlo. Multi-layered explanations from algorithmic impact assessments in the GDPR. *FAT*'2020 – Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency,* p. 68-79, 2020.

KIM, Nemo. South Korea struggles to contain new outbreak amid anti-gay backlash. *The Guardian*, 11 mai. 2020. Disponível em: https://amp.theguardian.com/world/2020/may/11/south-korea-struggles-to-contain-new-outbreak-amid-anti-lgbt-backlash?__twitter_impression=true. Acesso em: 26 jul. 2020.

KLOZA, Dariusz *et al*. Towards a method for data protection impact assessment: Making sense of GDPR requirements. *d.pia.lab*, Policy Brief n. 1, 2019, p. 2. Disponível em: https://cris.vub.be/files/48091346/dpialab_pb2019_1_final.pdf. Acesso em: 21 set. 2020.

KRANZBERG, Melvin. Technology and History: "Kranzberg's Laws". *Johns Hopkins University Press*, v. 27, n. 3, p. 544-560, 1986.

LOTEMPIO, Jonathan *et al*. We Can Do Better: Lessons Learned on Data Sharing in COVID-19 Pandemic Can Inform Future Outbreak Preparedness and Response. *Science & Diplomacy*, v. 9, n. 2, jun. 2020. Disponível em: https://www.sciencediplomacy.org/article/2020/we-can-do-betterlessons-learned-data-sharing-in-covid-19-pandemic-can-inform-future. Acesso em: 27 ago. 2020.

MCDONALD, Sean M. Ebola: A Big Data Disaster - Privacy, Property, and the Law of Disaster Experimentation. *The Centre for Internet and Society*, n. 2016.01, 2016.

MANTELERO, Alessandro. From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era. *In*: TAYLOR, Linnet; FLORIDI, Luciano; SLOOT, Bart van der (Ed.). *Group Privacy:* New Challenges of Data Technologies. Dordrecht: Springer, 2017. p. 139-158.

MANTELERO, Alessandro. Responsabilità e rischio nel Reg. UE 2016/679. *Le Nuove Leggi Civili Commentate*, v. XL, n. 1, p. 144-164, 2017.

MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo G. *Curso de direito constitucional*. 3. ed. São Paulo: Saraiva, 2008.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor:* linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. *In*: SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscila (Coord.). *Lei Geral de Proteção de Dados* – Caderno Especial. São Paulo: Revista dos Tribunais, 2019. p. 35-56.

MITTELSTADT, Brent. From Individual to Group Privacy in Big Data Analytics. *Philosophy and Technology*, v. 30, n. 4, p. 475-494, 2017.

NAKAGAWA, Liliane. LGPD: Bolsonaro sanciona e lei começa a valer nesta sexta-feira. *Olhar Digital*, 17 set. 2020. Disponível em: https://olhardigital.com.br/noticia/lgpd-bolsonaro-sanciona-e-lei-comeca-a-valer-nesta-sexta-feira/107251. Acesso em: 25 set. 2020.

OLIVER, Nuria *et al*. Mobile phone data for informing public health actions across the COVID-19 pandemic life cycle. *Science Advances*, v. 6, n. 23, p. 1-7, 2020.

PEIXOTO, Pedro S. *et al*. Potential dissemination of epidemics based on Brazilian mobile geolocation data. Part I: Population dynamics and future spreading of infection in the states of Sao Paulo and Rio de Janeiro during the pandemic of COVID-19. *medRxiv*, April, 2020. Disponível em: https://www.medrxiv.org/content/10.1101/2020.04.07.20056739v1.full.pdf. Acesso em: 28 jul. 2020.

PRIVACY INTERNATIONAL. *Quarantine enforcement and Covid-19.* Disponível em: https://privacyinternational.org/examples/quarantine-enforcement-and-covid-19. Acesso em: 28 jul. 2020.

PYRGELIS, A.; DE CRISTOFARO, E.; ROSS, G. J. Privacy-friendly mobility analytics using aggregate location data. *GIS: Proceedings of the ACM International Symposium on Advances in Geographic Information Systems*, n. 1, 2016. Disponível em: https://arxiv.org/pdf/1609.06582.pdf. Acesso em: 27 jul. 2020.

PYRGELIS, Apostolos; TRONCOSO, Carmela; DE CRISTOFARO, Emiliano. What Does The Crowd Say About You? Evaluating Aggregation-based Location Privacy. *Proceedings on Privacy Enhancing Technologies*, v. 2017, n. 4, p. 156-176, 2017.

PYRGELIS, Apostolos; TRONCOSO, Carmela; DE CRISTOFARO, Emiliano. Measuring Membership Privacy on Aggregate Location Time-Series. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, v. 2, n. 4, 2020.

QUELLE, Claudia. Privacy, Proceduralism and Self-Regulation in Data Protection Law. *Teoria Critica Della Regolazione Sociale*, v. 1, n. 14, p. 89-106, 2017.

RAHMAN, Zara. Dangerous Data: The Role of Data Collection in Genocides. *The Engine Room*, 2016. Disponível em: https://www.theengineroom.org/dangerous-data-the-role-of-data-collection-in-genocides/. Acesso em: 22 jul. 2020.

RICOEUR, Paul. *O si-mesmo como outro*. São Paulo: Martins Fontes, 2014.

RIOS, Rafael S.; ZHENG, Kenneth I.; ZHENG, Ming-Hua. Data sharing during COVID-19 pandemic: what to take away. *Expert Review of Gastroenterology & Hepatology*, 2020. Disponível em: https://www.tandfonline.com/doi/full/10.1080/17474124.2020.1815533. Acesso em: 27 ago. 2020.

ROCHA, Roberto. The data-driven pandemic: Information sharing with COVID-19 is "unprecedented". *CBC*, 2020. Disponível em: https://www.cbc.ca/news/canada/coronavirus-date-information-sharing-1.5500709. Acesso em: 25 jun. 2020.

SANDVIK, Kristin; RAYMOND, Nathaniel. Beyond the Protective Effect: Towards a Theory of Harm for Information Communication Technologies in Mass Atrocity Response. *Genocide Studies and Prevention*, v. 11, n. 1, p. 9-24, 2017.

SCHREURS, Wim *et al*. *Cogitas Ergo Sum:* The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector. *In*: GUTWIRTH, Serge; HILDEBRANDT, Mireille (Ed.). *Profiling the European Citizen:* Cross-Disciplinary Perspectives. New York: Springer, 2008. p. 241-270.

SOLOVE, Daniel J. *The digital person:* technology and privacy in the information age. New York: New York University, 2004.

SOLOVE, Daniel. J. *Understanding Privacy*. Cambridge; London: Harvard University Press, 2008.

SPENCER, Shaun B. Privacy and Predictive Analytics in E-Commerce. *New England Law Review*, v. 49, p. 629-647, jan. 2015.

SUH, Jennifer J. et al. Distinguishing Group Privacy From Personal Privacy. *Proceedings of the ACM on Human-Computer Interaction*, v. 2, n. CSCW, p. 1–22, nov. 2018.

TAYLOR, Linnet. Safety in Numbers? Group Privacy and Big Data Analytics in the Developing World. *In*: TAYLOR, Linnet; FLORIDI, Luciano; SLOOT, Bart van der (Ed.). *Group Privacy:* New Challenges of Data Technologies. Dordrecht: Springer, 2017. p. 13-36.

THE TURNING POINT PUBLIC HEALTH STATUTE MODERNIZATION COLLABORATIVE. *The Model State Public Health Act*. Disponível em: https://law.asu.edu/sites/default/files/multimedia/faculty-research/centers/phlp/turning-point-model-act.pdf. Acesso em: 28 jul. 2020.

UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 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*, Estrasburgo, 04/05/2016. Disponível em: https://op.europa.eu/s/oe9q. Acesso em: 28 ago. 2020.

VALENTINO-DEVRIES, Jennifer; SINGER-VINE, Jeremy Singer-Vine; SOLTANI, Ashkan. Websites Vary Prices, Deals Based on Users' Information. *The Wall Street Journal*. Disponível em: https://www.wsj.com/articles/SB10001424127887323777204578189391813881534. Acesso em: 19 jul. 2020.

WACHTER, S. Affinity Profiling and Discrimination by Association in Online Behavioural Advertising. *Berkeley Technology Law Journal*, v. 35, n. 2, 2020 (no prelo).

WEISER, Mark. Ubiquitous computing. *Computer*, [s.l.], v. 26, n. 10, p. 72-73, out. 1993.

WESTIN, Alan F. *Privacy and Freedom*. New York: Atheneum, 1967.

WORLD HEALTH ORGANIZATION. *Q & A: How is COVID-19 transmitted?.* Disponível em: https://www.who.int/news-room/q-a-detail/q-a-how-is-covid-19-transmitted. Acesso em: 25 jul. 2020.

ZANFIR, Gabriela. Forgetting About Consent. Why The Focus Should Be On "Suitable Safeguards" in Data Protection Law. *In*: GUTWIRTH, Serge; LEENES, Ronald; DE HERT, Paul (Ed.). *Reloading Data Protection Law:* Multidisciplinary Insights and Contemporary Challenges. London: Springer, 2008. p. 237-257.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

MACHADO, Diego Carvalho; MENDES, Laura Schertel. Tecnologias de perfilamento e dados agregados de geolocalização no combate à COVID-19 no Brasil: uma análise dos riscos individuais e coletivos à luz da LGPD. *Direitos Fundamentais & Justiça,* Belo Horizonte, ano 14, p. 105-148, nov. 2020. Número especial.

Recebido em: 30.07.2020
Pareceres: 24.08.2020, 25.08.2020
Aprovado em: 14.09.2020