

**GOUVÊA ADVOCACIA  
CONSULTORIA**

**Workplan**  
GROUP

ebook

# **PROTEÇÃO DE DADOS PESSOAIS E COVID-19**



**NO BRASIL, EUROPA E CHINA**

*No momento a pergunta que se faz é: Como proteger a privacidade do cidadão e garantir a segurança pública em tempos de pandemia? Como encontrar o equilíbrio?*

Com o avanço da doença, os países têm adotado medidas na utilização de dados pessoais como forma de políticas públicas no combate à crise.

Isto tem causado divisão nos entendimentos de como esses dados são tratados e quais são os limites da vigilância estatal. Vejamos sucintamente como tem sido tratados:

## **CHINA**

O jornal chinês South China Morning Post publicou o artigo intitulado *"Coronavirus accelerates China's big data collection, but privacy concerns remain"* <sup>1</sup> onde relata que há pouca resistência por parte das pessoas no fornecimento de dados, já que a maioria da população mostra simpatia pelos pacientes infectados e está mais disposta a sacrificar a privacidade para segurança pública.

E, adotaram, como medidas:

- 1)** Província de Guangdong, sul: Na compra de medicamentos contra febre e tosse em farmácias, era obrigatório o fornecimento de nome completo para que os funcionários pudessem acompanhá-los.
- 2)** No centro de tecnologia de Shenzhen, passageiros deveriam fornecer nomes completos antes de usarem o metrô.
- 3)** Sistemas desenvolvidos por empresas de tecnologia, incluindo a plataforma de entrega de alimentos Meituan Dianping e Dida Chuxing, rival do gigante Didi Chuxing, exigiam que viajantes de todo o país fornecessem suas informações pessoais através da leitura de códigos QR antes de pegar ônibus, trens e táxis. Aqueles que recusassem não poderiam viajar."

- 4) Um mapa epidêmico, publicado pelo gigante chinês de buscas Baidu, mostra a localização de casos confirmados e suspeitos em tempo real, para que as pessoas possam evitar ir aos mesmos lugares.
- 5) O Qihoo 360, a maior empresa de cibersegurança da China, está oferecendo um aplicativo que permite aos usuários verificar se eles estiveram em um trem ou avião com alguém que contraiu o vírus.

O artigo supra citado também esclarece que a pressa em coletar mais dados para combater o surto levou à violações da privacidade, especialmente para os residentes no epicentro de Wuhan, alguns dos quais tiveram seus nomes, endereços, movimentos diários e outros dados pessoais vazados na Internet em meio ao medo causado pela propagação da doença.

Em meio a tudo isso, esclarecem que: "A China está reforçando a proteção da privacidade, mas, ao mesmo tempo, buscará um equilíbrio entre o uso da informação para segurança pública e a proteção da informação", disse Tian. "O Comitê Permanente do Congresso Nacional do Povo estabelecerá legislação para proteger as pessoas. informações este ano, e o saldo pode ser refletido até certo ponto".

No entanto, nos resta aguardar de que forma esses dados serão tratados e como encontrarão o equilíbrio.

1 - <https://www.scmp.com/tech/apps-social/article/3052232/coronavirus-accelerates-chinas-big-data-collection-privacy> / \* Luiz Henrique Levy é sócio do escritório Lacaz Martins, Pereira Neto, Gurevich & Schoueri Advogados.

## UNIÃO EUROPEIA

Os países da União Europeia adotaram políticas baseadas em países como Coreia do Sul e Cingapura, que utilizaram práticas **de monitoramento pelos usos dos celulares no combate ao Covid 19 para acompanhar aglomerações**.

Assim para que fossem resguardados os direitos dos cidadãos, Wojciech Wiewiórowski, Autoridade Independente de Proteção de Dados da União Europeia, esclareceu à Roberto Viola, Diretor Geral da DG CONNECT (Direção Geral de Comunicação, Redes, Conteúdo Tecnologia) da Comissão Europeia<sup>2</sup> em relação a consulta que lhe foi efetuada as regras de proteção de dado em vigor na Europa são flexíveis, permitindo várias medidas no combate a pandemia.

A autoridade respondeu, ainda, com relação a carta enviada pelo diretor da DG Conenect, que o uso apenas de **dados anônimos** para mapear movimentos de pessoas com o objetivo de garantir a estabilidade do mercado interno e coordenar a resposta a crises ficam fora do escopo das regras de proteção de dados.

Porém, esclarece que ao mesmo tempo, o anonimato eficaz exige mais do que simplesmente **remover identificadores óbvios, como como números de telefone e números IMEI**.

Deste modo, a autoridade requer que seja definido de forma clara o conjunto de dados que se deseja obter para garantir transparência pública evitando possíveis mal-entendidos.

E, solicita que seja compartilhada cópia do modelo de dados, uma vez definido, para obter informações de segurança e acesso a dados, na medida em que os dados obtidos pela Comissão forem anônimos excluem-se do escopo das regras de proteção de dados.

No entanto, as obrigações de segurança da informação sob Decisão 2017/46<sup>3</sup> da Comissão ainda se aplicam, assim como as obrigações de confidencialidade previstas no Estatuto para qualquer pessoa da Comissão que processe a informação. Caso a Comissão conte com terceiros para processar as informações, esses terceiros devem aplicar medidas de segurança equivalentes e são obrigados por estritas obrigações de confidencialidade **e proibições de uso posterior**.

E, enfatiza a importância de aplicar medidas adequadas para garantir a segurança de transmissão de dados dos provedores de telecomunicações. Também seria preferível limitar o acesso aos dados a especialistas autorizados em epidemiologia espacial, proteção de dados e ciência de dados.

Já no que se refere à retenção de dados, requer que os dados obtidos das operadoras de telefonia móvel sejam excluídos assim que a atual emergência chegar e que os serviços implantados são devidos à crise e são de CARÁTER TEMPORÁRIO.

Nota-se que todas as coletas e armazenamentos de dados são permitidos pela autoridade de proteção de dados, desde que sejam anonimizados e esclarecidos ao público, bem como a retenção não será permitida após o fim da decretação da calamidade.

2 - [https://edps.europa.eu/sites/edp/files/publication/20-03-25\\_edps\\_comments\\_concerning\\_covid-19\\_monitoring\\_of\\_spread\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/20-03-25_edps_comments_concerning_covid-19_monitoring_of_spread_en.pdf)

3 - <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32017D0046&from=EN>

## BRASIL

No país, o Governo do Estado de São Paulo adotou medidas de controle por empresas de telefonia por meio da geolocalização dos celulares para verificar onde há maior concentração de pessoas e avaliar possíveis aglomerações.

No entanto, houve manifestações a favor e contra a decisão governamental. Fato é que o Presidente da República vetou a utilização do uso de informações coletadas através dos celulares por entender que havia violação à privacidade de dados.

Assim, em que pese a Lei Geral de Proteção de Dados Brasileira – LGPD (Lei nº 13.709/18) só entre em vigor em agosto deste ano, as autoridades devem observar os limites e a proporcionalidade dos dados coletados, ainda, que em situação de calamidade como a que estamos enfrentando.

Além das autoridades governamentais, empresas, estabelecimentos comerciais e condomínios residenciais também adotam suas políticas de controle e, entre elas, está a medição da temperatura de seus moradores, funcionários e clientes e, nos casos em que a pessoa apresente febre, orientam consultar um médico.

Assim, como buscar o equilíbrio?

Ocorre que, se tivéssemos a Autoridade Nacional de Proteção de Dados (ANPD), conforme preceitua a Lei Geral de Proteção de Dados nº 13709/18, no qual uma de suas atribuições no artigo 55 J , inciso I é **“zelar pela proteção de dados pessoais,”** assim como ocorreu na União Europeia, poderia estabelecer limites e pedir esclarecimentos e transparência no tratamento destes dados.

No entanto, em que pese a *vacatio legis*, é notório que o controle do Estado sobre os cidadãos, assim, como as práticas adotadas pela iniciativa privada não poderão violar a vida privada das pessoas e direitos conexos.

De modo que os dados armazenados sejam utilizados exclusivamente e temporariamente para a finalidade que foi coletado, qual seja, monitoramento e combate ao Covid-19 e deverão ser descartados com o fim da emergência.

## GOUVÊA ADVOCACIA CONSULTORIA

Adriana Gouvêa, advogada, com expertise em Direito Empresarial, Contratos e certificada internacionalmente pela EXIN como **DPO (Data Protection Officer)**, Privacy and Data Protection Essentials, Privacy and Data Protection Foundation, **Privacy and Data Protection Practitioner**, ISO 27001 Foundation, experiência em consultoria, treinamento, adequação e implantação GDPR e LGPD.

### Contato:

[adriana@gouveadvocaciaconsultoria.com.br](mailto:adriana@gouveadvocaciaconsultoria.com.br) | 11 5087-8837 | 11 9 8220-4387



**Workplan** é uma consultoria especializada em soluções integradas de saúde, benefícios corporativos e segurança do trabalho atuando diretamente com o setor de Recursos Humanos em busca de resultados, eficiência e alcance das metas propostas.

Elaboramos um conjunto de ações para a correta implantação dos processos internos relacionados à nova LGPD com a eficiência e eficácia necessárias.

Nossa equipe atende demandas que envolvam *cibersecurity*, relação de trabalho, comerciais, empresariais e demais áreas impactadas fortemente pela nova LGPD - Lei Geral de Proteção de Dados, desde a elaboração de políticas, revisão das eventualmente existentes ou mesmo orientando na mitigação de eventuais riscos atuais e futuros.

### Contato:

[contato@workplanbrasil.com.br](mailto:contato@workplanbrasil.com.br) | 11 2737.1964 | 11 9.8291.7070 | 11 99307-2300