# XXIX CONGRESSO NACIONAL DO CONPEDI BALNEÁRIO CAMBORIU - SC

## DIREITOS E GARANTIAS FUNDAMENTAIS II

**ELOY PEREIRA LEMOS JUNIOR**

**JONATHAN CARDOSO RÉGIS**

**DIOGO DE ALMEIDA VIANA DOS SANTOS**

D597

Direitos e garantias fundamentais II [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Diogo De Almeida Viana Dos Santos; Eloy Pereira Lemos Junior; Jonathan Cardoso Régis. – Florianópolis: CONPEDI, 2022.

Inclui bibliografia
ISBN: 978-65-5648-624-6
Modo de acesso: www.conpedi.org.br em publicações
Tema: Constitucionalismo, Desenvolvimento, Sustentabilidade e Smart Cities

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direitos. 3. Garantias fundamentais. XXIX Congresso Nacional do CONPEDI Balneário Camboriu - SC (3: 2022: Florianópolis, Brasil).

CDU: 34


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

# XXIX CONGRESSO NACIONAL DO CONPEDI BALNEÁRIO CAMBORIU - SC

## DIREITOS E GARANTIAS FUNDAMENTAIS II

---

## Apresentação

Advindos de estudos aprovados para o XXIX Congresso Nacional do Conpedi Balneário Camboriú - SC, realizado entre os dias 07, 08 e 09 de dezembro de 2022, apresentamos à comunidade jurídica a presente obra voltada ao debate de temas contemporâneos, cujo encontro teve como tema principal "Constitucionalismo, Desenvolvimento, Sustentabilidade e Smart Cities".

Na coordenação das apresentações do Grupo de Trabalho "Direitos e Garantias Fundamentais II" pudemos testemunhar relevante espaço voltado à disseminação do conhecimento produzido por pesquisadores das mais diversas regiões do Brasil, vinculados aos Programas de Mestrado e Doutorado em Direito. Os estudos, que compõem esta obra, reafirmam a necessidade do compartilhamento das pesquisas direcionadas aos direitos e garantias fundamentais, como também se traduzem em consolidação dos esforços para o aprimoramento da área e da própria Justiça.

Nossas saudações aos autores e ao CONPEDI pelo importante espaço franqueado a reflexão de qualidade voltada ao contínuo aprimoramento da cultura jurídica nacional.

Diogo De Almeida Viana Dos Santos

Universidade Estadual do Maranhão - UFMA, e Universidade UNICEUMA

Eloy Pereira Lemos Junior

Universidade de Itaúna - MG

Jonathan Cardoso Régis

Universidade do Vale do Itajaí - Univali

# INTELIGÊNCIA ARTIFICIAL, DIREITO À PRIVACIDADE E A COVID-19: ANÁLISE DA CONSTITUCIONALIDADE DO COMPARTILHAMENTO DE DADOS DE LOCALIZAÇÃO COM O GOVERNO FEDERAL SOB PERSPECTIVA COMPARADA

# ARTIFICIAL INTELLIGENCE, RIGHT TO PRIVACY AND COVID-19: ANALYSIS OF THE CONSTITUTIONALITY OF SHARING LOCATION DATA WITH THE FEDERAL GOVERNMENT UNDER A COMPARATIVE PERSPECTIVE

**Carlos Alberto Rohrmann** [1]
**Ivan Luduvice Cunha** [2]
**Josiane Oliveira de Freitas** [3]

**Resumo**

A pandemia da COVID-19 fez que governos impusessem uma série de restrições à liberdade das pessoas em vários países do mundo. Uma das mais relevantes restrições está ligada ao confinamento imposto aos cidadãos comuns, algo sem precedentes, nos últimos cem anos, nos países democráticos. Uma forma de se monitorar se as pessoas ficam em casa é o compartilhamento dos dados de localização dos celulares, por parte das operadoras, com o governo federal. Notícias que o Google ofereceu para compartilhar os dados de localização com autoridades de saúde do governo federal norte-americano para monitorar o coronavírus e que as operadoras de celular brasileiras fizeram o mesmo é o tema problema deste artigo. Assim, sob a perspectiva do direito comparado, analisa-se a constitucionalidade de tais medidas em face da proteção constitucional à privacidade. Aplicando-se a metodologia dedutiva, o artigo conclui que o direito à privacidade pode ser violado se não houver prévio consentimento plenamente informado e consciente do indivíduo quanto ao uso de seus dados.

**Palavras-chave:** Covid-19, Dados de localização celular, Direito comparado, Direito à privacidade, Inteligência artificial

**Abstract/Resumen/Résumé**

Governments around the world have imposed many restrictions to the freedom of the people in order to fight COVID-19 pandemic. One of the most relevant restrictions is the total lockdown imposed in many democratic countries, something with no precedents in the past one hundred years. In order to monitor the behavior of the people: if they are staying home, one solution is mobile operating companies sharing location data with the federal

[1] Doctor of the Science of Law (UC Berkeley, 2001), LL.M. (UCLA, 1999), Professor do Corpo Permanente do Mestrado (FDMC) desde 2001. Procurador do Estado de Minas Gerais. Advogado

[2] Mestre em Direito (FDMC, 2018), doutorando em direito (ESDHC).

[3] Mestra em direito (FMDC). Pós-graduada em Direito Civil (PUC/MG). Bacharela em direito (FDMC). Advogada.

government. There are news that Google offered user location data to US health officials tackling coronavirus and that Brazilian mobile operators are willing to do the same. This is the problem addressed in this article. Under a comparative perspective, the article analyzes the constitutionality of those measures in the light of the right to privacy. Applying the deductive methodology, this article concludes that the constitutional right to privacy can be violated if there is no prior, fully informed and conscious consent of the individual regarding the use of his or her data.

**Keywords/Palabras-claves/Mots-clés:** Covid-19, Mobile location data, Comparative law, Right to privacy, Artificial intelligence

## 1. INTRODUÇÃO

A pandemia da COVID-19 apresentou-se como um desafio novo e sem precedentes para os sistemas de saúde pública dos mais variados países do mundo. Embora não haja um protocolo rígido a ser observado, a OMS recomendou o isolamento social como uma medida a ser usada para retardar o número de casos em um primeiro momento. Paralelamente, a adoção do isolamento social permitiria que os sistemas de saúde pública se adequassem às necessidades de maior número de leitos, de aquisição de máquinas de respiradores e da construção de hospitais de campanha para acomodar os doentes da COVID-19 que estariam por vir a números muito grandes, retardando-se, assim, o chamado "colapso do sistema de saúde".

Após algumas semanas de isolamento social, a observância pela população vai se tornando mais difícil, dadas não só as necessidades de compras de bens, manutenções que se fazem necessárias, mas do próprio cansaço que a vida enfadonha impõe aos confinados. Curiosamente, caso o confinamento dê resultado, e impeça a disseminação da COVID-19, uma sensação de que "não há nenhum risco lá fora" pode se apoderar das pessoas que passam a sair de casa, vencendo o temor inicial da contaminação.

Governos democráticos têm mais limitações legais e constitucionais ao imporem aos seus cidadãos medidas restritivas da liberdade de ir e vir. Especialmente quando o risco à saúde pública ainda é inicial, isto sem contar que é absolutamente invisível como o vírus da COVID-19.

Notícias que a Coreia do Sul teve bom resultado com políticas de confinamento e controle do deslocamento da população, aliadas à vedação de aglomerações de mais de dez pessoas, confrontadas com as terríveis notícias de mortes no norte da Itália, que teria se oposto às medidas de confinamento no início da epidemia por lá, fizeram com que as medidas de aplicação das restrições à saída de casa fossem investigadas para se tornarem mais efetivas. Enquanto líderes de países orientais chegaram a ameaçar de morte quem desobedecesse ao confinamento (como na Indonésia), países com tradição democrática não podem (e definitivamente não devem) ir tão longe.

Uma solução para fazer valer o confinamento é o Estado monitorar os passos das pessoas por meio dos dados de localização fornecidos pelos celulares. Esta medida tem sido cogitada nos Estados Unidos e no Brasil. O presente artigo analisa este tema problema com a discussão da constitucionalidade da medida em face da proteção constitucional à privacidade sob uma metodologia dedutiva e perspectiva comparativa. O nosso marco teórico será o clássico *The right to privacy*, de Warren e Brandies em seu artigo na Harvard Law Review. O capítulo

dois apresenta as medidas propostas e faz breve explicação dos aspectos técnicos envolvidos, bem como do uso de robôs de inteligência artificial para coleta e tratamento de dados de pacientes que passam a poder ser monitorados com riscos para a privacidade em face da confiança que as pessoas podem depositar na tecnologia. No capítulo três trata sobre a proteção à privacidade nos Estados Unidos e sua comparação com os aspectos constitucionais do Brasil. Por fim, o capítulo quatro enfrenta o problema com aplicação da teoria de ser deixado a sós, conclui pela inconstitucionalidade e demonstra que essa medida nada mais é do que a reedição de políticas públicas de saúde que buscam "jogar a culpa da doença na vítima".

## 2. SOLUÇÕES TÉCNICAS EM INTELIGÊNCIA ARTIFICIAL PARA FAZER VALER O CONFINAMENTO

A digitalização da tecnologia de comunicação, fenômeno que data da década de 1960, mas que somente chegou ao grande público a partir da década de 1980 nos Estados Unidos e com bastante força em meados da década de 1990 no Brasil, trouxe consigo profundas mudanças na forma de coleta e de armazenamento de dados. Trata-se de uma grande alteração na vida humana que aos poucos os indivíduos foram se dando conta: os dados que antes eram armazenados em fichas de papel, agora digitais, podem ser coletados, reproduzidos, compartilhados e, principalmente, **processados**, com uma rapidez e perspicácia antes digna de espiões de filmes de ficção. O auge do processamento dos dados hoje está sendo abarcado por aquilo que se convencionou chamar "inteligência artificial".

A aplicação de programas de computador com inteligência artificial e big data na vigilância de pessoas doentes (com COVID19) ocorreu em países que variam da China aos Estados Unidos (ROHRMANN; et. al., 2022, p. 72).

Pierre Lévy afirma que "A universalização da cibercultura propaga a copresença e a interação de quaisquer pontos do espaço físico, social ou informacional" (LEVY, 1999, P. 49). Parece-nos que tal processamento com interação entre o mundo físico e o digital pode parecer divertido ou interessante quando envolve dados dos outros, mas, quando esbarra em nossos dados, perde um pouco o *glamour*.

Com o avento da *internet* e o desenvolvimento tecnológico, as relações em sociedade passaram a ser mais facilitadas, se antes era necessário desenhar um mapa para que as pessoas localizassem o endereço, hoje com os GPS (termo em inglês, para dispositivo tecnológico de localização), basta digitar o endereço que facilmente é possível encontrar determinado local.

Não obstante, referida facilidade, muito além de apontar um caminho a ser seguido, o GPS também indica a localização exata do aparelho em que aquele dispositivo que foi ligado está, bem como em qual local a pessoa que porta aquele dispositivo quer chegar.

Em atenção a isso, governos federais de alguns países como Brasil, Coreia do Sul e Itália, implantaram o monitoramento via celular de pacientes médicos em seus territórios. Há países inclusive, em que os programas de rastreamento identificam, isolam o doente e acessam a rotina dele para avisar quem cruzou seu caminho.

A busca do monitoramento do isolamento social, tanto no Brasil como nos Estados Unidos, foi uma política considerada e efetivamente adotada. Nos Estados Unidos, por exemplo, "em 18 de abril de 2020, quarenta e dois governadores já tinham decretado isolamento social para reduzir o risco de hospitalizações pelo novo coronavírus, a fim de não sobrecarregar a infraestrutura de saúde estadual" (SEN; KARACA-MANDIC;GEORGIOU, 2020, p.2522). Nesse sentido, "fatores que potencialmente reduziram a taxa de contágio pelo vírus e a consequente taxa de ocupação dos hospitais incluíram o fechamento de escolas, bem como as políticas de afastamento social e o temor geral da pandemia" (SEN; KARACA-MANDIC; GEORGIOU, 2020, p.2523).

Um primeiro exemplo de vigilância virtual, em face da COVID-19, ocorreu no estado do Kansas, nos Estados Unidos, quando o departamento de saúde do estado anunciou que iria usar dados de GPS para monitorar a localização dos seus residentes (HATHAWAY, 2020). Ocorre que o Instituto de Justiça do Kansas considera que a pandemia da COVID-19 não justifica a obtenção de dados por parte do Estado e tampouco a falta de transparência do Estado quanto à forma de obtenção.

No Brasil, contrariamente ao previsto em legislação, a adoção de tais medidas não precedeu de autorização expressa dos usuários de aparelhos de telefonia com GPS integrado. A obtenção de informações, denominada como parceria entre o governo federal e as operadoras de telefonia móvel (Algar, Claro, Oi, Tim e Vivo) enviará ao Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) os dados de geolocalização de seus clientes, de forma anônima com o objetivo de auxiliar no combate ao COVID-19.

As referidas operadoras de telefonia móvel compilarão todos os dados e enviarão a uma nuvem pública, momento em que os dados serão então agregados e anonimizados para não permitir a identificação das pessoas. Frisa-se, que o Governo Federal afirma que os dados serão utilizados apenas para o combate a pandemia.

Cumpre destacar que, em razão da pandemia, o Ministério da Economia brasileiro tomou a iniciativa de publicar, em 20 de março de 2020, duas resoluções, resolução nº 1 e 2 de

16 de março de 2020, permitindo o compartilhamento de dados entre órgãos do executivo federal sem que o cidadão autorize o compartilhamento e ainda sem justificativa por parte do órgão para a requisição dos dados, o que gera certa estranheza quanto a finalidade.

Nesse diapasão, importante salientar sistema criado pelo governo do estado de São Paulo denominado Sistema de Monitoramento Inteligente de São Paulo (Simi-SP) em parceria com as operadoras de telefonia Vivo, Claro, Oi e Tim, usando dados digitais com a finalidade de medir a adesão a quarentena em todo o Estado. Além disso, são enviadas mensagens com alerta para as regiões em que o índice de incidência do COVID-19 é maior. Referido sistema, permite ao Estado de São Paulo consultar informações georreferenciadas de localização e deslocamentos das pessoas nos municípios paulistas em tempo real.

No Estado de São Paulo, o governo alega que a privacidade é totalmente garantida, uma vez que "o monitoramento é feito com base em dados coletivos coletados em aglomerados a partir de 30 mil pessoas" (GOVERNO DE SÃO PAULO, 2020).

Ainda quanto às parcerias firmadas pelo Estado de São Paulo, recentemente foi ajustada parceria com a Vivo e o Instituto de Pesquisas Tecnológicas (IPT) com a finalidade de verificar por meio de dados de Big Data e inteligência artificial, em tempo real, o deslocamento populacional de São Paulo. Nessa parceria, ao contrário da anteriormente firmada, em que eram analisados dados de forma coletiva, além de verificar os bairros, há dados por gênero, classe social e faixa etária. O que soa um tanto estranho, vez que, em primeiro momento, os dados coletados seriam anonimizados e agregados apenas para fins de identificação de aglomeração, contudo com a nova parceria implantada, paira a dúvida sobre qual finalidade pretende o governo de São Paulo ao fragmentar as informações obtidas a ponto de saber tais dados.

Já a prefeitura do Rio de Janeiro, em parceria com a operadora de telefonia Tim firmou acordo para seja permitido o rastreamento de movimentações de grupos de pessoas, dados que podem identificar o indivíduo, apesar de ser garantida a confidencialidade da informação. Contrastando o projeto de monitoramento do Estado de São Paulo e o do Estado do Rio de Janeiro, percebe-se que há certa insegurança jurídica a sociedade quanto a proteção de dados e ainda a privacidade de quem utiliza referidos sistemas.

Importante frisar que, atualmente, antes mesmo de utilizar o dispositivo de localização constante em aparelhos de telefonia, em momento inicial de aceite do aplicativo no telefone, é necessário aderir a termos de autorização para utilização da plataforma, que em regra, não é lido pelos usuários. Além de autorizar o telefone a utilizar o GPS do referido aparelho, há aplicativos que solicitam aceite para acesso à agenda telefônica, galeria de fotos, dentre outros,

e, se o usuário do aplicativo não autorizar aquelas permissões, em muito dos casos, não tem acesso ao aplicativo.

Contudo, muito além da informação como a localização do dispositivo, não se sabe até que ponto, todas as informações obtidas citadas acima, são repassadas ao Governo, ou ainda, quais efeitos a suposta utilização de dados de georreferenciamento, sem autorização, podem trazer no futuro (inclusive quanto à sua utilização em tribunais, como veremos na seção seguinte, em face do precedente norte-americano *Califórnia v. Ciraolo*).

Essas iniciativas vão ao encontro da utilização de recursos de inteligência artificial (IA) para o monitoramento das pessoas. Já existem robôs que, alimentados com dados de localização de pessoas, valendo-se de *drones*, são usados para vigilância individual. (SINGER, 2009, p. 50). Os algoritmos incluem até mesmo a possibilidade de o robô esconder-se quando a pessoa que está sendo vigiada se aproxima.

Somos da posição que o excesso de vigilância, quando imposta pelo Estado, além de interferir com a privacidade, ainda viola o direito de liberdade de expressão. Esta nossa posição vai ao encontro de uma decisão da Suprema Corte dos Estados Unidos, segundo a qual, medidas excessivas de vigilância violam o direito de liberdade de expressão e o direito de livre associação, assegurados pela Primeira Emenda à Constituição dos Estados Unidos. (ESTADOS UNIDOS DA AMÉRICA, 1972, p. 297).

O motivo de nossa posição é que, do contrário, o Estado passa a poder usar *drones*, com robôs dotados de algoritmos de inteligência artificial para operações policiais, sem mandado de busca para, por exemplo, vigiar o que acontece até mesmo dentro das casas de indivíduos. Robôs com programas de IA, instalados em celulares, podem não somente captar dados de localização, como gravar conversas, processar mensagens enviadas, manter arquivos digitais de trocas de mensagens entre a pessoa e terceiros, enfim, conhecer quase tudo dos gostos, das posições políticas e até das amizades de cada um. Todavia, "a privacidade somente pode ceder diante de justificativa consistente e legítima" (SUPREMO TRIBUNAL FEDERAL, 2020).

Ademais, nunca se pode desconsiderar o risco de *hackers* se infiltrarem nos programas de computador de inteligência artificial dos robôs e passarem a controlar e a ter acesso a dados que, a princípio, seriam apenas bem usados pelo Estado, para vigiar um paciente doente de COVID-19 (e ainda cuidar dele). Há muito se sabe da insegurança das *webcams* que são usadas para capturar imagens de usurários da Internet, sem que eles saibam (e sem que elas sequer aparentem estar ligadas).

Por fim, temos que as pessoas tendem a acreditar bastante nos computadores e na tecnologia digital, um exemplo é a urna eletrônica brasileira que merece dos eleitores brasileiros uma "sincera crença" de que se trata de uma máquina que nunca erra, ou que, quando erra, sempre "avisa" que errou para que seus votos não sejam contabilizados (ROHRMANN, 2011, p. 115).

O risco de as pessoas depositarem bastante confiança em robôs de monitoramento de localização e de informações médicas para compartilhamento com órgãos estatais é grande. A partir desta confiança, excessos que possam colocar em risco a privacidade dos indivíduos em face do estado são de grande possibilidade de acontecerem: criação de um conjunto de hábitos de cada pessoa tais como que hora chegam em casa, o que fazem em casa, o que compram, que remédios tomam, ou até mesmo o que comem.

Robôs podem captar imagens e sons que evidenciem até mesmo situações de crimes praticados pelos usuários (sem que eles saibam) e os dados ainda permanecem gravados em servidores na nuvem, para futuramente serem usados em processos. Tudo muito bem analisado e processado por robôs de inteligência artificial que podem, em caso de uma ação judicial, ser objeto de busca, apreensão e exposição nos tribunais.

Gradualmente, usamos cada vez mais robôs de inteligência artificial em nossas casas, neles acreditamos e pouco nos preocupamos com os efeitos daquilo que Bill Gates já disse que seria ter "um robô em cada casa" (GATES, 2008).

## 3. DIREITO À PRIVACIDADE COMPARADO: BRASIL E ESTADOS UNIDOS

Os primeiros estudos nos Estados Unidos, acerca do direito à privacidade, remontam ao Século XIX, quando os professores Warren e Brandeis publicaram o artigo *The right to privacy*, na *Harvard Law Review* (WARREN;BRANDEIS, 1890, p. 193). Os autores deslocaram o direito à privacidade do direito de propriedade para caracterizá-lo como um direito de ser deixado a sós (*the right to be left alone*), independentemente de o seu titular estar em sua propriedade. Assim, mesmo na rua, o direito à privacidade deve ser assegurado e respeitado (porque há uma expectativa de "ser deixado a sós", por seu titular).

O direito à privacidade refere-se ao direito que seu titular tem de subtrair, do conhecimento de terceiros, a divulgação de alguns aspectos da vida privada, da sua intimidade, na conformidade com um sentimento comum da sociedade em um determinado momento histórico (SILVA, 1998, P.39).

Tomamos como exemplo a adoção de aparelhos de *scans* em aeroportos nos Estados Unidos no final da década de noventa, havia questionamentos acerca da violação da privacidade dos passageiros em face de os aparelhos poderem traçar os contornos corporais da pessoa (como se ela estivesse despida). A discussão perdeu força com os atendados terroristas de setembro de 2001 quando a sociedade preferiu renunciar de parte da privacidade em favor do endurecimento das medidas de segurança em aeroportos.

A Quarta Emenda à Constituição dos Estados Unidos, que regulamenta as buscas para fins criminais, é uma das bases legais do direito à privacidade norte-americano (ESTADOS UNIDOS DA AMÉRICA, 1789).

Ressaltamos, todavia, que a Suprema Corte dos Estados Unidos já decidiu que a referida Quarta Emenda não trata exclusivamente do que seria um "direito exclusivo à privacidade", conforme o precedente estabelecido pelo caso decidido pela Suprema Corte dos Estados Unidos, Charles Katz v. United States (UNITED STATES SUPREME COURT, 1967, p. 507): "A Quarta Emenda protege a privacidade individual contra alguns tipos de intrusões governamentais, mas sua proteção vai bem além, e em certos casos, não tem nenhuma relação com a privacidade".

O direito constitucional à privacidade norte-americano há muito tem efeitos na proteção dos dados dos usuários e de seu fluxo do mundo digital. Mais precisamente, a privacidade dos dados diz respeito ao controle de um indivíduo sobre a coleta, o processamento, o tratamento e o uso dos dados pessoais. Assim, a privacidade é invadida quando, por exemplo, alguém obtém dados médicos sensíveis vasculhando arquivos confidenciais sem autorização (KANG, 1998, p. 1205).

Há leis infraconstitucionais nos Estados Unidos que, desde o final do século passado, protegem o fluxo de dados no mundo digital, conforme leciona Rohrmann: "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. 91-115).

Por outro lado, a Suprema Corte dos Estados Unidos, há muito, em *California v. Ciraolo*, já decidiu que provas produzidas por helicópteros que filmam os terreiros das casas das pessoas são válidas em processos criminais, independentemente de mandados de busca e apreensão, em caso de cultivo, em casa, de plantas para produção de drogas (UNITED STATES SUPREME COURT, 1986, p. 207), o que, de forma análoga, não seria, a princípio, prova ilegal no Brasil por suposta ofensa à intimidade do réu. Preocupa-nos, bastante, a extensão dessa

interpretação no caso da utilização de robôs em *drones* para fiscalização do que acontece na casa e na vida das pessoas.

O direito de ser deixado sozinho, preconizado por Warren e Brandeis, ao ser aplicado no mundo digital, é traduzido pelo direito de usar as ferramentas de comunicação, sem ser monitorado, sem que os dados do usuário, que podem identificá-lo, descrevê-lo, sejam usados pelo Estado: da mesma forma que quando uma pessoa anda pelas ruas não quer ser identificada, quer ser "mais um na multidão", quem navega pela *internet* não quer ser identificado como tendo visitado esse ou aquele *web site*, por exemplo.

As operadoras de telefonia ou os provedores de serviços para celulares como o Google e a Apple têm acesso a dados como localização, *e-mails* enviados, compras efetuadas, que permitem que o perfil do usuário seja montado. Mesmo que as empresas argumentem que não guardam o CPF do usuário, por exemplo, um perfil muito próximo da pessoa física pode ser traçado e a obtenção do CPF seria de uma facilidade evidente.

Ainda no início da pandemia, uma iniciativa das duas empresas acima (Apple e Google) chamou a atenção porque elas pretendem avisar o usuário de celular se ele teve contato com alguém que foi contaminado pelo vírus, assim, as pessoas optariam por utilizar a ferramenta e comunicar voluntariamente se estivessem infectadas (NICAS; WAKABAYASHI, 2020).

Uma vez que a tecnologia obedece a uma regra de "*opt in*", ou seja, cabe ao usuário a opção de fornecer os dados e de aderir ao recurso digital, não nos afigura uma violação da privacidade ou da intimidade da pessoa (embora trate de um dado bastante sensível que é o dado médico do paciente).

Dados médicos são, pois, dados muito sensíveis porque estão relacionados àquilo de mais íntimo que a pessoa pode querer subtrair do conhecimento público, lembramos que o direito à intimidade é um dos direitos da personalidade. Trata-se de direito subjetivo privado que confere às pessoas um poder em face dos seus semelhantes de resguardar-se de intromissões e de publicidade na sua mais reservada esfera de proteção, sem vedar, por completo, a faculdade de fazer alguma concessão nesse campo (SILVA, 1998, p. 48).

Um precedente que vai ao encontro da proteção constitucional norte-americana à privacidade e sua relação com as escolhas que as pessoas têm para sua vida, para sua saúde e para seu corpo, sem a intervenção de terceiros (inclusive do Estado) é *Roe v. Wade* no qual a Suprema Corte dos Estados Unidos decidiu, em 1973, que "o direito à privacidade abrange o direito de a pessoa fazer escolhas significantes para sua vida sem a interferência indevida de terceiros", inclusive o direito de a mulher decidir o que fazer com o seu próprio corpo, com

repercussões até mesmo na opção de fazer um aborto. Importante apontar que o precedente protege a privacidade da mulher dentro do casamento em face do seu cônjuge, conforme tradução nossa, "o direito à privacidade pessoal [...]; esse direito tem alguma extensão a atividades relacionadas ao matrimônio", que não pode interferir com sua decisão de terminar a gravidez (UNITED STATES SUPREME COURT, 1973, p. 113).

A doutrina europeia, com forte inspiração na doutrina alemã, classifica a proteção do direito à privacidade em três esferas que vão da intimidade à vida pública, conforme a lição dos professores Marques e Martins (2000).

> Para tanto, é habitual recorrer-se à chamada *teoria das três esferas*, construída fundamentalmente pela doutrina alemã, e de acordo com a qual, na reserva da vida privada, se distinguem: (1º) a *vida íntima*, que compreende os gestos e os factos que devem, em absoluto, ser subtraídos ao conhecimento de outrem; (2º) a *vida privada*, que abrange os acontecimentos que cada indivíduo partilha com um número limitado de pessoas; (3º) e a *vida pública* que, por corresponder a eventos suscetíveis de serem conhecidos por todos, respeita à participação de cada um na vida da coletividade.

Assim como no Brasil, nos Estados Unidos os estados tiveram papel importante na adoção das medidas de combate ao novo coronavírus. Trata-se de mais um ponto de convergência que justifica a nossa pesquisa de direito comparado. Os dois países são duas grandes federações com realidades estaduais muito diversas. O federalismo tem, como uma de suas vantagens, o aprimoramento das regras democráticas porque os governos dos estados estão mais próximos das pessoas do que no governo central. Assim, segundo Chemerinsky (2008), tradução nossa: "Um segundo valor do federalismo frequentemente invocado é que os estados estão mais próximos do povo e, portanto, mais são propensos a responder às necessidades e preocupações públicas".

No Brasil, a proteção da privacidade é expressa na Constituição da República, no art. 5º, incisos, X e XII que tratam, respectivamente, da inviolabilidade da intimidade, da vida privada da honra e da imagem das pessoas e do sigilo da correspondência e das comunicações de dados.

Não obstante, a Constituição da República não usar o termo privacidade especificamente, é cristalino que o legislador a ela se refere quando trata sobre a inviolabilidade da intimidade, da vida privada, honra e imagem, do sigilo de dados, dentre outros não citados em referidos incisos, mas que também se relacionam com a vida privativa de cada pessoa, tal qual a inviolabilidade de domicílio, isso porque, no Brasil, a privacidade está relacionada à vida

particular de cada pessoa, àquilo que lhe é íntimo, pessoal e que se pretende guardar de intervenções alheias.

A proteção da privacidade é considerada um direito fundamental, tanto o é que referido direito consta do título da Constituição Federal que dispõe sobre os direitos e garantias fundamentais. Cumpre frisar que a Constituição manteve a inviolabilidade ao sigilo de dados, dispondo que é possível a quebra do sigilo por ordem judicial para fins de investigação criminal ou ainda instrução de processo penal.

Ora a obtenção de dados de georreferenciamento da população não está relacionada a aspectos criminais, logo, permanece seu caráter de inviolabilidade, não sendo possível o acesso nem mesmo mediante decisão judicial.

O Código Civil Brasileiro tratou do direito à privacidade no capítulo dos chamados "direitos da personalidade", cujo objetivo é a proteção da dignidade humana, trata-se de teoria antiga que informa nosso direito civil. É correto dizer que Direitos da Personalidade estão ligados ao desenvolvimento da pessoa humana, representando uma garantia para a preservação de sua dignidade (GIANNOTI, 1987, p. 36).

O artigo 21 do Código Civil trata sobre a inviolabilidade da vida privada da pessoa natural, sendo que cabe ao juiz, mediante requerimento, adotar as medidas necessárias para interromper ou fazer cessar a ofensa a esse direito.

Assim, o direito à privacidade como direito da personalidade, é reconhecido como o direito que cada pessoa tem de manter determinadas informações, referentes à sua pessoa, em sigilo, contra intromissões alheias. É o direito de se manter só consigo mesmo, de guardar somente para si, informações próprias, que pelo seu conteúdo, não devem ser conhecidas pelo outro. Mas como dizer que há informações que devem ser mantidas em sigilo em uma era em que tudo é publicado, tudo é sabido?

O uso de dados de geolocalização individual demonstra que há um encontro entre a regulamentação do mundo físico e do mundo virtual que pode ser regulamentado pelo direito, em face de sua dogmática jurídica (ROHRMANN, 2007, p. 85).

Com o advento da internet e a facilidade de obtenção de informações, os direitos da personalidade, dentre eles, o direito a privacidade, têm sido renunciados, em prol, supostamente, da defesa da coletividade. Em um âmbito em que tudo é dado a conhecer, porque não conhecer também os deslocamentos de determinada pessoa?

Os dados pessoais, inclusive os que tratam da eventual contaminação pela COVID-19, por parte de uma pessoa, não podem ser monitorados ou divulgados pelas tecnologias digitais sem a autorização expressa da pessoa (ou "do paciente").

Em face de duas premissas, quais sejam, primeira, da necessidade de autorização expressa para que dados pessoais sejam colhidos, armazenados e, principalmente, repassados para autoridades públicas e, segunda, que há limites para o Estado vigiar as pessoas, passamos para a análise específica do tema problema deste artigo.

## 4. O LIMITE DO USO DE DADOS DE LOCALIZAÇÃO E O DIREITO DE SER DEIXADO A SÓS

A maioria dos usuários de telefones celulares e de programas ou de aplicativos de localização como os oferecidos pelo Google não se dão ao trabalho de lerem os termos de uso destes aplicativos. Uma leitura rápida demonstra que o usuário autoriza o compartilhamento de um sem número de dados e de informações com o Google. Podemos citar como exemplo a autorização para o Google ler os *e-mails* do Gmail e manter os dados de localização.

Os usuários do Google têm conhecimento de que, uma vez estando ligada a localização do dispositivo, aquela empresa passa a ter acesso aos locais visitados, novos locais conhecidos, a quilometragem já caminhada até determinada data, além das cidades em que aquela pessoa passou.

Não obstante, as inúmeras informações acima citadas, o governo indicou que os dados obtidos dos usuários de telefonia seriam apenas aqueles referentes à localização, contudo, de forma anônima.

Entretanto, da leitura do *caput* do artigo 2º da Medida Provisória nº 954 (BRASIL, 2020), as empresas de telecomunicação, além de fornecer informações sobre a localização de seus usuários, devem fornecer também nomes, endereços e números de telefones. E, pasmem, todas as informações fornecidas sem autorização prévia dos usuários.

Diante disso, uma vez que a obtenção de informações tão pormenorizadas dos usuários de telefonia fere o direito de privacidade, no julgamento da Ação Direta de Inconstitucionalidade nº 6.387, foi suspensa a eficácia da Medida Provisória n. º 954/2020. Determinando inclusive que "o Instituto Brasileiro de Geografia e Estatística – IBGE se abstenha de requerer a disponibilização dos dados, objeto da referida medida provisória, e caso já o tenha feito, que suste tal pedido" (SUPREMO TRIBUNAL FEDERAL, 2000).

Como visto no capítulo anterior, o direito a *privacy* norte-americano, está relacionado ao direito de ser deixado a só, em seu nascedouro o direito à privacidade estava associado a um conceito de propriedade, logo, o direito estaria vinculado à possibilidade de ter sua privacidade preservada dentro de um domicílio, em um local em que a pessoa pudesse manter sigilo de

determinadas informações que não quisesse levar ao conhecimento de outros, por isso deste entendimento como direito de ser deixado a só.

Entretanto, com a evolução da sociedade torna-se necessária à percepção do direito a *privacy* ou do direito de ser deixado a só sob nova ótica, isso porque, com a facilidade de obtenção de dados e informações via satélite e outros meios, não mais necessita de invasão física da casa da pessoa ou do local em que ela esteja.

Assim, o direito de ser deixado a só, na atual conjuntura, deve ser interpretado como direito a escolha de resguardo de informações, esteja em qual ambiente esteja e, ainda, a possibilidade de que, referidos dados ou informações sejam obtidos apenas em razão de autorização prévia daquela pessoa. Indo além, não somente a obtenção das informações deve preceder de autorização prévia como também o uso de referidas informações, sob pena de ser considerado inócua a previsão legal de direito à privacidade.

Em sua legislação, o Brasil, busca resguardar direitos nomeados como fundamentais, como o direito à privacidade, dispondo sobre esse direito, inclusive no artigo 5º da Constituição Federal de 1988. A proteção ao direito à privacidade é tão importante que a Lei nº 12.965/2014 que estabeleceu o Marco Civil da Internet tratou de apontá-lo no inciso II do artigo 3º.

A lei de telecomunicações nº 9.472/1997 (BRASIL, 1997) no livro que dispõe sobre os princípios fundamentais, elenca como direito dos usuários dos serviços de telecomunicações à inviolabilidade e ao segredo de sua comunicação, a não divulgação de seu código de acesso e ainda, o respeito a sua privacidade na utilização de dados pessoais pela prestadora do serviço.

Além disso, nos termos do parágrafo único do artigo 39 da Lei nº 9.472/1997 há previsão expressa de garantia de tratamento confidencial das informações técnicas, operacionais, econômico-financeiras e contábeis que solicitar às empresas prestadoras dos serviços de telecomunicações.

Apesar de ainda não ter entrado em vigor, merece também destaque o respeito à privacidade, previsto no inciso I, do artigo 2º da Lei nº 13.709/2018 (BRASIL, 2018). Outro ponto relevante é a necessidade de consentimento do titular de dados para a obtenção destes, nos termos do inciso I, do artigo 7º da referida Lei.

O conceito de privacidade sofreu evolução ao longo dos anos, se antes estava relacionado ao direito de ser deixado a só, hoje em face das mídias sociais, assumiu novo viés (PEIXOTO, 2016. p. 358), "o conceito de privacidade evolui de direito de estar só para direito a ter controle sobre as próprias informações e de determinar a maneira de construir a própria esfera particular – o direito à autodeterminação informativa".

Na contramão de toda previsão legal de proteção da privacidade, da intimidade e do direito de ser deixado a só, os governos estaduais no Brasil têm utilizado como justificativa à obtenção de dados de localização o enfrentamento a pandemia da COVID-19, nota-se que referida utilização passou a ser percebida como "arma" de saúde pública.

É o que se depreende do discurso da presidente da Associação dos Magistrados Brasileiros, em entrevista dada ao programa UOL Debate (UOL, 2020) e também do Governador do Maranhão, que consideram que o uso restritivo pode e deve ser feito em nome da saúde coletiva.

Além disso, cumpre trazer ao artigo, o entendimento do judiciário do Estado de São Paulo (2020) que considera a pandemia como motivo suficiente para justificar que o direito a locomoção não é absoluto, mas deve ser sopesado com outros direitos e deveres constitucionais, além de entender que a interpretação jurídica dos direitos fundamentais deve ser sistematizada e priorizar o coletivo em detrimento de convicções particulares.

Não se olvide que a saúde é direito de todos e dever do Estado e que será garantida por políticas sociais e econômicas para permitir a redução do risco da doença, além do acesso universal e igualitário às ações para proteção da saúde, nos termos do artigo 196 da Constituição Federal (BRASIL, 1988).

Em atenção a isso, foi sancionada lei nº 13.979 (BRASIL, 2018) que trata a respeito das medidas para enfrentamento da emergência de saúde pública, o texto destaca como medidas necessárias ao combate à pandemia o isolamento, a quarentena, determinação de realização compulsória de exames ou até mesmo tratamentos médicos específicos, dentre outros.

Como medida de enfrentamento da emergência de saúde pública há, também, a vigilância que pode ser entendida como ponto de partida para a saúde pública, uma vez que a vigilância pode fornecer dados aos epidemiologistas para identificar ameaças e traçar estratégias para enfrentamento (RICHARDS, 2009, p.27).

Por outro lado, uma solução que pode atender as necessidades do Estado de percepção das taxas de isolamento social é a elaboração de pesquisas voluntárias com a população, nos moldes de pesquisa realizada nos Estados Unidos, pelo *U.S. Department of Health and Human Services Centers for Disease Control and Prevention,* por meio da internet, de 5 a 12 de maio de 2020. Interessante que a pesquisa concluiu que "a população se sentiria insegura se as restrições fossem abrandadas" (CZEISLER, 2020, p. 2).

Contudo, analisando o texto da lei nota-se que há previsão expressa no inciso III, do §2º, do artigo 3º, que não obstante, todas as referidas medidas ficam asseguradas as pessoas afetadas o respeito à dignidade, aos direitos humanos e ainda às liberdades fundamentais.

O direito à privacidade é uma garantia constitucional vinculada as liberdades fundamentais, posto que cada pessoa tem o direito a manter sigilo quanto a certos aspectos de sua vida, bem como o direito a ser deixado a só, esteja onde esteja. “No balanceamento de bens jurídicos, por exemplo, pode haver, em certas circunstâncias, a prevalência de interesse social, como no caso de uma doença grave que possa vir a colocar em risco toda coletividade” (OTERO; TENA, 2016. p. 495).

Compreende-se que em momento de pandemia, a proteção à vida e por consequência a saúde têm atenção primordial, porém, não se pode cogitar tolher o direito à privacidade em benefício da defesa de referidos direitos.

Como direito fundamental que é, limitar o direito à privacidade só pode ser defendido quando estiver em choque com outro direito fundamental, o que não é o presente caso.

Inclusive, pesquisadores sobre a inteligência artificial no direito têm indicado nos últimos dias que, permitir no momento atual o acesso ao Estado e ainda o uso de dados de localização, poderá abrir um precedente para que o direito à privacidade seja esquecido (AGÊNCIA BRASIL, 2020). É o que se nota na China, país autoritário que tem utilizado de inúmeros aparatos de inteligência artificial para “vigiar” os cidadãos.

“A manipulação de dados pessoais digitalizados, por agentes públicos ou privados, consiste em um dos maiores desafios contemporâneos do direito à privacidade” (SUPREMO TRIBUNAL FEDERAL, 2020).

Importante, ainda, destacar entendimento da Ministra Rosa Weber no julgamento da ADI6387 (SUPREMO TRIBUNAL FEDERAL, 2020) no tocante ao monitoramento como política pública voltada para saúde, que considera, que apesar da gravidade do cenário de urgência decorrente da crise sanitária, o combate não pode legitimar o atropelo de garantias fundamentais consagradas na Constituição. Outro ponto sério é a possibilidade de se usar tal conjunto de dados para realizar prova em processos criminais contra o doente (ROHRMANN, 2006).

O que de fato se observa é que o governo, se beneficiando da construção de políticas públicas para enfrentamento da pandemia, está de fato negando o pleno exercício do direito de privacidade.

## 5. CONCLUSÃO

Direitos constitucionais individuais são a base da democracia e sua restrição, por menor que seja, coloca um risco às sociedades democráticas. Não negamos que, do ponto de

vista do Estado, especialmente do seu Poder Executivo, os direitos constitucionais individuais muitas vezes parecem um obstáculo, uma espécie de um mínimo detalhe a proteger uma pessoa em contraponto a tudo de bom que o governante gostaria de fazer pelo bem do público, pela segurança da nação, pela saúde do povo, e por tantas outras causas coletivas que transcendem o escopo deste artigo.

O presente estudo adotou o método dedutivo para, após revisão de decisões e precedentes, sob a perspectiva comparada, enfrentar o tema problema da inconstitucionalidade da coleta, compartilhamento e do monitoramento dos dados de localização das pessoas, pelo Estado, em face da pandemia do novo coronavírus.

O artigo apresentou exemplos de coletas de dados de celulares e seu tratamento por meio de robôs de inteligência artificial. Em face da perspectiva comparativa, o texto apresentou precedentes da Suprema Corte dos Estados Unidos que interpretam o direito à privacidade e seus contornos em face da tecnologia digital cada vez mais intrusiva a vida as pessoas.

Sob a teoria do direito à privacidade como o direito de ser deixado a sós, o artigo conclui que a expectativa de privacidade que as pessoas têm quando usam o celular é, em face de uma sincera crença na tecnologia, que todas suas conversas, seus acessos a sites da *internet* e suas mensagens trocadas em redes sociais são absolutamente protegidas e não são compartilhadas com terceiros. As pessoas realmente sentem-se confiantes que o celular é uma extensão de sua privacidade e de sua intimidade que desfrutam em casa. Não é incomum que casais não compartilhem a senha de acesso ao celular, respeitando a intimidade de cada um (e daqueles que trocam mensagens com seus cônjuges).

Há muitos riscos quando se trata dados de pessoas. Vazamentos de dados, riscos de programas inseridos por *hackers* e vigilância exagerada do Estado sobre a conduta das pessoas foram exemplos tratados no presente texto.

Não há fórmula pré-estabelecida para criação de medidas de saúde pública necessárias ao confronto da pandemia, contudo, considera-se que a negação a direitos fundamentais tais como o direito à privacidade, não pode ser utilizada como suposta medida de saúde, quando o seu fim precípuo é de fato investigar, negar o direito de estar a só e o direito de privacidade dos cidadãos.

Assim, o risco de esses dados serem usados por robôs de inteligência artificial do Estado não é sequer compreendido pela maioria das pessoas que poderiam, sob a justificativa de proteção da saúde, ter uma série de dados que descrevem quase tudo do indivíduo, processados pelo Estado podendo, posteriormente, ser usado até mesmo para fazer prova em processo criminal contra a pessoa. Conclui-se, pois, sob a metodologia dedutiva, que o direito

constitucional à privacidade pode ser violado se não houver prévio consentimento plenamente informado e consciente do indivíduo (ou paciente) quanto ao uso de seus dados para os fins especificamente autorizados.

## REFERÊNCIAS


BENTIVEGNA. Carlos Frederico Barbosa. **Liberdade de Expressão, honra, imagem e privacidade**: os limites entre o lícito e o ilícito. Editora Manole. 2019.

CHEMERINSKY, Ervin. **Enhancing government**: federalism for the 21st century. Stanford: Stanford Law Books, 2008.

COVID-19: iniciativas usam monitoramento e geram preocupações – Uma das metas é monitorar aglomerações, principalmente em capitais. Agência Brasil. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2020-04/covid-19-iniciativas-usam-monitoramento-e-geram-preocupacoes. Acesso em: 12 out. 2022.

CZEISLER, Mark É. et al. Public attitudes, behaviors, and beliefs related to COVID-19, stay-at-home orders, nonessential business closures, and public health guidance — United States, New York City, and Los Angeles, May 5–12, 2020. U.S. Department of Health and Human Services Centers for Disease Control and Prevention. **Morbidity and Mortality Weekly Report**, vol 69, 12 de junho de 2020, p. 2.

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. 09/04/2020. 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: 15 abr. 2022.

ESTADOS UNIDOS DA AMÉRICA. **Constituição dos Estados Unidos da América**, 1789.

ESTADOS UNIDOS DA AMÉRICA. United States Supreme Court. California v. Ciraolo, **United States Reports**, n. 476, p. 207, 1986.

ESTADOS UNIDOS DA AMÉRICA. United States Supreme Court. Charles Katz v. United States, **United States Reports**, n. 88, p. 507, 1967.

ESTADOS UNIDOS DA AMÉRICA. United States Supreme Court. Roe v. Wade, **United States Reports**, n. 410, p. 113, 1973.

ESTADOS UNIDOS DA AMÉRICA. United States Supreme Court. United States v. U.S. District Court, **United States Reports**, n. 407, p. 297, 1972.

GASTIC. COVID-19 Community Mobility Report – created by GOOGLE. Disponível em: https://www.gstatic.com/covid19/mobility/2020-04-05_BR_Mobility_Report_en.pdf. Acesso em: 17 out. 2022.

GATES, Bill. A Robot in Every Home. **Scientific American**, fev. 2008. Disponível em: https://www.scientificamerican.com/article/a-robot-in-every-home-2008-02/. Acesso em: 8 mai. 2022.

GIANNOTI, Edoardo. **A tutela constitucional da intimidade**. Rio de Janeiro: Forense, 1987.

HATHAWAY, Ellen. **Demanding legal answers on Kansas COVID-19 tracking.** Disponível em: https://kansasjusticeinstitute.org/2020/04/press-release-demanding-legal-answers-on-ks-covid-19-tracking/. Acesso em: 20 out. 2022.

IPT. Inteligência artificial contra o coronavírus. IPT. Datado de 09/04/2020. Disponível em: https://www.ipt.br/ipt_na_midia/623-inteligencia_artificial_contra_o_coronavirus_.htm. Acesso em: 19 out. 2022.

KANG, Jerry. Information Privacy in Cyberspace Transactions. **Stanford Law Review**, vol. 50, p. 1193, 1998.

LÉVY, Pierre. **Cibercultura**. Trad. Carlos Irineu da Costa. São Paulo: 34, 1999.

MARQUES, Garcia; MARTINS, Lourenço. **Direito da informática**. Coimbra: Livraria Almedina, 2000.

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: 17 abr. 2020.

OTERO, Cleber Sanfelici; TENA, Lucimara Plaza. Fundamentos que justificam os direitos a privacidade: a dignidade da pessoa humana como núcleo pétreo dos direitos da personalidade e situações na odontologia que permitem uma flexibilização (Cadastro e Ficha de Anamnese). **Revista Eletrônica do Curso de Direito UFSM**, v.11, n.2/2016. p. 476-498. Disponível em: https://periodicos.ufsm.br/revistadireito/article/view/19683. Acesso em: 20 jun. 2022.

PEIXOTO, Erick Lucena Campos Peixoto. JÚNIOR, Marcos Ehrhardt. **O direito à privacidade na sociedade da informação**. 2016. p. 353 a 369. Disponível em: http://enpejud.tjal.jus.br/index.php/exmpteste01/article/view/63. Acesso em: 17 abr. 2020.

RICHARDS, Edward P. Dangerous people, unsafe conditions: The constitutional basis for public health surveillance. **Journal of Legal Medicine**, vol. 30, p. 27, 2009.

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

ROHRMANN, Carlos A. Legal aspects of electronic criminal evidence in Brazil. **International Review of Law, Computers and Technology**, vol. 20, p. 77-93, 2006.

ROHRMANN, Carlos Alberto; CAMPOS, M. A. M. E. Technological barriers to the right to vote: Biometric data, electronic voting machines and the dignity of the electors. **Anuário brasileiro de direito internacional**, v. 1, p. 112-127, 2011.

ROHRMANN, Carlos A. The role of the dogmatic function of law in cyberspace. **International Journal of Liability and Scientific Enquiry**, v. 1, ed 1-2, p. 85, 2007.

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.

R7. Google quer usar localização de usuários para conter coronavírus – Senador norte-americano pede cautela nos esforços do governo de grandes companhias de tecnologia contra a pandemia. R7. Disponível em: https://noticias.r7.com/tecnologia-e-ciencia/google-quer-usar-localizacao-de-usuarios-para-conter-coronavirus-20032020. Acesso em: 7 abr. 2022.

SEN, Soumya; KARACA-MANDIC, Pinar; GEORGIOU, Archelle. Association of stay-at-home orders with COVID-19 hospitalizations in 4 states. **Journal of the American Medical Association**, Vol. 323, N. 24, junho 23/30, p. 2522-2524, 2020.

SILVA, Edson Ferreira da. **Direito à intimidade**. São Paulo: Oliveira Mendes, 1998.

SINGER, Peter W. **Wired for war**. New York: The Penguin Press, 2009.

TILT. Governo vai monitorar celular para controlar aglomeração na pandemia. UOL. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/04/02/para-combater-a-covid-19-o-governo-federal-vai-monitorar-o-seu-celular.htm. Acesso em: 7 out. 2022.

TIM. Tim ajuda prefeitura do Rio com mapa de deslocamento de pessoas. Tecnoblog. Disponível em: https://tecnoblog.net/330676/tim-ajuda-prefeitura-do-rio-com-mapa-de-deslocamento-de-pessoas/. Acesso em: 17 out. 2022.

TOGOH, Isabel. Google publica dados de localização em 130 países para monitorar isolamento social. Forbes. Disponível em: https://forbes.com.br/negocios/2020/04/google-publica-dados-de-localizacao-em-130-paises-para-monitorar-isolamento-social/. Acesso em: 7 out. 2022.

WARREN, Samuel Warren; BRANDEIS, Louis. The right to privacy. **Harvard Law Review**, vol. 4, p. 193, 1890. Disponível em: http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm. Acesso em: 17 out. 2022.

WSJ. Google offers user location data to health officials Tackling Coronavirus. WSJ. Disponível em: https://www.wsj.com/articles/google-offers-user-location-data-to-health-officials-tackling-coronavirus-11585893602?tesla=y&mod=article_inline. Acesso em: 17 out. 2022.