VII ENCONTRO VIRTUAL DO CONPEDI

INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL

EUDES VITOR BEZERRA

JÉSSICA AMANDA FACHIN

I61

Internet: dinâmicas da segurança pública internacional [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Eudes Vitor Bezerra; Jéssica Amanda Fachin – Florianópolis: CONPEDI, 2024.

Inclui bibliografia
ISBN: 978-85-5505-912-4
Modo de acesso: www.conpedi.org.br em publicações
Tema: A pesquisa jurídica na perspectiva da transdisciplinaridade

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Internet. 3. Segurança pública internacional. VII Encontro Virtual do CONPEDI (1: 2024 : Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

VII ENCONTRO VIRTUAL DO CONPEDI

INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL

Apresentação

O conjunto de pesquisas que sao apresentadas neste livro faz parte do Grupo de Trabalho de "INTERNET: DINAMICAS DA SEGURANCA PUBLICA E INTERNACIONAL", ocorrido no ambito do VII Encontro Virtual do CONPEDI,

realizado por meio de plataformas digitais, entre os dias 24 e 28 de junho de 2024, promovido pelo Conselho Nacional de Pesquisa e Pos-Graduacao em Direito – CONPEDI e que teve como tematica central ""A Pesquisa Juridica na Perspectiva da Transdisciplinaridade".

Os trabalhos expostos e debatidos abordaram de forma geral distintas tematicas atinentes ao a uso da internet, ciberespaco, inteligencia artificial e ferramentas e uso das tecnologias digitais, dando base para uma analise aprofundada das dinamicas da seguranca publica e internacional, especialmente relacionadas aos principais desafios que permeiam o uso da internet no direito.

O Grupo de Trabalho em comento ocorreu no segundo dia do evento, ou seja, 25/06/2024, oportunidade na qual foram realizadas as comunicacoes orais dos seguintes temas e respectivos autores:

1o) A ATUACAO DO DIREITO NA PRIVACIDADE DE DADOS. Apresentado pela Autora Antonia Ladymilla Tomaz Caracas Bandeira;

2o) QUANDO A ORIENTACAO PODE SER PREJUDICIAL: ANALISE DA RESPONSABILIDADE CIVIL E CRIMINAL DE USUARIOS DO CHATGPT. Apresentado pelo Autor Guilherme Manoel de Lima Viana;

3o) GESTAO DE RISCOS E ESTRATEGIAS DE COMUNICACAO DIGITAL NO

JUDICIARIO: UM ESTUDO DE CASO DO TRIBUNAL DE JUSTICA DO ESTADO DO PARANA (TJPR). Apresentado Malcon Jackson Cummings;

4o) DIREITO E ALTERIDADE EM TEMPOS DE INTELIGENCIA ARTIFICIAL.

Apresentado pela Autora Nadieje de Mari Pepler;

5o) A ERA DA "DEMOCRACIA DIGITAL": CULTURA, NOTICIAS FALSAS E LIBERDADE DE EXPRESSAO NO PROCESSO DEMOCRATICO BRASILEIRO. Apresentado pelos Autores Manuella Oliveira Toscano Maia e Ikaro Grangeiro Ferreira;

6o) DEMOCRACIA ESFAQUEADA: O dano imaterial dos atos antidemocraticos de 08 de janeiro de 2023 para alem das facadas no quadro “As Mulatas” de Di Cavalcanti. Apresentado pelos Autores Nicolas Schuindt de Andrade e Mayara Rayanne Oliveira de Almeida;

7o) O emprego da internet no recrutamento e exploracao das vitimas do crime de trafico de pessoas. Apresentado pela Autora Jordana Martins Perussi;

8o) MEU CELULAR PODE FAZER PROVA CRIMINAL CONTRA MIM? UMA ANALISE COMPARADA SOB A TEORIA DE WARREN E BRANDEIS. Apresentado pelos Autores Carlos Alberto Rohrmann e Ely Candida Procopio Pires;

9o) O COMBATE AOS CRIMES CONTRA A SEGURANCA NACIONAL E AS NOVAS TECNOLOGIAS: UMA ANALISE ACERCA DO USO DA INTELIGENCIA ARTIFICIAL. Apresentado pelos Autores Roberto Carvalho Veloso; Anna Carollina de Oliveira Abreu Melo e Neila Marilda Soares Moraes;

10o) MUITO ALEM DAS TELAS: UMA ANALISE SOBRE O CYBERBULLYING E A VIOLENCIA DIGITAL NO BRASIL. Apresentado pela Autora Adriana Rossini;

11o) A RESPONSABILIDADE DOS PROVEDORES DE INTERNET PELA LIVRE PUBLICIDADE DO COMERCIO ILEGAL DE ANIMAIS SILVESTRES EM SUAS PLATAFORMAS NA SOCIEDADE DE CONSUMO. Apresentado pela Autora Ediani Da Silva Ritter;

12o) DESVENDANDO AS FAKE NEWS: IMPACTOS E ESTRATEGIAS ELEITORAIS NO MUNDO DIGITAL. Apresentado pelas Autoras Elen Cristina Do Nascimento e Julia Tiburcio Miranda;

13o) A RESPONSABILIZACAO DOS PARTIDOS POLITICOS PELO

TRATAMENTO INADEQUADO DOS DADOS PESSOAIS NO CONTEXTO DAS PROPAGANDAS ELEITORAIS. Apresentado pelas Autoras Ana Claudia Correa Zuin Mattos do Amaral e Maria Eduarda Gobbo Andrades;

14o) A MERITOCRACIA NA CONTEMPORANEIDADE: AS NOVAS

TECNOLOGIAS E O NEOCAPITALISMO COMO AMEACA AS FACES DOS DIREITOS DA PERSONALIDADE. Apresentado pelo Autor Joao Lucas Foglietto de Souza;

15o) A REGULAMENTACAO DO COMBATE A DESINFORMACAO: UMA ANALISE COMPARATIVA ENTRE O PROJETO LEI No 2630/2020 E O REGULAMENTO (UE) 2022/2065 DO PARLAMENTO EUROPEU E DO CONSELHO DA UNIAO EUROPEIA. Apresentado pelas Autoras Liege Alendes De Souza e Francielle Benini Agne Tybusch;

16o) FAKE NEWS: LIMITACAO E CONTROLE DA LIBERDADE DE EXPRESSAO. Apresentado pelo Autor Eloy Pereira Lemos Junior;

17o) LIBERDADE DE EXPRESSAO E CENSURA ONLINE: UMA ANALISE DO DIREITO DIGITAL E DOS DIREITOS FUNDAMENTAIS. Apresentado pelos Autores Luiz Eduardo Simoes de Souza; Claudia Maria Da Silva Bezerra e Jose Mariano Muniz Neto;

18o) RESPONSABILIDADE CIVIL NO TRANSPORTE POR APLICATIVOS: REFLEXOES JURIDICAS SOBRE A PROTECAO DOS DIREITOS DOS CONSUMIDORES USUARIOS GT:DIREITO, GLOBALIZACAO E RESPONSABILIDADE NAS RELACOES DE CONSUMO. Apresentado pelos Autores Alexsandro Jose Rabelo Franca; Eudes Vitor Bezerra e Diogo Vieira Pereira.

Considerando todas essas tematicas de extrema relevancia, nao pode ser outro senao de satisfacao o sentimento que nos coordenadores temos ao apresentar a presente obra. E necessario, igualmente, agradecer enormemente aos pesquisadores que estiveram

envolvidos tanto na confeccao dos trabalhos quanto nos excelentes debates proporcionados neste Grupo de Trabalho. Outrossim, fica o reconhecimento ao CONPEDI pela organizacao e realizacao de mais um relevante evento virtual.

A expectativa e de que esta obra possa contribuir com a compreensao das dores e possivel solucoes do cenario contemporaneo brasileiro e internacional no que tange ao uso etico e consciente da internet, com o a esperanca de que as leituras dessas pesquisas ajudem na

reflexao e compreensao sobre a interacao da INTERNET: DINAMICAS DA SEGURANCA PUBLICA E INTERNACIONAL.

Esperamos que desfrutem da leitura.

Prof. Dr. Eudes Vitor Bezerra (PPGDIR/UFMA)

Profa. Dra. Jessica Amanda Fachin (Faculdades Londrina e UnB)

MEU CELULAR PODE FAZER PROVA CRIMINAL CONTRA MIM? UMA ANÁLISE COMPARADA SOB A TEORIA DE WARREN E BRANDEIS

MY CELL PHONE AS CRIMINAL EVIDENCE AGAINST ME? A COMPARATIVE ANALYSIS UNDER THE THEORY OF WARREN AND BRANDEIS

Carlos Alberto Rohrmann [1]
Ely Cândida Procópio Pires [2]
Hellen Cristine Vianna Dias [3]

Resumo

Este artigo apresenta questões constitucionais de privacidade em face de decisões que usam dados de georreferenciamento do celular para fazer prova contra seu dono, adotando como marco teórico a doutrina de Warren e Brandeis que trata da expectativa de privacidade. A importância da pesquisa decorre não somente da crescente digitalização das atividades como também da ausência de normas específicas sobre a regulamentação do uso de dados de celulares para fins de produção de prova criminal. O artigo adota metodologias exploratórias e indutivas, sob a perspectiva do direito comparado, tendo em vista que as cortes norte-americanas já estão enfrentando a matéria há algum tempo. Desta forma, a partir da análise de casos julgados nos Estados Unidos, o artigo apresenta desafios tecnológicos para o direito à privacidade em questões de direito criminal, no tocante à produção de prova contra o titular muitas vezes sem o seu conhecimento e sem ordem judicial. O resultado da pesquisa é no sentido de que a expectativa de direito à privacidade do titular do celular faz com que o seu uso seja constitucionalmente protegido a fim de se impedir que os dados gerados por aplicativos de celular bem como os dados de georreferenciamento sejam usados para produzir prova em processo criminal sem a prévia autorização judicial.

Palavras-chave: Direito constitucional à privacidade, Dados de celulares, Prova criminal, Segurança, Direito comparado

Abstract/Resumen/Résumé

This article addresses constitutional privacy issues in the face of decisions that use cell phone georeferencing data to prove against its owner, adopting as a theoretical framework the Warren and Brandeis doctrine that deals with the expectation of privacy. The importance of the research arises not only from the increasing digitalization of activities but also from the absence of specific rules on regulating the use of cell phone data for the purposes of producing criminal evidence. The article adopts exploratory and inductive methodologies,

---

[1] Doutor em direito pela Universidade da Califórnia em Berkeley (2001), LL.M. (UCLA, 1999), Professor do Corpo Permanente do Mestrado da Faculdade de Direito Milton Campos desde 2001. Advogado.

[2] Mestranda em Direito (FDMC, 2023). Professora da Fundação Comunitária de Ensino Superior de Itabira.

[3] Bacharelanda em direito (FMDC). Aluna de iniciação científica (IA, 2024).

from the perspective of comparative law, given that North American courts have already been dealing with the matter for some time. Thus, based on the analysis of cases judged in the United States, the article presents technological challenges for the right to privacy in matters of criminal law, regarding the production of evidence against the holder, often without their knowledge and without a court order. The result of the research is that the cell phone holder's expectation of right to privacy means that its use is constitutionally protected in order to prevent data generated by cell phone applications as well as georeferencing data from being used for producing evidence in criminal proceedings without prior judicial authorization.

Keywords/Palabras-claves/Mots-clés: Constitutional right to privacy, Cellular data, Criminal evidence, Safety, Comparative law

1. INTRODUÇÃO

A aproximação do mundo virtual do mundo real tem sido uma tendência desde o amplo uso de câmeras de segurança nas cidades norte-americanas, na década de noventa. Os smartphones e advento da tecnologia 5G tornam tal aproximação ainda mais intensa a cada dia.

Mesmo no Brasil, já se vão mais de duas décadas da instalação de câmeras de fotografar automóveis para aplicação de multas de trânsito. Interessante que as primeiras as primeiras multas que chegavam com fotos que poderiam, por um lado, desencadear reações de supostas ofensas ao direito à privacidade do condutor, mas, por outro lado, permitiam a aplicação de multas de trânsito sem a presença de uma autoridade policial física.

Há mais de décadas, o uso de imagens de câmeras de segurança para fazer prova contra crimes que acontecem em vias públicas já é uma realidade nas cortes brasileiras e, nos tribunais norte-americanos, como se terá oportunidade de apresentar ao longo deste artigo.

O objetivo do presente trabalho é realizar uma pesquisa sob a ótica do direito comparado acerca do uso de dados de georreferenciamento de celulares, bem como o uso de dados gerados por aplicativos utilizados no celular e que possam ser capturados por meio eletrônico ou mesmo por meio de câmeras de segurança que filmam o local de um crime, analisando-se caso nos Estados Unidos e buscando propor como se regulamentar no Brasil. O artigo apresenta um caso recente nos Estados Unidos que traz argumentos constitucionais acerca de tal utilização. O resultado que o artigo chega, sob os métodos exploratório e indutivo é no sentido de que o direito constitucional à privacidade deve ser considerado para impedir que os dados gerados por aplicativos de celular utilizados por uma pessoa possam ser vendidos, ou mesmo cedidos para órgãos de persecução criminal com a finalidade de incriminar o titular sem seu conhecimento ou sem ordem judicial.

O capítulo dois fará uma breve apresentação do direito constitucional à privacidade sob a perspectiva comparada e tomando como base o marco teórico escolhido, o clássico artigo *Right to Privacy* de Warren e Brandeis (Warren; Brandeis, 1890). O capítulo três apresenta casos recentes decididos nos Estados Unidos sobre a questão objeto do artigo. O capítulo quatro apresenta questões constitucionais brasileiras pertinentes ao tema, bem como caso que envolve a matéria. Utilizando-se o método exploratório e indutivo e partindo das normas constitucionais e dos precedentes

apresentados, o artigo vai concluir, sob a perspectiva comparada, que o direito à privacidade dos dados de georreferenciamento deve ser respeitado, ressalvada ordem judicial anterior ou em hipóteses excepcionais como quando há outras evidências significativas da prática de crime em uma determinada região geográfica bem delimitada, especialmente quando se trata de crimes de homicídio.

Importante destacar que se trata de um tema recente, em decorrência disso, as pesquisas ainda se encontram em fase inicial. Contudo, no presente trabalho, buscou-se trazer casos ocorridos nos Estados Unidos (EUA), uma vez que o país detém liderança tecnológica na área de computação, já que as principais empresas de computação - Google, Microsoft e a Apple - são de origem norte-americana. Dessa forma, trata-se de um tema de recorrência no EUA, sendo pauta abrangente para estudos sob a perspectiva do direito comparado, em face da abrangência das questões e da semelhança com casos decididos na realidade brasileira.

2. O DIREITO CONSTITUCIONAL À PRIVACIDADE SOB PERSPECTIVA COMPARADA

Adota-se, como marco teórico deste artigo, a teoria de Warren e Brandeis, consolidada no famoso artigo *The right to privacy*, publicado em 1890 pela *Harvard Law Review*, por meio do qual o direito de privacidade foi conceituado como o "direito de ser deixado a sós", ou, em inglês, "*the right to be left alone*" (Warren; Brandeis, 1890). Esse direito de ser deixado a sós não se aplica apenas dentro da casa do titular, ou seja, ele não está necessariamente atrelado ao conceito de propriedade privada para ser exercido: há, pois, uma expectativa de proteção à privacidade também em ambientes públicos ou quando o titular do direito de privacidade está em local que pertence a terceiros (como, por exemplo, casas de particulares, estabelecimentos comerciais ou órgãos públicos).

Uma consequência lógica do exercício do direito à privacidade é o direito que o seu titular passa a deter de subtrair do conhecimento de outrem (inclusive do Estado), o conhecimento de questões ínsitas à sua vida privada, à sua intimidade, como, por exemplo, os locais que frequenta, as lojas onde compra, os passeios e as viagens que faz, por onde ele caminha.

Em face deste artigo adotar a perspectiva comparada, é feita referência à Constituição dos Estados Unidos da América, especificamente à sua quarta emenda, que rege buscas para fins de investigação e instrução em questões criminais, e que é utilizada

como uma norma de proteção ao direito à privacidade que muito se relaciona com a questão problema tratada a seguir:

> O direito das pessoas de estarem seguras em suas personalidades, casas, papéis e efeitos, contra buscas e apreensões irracionais, não deve ser violado e nenhum mandado emitido, por causa provável, mas apoiado por juramento ou afirmação, e particularmente descrevendo o local a ser revistado e as pessoas ou coisas a serem apreendidas. (tradução nossa)
> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. (Estados Unidos da América, 1789)

O sistema da *Common Law*, nos Estados Unidos, torna bastante relevante a regra do precedente, especialmente as decisões da Suprema Corte dos Estados Unidos que se tornam direito nos Estados Unidos ("*law of the land*"). Assim, a referida Suprema Corte, ao aplicar a Quarta Emenda, em caso concreto, afirmou que ela não cuida apenas de um "direito exclusivo à privacidade". Trata-se do caso *Charles Katz v. United States*: "Fourth Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all" (Estados Unidos da América, 1967). Ou seja, "A Quarta Emenda protege a privacidade dos indivíduos contra alguns tipos de intrusão por parte do Estado, mas a sua proteção vai mais além, e em alguns casos, não há absolutamente nenhuma relação com privacidade" (tradução nossa).

Interessante verificarmos a intersecção entre o mundo digital, virtual e o mundo físico, cada vez mais presente nas vidas das pessoas. As câmeras de filmagens que gravam as imagens das pessoas, aliadas aos dados coletados de georreferenciamento são exemplos importantes dessa crescente intersecção.

A proteção constitucional do direito à privacidade nos Estados Unidos recai também sobre os dados das pessoas naturais e sobre o fluxo dos referidos dados dentro do mundo virtual. Já faz mais de trinta anos que se encontram leis americanas que tratam da proteção ao fluxo de dados no mundo virtual, por exemplo: "Temos ainda, nos Estados Unidos, o *Electronic Communications Privacy Act* de 1986 (ECPA) que proíbe a interceptação e divulgação de dados armazenados durante comunicação de dados" (Rohrmann, 2000, p. 95).

A intersecção do mundo real com o mundo eletrônico é antiga nos Estados Unidos e já ensejou casos interessantes relacionados à filmagem produzida por aeronaves.

Por exemplo, ainda no ano 1986, o caso Ciarolo, na Califórnia, regulou que imagens de casas de pessoas feitas por helicóptero podem legalmente ser utilizadas em casos criminais para a produção de provas que a pessoa estava plantando plantas para produzir drogas. Ou seja, as imagens são provas lícitas mesmo que não sejam precedidas de um mandado judicial (Estados Unidos da América, 1987, p. 207). Atualmente podemos verificar a abrangência de uma decisão como a do Caso Ciarolo, na Califórnia, nas hipóteses, por exemplo, da ampla utilização de aparelhos voadores do tipo drones para colheita das imagens com finalidade de produção de prova judicial.

O excesso de proteção de privacidade em dados pessoais digitais já foi objeto de estudos acerca da evolução a um "quase direito de propriedade" (Rohrmann; Santos, 2002).

> Assim, por indução, temos que a coleção de dados pessoais não está protegida por direito de propriedade intelectual. A teoria de Pamela Samuelson caminha nesse sentido de que uma proteção grande de privacidade para tais dados acabaria por levar a tronar um "quase direito de propriedade" sobre dados pessoais que poderiam até mesmo cobrar para "licenciar" o uso dos dados pessoais. Nesse sentido, o próximo capítulo cuidará da análise dos aspectos econômicos da proteção conferida pela LGPD. (Rohrmann; Santos, 2002, p. 136).

Retornando ao marco teórico de Warren e Brandeis, o direito de ser deixado a sós, em face da intersecção crescente entre o mundo digital e o mundo físico, passa a desafiar questões relacionadas à dificuldade de se assegurar que, até mesmo ao se deslocar por uma cidade, o indivíduo não tenha seus passos monitorados por terceiros. Isso, porque a pessoa pode ser "mapeada" pelas empresas de celular, pelas gigantes da tecnologia que armazenam dados de localização e de movimentação, o que lhes possibilita identificar seus clientes e suas atividades. Uma análise específica acerca da legislação brasileira de proteção de dados (Brasil, 2018) e consentimento, está fora do escopo deste artigo, todavia, ressalta-se que mesmo sob a LGPD, o consentimento não foi inserido dentro das bases legais a serem observadas especificamente pela Administração Pública:

> Ressalte-se que o consentimento não foi inserido dentro das opções de bases legais a serem observadas pela administração pública, e consequentemente seus agentes políticos, dentre estes os parlamentares. Tal fato decorre da obrigação legal do Estado em documentar todos os atos praticados, não podendo ser limitado por autorizações individuais de pessoas naturais. Por outro lado, conforme previsto no art. 7º, inciso I, o consentimento é definido no art. 5º, inciso XII, da LGPD como sendo "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". (Rohrmann; Fernandes, 2022, p. 282)

O artigo se volta, agora, em face de sua perspectiva comparativa, para a apresentação e a análise de casos judiciais e suas decorrentes questões que envolvem a matéria, decididos nos Estados Unidos.

3. CASOS NORTE-AMERICANOS SOBRE A LEGALIDADE DO USO DE DADOS DE GEORREFERENCIAMENTO DE CELULARES EM SITUAÇÕES DE CRIMES

Embora haja muita proteção jurídica ao direito à privacidade, tanto no Brasil, como nos Estados Unidos, inclusive sob a ótica de um direito constitucional, as novas tecnologias passaram a desafiar o direito por meio de novas formas de ofender o chamado "direito de ser deixado a sós". Como foi demonstrado no capítulo anterior, desde a década de 1980, na Califórnia, já se utilizava imagem de câmeras em helicópteros para fazer prova contra pessoas. O advento da tecnologia celular e a possibilidade de cada pessoa carregar consigo um aparelho que coleta dados de localização e, continuamente, os transfere para mais de uma empresa (tais como uma operadora de celular e uma empresa de busca), trouxe desafios ainda maiores para o efetivo exercício do direito à privacidade.

A título de exemplo, o artigo "Apple and Google Team Up to 'Contact Trace' the Coronavirus" publicado pelo The New York Times ainda no começo de 2020, noticiou que em uma abrangente estratégia para conter a disseminação do novo coronavírus, empresas como a Google e a Apple declararam que estavam a desenvolver um programa de computador que iria informar às pessoas que elas tiveram contato recente com alguém contaminado pelo COVID-19 (Nicas; Wakabayashi, 2020). As duas referidas empresas de tecnologia afirmaram que estavam trabalhando em conjunto com o objetivo de fornecer o software em apenas poucos meses, a fim de os oferecer aos sistemas operacionais dos bilhões de *smartphones* tanto *iPhones* quanto *Android* ao redor do globo, tal estratégia iria possibilitar que os telefones celulares detectassem continuamente demais celulares ao redor, o que levaria ao chamado "rastreio de contato" da COVID-19. Obviamente, as pessoas que são os titulares poderiam escolher se usariam, ou não, o novo *software* e comunicariam voluntariamente a própria condição de infectados pelo novo coronavírus que tanto assola o planeta na pandemia da COVID-19 (Nicas; Wakabayashi, 2020).

A tecnologia é bastante impulsionada em situações de crise e a pandemia do novo coronavírus foi um marco relevante para o desenvolvimento de tecnologias de

rastreamento de dados. A relevância do uso de máscaras para o combate à pandemia (Guarino; Taylor, 2021), e a resistência de parte da população são exemplos de ocasiões nas quais o monitoramento por câmeras chegou a ser usado, o que pode ser importante até mesmo para monitorar o descarte das máscaras em locais não indicados (Grennberg, 2021).

Medidas no sentido de combate à pandemia também foram prontamente adotadas no Brasil (Brasil, 2020), sendo que o Estado de São Paulo chegou a apresentar o seu "Sistema de Monitoramento Inteligente contra coronavírus". Trata-se do resultado de uma parceria do governo do estado de São Paulo com quatro (4) operadoras de telefonia celular, sendo elas: Claro, Vivo, Tim e Oi. O sistema utilizou os dados digitais coletados dos usuários que a ele aderirem na busca de uma medição do distanciamento social e ainda buscou enviar alertas sobre regiões com maior número de casos da COVID-19 (Estado de São Paulo, 2020).

Tratando-se de questões criminais, tome-se um caso em que ocorreu homicídio em um beco e que foi filmado por uma câmera de vigilância próxima. O vídeo é claro o suficiente para ver o crime, mas não é suficientemente visível para identificar o autor. É óbvio pelo vídeo, no entanto, que o criminoso está verificando o seu telefone celular enquanto sai do beco após o crime. Uma vez que o vídeo fornece dados sobre o local e a hora do crime, seria legal que polícia obtivesse um mandado aproveitando a capacidade de rastreamento dos dispositivos móveis para identificar de quem era o celular que estava na área do crime quando ocorreu?

Em 6 de outubro de 2021, o Tribunal Federal do *District Court of Columbia* recebeu uma petição com tal pedido. Trata-se de um mandado chamado de "cerca geográfica", ou de georreferenciamento. O pedido da polícia ao Tribunal era para que pedisse à empresa de tecnologia Google para identificar, por meio de um processo de várias etapas, os titulares de telefones celulares que cruzaram uma área geográfica definida em torno de onde ocorreu a atividade criminosa sob investigação (Estados Unidos da América, 2021).

Segundo o artigo "Google moves to end geofence warrants, a surveillance problem it largely created", publicado ainda em 2021, a Google recebeu mais de 11.500 mandados de georreferenciamento em 2020, contra 982 em 2018. Em agosto de 2021, tais mandados compreendiam quase um quarto de todos os mandados cumpridos pela Google. Cada um desses mandados foi deferido por um juiz. Portanto, parece que muito

mais mandados de georreferenciamento estão sendo concedidos pelos tribunais do que negados pela justiça nos Estados Unidos (Whittaker, 2021).

Considerando que quando se utiliza a função de "mapa" dos celulares, os smartphones que operam com o Google OS usam um GPS interno para determinar a localização exata dos telefones. Quando os telefones do Google OS se conectam à Internet via wi-fi ou verificam seus ambientes em busca de dispositivos Bluetooth, ou até mesmo utilizam o GPS, também enviam informações sobre a localização do telefone de origem para a empresa Google (Estados Unidos da América, 2020).

A Google, por sua vez, também coleta informações de localização de smartphones que não usam o Google OS (o caso dos iPhones), mas que usam outros aplicativos da Google, como o Gmail; o YouTube; o Google Maps; e o navegador de Internet da Google, o Chrome, por exemplo (Estados Unidos da América, 2020, 2).

Assim, podemos concluir que quase a totalidade dos smartphones que operam no Brasil, de forma direta ou indireta, têm seus dados de localização coletados de alguma forma pela Google. E, mais interessante, a maioria dos seus titulares parece ignorar tal fato pelo simples motivo de não lerem os termos de uso de tais aplicativos Google quando os instalam em seus aparelhos celulares.

A Suprema Corte dos Estados Unidos já decidiu, no caso "Carpenter v. United States", que seria possível que a coleta de informações de localização pelo Estado, particularmente dados de localização cobrindo apenas curtos períodos de tempo, não seja considerada uma "busca" que requer um mandado judicial (Estados Unidos da América, 2018). Por ouro lado, o Estado não pode ficar continuamente monitorando os passos de uma pessoa, por exemplo, um carro, sem um mandado judicial (isto seria uma "busca"), conforme precedente "United States v. Jones", de2012 (Estados Unidos da América, 2012, p. 430). Por outro lado, o Case Nº 21-SC-3217 (GMH), recente decisão do tribunal federal do sétimo circuito dos Estados Unidos já admitiu que o Estado pode rastrear os dados de um celular por até seis (6) horas consecutivas, o que não seria uma busca que exige o prévio deferimento de um mandado judicial (Estados Unidos da América, 2021, 2, p. 387).

A Google afirma que o número de pedidos de georreferenciamento tem aumentado significativamente desde 2018, e que se esforça para proteger a privacidade de seus ususários, embora tenha também que cumprir ordens judiciais e cooperar com o trabalhos dos órgãos de aplicação da lei (*law enforcement*), revendo cada pedido e verificando se está de acordo com a legislação (Google, 2020, p. 1).

Retornando ao caso específico do homicídio mencionado neste instrumento, a decisão da corte federal norte-americana foi pelo deferimento do mandado judicial sob o argumento que a busca deve ser razoável em face da situação fática (Estados Unidos da América, 2021, 1). A decisão ressalta que a maioria das pessoas carrega seus *smartphones* consigo a maior parte do tempo, o que conferiu um poder de monitoramento constante da própria localização e os transformou em dispositivos de rastreamento pessoal altamente precisos, identificando a localização onde quer que o usuário esteja no mundo em um raio de até vinte metros. A fundamentação da decisão que deferiu o mandado de busca de dados de georreferenciamento deste caso nos Estados Unidos vai além e diz que, para o bem ou para o mal, o georreferenciamento que torna os *smartphones* tão úteis para seus titulares, pois ajudam quando eles estão perdidos e possibilitam que os telefones sejam achados quando desaparecem, também deixam um rastro digital atrás dos seus donos, cuja divulgação muitos considerariam uma invasão de privacidade. Assim, a corte norte-americana afirma que, sem surpresa, a capacidade de rastreamento dos passos também provou ser de grande valor para a aplicação da lei ao tentar determinar quem estava em um determinado local quando ocorreu a atividade criminosa (Estados Unidos da América, 2021, 1).

A colisão entre o direito constitucional à privacidade e o direito à segurança pública com o combate ao crime estabelece, pois, uma tensão entre preocupações de privacidade e interesses legítimos de aplicação da lei que a Quarta Emenda à Constituição dos Estados Unidos (Estados Unidos da América, 1789) regulamenta, e que garante uma consideração cuidadosa dos requisitos constitucionais ao avaliar a legalidade do uso dos dados gerados e armazenados pelos aplicativos de georreferenciamento. Esses interesses conflitantes são avaliados em reconhecimento à proibição da Quarta Emenda de apenas buscas e apreensões "irrazoáveis". Portanto, aplicando-se a teoria de Warren e Brandeis (Warren; Brandeis, 1890), quando se usa um *smartphone*, há uma expectativa de proteção ao direito de ser deixado a sós em questões criminais. Em outras palavras, há expectativa de privacidade dos dados de georreferenciamento do aparelho celular.

4. O USO DE DADOS DE GEORREFERENCIAMENTO DE CELULARES NO BRASIL E A CONSTITUIÇÃO

O direito à privacidade no Brasil é uma garantia constitucional, nos termos do artigo 5º, X, da CF/88, que considera invioláveis a intimidade, a vida privada, a honra e

a imagens de pessoas assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação. Em seguida o inciso VII do mesmo diploma legal garante também a inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal, observando o disposto na lei de comunicações telefônicas (lei nº 9.296/1996).

Com o avanço da tecnologia, o acesso à internet tornou-se acessível para 81% da população brasileira. De acordo com dados da Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros, em 2022, o telefone celular emergiu como o principal meio de acesso à internet para 99% dos brasileiros, seguido pela televisão 55% (Tic Domicílios, 2022). Ao analisar esses dados, pode-se deduzir que a ampla utilização de informações de georreferenciamento de dados no Brasil é resultado direto do progresso tecnológico e da ampla integração de dispositivos móveis.

Entretanto, observa-se a expansão do uso das tecnologias para além do âmbito comercial. Para as investigações policiais, o uso de dados de georreferenciamento de celulares representa um avanço significativo, especialmente na obtenção de provas contra indivíduos suspeitos de envolvimento em atividades criminosas. O usuário, ao interagir com a internet, poder deixar um rastro de informações, que permitem identificar a pessoa e o uso do aparelho (Smanio, 2021).

Os dados de localização podem ser obtidos por meio de sistemas de posicionamento global (GPS) integrados aos dispositivos móveis, bem como de redes celulares e conexões Wi-Fi, permitindo à autoridade policial rastrear e registrar a localização geográfica de um aparelho celular em tempo real ou através de históricos de armazenamos de dados ao utilizar aplicativos como Waze ou o Uber, por exemplo. Caso a localização fique armazenada na plataforma, independentemente da forma como foi adquirida, a autoridade judiciária pode solicitar à empresa armazenadora o envio dos dados ao Juízo, desde que fundamente a decisão (Smanio, 2021).

Assim como na Suprema Corte Norte-americana, a busca reversa por dados de localização tem sido objeto de discussão nos Tribunais Brasileiros. Nessa técnica de busca, um juiz solicita a um servidor, como o Google, os IPs de todos os indivíduos logados em um local específico durante um intervalo de tempo determinado (Smanio, 2021).

As empresas responsáveis pelo armazenamento de dados, invocam os direitos de intimidade e privacidade para negar o acesso ao conteúdo às Autoridades Judiciárias. A

principal polêmica desse tipo de requisição é a quebra de sigilo de dados de terceiros que não tem relação com os fatos investigados, uma vez que os usuários são definidos, abrangendo localização e hora (Smanio, 2021). Nesse ponto, o Estado teria acesso a informações sobre a privacidade de indivíduos, que muito provavelmente não forneceriam os seus dados ao Google para vigilância (Maia; Paulino, 2020).

Além disso, surge outra preocupação quanto à potencial manipulação de dados, uma vez que essas informações poderiam ser exploradas por agentes para fins de vigilância ou mesmo para atingir utilizadores específicos, semelhante a um regime totalitário e autoritário (Cortez, 2023). Portanto, torna-se cada vez mais necessário discutir a regulamentação da tecnologia e suas implicações para a preservação dos direitos em um regime democrático.

No Brasil, o caso mais conhecido é o da vereadora Marrielle Franco, que foi assinada a tiros, junto com o seu motorista e que até hoje não está solucionado. No curso das investigações, o Juiz da 4ª Vara Criminal do Rio de Janeiro, determinou que o Google fornecesse a identificação dos usuários de seus aplicativos entre os pontos das coordenadas especificadas, qual seja, local do crime (Rua Joaquim Palhares) e onde a vereadora saiu (Rua dos Inválidos). A investigação buscava identificar todas as pessoas que estiveram nos locais, durante o lapso temporal determinado.

Embora os detalhes do processo tenham sido mantidos em sigilo, foi divulgado no portal do Superior Tribunal de Justiça (STJ) que o Google apresentou recurso solicitando a revisão da decisão do Tribunal de Primeira Instância. A empresa argumenta que o ordenamento jurídico brasileiro proíbe a violação de sigilo e interceptações genéricas sem identificação dos indivíduos afetados, o que contrariaria a proteção constitucional da privacidade e dos dados pessoais (Brasil, 2020).

No entanto, no julgamento do recurso de mandado de segurança 61302/RJ interposto pela Google, a Terceira Turma do Superior Tribunal de Justiça, sob a relatoria do Ministro Rogério Shietti Cruz, negou provimento ao recurso e manteve a decisão que determinou o compartilhamento dessas informações, sob o argumento de que os direitos e garantias individuais, não são absolutos e numa ponderação de interesses é possível relativizar o direito à privacidade, considerando que as interpretações jurídicas de proteção devem basear-se na perspectiva dos interesses individuais e sociais.

Atualmente, o tema encontra-se em discussão Supremo Tribunal Federal no Recurso Extraordinário 1.301.250, de relatoria da Ministra Rosa Weber, julgado em 27/05/2021, reconhecendo a repercussão geral da matéria:

> DIREITO CONSTITUCIONAL DIREITO PROCESSUAL PENAL QUEBRA DE SIGILO DE DADOS PESSOAIS, REGISTROS DE ACESSO À INTERNET E FORNECIMENTO DE IP. DECISÃO GENÉRICA. NÃO INDICAÇÃO DE PARAMETROS MINIMOS PARA IDENTIFICAÇÃO DOS USUÁRIOS, NÃO DELIMITAÇÃO ADEMAIS, DO ESPAÇO TERRITORIAL EM QUE VEICULADA A ORDEM PROTEÇÃO À INTIMIDADE E AO SIGILO DE DADOS (ART. 5, Xe XII, CF). QUESTÃO CONSTITUCIONAL POTENCIAL MULTIPLICADOR DA CONTROVERSIA REPERCUSSÃO GERAL RECONHECIDA 1. Possui índole constitucional e repercussão geral a controvérsia relativa aos limites a ao alcance de decisões judiciais de quebra de sigilo de dados pessoais, nas quais determinado fornecimento de registros de acesso à internet e de IPs (Internet protocol address), circunscritos a um lapso temporal demarcado, sem, contudo, a indicação de qualquer elemento concreto apto a identificar Repercussão geral reconhecida.

Outro caso que ganhou atenção nacional, envolveu o ataque às sedes dos Três Poderes em Brasília. No curso das investigações do Inquérito nº 4.879, o Ministro do Supremo Tribunal de Justiça Alexandre de Moraes, determinou que as operadoras de telefonia móvel armazenassem, pelo prazo de 90 dias, os registros de conexão para determinar a geolocalização dos usuários que estavam nas imediações da Praça dos Três Poderes e do Quartel-General do Distrito Federal no dia 8 de janeiro de 2023 com o intuito de identificar e responsabilizar os criminosos.

Assim, os casos citados de repercussão nacional, demonstram claramente um debate crescente e contínuo nos tribunais superiores brasileiros sobre a busca reversa por dados de localização, bem como uma necessidade de se respeitar o direito constitucional à privacidade.

5. CONCLUSÃO

A pandemia de COVID-19, com impactos de digitalização em mais de três anos (Rohrmann; et. al., 2022), associada ao avanço da tecnologia e da internet de alta velocidade, modificou bastante o comportamento humano no mundo digital, fazendo surgir uma nova dinâmica social e digital. Desta forma, torna-se imprescindível também, uma mudança na forma como o direito é interpretado e aplicado, no novo ambiente virtualizado e digital, como o que ocorre com a proteção da privacidade.

O artigo usou metodologias exploratória e indutiva, a partir da análise de casos e sob a perspectiva comparada, concluiu que, neste momento, há uma tendência das cortes no sentido de o direito à privacidade dos dados de georreferenciamento não poder se sobrepor às normas de segurança pública apenas quando há outras evidências

significativas da prática de crime em uma determinada região geográfica bem delimitada e, especialmente, quando se tratar de crimes contra a vida. Aplicando-se o marco teórico elegido, o artigo pode concluir que, em face da grande digitalização da vida atual, as pessoas sinceramente têm uma elevada expectativa de privacidade de seus dados de georreferenciamento e de dados gerados por aplicativos de seus celulares.

Desta forma, o impacto com o uso do georreferenciamento de dados na privacidade dos usuários é um tema de debate crescente e contínuo nos Tribunais Superiores. A adoção dessa tecnologia está, sem dúvida, transformando a investigação criminal, oferecendo ferramentas poderosas para a resolução de crimes e a administração da justiça.

No entanto, as implicações de longo prazo dessas mudanças são profundas. A linha entre segurança pública e privacidade individual torna-se cada vez mais tênue à medida que há mais avanço em direção a uma sociedade onde cada movimento pode ser monitorado e analisado.

Portanto, é imperativo que haja um equilíbrio cuidadoso entre o uso de tecnologias de georreferenciamento para fins de investigação e a salvaguarda dos direitos à privacidade e à liberdade individual. Isso exige um quadro legal robusto, transparente e responsável, que assegure o uso ético da tecnologia, com salvaguardas adequadas e mecanismos de supervisão para prevenir abusos.

REFERÊNCIAS

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 06 abr. 2024.

BRASIL. **Lei Federal nº 13.709, de 14 de agosto de 2018**. Lei geral de proteção de dados pessoais (LGPD). In: Diário Oficial da União, Brasília, 15 de agosto de 2018, e republicado parcialmente em 15 de agosto de 2018. Edição extra, Imprensa Nacional, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato20152018/2018/lei/L13709compilado.htm. Acesso em: 10 abr. 2024.

BRASIL. **Ato da mesa nº 152 de 16 de dezembro de 2020**. Regulamenta a aplicação da Lei 13.709 de 14 de agosto de 2018 – Lei de Proteção de Dados Pessoais (LGPD) – no âmbito da Câmara dos Deputados. Brasília/DF, dez de 2020. Disponível em: https://www2.camara.leg.br/legin/int/atomes/2020/atodamesa-152-16-dezembro-2020790919-publicacaooriginal-161982-cd-mesa.html?fbclid=IwAR2_UxYh3by30fM2k_DX4YJrfdH6DDlShWsJwBdvBAoEgZVw2Y5DdWi3QY. Acesso em: 10 abr. 2024.

BRASIL. **Lei Federal nº 13.979, de 06 de fevereiro de 2020**. Dispõe sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019. In: **Diário Oficial da União**, Brasília, 07 de fevereiro de 2020, n. 27, Imprensa Nacional, 2020b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Lei/L13979.htm. Acesso em 06 abr. 2024.

BRASIL. **Supremo Tribunal de Justiça.** Terceira Seção rejeita recurso da Google contra fornecimento de dados no caso Marielle Franco. 26 ago.2020. Disponível em: https://scon.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisar&livre=%22RMS%22+com+%2261302%22. Acesso em: 02 mar. 2024.

CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO. **Pesquisa sobre o uso das Tecnologias de Informação e Comunicação nos domicílios brasileiros – TIC Domicílios 2022.** Disponível em: https://cetic.br/media/docs/publicacoes/2/20230825143720/tic_domicilios_2022_livro_eletronico.pdf. Acesso em: 21 fev. 2024.

CORTEZ, Raphaela Jéssica Reinaldo. **Prova digital no processo penal brasileiro: o uso de dados de geolocalização na segurança pública e na investigação criminal**. Orientador: Walter Nunes da Silva Júnior. 2023. 104f. Dissertação (Mestrado em Direito) - Centro de Ciências Sociais Aplicadas, Universidade Federal do Rio Grande do Norte, Natal, 2023. Disponível em: https://repositorio.ufrn.br/handle/123456789/54402. Acesso em: 05 abr. 2024.

ESTADO DE SÃO PAULO. Governo de SP apresenta Sistema de Monitoramento Inteligente contra coronavírus: Parceria com operadoras Vivo, Claro, Oi e Tim usa dados digitais para medir distanciamento social e envia alerta sobre áreas com mais casos. **Portal do Governo de São Paulo**, 09 de abril de 2020. Disponível em: https://www.saopaulo.sp.gov.br/sala-de-imprensa/release/governo-de-sp-apresenta-sistema-de-monitoramento-inteligente-contra-coronavirus-2/. Acesso em 05 abr. 2024.

ESTADOS UNIDOS DA AMÉRICA. **Constituição dos Estados Unidos da América**, 1789. Disponível em: https://constitution.congress.gov/constitution/. Acesso em: 05 abr. 2024.

ESTADOS UNIDOS DA AMÉRICA. United States District Court District of Columbia. In the matter of the search of information that is stored at the premises controlled by Google LLC. **Case No. 21-SC-3217 (GMH)**, 23 de dezembro, 2021. Disponível em: In re Search of Info. That is Stored at the Premises Controlled by Google LLC, 579 F. Supp. 3d 62 | Casetext Search + Citator. Acesso em: 05 abr. 2024.

ESTADOS UNIDOS DA AMÉRICA. United States District Court N.D. California. Lewis v. Google. **Federal Supplement Third Series**, n. 461, p. 938, 2020. Disponível em: https://casetext.com/case/lewis-v-google-llc-1. Acesso em: 05 abr. 2024.

ESTADOS UNIDOS DA AMÉRICA. United States District Court N.D. Illinois. Matter of search warrant application for geofence location data stored at google concerning an

arson investigation. **Federal Supplement Third Series**, n. 497, p. 345, 2020. Disponível em: https://casetext.com/case/in-re-search-warrant-application-for-geofence-location-data-stored-at-google-concerning-an-arson-investigation. Acesso em: 05 abr. 2024.

ESTADOS UNIDOS DA AMÉRICA. United States District Court. United States v. Hammond, **Federal Supplement Third Series**, n. 996, p. 374, 2021. Disponível em: https://casetext.com/case/united-states-v-hammond-94. Acesso em: 05 abr. 2024.

ESTADOS UNIDOS DA AMÉRICA. United States Supreme Court. California v. Ciraolo, **United States Reports**, n. 476, p. 207, 1986. Disponível em: https://supreme.justia.com/cases/federal/us/476/207/. Acesso em: 05 abr. 2024.

ESTADOS UNIDOS DA AMÉRICA. United States Supreme Court. Carpenter v. United States, **Supreme Court Reports**, n. 138, p. 2206-2234, 2018. Disponível em: https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf. Acesso em: 05 abr. 2024.

ESTADOS UNIDOS DA AMÉRICA. United States Supreme Court. Charles Katz v. United States, **United States Reports**, n. 88, p. 507, 1967. Disponível em: https://www.law.cornell.edu/supremecourt/text/389/347. Acesso em: 05 abr. 2024.

ESTADOS UNIDOS DA AMÉRICA. United States Supreme Court. Rilay v. California, **United States Reports**, n. 573, p. 273, 2014. Disponível em: https://supreme.justia.com/cases/federal/us/573/373/. Acesso em: 05 abr. 2024.

ESTADOS UNIDOS DA AMÉRICA. United States Supreme Court. United States v. Jones, **United States Reports**, n. 565, p. 400, 2012. Disponível em: https://supreme.justia.com/cases/federal/us/565/400/. Acesso em: 05 abr. 2024.

GOOGLE. **Supplemental information on geofence warrants in the United States**. 2020. Disponível em: https://s3.documentcloud.org/documents/21046081/google-geofence-warrants.pdf. Acesso em: 05 abr. 2024.

GRENNBERG, Susan H. CDC report finds masks curb spread of COVID-19 on campus. **Inside Higher Ed**, 10 de setembro de 2021. Disponível em: https://www.insidehighered.com/quicktakes/2021/09/10/cdc-report-finds-masks-curb-spread-covid-19-campus. Acesso em: 05 abr. 2024.

GUARINO, Ben; TAYLOR, Adam. Massive randomized study is proof that surgical masks limit coronavirus spread, authors say. **The Washington Post**, 01 de setembro de 2021. Disponível em https://www.washingtonpost.com/world/2021/09/01/masks-study-covid-bangladesh/?utm_campaign=wp_to_your_health&utm_medium=email&utm_source=newsletter&wpisrc=nl_tyh&wpmk=1&pwapi_token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJjb29raWVuYW1lIjoid3BfY3J0aWQiLCJpc3MiOiJDYXJ0YSIsImNvb2tpZXZhbHVlIjoiNTk2YjE2YTFhZGU0ZTI0MTE5YWQ1YzNmIiwidGFnIjoiNjEyZmUxZWI5ZDJmZGE5YmI3YWIxYjkwIiwidXJsIjoiaHR0cHM6Ly93d3cud2FzaGluZ3RvbnBvc3QuY29tL3dvcmxkLzIwMjEvMDkvMDEvbWFza3Mtc3R1ZHktY292aWQtYmFuZ2xhZGVzaC8_dXRtX2NhbXBhaWduPXdwX3RvX3lvdXJfaGVhbHRoJnV0bV9tZWRpdW09ZW1haWwmdXRtX3NvdXJjZT1uZXdzbGV0dGVyJndwaXNyYz1ubF90

eWgmd3Btaz0xIn0.metiDBMxx5cWUtTf4Tqeg0RGqwKO4fSJD4IGKu284Uk. Acesso em 05 abr. 2024.

MAIA, Tiago Dias; PAULINO, Galtiênio da Cruz. **A quebra de sigilo de dados baseada em coordenadas geográficas e o princípio da proporcionalidade**. In: BRANCO, Paulo Gustavo Gonet; SILVA NETO, Manoel Jorge e; MOTA, Helena Mercês Claret da; MONTENEGRO, Cristina Rasia; RIBEIRO, Carlos Vinícius Alves (Orgs.). Direitos fundamentais em processo: estudos em comemoração aos 20 anos da Escola Superior do Ministério Público da União. Brasília: ESMPU, 2020, p. 769-787. Disponível em: https://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/BibliotecaDigital/BibDigitalLivros/TodosOsLivros/Direitos%2BFundamentais%2Bem%2BProcesso_20%2BAnos%2Bda%2BESMPU.pdf. Acesso em: 05 abr. 2024.

NICAS, Jack; WAKABAYASHI, Daisuke. Apple and Google Team Up to 'Contact Trace' the Coronavirus. **The New York Times**, 16 de abril de 2020. Disponível em: https://www.nytimes.com/2020/04/10/technology/apple-google-coronavirus-contact-tracing.html. Acesso em 05 abr. 2024.

ROHRMANN, Carlos Alberto. Notas acerca do direito à privacidade na internet: a perspectiva comparativa. **Revista da Faculdade de Direito da Universidade Federal de Minas Gerais**, vol. 38, p. 91-115, 2000.

ROHRMANN, Carlos Alberto; FERNANDES, P. T. V. S. Big Data: LGDP indutora para a transparência no legislativo? uma análise da tecnologia e democracia sob a teoria de Chemerinsky. In: V Encontro Virtual do CONPEDI, 2022, Online. **Direito, governança e novas tecnologias II**. Florianópolis: Conpedi, 2022. v. 1. p. 132-147. Disponível em: http://site.conpedi.org.br/publicacoes/P7b2Dgpz4JL2OxaK.pdf (conpedi.org.br). Acesso em: 10 abr. 2024.

ROHRMANN, Carlos Alberto; MARQUES, B. H.; XAVIER, M. E. P. Inteligência artificial, big data e a vigilância de doentes em face da covid-19 sob a teoria de Edward P. Richards. In: V Encontro Virtual do CONPEDI, 2022, Online. **Direito e Saúde**. Florianópolis: Conpedi, 2022. v. 1. p. 68-85. Disponível em: http://site.conpedi.org.br/publicacoes/465g8u3r/345136gj/4OYX3On7iQTz4kDA.pdf. Acesso em: 10 abr. 2024.

ROHRMANN, Carlos Alberto; SANTOS, B. B. H. Estudo comparado sobre proteção de dados pessoais, em face da inteligência artificial, sob a teoria de licenciamento de dados pessoais de Pamela Samuelson. In: V Encontro Virtual do CONPEDI, 2022, Online. **Direito, governança e novas tecnologias II**. Florianópolis: Conpedi, 2022. v. 1. p. 132-147. Disponível em: site.conpedi.org.br/publicacoes/465g8u3r/v73ig2ae/7F17KlDKtfSDnISj.pdf. Acesso em: 10 abr. 2024.

SMANIO, G. M. A busca reversa por dados de localização na jurisprudência do Superior Tribunal de Justiça: análise crítica do RMS 61.302/RJ. **Revista Brasileira de Ciências Policiais**, Brasília, Brasil, v. 12, n. 5, p. 49–76, 2021. DOI: 10.31412/rbcp.v12i5.840. Disponível em: https://periodicos.pf.gov.br/index.php/RBCP/article/view/840. Acesso em: 05 abr. 2024.

SUPREME COURT OF THE UNITED STATES. **About de court**. Disponível em: https://www.supremecourt.gov/about/about.aspx. Acesso em 05 abr. 2024.

SUPREMO TRIBUNAL FEDERAL. **Institucional**. Disponível em: http://www.stf.jus.br/portal/cms/verTexto.asp?servico=sobreStfConhecaStfInstitucional. Acesso em: 05 abr. 2024.

WARREN, Samuel; BRANDEIS, Louis. The right to privacy. **Harvard Law Review**, vol. 4, n. 5, p. 193, 1890. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em 05 abr. 2024.

WHITTAKER, Zack. **Google moves to end geofence warrants, a surveillance problem it largely created.** Law enforcement have long tapped users' location data hoarded by tech giants. Disponível em: Google moves to end geofence warrants, a surveillance problem it largely created | TechCrunch. Acesso em: 15 abr. 2024.