DATA PRIVACY BRASIL

RELATÓRIO

PRIVACIDADE E PANDEMIA:

RECOMENDAÇÕES PARA O USO LEGÍTIMO DE DADOS NO COMBATE À COVID-19

Bruno Bioni | Rafael Zanatta | Renato Leite Monteiro
e Mariana Rielli

DataPrivacyBR RESEARCH

Data Privacy Brasil

RELATÓRIO

PRIVACIDADE E PANDEMIA:

RECOMENDAÇÕES PARA O USO LEGÍTIMO DE DADOS NO COMBATE À COVID-19

São Paulo
13 de abril de 2020

APRESENTAÇÃO

O Data Privacy Brasil foi fundado para desenvolver uma cultura de proteção de dados pessoais no Brasil. O Instituto está sediado em São Paulo e, em menos de dois anos, treinou mais de 2.000 profissionais de diferentes origens, incluindo profissionais do setor privado, público, academia, membros de organizações não-governamentais e membros da Defensoria e Ministério Público. Um dos objetivos do Data Privacy Brasil é ajudar gestores públicos, reguladores, magistrados e profissionais do direito e outras áreas afetas à proteção de dados a lidar com questões complexas que exigem conhecimento profundo sobre como os sistemas sócio técnicos afetam direitos fundamentais.

A Associação Data Privacy Brasil de Pesquisa, criada em 2020 a partir da experiência da escola, concentra-se em investigações sócio jurídicas sobre a interconexão entre proteção de dados pessoais, tecnologia e direitos fundamentais. Por meio do Observatório da Privacidade, a área monitora constantemente as decisões regulatórias das autoridades de proteção de dados em todo o mundo, casos estratégicos no judiciário brasileiro e nos tribunais internacionais e novos projetos de lei no Brasil que podem mudar o cenário regulatório. Ainda, um dos seus objetivos é a produção de documentos técnicos de posição e *policy papers* para auxiliar as autoridades responsáveis por tomadas de decisão.

Combinando habilidades de pesquisa e vasta experiência no movimento brasileiro de direitos digitais, a Associação Data Privacy Brasil de Pesquisa concentra-se em projetos estratégicos que podem aprimorar a proteção dos direitos fundamentais, melhorar a capacidade regulatória do Estado e restringir abusos e práticas discriminatórias pelo setor privado com o objetivo de contribuir para um desenvolvimento econômico sustentável.

Para mais informações sobre o Observatório, visite https://observatorioprivacidade.com.br. Para mais informações sobre a Associação Data Privacy Brasil de Pesquisa, bem como acesso à Política de Financiamento Ético, visite https://dataprivacybr.org.

Membros do Comitê Multissetorial
O Comitê Multissetorial foi constituído com experts da sociedade civil e de empresas privadas, que opinaram sobre uma versão preliminar do relatório em abril de 2020. Participaram do Comitê de forma voluntária: Bárbara Prado Simão (Instituto Brasileiro de Defesa do Consumidor), Luiza Brandão (Instituto de Referência em Internet & Sociedade), Francisco Brito Cruz (InternetLab) e Raíssa Moura (InLoco). As opiniões manifestadas neste relatório não representam a visão dos membros do Comitê, que se manifestaram em suas capacidades individuais.

Consultora para Revisão

O relatório foi revisado por Clara Iglesias Keller, pós-doutoranda no Leibniz Institut für Medienforschung | Hans-Bredow-Institut e pesquisadora associada ao Alexander von Humboldt Institut für Internet und Gesellschaft (HIIG).

Autore(A)S:

Bruno Ricardo Bioni

Doutorando em Direito Comercial e Mestre com louvor em Direito Civil na Faculdade de Direito da Universidade de São Paulo (USP). Foi pesquisador visitante do European Data Protection Board/EDPB e do Departamento de Proteção de Dados Pessoais do Conselho da Europa. Além disso, foi pesquisador visitante no Centro de Pesquisa de Direito, Tecnologia e Sociedade da Faculdade de Direito da Universidade de Ottawa e assessor jurídico e de relações governamentais do Comitê Gestor da Internet no Brasil/CGI.br e do Núcleo de Informação e Coordenação do Ponto BR/NIC.br. Integra a Rede Latino-Americana de Estudos sobre Vigilância, Tecnologia e Sociedade/LAVITS. É diretor e fundador do Data Privacy Brasil.

Rafael A. F. Zanatta

Doutorando pelo Instituto de Energia e Ambiente da Universidade de São Paulo (USP). É mestre pela Faculdade de Direito da USP. Mestre em direito e economia pela Universidade de Turim. Alumni do Privacy Law and Policy Course da Universidade de Amsterdam. Foi coordenador do programa de direitos digitais do Instituto Brasileiro de Defesa do Consumidor – IDEC, líder de projetos do InternetLab e pesquisador da Escola de Direito da Fundação Getúlio Vargas – FGV/SP. Pelo IDEC, foi representante do Comitê de Defesa dos Usuários de Telecomunicações da Anatel e membro do grupo de trabalho em Tecnologia e Consumo do Ministério da Justiça. Integra a Rede Latino-Americana de Estudos sobre Vigilância, Tecnologia e Sociedade/LAVITS. É coordenador de pesquisas do Data Privacy Brasil.

Renato Leite Monteiro

Doutorando em Filosofia e Teoria Geral do Direito na Universidade de São Paulo (USP). LL.M em Technology Law pela NYU e NUS. Foi pesquisador visitante e consultor do Departamento de Proteção de Dados do Conselho da Europa. Professor convidado de diversas instituições como a USP, Mackenzie, FGV e Insper. Colaborou ativamente com as discussões e redação da Lei Geral de Proteção de Dados do Brasil - LGPD. É co-chair, no Brasil, da Associação Internacional de Profissionais de Privacidade – IAPP, e tem certificação CIPP/E, CIPM e FIP. Fundador e Diretor do Data Privacy Brasil.

Mariana Rielli

Advogada, graduada pela Universidade de São Paulo (USP). Foi assessora jurídica e de incidência da ARTIGO 19 Brasil. Foi consultora da Alianza Regional por la Libertad de Expresión e Información. É pesquisadora líder de projeto no Data Privacy Brasil

Apoio Institucional

A elaboração deste relatório contou com auxílio financeiro da entidade sem fins lucrativos AccessNow, sediada nos Estados Unidos. Para mais informações sobre o papel da entidade na promoção dos direitos digitais, ver https://www.accessnow.org/about-us/.

Como citar este documento

BIONI, Bruno; ZANATTA, Rafael; MONTEIRO, Renato; RIELLI, Mariana. Privacidade e pandemia: recomendações para o uso legítimo de dados no combate à COVID-19. *Conciliando o combate à COVID-19 com o uso legítimo de dados pessoais e o respeito aos direitos fundamentais*. São Paulo: Data Privacy Brasil, 2020.

SUMÁRIO EXECUTIVO

O Relatório *"Conciliando o combate à COVID-19 com o uso legítimo de dados pessoais"* apresenta princípios e recomendações para a formulação de políticas de compartilhamento de dados pessoais, entre entidades da Administração Pública e/ou destas com entidades do setor privado, no âmbito do Regulamento Sanitário Internacional (aprovado pelo Decreto 10.212/2020) e da Lei 13.979/2020 (que estabelece as medidas para enfrentamento da emergência de saúde pública decorrente do COVID-19, também conhecida como "Lei da Quarentena").

O objetivo do Relatório é informar processos decisórios atualmente em curso no Brasil, tanto no setor público quanto no setor privado, com vistas ao desenvolvimento de soluções inovadoras que se valem do uso de dados[1] para auxiliar no combate a uma das maiores pandemias do último século.

Independentemente da vigência da Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), as partes envolvidas em ações dessa natureza possuem o dever de incorporação de salvaguardas e mecanismos de mitigação de riscos a direitos fundamentais, decorrente do ordenamento jurídico brasileiro. Esse dever pode ser extraído de legislação difusa já vigente no país, sendo fontes normativas das propostas contidas neste relatório, além dos já citados Regulamento Sanitário Internacional e da Lei da Quarentena, as normas setoriais de proteção de dados pessoais em vigor (como a Lei 12.965/2014 - Marco Civil da Internet, o Decreto 8.771/2016, a Lei 12.527/2011 - Lei de Acesso à Informação, a Lei 9.472/1997 - Lei Geral de Telecomunicações[2], dentre outras) e as normas protetoras de direitos fundamentais resguardadas pela legislação nacional, em especial a Constituição Brasileira de 1988 e demais tratados internacionais de direitos humanos dos quais o Brasil é signatário.

Nesse cenário, a LGPD, apesar de ainda não vigente, assume um papel norteador dessas políticas públicas, uma vez que representa um quadro principiológico já aprovado pelo legislador brasileiro como fundamental para o tratamento constitucional da proteção de dados no território nacional. Esse papel independe da vigência das suas regras deônticas, e apesar dos princípios e recomendações deste relatório seguirem suas orientações, sua pertinência prescinde da vigência da LGPD, derivando do conjunto de leis em vigor já referidas.

Quais são as implicações práticas desse arcabouço legal no momento de uso de dados para combate à pandemia do COVID-19? Como ele afeta e condiciona a conduta prática de gestores públicos e atores privados envolvidos na formulação dessas medidas?

---

[1] Neste relatório, usamos os termos "dados pessoais" e "dados" de forma intercambiável para facilitação de leitura. Além disso, é importante destacar que o conceito de dado pessoal segue uma lógica expansionista sendo uma informação relacionada a uma "pessoa identificada ou identificável". Desta forma, dados pessoais vão muito além do número de RG, CPF, nome e endereço, podendo, também ser considerados como tal dados locacionais - (e.g., dados de geolocalização) ou identificadores eletrônicos (endereço IP, MEI, Mac address) se estiverem relacionados a uma pessoa - artigo 14, I, do Decreto 8.771/2016. Nesse sentido, BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Grupo Editorial Nacional, 2020 (2a edição).

[2] Art. 72. Apenas na execução de sua atividade, a prestadora poderá valer-se de informações relativas à utilização individual do serviço pelo usuário. (...) § 2° A prestadora poderá divulgar a terceiros informações agregadas sobre o uso de seus serviços, desde que elas não permitam a identificação, direta ou indireta, do usuário, ou a violação de sua intimidade.

Enfrentando essas questões, o Relatório do Data Privacy Brasil apresenta uma série de recomendações sobre como os requerimentos de acesso aos dados devem ser feitos, e quais as melhores práticas para projetos de colaboração entre empresas e as diferentes esferas da Administração Pública. Apesar de seu caráter geral e aplicabilidade a atividades diversas relacionadas à regulação e tratamento de dados, essa elaboração teve como foco à constituição de protocolos para o tratamento de dados, em especial o uso compartilhado[3] para fins de combate à COVID-19.

Conforme exposto na Metodologia, essas recomendações são resultado de um processo de elaboração de cinco passos que devem estar presentes nos processos institucionais decisórios afetos à matéria coberta pelo Relatório:

Passo 1: Avaliação da necessidade da elaboração de política de saúde centrada em dados
Passo 2: Definição da finalidade e necessidade do tratamento de dados
Passo 3: Definição do ciclo de vida e descarte dos dados
Passo 4: Definição de salvaguardas específicas para direitos fundamentais
Passo 5: Garantia de publicidade, transparência e participação

Ao longo desses passos, foram identificados um total de 10[4] princípios[5] a serem observados em cada uma dessas etapas pelos gestores públicos e agentes privados nelas envolvidos. São os seguintes princípios:

Princípio 1 - Motivação fundamentada
Princípio 2 - Amparo em autorização legal
Princípio 3 – Formalização em instrumento contratual ou congênere
Princípio 4 - Definição de finalidade específica de forma expressa
4.1. Vedação do uso com finalidades lucrativas e discriminatórias abusivas
Princípio 5 - Limitação ao mínimo necessário
Princípio 6 - Definição do ciclo de vida dos dados
6.1. Limitação temporal

[3] A LGPD define, em seu artigo 5o, XVI, uso compartilhado como: "comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados"

[4] Além dos 10 princípios, foram formulados 8 subprincípios, totalizando 18 diretrizes.

[5] A formulação em princípios se baseia no entendimento de que essas propostas constituem noções e valores fundamentais que devem reger os processos decisórios relativos ao uso e compartilhamento de dados pessoais no combate à pandemia de COVID-19. Reconhece-se, contudo, que a discussão teórica sobre o que diferencia os princípios como regras contém dissenso e ambiguidades que vão além do escopo deste trabalho. Sobre essas discussões, veja-se: SILVA, Virgílio Afonso da. Princípios e regras: mitos e equívocos acerca de uma distinção. Revista Lationamericana de Estudos Constitucionais. v. 1, 2003. PEREIRA, Jane Reis Gonçalves. Interpretação Constitucional e Direitos Fundamentais. Saraiva: São Paulo, 2018. Registra-se, ainda, que essa formulação não se confunde com a técnica regulatória de "regulação por princípios", cuja pertinência o documento não testa ou encampa (sobre a técnica, v. BLACK, Julia. The Rise Fall and Fate of Principles Based Regulation. LSE Law, Society and Economy Working Papers, n. 17, 2010.)

6.2. Exclusão posterior ao uso adequado
6.3. Qualidade dos dados
Princípio 07 - (Pseudo)anonimização de forma a garantir baixos riscos de reidentificação de pessoas
7.1. Compromisso de não reidentificação pelo recipiente
7.2. Priorização da informação (*output*) e o não repasse de dados (*input*)
7.3. Inclusão de recipientes terceiros confiáveis caso seja necessária a agregação de base de dados
7.4. Não divulgação de identidade de recuperados, infectados ou suspeitos
Princípio 8 - Garantia de segurança da informação
Princípio 9 - Transparência ativa
Princípio 10 - Preferência por aplicativos e tecnologias de código aberto

A partir dessa análise e dos princípios identificados, o Relatório apresenta, ao fim de cada passo, um resumo com recomendações concretas referentes àquela etapa. Abaixo, destaca-se o conjunto dessas recomendações de forma individualizada:

- **Necessidade de fundamentação técnica e científica quanto à necessidade e eficiência do uso de dados pessoais:** a partir de um cenário no qual pode haver uma escalada no uso de dados para o combate ao COVID-19, deve-se garantir que tais ações sejam motivadas e respaldadas em evidências técnicas e científicas quanto à necessidade e eficiência do uso de tais informações;
- **Necessidade de lei e outras normas jurídicas específicas para respaldar a cooperação entre setor público e privado:** em se tratando de cooperação com setor privado, é necessária a previsão em lei formal para as medidas adotadas, em vista do princípio da reserva legal. Recomenda-se, ainda, a detalhamento por instrumento jurídico que procedimentalize o uso compartilhado de dados dentro do próprio setor público e deste com o setor privado, conferindo maior grau de segurança jurídica ao arranjo;
- **Todas as medidas empregadas devem se pautar pela menor intrusão à privacidade possível**: havendo a necessidade do uso de dados de pessoas individualizadas, ele deve estar amparado em fundamentação jurídica robusta, lastreada em preceito legal, que evidencie de forma clara e evidente que tal forma de coleta e uso dos dados é estritamente necessária, e que tal objetivo não pode ser atingido de outra forma menos invasiva e intrusiva;
- **Respeito à ideia de finalidade bem delimitada:** Toda e qualquer atividade de tratamento de dados para o combate à COVID-19 deve ter uma finalidade estritamente delimitada, mediante a indicação de qual é a medida aplicada em específico, e somente se valer dos dados que são necessários para atingir essa finalidade. A partir disso, é possível verificar se a modelagem de dados considerada minimiza e maximiza, respectivamente, os riscos à privacidade e a eficiência no combate à pandemia;
- **Toda e qualquer operação de uso de dados para o Combate à COVID-19 deve ter início, meio e fim:** toda e qualquer operação de uso de dados para o Combate à COVID-19 deve ter ciclo de vida pré-definido com início, meio e fim, incluindo especificação de técnicas aplicadas, dos dados que serão coletados e processados e meios posteriores de descarte. O gestor público deve prever tempo determinado de vida útil e descarte, definido anteriormente à implementação de um projeto de colaboração para uso compartilhado de dados nos termos da Lei 13.979/2020;

- **Medidas de contenção a riscos à privacidade devem ser articuladas em todos os casos:** a partir da premissa que toda e qualquer atividade de tratamento de dados carrega consigo riscos à privacidade dos seus titulares, deve-se sempre articular medidas de contenção dos possíveis efeitos colaterais. De técnicas de (pseudo)anonimização, passando por segregação ou, ao menos, agregação de base de dados com filtros (recipientes confiáveis), chegando ao estabelecimento de medidas robustas de segurança da informação, várias são as ações necessárias para garantir os menores riscos possíveis para liberdades e direitos fundamentais ao longo de todo o ciclo de utilização de dados;
- **Transparência máxima às medidas e à sua governança:** o poder público deve dar máxima transparência aos acordos de compartilhamento de dados, de forma proativa, mediante a publicação de quais são as ações, dados gerados e arranjos contratuais de uso compartilhado em seus portais de transparência, por exemplo. Não só as atividades em si de tratamento de dados, mas, sobretudo, os seus detalhes técnicos e os processos decisórios que levaram à sua adoção devem ser divulgados; e
- **Tecnologias de código aberto:** as soluções adotadas pelos setores público e privado devem ser, preferencialmente, de código aberto, a fim de permitir maior, acesso, participação democrática, escrutínio público e, em última instância, eficiência.

A aplicação desses princípios e recomendações deve se materializar tanto em políticas públicas no nível federal, estadual e municipal, quanto em práticas voluntárias. Sua adoção pode ser formalizada a partir de Decreto, portaria interinstitucional ou norma técnica a ser publicada por órgão competente; ou, ainda, através de cartas de compromisso e diretrizes do setor público ou privado, convênios e instrumentos congêneres do direito administrativo.

SUMÁRIO

I - INTRODUÇÃO

A pandemia da COVID-19, doença infecciosa causada pelo coronavírus da síndrome respiratória aguda grave 2 (SARS-CoV-2), tem mobilizado ações políticas, econômicas e sociais de proporções inéditas. Em menos de quatro meses desde sua descoberta na China, a doença atingiu um milhão de pessoas, levando milhares a óbito, em especial pessoas com algum tipo de comorbidade e em idade avançada. Nesse contexto, governos criaram legislações específicas de enfrentamento da COVID-19, incluindo medidas de isolamento, quarentena e distanciamento social, bem como para compartilhamento de dados entre setor público e setor privado com a finalidade embasar e monitorar as medidas de contenção.

Em comparação com outros momentos críticos para a saúde pública em âmbito mundial, uma das diferenças essenciais da COVID-19 é que a doença se dissemina em um mundo extremamente digitalizado e conectado, em que os dados são produzidos com velocidade e em volume sem precedentes. Modelos computacionais, especialmente aqueles baseados em aprendizado de máquina, têm se mostrado úteis no desenvolvimento de tecnologias de monitoramento e rastreamento de pessoas e até de previsão sobre o avanço de doenças. Há, assim, interesse significativo, por parte de gestores públicos, no compartilhamento de dados dos cidadãos para essas finalidades.

No Brasil, a Lei Federal 13.979/2020[6], conhecida como "Lei da Quarentena", determinou critérios para atuação do Ministério da Saúde, incluindo a realização compulsória de testes e a mobilização de forças policiais para cumprimento de medidas de *isolamento e quarentena* (que incluem a separação de pessoas doentes ou contaminadas, ou de bagagens, meios de transporte, mercadorias ou encomendas postais afetadas, de maneira a evitar a contaminação ou a propagação do coronavírus, e a restrição de atividades e separação, nos mesmos termos, de pessoas suspeitas de contaminação). A legislação prevê que tais medidas, que implicam limitação de direitos constitucionais básicos, tais como o de locomoção e liberdade econômica, "poderão ser determinadas com base em evidências científicas e em análises sobre as informações estratégicas em saúde e deverão ser limitadas no tempo e no espaço ao mínimo indispensável à promoção e à preservação da saúde pública". A legislação reconhece o respeito à dignidade, aos direitos humanos e às liberdades fundamentais das pessoas, conforme preconiza o Artigo 3º do Regulamento Sanitário Internacional produzido pela Organização Mundial da Saúde (OMS) e adotado pelo Brasil por meio do Decreto 10.212/2020.[7]

Tal Regulamento dedica especial atenção à proteção de dados pessoais. Seu artigo 45 dispõe que as informações de saúde devem ser mantidas em sigilo e processadas anonimamente, mediante balizas de leis nacionais. Seu Parágrafo 1º prevê que os Estados podem tratar dados pessoais "quando isso for essencial para os fins de avaliação e manejo de um risco para a saúde pública", garantindo que os dados pessoais sejam (i) processados de modo justo e legal, e sem outros processamentos desnecessários e incompatíveis com tal propósito, (ii)

[6] BRASIL. LEI Nº 13.979, DE 6 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. Disponível em: http://www.in.gov.br/en/web/dou/-/lei-n-13.979-de-6-de-fevereiro-de-2020-242078735

[7] BRASIL. DECRETO Nº 10.212, DE 30 DE JANEIRO DE 2020. Promulga o texto revisado do Regulamento Sanitário Internacional, acordado na 58ª Assembleia Geral da Organização Mundial de Saúde, em 23 de maio de 2005. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10212.htm

adequados, relevantes e não excessivos em relação a esse propósito, (iii) acurados e, quando necessário, mantidos atualizados, garantindo-se que todas as medidas razoáveis serão tomadas para garantir que dados imprecisos ou incompletos sejam apagados ou retificados; e (iv) conservados apenas pelo tempo necessário.

O uso de dados de maneira legítima é essencial à formulação de políticas públicas e iniciativas privadas para o combate a COVID-19. **Entender como a população tem se comportado pode ajudar o poder público a antecipar demandas e alocar recursos, pessoal e medidas de contenção de forma mais eficiente**.

Nesse contexto, o art. 6º da Lei 13.979/2020 determina que "é obrigatório o compartilhamento entre órgãos e entidades da administração pública federal, estadual, distrital e municipal de dados essenciais à identificação de pessoas infectadas ou com suspeita de infecção pelo coronavírus, com a finalidade exclusiva de evitar a sua propagação". Essa regra estende-se ao setor privado quando os dados forem solicitados por autoridade sanitária, e no caso de compartilhamento de dados entre empresas e governo deve ser observado o pleno respeito à dignidade, aos direitos humanos e às liberdades fundamentais, como também preconiza o Regulamento Sanitário Internacional.

A incorporação de princípios da proteção de dados é crucial para dar concretude ao Regulamento Sanitário Internacional, que menciona expressamente a necessidade e o respeito a leis nacionais de proteção de dados. Nesse sentido, devem ser garantidas salvaguardas como limitação temporal, exclusão após uso, medidas técnicas robustas de anonimização e proibição de monetização de dados sensíveis ou uso para quaisquer outras finalidades além das necessárias para o combate à pandemia.

O reconhecimento da dignidade, dos direitos humanos e das liberdades fundamentais está profundamente conectado com o direito à proteção de dados pessoais, já reconhecido pelo legislador brasileiro na forma da Lei Geral de Proteção de Dados (LGPD) e que em breve pode se tornar um direito constitucionalmente afirmado no Brasil.[8] No contexto atual da pandemia, a Lei 13.979/2020 e as demais normas pertinentes (e.g, Marco Civil da Internet, Decreto 10.212/2020) devem ser vistas, antes de tudo, dentro dos parâmetros dos direitos fundamentais assegurados no artigo 5º da Constituição da República, que garante aos brasileiros e aos estrangeiros residentes no País, dentre outros, a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, à honra, liberdade de reunião e etc.

A fim de garantir esses bens constitucionais, o uso de dados essenciais à identificação de pessoas infectadas ou com suspeita de infecção pelo coronavírus, em especial o compartilhamento de dados entre empresas e o governo, necessita de parâmetros claros que podem ser inspirados pela LGPD, aprovada em 2018 pelo Congresso Nacional e sancionada pelo Presidente da República. Sua base principiológica se conecta claramente com o Artigo 45 do Regulamento Sanitário Internacional e demais dispositivos aplicáveis à matéria, servindo como parâmetros relevantes de atuação do legislador e do gestor público diante da emergência sanitária que se apresenta.

[8] Projeto de Emenda Constitucional n. 17/2019.

A LGPD viabiliza e procedimentaliza o uso de dados pessoais em situações de emergência, de comprovado interesse público e necessidade iminente de proteção de vidas. Ao mesmo tempo, confere segurança jurídica para tais usos, principalmente no compartilhamento de dados entre entes privados e públicos. **Assim, a LGPD não deve ser encarada como obstáculo ao uso de dados pessoais para tais finalidades, mas sim como mais uma referência normativa da forma balanceada de fazê-lo protegendo direitos e liberdades fundamentais e garantindo a saúde pública ao mesmo tempo**.

O uso de dados pessoais no Brasil, dentro ou fora de uma situação de pandemia como a COVID-19, deve ter como fundamento os direitos humanos[9], o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. Por isso, grande parte das práticas e princípios aqui sugeridos tem aplicação transversal ao uso de dados para informar políticas públicas de natureza diversa. No contexto atual, a aplicação correta da Lei 13.979/2020 deve ocorrer a partir de alguns princípios basilares, que resultam de uma interpretação conjunta dos instrumentos jurídicos que regem a matéria.

II – METODOLOGIA E INFOGRÁFICO

Ao observar os 05 (cinco) passos descritos nesse Relatório, o agente decisório terá elementos de análise sequenciais e eliminatórios para a tomada de decisão sobre como fazer um uso legítimo de dados pessoais no combate ao COVID-19. É uma espécie de teste em torno da legalidade, legitimidade e utilidade da medida.

Os dois primeiros dizem respeito ao binômio necessidade-adequação da medida cogitada com o objetivo de que seja feita uma modelagem de dados que seja legítima e menos invasiva à privacidade. Uma vez bem definido quais dados serão utilizados, os dois passos seguintes atacam quais devem ser as ações de gerenciamento de riscos durante o processamento dos dados, bem como definem parâmetros sobre quando ele deve ser descontinuado. Por fim, o quinto e último passo atravessa todos os anteriores para que seja dada a devida transparência com o objetivo de viabilizar colaboração e escrutínio público. Se observado tal roteiro, o uso de dados tende a minimizar os riscos aos titulares dos dados e maximizar a eficiência no combate à pandemia.

[9] Os organismos internacionais de direitos humanos também têm se posicionado em relação ao uso de dados pessoais, dentre outras questões, no contexto do combate à COVID-19. Nesse sentido, ver Resolución 01/20. Pandemia y Derechos Humanos en las Américas. Comisión Interamericana de Derechos Humanos. Disponível em: http://oas.org/es/cidh/decisiones/pdf/Resolucion-1-20-es.pdf

Em que condições posso usar dados no combate à COVID de acordo com as normas nacionais e internacionais?

PASSO 1: Avaliação da necessidade da elaboração de política de saúde centrada em dados pessoais.

PASSO 2: Definição da finalidade e necessidade do tratamento de dados.

PASSO 3: Definição do ciclo de vida e descarte dos dados.

PASSO 4: Definição de salvaguardas específicas para direitos fundamentais.

PASSO 5 Garantia de publicidade, transparência e participação.

Detalhando os Princípios...

Motivação: Possuo evidências científicas que embasem o uso de dados pessoais?	CF + Regulamento Sanitário Internacional (Decreto Nº 10212/2020)
Previsão legal: há previsão do uso em lei ou regulamento?	
Instrumento: há instrumento contratual ou congênere?	
Finalidade: há finalidade delimitada?	Lei da Quarentena, MCI e Decreto Nº 8771/2016
Minimização: são usados apenas os dados estritamente necessários para atingir a finalidade?	
Ciclo de vida: foi delimitado um período de uso e descarte seguro?	
(Pseudo)anonimização: foram aplicadas técnicas adequadas de remoção de identificadores e elementos de individualização?	MCI e Decreto Nº 8771/2016
Segurança da informação: as melhores práticas de segurança foram observadas?	
Transparência: a documentação e métodos são públicos e auditáveis?	LAI, CDC, CF
Código aberto: os códigos utilizados estão sujeitas a escrutínio público?	

"A modelagem de dados pensada minimiza os riscos à privacidade e maximiza a eficência no combate à pandemia."

III - PRINCÍPIOS E RECOMENDAÇÕES

A partir da interpretação conjunta do Regulamento Sanitário Internacional com as normas jurídicas em vigor no Brasil, chega-se a um conjunto de princípios que devem orientar os processos de tomada de decisão em eventuais acordos de cooperação para uso de dados no enfrentamento da COVID-19. Tais princípios devem ser aplicados a partir de cinco passos no processo de construção desses acordos, conforme se expõe a seguir.

PASSO 1: AVALIAÇÃO DA NECESSIDADE DA ELABORAÇÃO DE POLÍTICA DE SAÚDE CENTRADA E ORIENTADA POR DADOS

O primeiro passo consiste na decisão sobre uso compartilhado de dados pessoais entre entes da Administração Pública e destes com entidades do setor privado. Tal decisão pode ser formalizada por meio de protocolo de cooperação, convênio ou requisição. Essa primeira etapa deverá seguir as seguintes diretrizes.

Princípio 1: *Motivação Fundamentada*

Para que o tratamento de dados pessoais ocorra por meio do acesso ou uso compartilhado de dados entre entidades públicas ou entre entidades do setor privado, é necessário que ele ocorra de forma justa e legal, com uma necessidade clara, conforme demanda o Artigo 45 do Regulamento Sanitário Internacional. Essa necessidade precisa ser demonstrada por meio de uma *motivação fundamentada* - princípio que rege a administração pública brasileira, de acordo com o art. 2º da Lei 9.784/1999. O objetivo deste princípio é impedir o exercício de arbitrariedades pelo gestor público, exigindo justificação legítima para intervenção na esfera particular dos administrados.[10]

Especificamente, a motivação do uso compartilhado de dados cujos controladores (responsáveis) são entidades privadas (*e.g.* empresas de telecomunicações ou empresas de tecnologia) e/ou entidades públicas (e.g., ministérios, autarquias, secretarias) exige:

> (i) a exposição das razões pelas quais se acredita que aquele conjunto de dados é essencial para a política de saúde pública;
> (ii) evidências científicas ou empíricas de que a utilização dessas informações é importante para medidas de distanciamento social e outras para a contenção da COVID-19.[11]

Não se pode admitir requerimentos genéricos e atos discricionários, como um mero pedido de compartilhamento de dados, sem a devida fundamentação que ateste a necessidade e eficiência da medida programada.

---

[10] SUNDFELD, Carlos Ari. Motivação do ato administrativo como garantia dos administrados. *Revista de direito público*, nº 75, 1985, p. 118.

[11] Não analisaremos a questão específica do que significa "evidência científica". Sabe-se que a produção de artigos científicos, papers e colaboração internacional de cientistas e universidades para enfrentamento da COVID-19 tem sido enorme. Esse conhecimento precisa servir de apoio para tomada de decisão. O argumento de que "não há conhecimento científico" sobre o assunto não pode prosperar.

A implementação de políticas públicas no âmbito de tecnologias é caracterizada por alta complexidade e incerteza sobre as implicações de fato das medidas adotadas. Nesse sentido, em contextos não emergenciais e em que não haja risco iminente para a coletividade, esses processos devem ser, idealmente, precedidos de análises de impacto que avaliem as opções do gestor público diante da demanda por intervenção que se apresenta.

Nesse cenário, torna-se ainda mais importante a exposição da motivação fundamentada da ação do administrador. Principalmente agora, em que as circunstâncias exigem medidas ágeis e eficientes, gestores públicos precisam apresentar evidências científicas que sustentem a importância da aplicação de certa técnica de análise de dados (*e.g. contact tracing*) e que apresentem resultados confiáveis de sua utilização. Essas evidências precisam ser parte da fundamentação que dá sustentação à intervenção da Administração Pública. A situação emergencial não significa que o Poder Público pode se eximir do dever de motivação; pelo contrário, ela se torna ainda mais importante.

Princípio 2: *Amparo em Autorização Legal*

Pelo princípio da reserva legal, a obrigatoriedade de compartilhamento de dados por parte do setor privado para o setor público deve estar amparada em lei formal (papel cumprido no contexto atual pela Lei da Quarentena). Preferencialmente, tal obrigatoriedade deve ser regulamentada por decreto, para que o tratamento de dados seja procedimentalizado em coerência com o que exige o rol de garantias que se relacionam com a proteção de dados.

Em matérias como esta, em que o potencial de restrição a direitos fundamentais é alto, o embasamento e previsão em regulamento infralegal reforça a segurança jurídica e a legitimidade da medida adotada. Garante-se, ainda, um circuito decisório com freios e contrapesos, nesse caso entre Poder Executivo e Poder Legislativo.

Tendo em vista que a saúde pública é uma competência comum e concorrente entre União, Estados e Municípios, requisições de parcerias para compartilhamento de dados com diferentes entes da federação tendem a se multiplicar e ser difusas. Nesse sentido, o respaldo na reserva legal visa, também, evitar abusos no contexto de uma escalada de requisições.[12]

O princípio de amparo em autorização legal impede interpretações alargadas da Lei 13.979/2020. Como exemplo, cita-se a tese de que Secretarias de Segurança Pública sejam consideradas tipo de "autoridade sanitária" e, por conseguinte, possam exercer o direito de requisição de dados no âmbito do Parágrafo 1º do artigo 6[13]). Nesse caso, a norma infralegal cumpre o importante papel de esclarecer quais órgãos da administração pública se enquadram nesse conceito. Nesse caso já há legislação infralegal aplicável, que exige

[12] Ressalta-se que o princípio da legalidade também funciona como garantia ao agente privado que não queira estabelecer parcerias de compartilhamento de dados de forma voluntária.

[13] "Art. 6º É obrigatório o compartilhamento entre órgãos e entidades da administração pública federal, estadual, distrital e municipal de dados essenciais à identificação de pessoas infectadas ou com suspeita de infecção pelo coronavírus, com a finalidade exclusiva de evitar a sua propagação. § 1º A obrigação a que se refere o caput deste artigo estende-se às pessoas jurídicas de direito privado quando os dados forem solicitados por autoridade sanitária."

interpretação em sentido restritivo da expressão "autoridade sanitária". Trata-se aqui, além dos parâmetros da Lei do Sistema Único de Saúde (Lei 8.080/1990), da Portaria n. 1.139/2013 do Ministério de Saúde, segundo a qual "autoridade sanitária" é "órgão ou agente público competente da área da saúde, com atribuição legal no âmbito da vigilância e da atenção à saúde".

Princípio 3: *Formalização em Instrumento Contratual ou Congênere*

Todo e qualquer uso compartilhado de dados dentro do próprio setor público e deste com o setor privado deve ser formalizado por meio de um instrumento contratual ou congênere legalmente previsto. Além do respeito à legalidade, a formalização permite que princípios e boas práticas consensuados fiquem registrados e tenha ainda maior grau de vinculação.[14]

RECOMENDAÇÃO PARA PASSO 1: A partir de um cenário no qual pode haver uma escalada no uso de dados para o combate à COVID-19, deve-se considerar que tais ações sejam motivadas e respaldadas em evidências técnicas e científicas quanto à necessidade e eficiência do uso de tais informações. Em se tratando de cooperação com o setor privado, deve haver amparo em lei formal, em vista do princípio da reserva legal, bem como regulamentação por norma secundária (que procedimentalize o uso compartilhado de dados dentro do próprio setor público e deste com o setor privado) e, por fim, a formalização em instrumento contratual ou congênere.

PASSO 2: DEFINIÇÃO DA FINALIDADE E NECESSIDADE DO TRATAMENTO DE DADOS

Uma vez definida a fundamentação do uso de dados pessoais e sua pertinência de acordo com as melhores evidências científicas disponíveis, bem como o amparo legal-infralegal e o desenho de um possível instrumento jurídico adequado, um segundo passo é a definição da finalidade precisa do tratamento de dados pessoais. A definição expressa da finalidade é essencial à garantia de que o tratamento seja "adequado e não excessivo", nos termos do artigo 45 do Regulamento Sanitário Internacional. Para ser adequado e não excessivo, um tratamento de dados depende da definição clara de uma finalidade, em coerência com um princípio basilar da finalidade do tratamento de dados (previsto no art. 6º, I da LGPD e conhecido no direito internacional como *purpose limitation*).

Princípio 4: *Definição de Finalidade Específica de Forma Expressa*

Consequência lógica de qualquer pedido motivado é que seja especificada a finalidade do tratamento de dados. Nesse sentido, não basta apenas apontar que o uso de dados será para, de forma genérica, *evitar a propagação da COVID-19*, mas também e sobretudo, qual é a medida de combate em específico cogitada. Por exemplo, para além do distanciamento social, hoje a prática mais comumente adotada, existem outras em discussão para o rastreamento de pessoas infectadas e do próprio vírus. Cada uma das estratégias deve ser justificada e, com

[14] Essa é a lógica, por exemplo, estabelecida pela LGPD ao prever a transferência e uso compartilhado entre Setor Público e Setor Privado, bem como o tratamento de dados pela administração pública devem estar previstos ou respaldados em contratos, convênios ou instrumentos congêneres (interpretação sistemática entre artigo 7o, III e capítulo IV).

isso, deve se verificar a sua adequação[15] frente ao conjunto de dados demandados. Com isso, veda-se qualquer utilização dessas informações para finalidades posteriores e que não sejam aquelas exclusivamente relacionadas ao enfrentamento da COVID-19 em cidades onde há casos confirmados.

Com isso, ficam mitigados os riscos de que os dados usados para combate à pandemia sejam usados para fins discriminatórios abusivos ou ainda, que influenciem o acesso dos indivíduos a bens e serviços públicos e privados (o que se aplica a uma diversidade de situações, como locomoção em espaços públicos ou contratação futura de serviços de saúde e seguridade).

A delimitação expressa e precisa da finalidade precisa constar no instrumento jurídico que institui o acordo de compartilhamento-acesso a dados, como convênio ou termo de cooperação (Princípio 3), definindo com precisão qual será a finalidade do uso dos dados (*e.g.* construção de análise cartográfica de aglomerações para inferências sobre regiões mais afetadas e que podem demandar investimento em leitos e Unidades Intensivas de Tratamento). Essa definição expressa é crucial para um controle posterior de desvio de finalidade, o que é vedado pelo Regulamento Sanitário Internacional e pelas normas de proteção de dados pessoais.

4.1. Vedação do uso com finalidades lucrativas e discriminatórias abusivas

Deve ser absolutamente vedada a possibilidade de celebração de parcerias com fins de ganhos econômicos, por parte de empresas, a partir do uso compartilhado de dados com o poder público no contexto do enfrentamento da COVID-19. Não pode existir interesse lucrativo na utilização de informações de saúde, que são consideradas dados pessoais sensíveis, para fins de combate à COVID 19.

É papel das Autoridades Públicas garantir que o uso dos dados seja exclusivo ao interesse público, sem finalidades lucrativas, de combate à COVID-19. Parcerias e arranjos de *data lakes* não podem ter "taxas de acesso" por parte de empresas privadas responsáveis por sua organização, devendo ser encarada como parte da sua respectiva responsabilidade social corporativa.

No mesmo sentido, e conforme já mencionado nesse Princípio, deve ser vedada a utilização dos dados para finalidades discriminatórias que sejam ilícitas ou abusivas, em obediência ao princípio da isonomia, previsto no 5º, caput da Constituição Federal, verticalizado no art. 6º, inciso IX, da LGPD e, por fim, repisado, de forma expressa, no artigo 42 do Regulamento Sanitário Internacional.

Princípio 5: *Limitação ao Mínimo Necessário*

Políticas de contenção da propagação da COVID-19 e de monitoramento do impacto da doença devem ser feitas a partir da minimização da coleta de dados. Somente devem ser coletados e usados os dados que são estritamente necessários para o atingimento da

[15] Esse é o conteúdo normativo do princípio da adequação na LGPD - artigo 6o, II: "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento"

finalidade pretendida,[16] o que pode impactar de forma indesejada direitos fundamentais. Uma das formas de implementar esse princípio é o uso de mecanismos de "autoavaliação" da população por meio de Dados de Serviços Suplementares Não Estruturados (*Unstructured Supplementary Service Data - USSD*), tecnologia GSM que permite que a população responda perguntas em protocolo ágil, que não exige coleta de dados pessoais. Sempre que possível, o gestor público deve optar por soluções técnicas menos invasivas e adequadas para as finalidades almejadas. Referido princípio minimiza os riscos à privacidade e a outros direitos fundamentais, ao mesmo tempo em que maximiza a eficiência, por concentrar capacidade de processamento de informação em uma menor quantidade de dados de qualidade.

Soluções técnicas de *contact tracing* baseadas em troca de chaves e IDs aleatórios gerados por bluetooth (tecnologia de troca de contatos por proximidade), que dispensam a coleta de dados de geolocalização e identificadores únicos do dispositivo, podem ser opções de limitação ao mínimo necessário, que devem ser avaliados caso a caso.

RECOMENDAÇÃO PARA PASSO 2: Toda e qualquer atividade de tratamento de dados para o combate à COVID-19 deve ter uma finalidade bem delimitada, mediante a indicação de qual é a medida cogitada em específico, e somente se valer dos dados que são estritamente necessários para atingir essa finalidade. A partir disso, é possível verificar se a modelagem de dados pensada minimiza e maximiza, respectivamente, os riscos à privacidade e direitos fundamentais e a eficiência no combate à pandemia.

PASSO 3: DEFINIÇÃO DO CICLO DE VIDA E DESCARTE

Uma vez definida precisamente qual é a finalidade do uso de dados e se os dados são realmente necessários para o objetivo de política pública pretendido, empresas e governos devem definir a temporalidade da cooperação e, mais importante, o ciclo de vida dos dados, ou seja, começo, meio e fim do seu uso. Nesse passo, ganha relevância a observação da regra de "conservação pelo tempo necessário" do Regulamento Sanitário Internacional (art. 45, 2, d).

Princípio 6: *Definição do Ciclo de Vida dos Dados*

Cada medida de combate à COVID-19 e a sua respectiva atividade de tratamento de dados deve ter um prazo de validade pelo qual é concebida, implementada e, por fim, descontinuada. Essa já é uma obrigação vigente no quadro jurídico brasileiro, a exemplo do que preceitua o art. 13,§ 2º, I, do Decreto No 8.771/2016. Um ciclo pelo qual o dado é

[16] O princípio da necessidade já está vigente no quadro jurídico brasileiro (e.g., art. 13,§ 2º, do Decreto No 8.771/2016), tendo sido sistematizado pela LGPD em seu artigo 6o, III: "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados".

coletado, processado e descartado se a sua finalidade foi atingida, o que pode se dar pelo controle da pandemia como um todo ou pelo sucesso de uma medida específica adotada.

Recomenda-se que um "plano de ciclo de vida", em sentido macro, seja elaborado como anexo à documentação técnica da cooperação entre poder público e privado. Isso significa que, para além das informações sobre quais dados serão compartilhados, devem ser estabelecidos quais serão os sistemas utilizados e formatos de arquivos.

6.1. Limitação temporal

Os dados tratados para instrumentalizar políticas de saúde pública e novas formas de conter a propagação da COVID-19 devem ser utilizados não somente com uma limitação de finalidade, mas também com uma limitação temporal clara. Deve ser vedado o uso por tempo indeterminado *ad aeternum* desses dados.

Por exemplo, o uso de dados para aplicativos ou aplicações de *contact tracing* e avisos automáticos por SMS ou por USSD devem ter uma limitação temporal clara, parametrizada de acordo com as normas que definem o período de quarentena e de medidas mais rigorosas do poder público. A situação de pandemia não durará para sempre e não é admissível que os dados sejam utilizados sem uma previsão clara de término. Nesse sentido, os termos de cooperação para uso compartilhado de dados devem ser vistos pela ótica de *projetos*, com início, meio e fim.

Em caso de necessidade de análises de dados por longos períodos de tempo, em razão da realização de estudos científicos colaborativos (e.g. modelagem da dinâmica espacial da epidemia e avaliação dos impactos de distanciamento social), a definição da importância do tempo de uso deve estar amparada em evidências técnicas e científicas, de forma fundamentada e em harmonia com o Princípio 1.

Passada a crise da COVID-19, o governo possui a obrigação de excluir os dados requeridos de pessoas jurídicas de direito privado, impedindo sua reutilização e transmissão para outras bases de dados dentro da Administração Pública. É dever do Estado promover a exclusão dessas informações.

Os instrumentos jurídicos que tratem do compartilhamento de dados entre entes da administração pública ou do setor privado poderão prever a contratação de auditoria posterior ao período de uso de dados, a fim de confirmar a sua exclusão.

6.2. Qualidade dos dados

O artigo 45 do Regulamento Sanitário Internacional, na mesma linha do que dispõe o artigo 6o, V, da LGPD, determina que os dados pessoais sejam acurados e, quando necessário, mantidos atualizados. Nesse processo, também se favorece a adoção de medidas razoáveis para garantir que dados imprecisos ou incompletos sejam apagados ou retificados. Assim, o princípio da qualidade dos dados favorece a legitimidade das decisões tomadas com base em tais dados, tornando-as condizentes com realidade e restritas aos dados relevantes.

RECOMENDAÇÃO PARA PASSO 3: Toda e qualquer operação de uso de dados para o combate à COVID-19 deve ter início, meio e fim, de modo que os dados serão coletados, processados, mantidos de forma atualizada e acurada e, ao final, descartados. O gestor público deve formular um plano de ciclo de vida dos dados, prevendo vida útil e descarte. Isso inclui a previsão de etapas de tratamento e técnicas utilizadas, além de limitação temporal expressa para o uso.

PASSO 4: DEFINIÇÃO DE SALVAGUARDAS ESPECÍFICAS PARA DIREITOS FUNDAMENTAIS

Após a definição das finalidades específicas e técnicas de minimização, bem como a construção do plano de ciclo de vida dos dados e a delimitação de sua temporalidade e medidas de exclusão, é crucial a adoção de medidas que resguardem "liberdades fundamentais das pessoas", nos termos do artigo 3 do Regulamento Sanitário Internacional. Tal respeito é obtido através de uma série de salvaguardas, que podem ser operacionalizadas a partir de um conjunto de princípios a serem seguidos pelos agentes envolvidos.

Princípio 07: *(Pseudo)Anonimização de Forma a Garantir Baixos Riscos de Reidentificação de Pessoas*

Qualquer tratamento de dados deve passar, sempre que possível, por uma etapa técnica que impeça a identificação de indivíduos aos quais originalmente se referem, o que é comumente chamado de anonimização[17]. Dados (pseudo)anonimizados são aqueles que podem ser reidentificados mediante a combinação com outras bases de dados, a partir de esforços razoáveis,[18] não deixando de ser dados pessoais. Por exemplo, os dados de geolocalização são, via de regra, considerados (pseudo)anonimizados para as operadoras de telefonia, já que elas possuem a capacidade de identificar as pessoas a quem eles se referem, de forma individualizada.

Conforme nos ensina literatura especializada[19], não é possível garantir um dado que seja, ao mesmo tempo, 100% útil e 100% anonimizado. Além disso, é conhecida a alta probabilidade de reidentificação de dados celulares de localização, inclusive aqueles supostamente anonimizados[20] por meio de metodologias estatísticas e de agrupamento. Por essas razões, a meta das políticas públicas e acordos de compartilhamento deve ser sempre garantir o maior nível possível de (pseudo)anonimização. Assim, sempre que se considerar abrir ou fazer uso compartilhado de base de dados (pseudo)anonimizados, deve-se explicitar quais são as

[17] Sobre a anonimização e as questões que a circundam, BIONI, Bruno. Compreendendo o conceito de anonimização e dado anonimizado. Cadernos Jurídicos, São Paulo, ano 21, nº 53, p. 191-201, Janeiro-Março/2020. Disponível em: https://api.tjsp.jus.br/Handlers/Handler/FileFetch.ashx?codigo=118902

[18] Veja o artigo 12 da LGPD e, em termos de análise comparativa, a consideranda 26 do Regulamento Europeu de Proteção de Dados.

[19] UBINSTEIN, Ira S. e HARTZOG, Woodrow. Anonymization and Risk. *New York University Public Law and Legal Theory Working Papers 530*, 2015.

[20] ZETTER, Kim. Anonymized Phone Location Data Not So Anonymous, Researchers Find. 2013. Disponível em: <https://www.wired.com/2013/03/anonymous-phone-location-data/>

respectivas técnicas e, preferencialmente, testá-las para mensurar seu nível de resiliência.[21] [22]

É importante dar preferência a técnicas que proporcionem o maior nível de anonimização possível. Por exemplo, quando se cogita iniciativas como de mapas de calor, recomenda-se o aumento da área do mapeamento para cobrir o máximo de propriedades possível, evitando a granularidade da informação. Além disso, pode-se, também, reduzir a frequência da atualização dos dados para abranger mais eventos e, com isso, dificultar a identificação de um caso recente (pessoa ou grupos de pessoas que descumpriram o isolamento social). Todas essas medidas dificultam a reversão do processo de (pseudo)anonimização.

As técnicas de anonimização ou de (pseudo)anonimização apresentadas em projetos de colaboração (e.g. construção de Índices de Isolamento Social por meio de análises cartográficas) devem passar por rigoroso processo de avaliação, preferencialmente por pares, na comunidade científica e da ciência da computação e de dados.

É desejável que o governo promova chamadas públicas e premiações para que pesquisadores e cientistas da computação possam demonstrar as falhas em processos de (pseudo)anonimização, evidenciando os casos em que é possível a reidentificação de indivíduos e riscos às liberdades públicas. Idealmente, essas chamadas podem ser consideradas obrigatórias como um "período de teste" para que a cooperação seja realizada, condicionando a implementação completa do projeto de compartilhamento de dados. Caso não haja tempo hábil realizar tais eventos, deve-se permitir que entes externos possam testar a robustez das bases de dados compartilhadas, cabendo ao poder público e entes privados desenvolver ambientes em que tais tentativas de reidentificação possam ser realizadas por meio de ferramentas e técnicas escolhidas pelos responsáveis pelos testes.

---

[21] Nesse sentido, uma das práticas previstas para se avaliar condutas pelo Modelo de Maturidade de Privacidade (Privacy Maturity Model), criado pelo Instituto Americano dos Contadores Públicos Certificados e pelo Instituto Canadense de Contadores (AICPA/CICA), é a otimização, i.e. "a revisão e a avaliação periódicas são utilizadas para garantir a melhoria contínua de determinado processo". Disponível em <https://iapp.org/media/pdf/resource_center/aicpa_cica_privacy_maturity_model_final-2011.pdf>.A aplicação desse modelo de análise (e a conformidade especificamente a essa prática) foi observada no tratamento de dados pessoais efetuado pela municipalidade de Seattle. Ver: Future of Privacy. City of Seattle: Open data risk assessment, 2018. Disponível em https://fpf.org/wp-content/uploads/2018/01/FPF-Open-Data-Risk-Assessment-for-City-of-Seattle.pdf

[22] Um exemplo da difícil dinâmica de balanceamento no uso de métodos de anonimização para combate a doenças se deu no âmbito do combate ao Ebola. Em artigo de Sean Mcdonald (MCDONALD, Sean Martin. Ebola: A Big Data Disaster - Privacy, Property, and the Law of Disaster Experimentation. CIS Papers 2016.1.), o autor explora como o uso de dados de rastreamento de contatos, no caso da doença, era mais efetivo a partir da reidentificação dos dados, isto é, de uma base de dados identificável e individualizada. A anonimização, embora possível, sequer era útil para a finalidade almejada. Destaca-se, ainda, o alerta de Kendal, Kerry e Montjoye, segundo o qual ''as melhores práticas devem aceitar que não há formas perfeitas de anonimizar dados e provavelmente nunca haverá' (KENDALL, Jake; KERRY, Cameron F. e MONTJOYE, Alexandre de. Enabling Humanitarian use of Mobile Phone Data, Technology Innovation, Novembro de 2014. Disponível em: <http://www.brookings.edu/~/media/research/files/papers/2014/11/12-enablinghumanitarian-mobile-phone-data/brookingstechmobilephonedataweb.pdf)'.

7.1. Compromisso de não reidentificação pelo recipiente

Caso haja o uso ou o mero acesso a dados (pseudo)anonimizados, o recipiente deve se comprometer a não fazer, ou tentar fazer, qualquer tipo de engenharia reversa ou processo que leve à reidentificação dos titulares dos dados, ainda que disponha dos métodos e técnicas para tanto. Tal obrigação deve constar expressamente em instrumento contratual ou congênere, de forma que não impeça membros da comunidade técnica e científica testar a robustez dos processos de (pseudo)anonimização.

7.2. Priorização da informação (output) e não do repasse de dados (input)

Quando suficiente para atender o objetivo da política pública, o repasse de informação deve ser priorizado sobre o repasse de dados.

Para muitas das ações de combate à COVID-19, como de distanciamento social, não se faz necessário que agentes do setor privado (e.g, telecomunicações e empresas tecnologias que possuem a geolocalização dos indivíduos), repassem tais dados, em formato bruto, para as autoridades sanitárias. Basta que eles mesmos tratem tais dados internamente e revelem as informações oriundas de tais tratamento, tais como os bairros, regiões ou mesmo cidades e estados que estão cumprindo tais medidas de restrição de locomoção. Esse é o caso, por exemplo, dos chamados "mapas de calor" que impedem, tecnicamente, qualquer acesso a identificadores pessoais, como IMEI, device ID ou rastreamento preciso de movimentação individual de dispositivos. Dessa forma, dados de localização - sejam eles obtidos por meio de GPS, triangulação de dados ou outras técnicas contemporâneas que reduziriam, em tese, o risco de de reidentificação de um indivíduo em específico.

O princípio de priorização da informação (*output*) também pode ser aplicado caso sejam necessárias campanhas de conscientização em determinados bairros ou regiões. Se tais agentes do setor privado já têm um ponto de contato com o titular, eles mesmos podem fazer disparo de mensagens em massa, ao invés de repassar dados dos seus usuários para que a entidade sanitária o faça.

7.3. Agregação de bases de dados e recipientes confiáveis

Para algumas ações, pode se mostrar necessário que haja a combinação de base de dados (*input*) para se extrair informações (*output*), como, por exemplo, o nível de eficácia de um medicamento. Nesse caso, para se construir uma amostra que seja representativa - pacientes com diferentes características genéticas e condições econômicas sociais -, pode ser que seja necessário que base de dados de diferentes hospitais, públicos e privados sejam agregadas.

Para que isso seja feito de forma segura para liberdades e direitos fundamentais em questão, pode-se eleger terceiros - "recipientes confiáveis" – para administrar os dados dos hospitais de posse dessas informações e com interesse em combiná-las. Estes recipientes confiáveis poderiam, ainda, atuar na anonimização desses dados, inclusive nas métricas de efetividade do medicamento (aproveitando o exemplo citado anteriormente). As empresas podem exigir dos recipientes a assinatura de um Termo de Compromisso com os Princípios deste relatório.

Além de recipientes confiáveis, podem ser utilizadas estruturas de dados probabilísticas. Essas estruturas preservam algumas propriedades dos dados ao mesmo tempo que aumentam o nível de anonimização. O HiperLogLog (HLL), por exemplo, é uma estrutura de dados probabilística que tem por objetivo coletar informações eficientes sobre um conjunto sem identificar o indivíduo no conjunto. É possível calcular a cardinalidade (números de coisas sem repetição) do conjunto e realizar uniões com outros HLLs. Essa técnica pode ser utilizada também, por exemplo, para analisar a capacidade de hospitais a fim de evitar a superlotação, mediante contagem de visitas com maior precisão, extraídas de dados de localização, sem identificar as pessoas.[23]

7.4. Não divulgação da identidade de recuperados, infectados ou suspeitos

Medidas específicas para evitar propagação não se confundem com divulgação de informações de pessoas que contraíram a COVID-19 e se recuperaram. Ainda não há informações científicas sobre o impacto da COVID-19 no sistema respiratório, de modo que a apresentação de informações pessoais daqueles que se recuperaram pode abrir caminhos para usos abusivos e discriminatórios desses dados por terceiros.

Tal como decidido pela Corte Superior de Justiça de Israel,[24] é recomendável que as medidas de análise individualizada sejam restritas às pessoas infectadas, sendo vedado a implementação de medidas de vigilância para todas as pessoas suspeitas, sob o risco de inverter a lógica constitucional de primazia das liberdades civis em um regime democrático e instauração de um ambiente permanente de vigilância sem devido processo legal.

Essa preocupação também está presente em iniciativas como a aplicação TraceTogether, implementada em Singapura,[25] e em outros projetos pilotos construídos na Itália que possuem técnicas de não identificação pessoal de infectados, apoiando-se em soluções como a análise de informações obtidas por protocolos de comunicação de smartphones. Medidas como essas devem ser priorizadas, evitando-se a divulgação de informações pessoais.[26]

---

[23] WEBER, Griffin M. YU, Yun William. HyperMinHash: MinHash in LogLog space. Journal of Latex Class Files, Vol. 14, no. 8, August 2015. Disponível em: https://arxiv.org/pdf/1710.08436.pdf, TSCHORSCH, Florian, VON VOIGT, Saskia Nuñez. RRTxFM: Probabilistic Counting for Differentially Private Statistics. Disponível em: https://eprint.iacr.org/2019/805.pdf, ALAGGAN, Mohammed; GAMBS, Sébastien; MATWIN, Stan, TUHIN, Mohammed. Sanitization of Call Detail Records via Differentially-Private Bloom Filters. 29th IFIP Annual Conference on Data and Applications Security and Privacy (DBSEC), Jul 2015, Fairfax, VA, United States. pp.223-230, ff10.1007/978- 3-319-20810-7_15ff. ffhal-01745827, BASIN, David; DESFONTAINES, Damien; LOCHBIHLER, Andreas. Cardinality Estimators do not Preserve Privacy. 2018. Disponível em: https://arxiv.org/pdf/1808.05879.pdf

[24] With Knesset Oversight in Place, High Court Greenlights COVID-19 Surveillance, JNS, 26 de março de 2020. Disponível em: https://www.algemeiner.com/2020/03/26/with-knesset-oversight-in-place-high-court-greenlights-covid-19-surveillance/

[25] Não há evidências científicas sobre o impacto positivo do TraceTogether, formulado pelo governo da Singapura. No entanto, trata-se de uma experiência de política pública de ampla notoriedade.

[26] O projeto "Coronavirus Outbreak" da Itália prioriza a análise de dados trocados pelo "Bluetooth LE handshaking protocol" dos smartphones de forma anonimizada. Sobre o tema, Dave Mosher, 'A new phone-tracing technology could tell if you've been exposed to the coronavirus — without sacrificing privacy. 130 researchers are offering it to countries for free', Business Insider, 04 de abril de 2020. Disponível em:

Princípio 8: *Garantia De Segurança Da Informação*

Na medida em que se intensifica o tratamento de dados mediante, inclusive, a expansão de pessoas e entidades que podem ter acesso a uma base de dados, é essencial a adoção de sistemas de gerenciamento de identidades que evitem incidentes de segurança. Deve haver não só mecanismos de autenticação, como, também, a criação de inventários detalhados sobre quem teve acesso a determinada base de dados, quais dados foram acessados, quando se deu tal acesso e o tempo de duração. Por exemplo, na hipótese de automonitoramento, que pode se dar por um aplicativo baixado pelo próprio cidadão, tais dados devem ser armazenados em seu próprio dispositivo e devidamente criptografados, a exemplo que está em desenvolvimento na União Europeia[27].

A título de exemplo, tais requisitos mínimos de segurança da informação encontram respaldo legal, de forma transversal, na seção II - Padrões de segurança e sigilo dos registros, dados pessoais e comunicações privadas - do capítulo III do Decreto No 8.771/2016, de forma setorial no setor financeiro, na Resolução No 4.658/2018, e, partir do que preceitua a Resolução No 2/2020 do Comitê Central de Governança de Dados.[28] Tais parâmetros de segurança podem ser incrementados a partir do cumprimento de *standards* de segurança da informação, como o padrão NIST[29] ou normas ISO específicas.

RECOMENDAÇÃO PARA PASSO 4: A partir da premissa que toda e qualquer atividade de tratamento de dados carrega consigo riscos à privacidade e aos direitos fundamentais dos seus titulares, deve-se sempre articular medidas de contenção desses possíveis efeitos colaterais. De técnicas de (pseudo)anonimização, passando por segregação ou, ao menos, agregação de base de dados com filtros (recipientes confiáveis), chegando ao estabelecimento de medidas robustas de segurança da informação, várias são as ações necessárias para garantir os menores riscos possíveis ao longo de todo o ciclo de utilização de dados.

https://www.businessinsider.com/coronavirus-covid-19-contact-tracing-mobile-phones-bluetooth-pepp-pt-2020-4

[27] Uma iniciativa denominada Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) pretende implantar a técnica de rastreamento de contatos sem comprometer a privacidade. Segundo os criadores, a ideia é que a aplicação crie IDs temporários que se comuniquem via bluetooth, sem a necessidade de armazenamento de nenhum dado pela empresa. Fonte: An EU coalition of techies is backing a 'privacy-preserving' standard for COVID-19 contact tracing, TechCrunch, 1o de abril de 2020. Disponível em: https://techcrunch.com/2020/04/01/an-eu-coalition-of-techies-is-backing-a-privacy-preserving-standard-for-covid-19-contacts-tracing/.

[28] A referida resolução estabelece regras para o compartilhamento de dados e os requisitos de segurança que devem ser observados pelos órgãos e entidades da administração pública federal direta, autárquica e fundacional, e os demais poderes da União. Em sua Cláusula Geral estabelece que o tratamento de dados realizados por terceiros (empresa contratada) também deverá respeitar os controles de segurança estabelecidos no documento. Inúmeros editais públicos estão sendo abertos para a contratação de Startups que desenvolvam soluções de combate à COVID-19, mas essas empresas precisam ter um nível suficiente de maturidade em segurança da informação para tratar dados pessoais, inclusive dados sensíveis, no contexto excepcional da pandemia, respeitando os requisitos mínimos de segurança da informação.

[29] NIELES, Michael, DEMPSEY, Kelley L., PILLITTERI, Victoria Y. An Introduction to Information Security. Special Publication (NIST SP). Disponível em: https://www.nist.gov/publications/inoduction-information-security.

PASSO 5: GARANTIA DE PUBLICIDADE, TRANSPARÊNCIA E PARTICIPAÇÃO

A delimitação de finalidades específicas, minimização, ciclo de vida e salvaguardas específicas para garantia de direitos fundamentais não são suficientes para o uso legítimo dos dados pessoais no enfrentamento da COVID-19, em cumprimento das normas internacionais e nacionais. Um último passo fundamental, que se apresenta como um requisito processual a ser observado ao longo de todos os demais passos, é o de garantia de publicidade e transparência desses processos. Além de conferir legitimidade ao processo em obediência à Constituição Federal e à Lei de Acesso à Informação, ele garante que as medidas de saúde sejam aplicadas "de maneira transparente e não discriminatória", conforme artigo 42 do Regulamento Sanitário Internacional.

Princípio 9: *Transparência Ativa*

O princípio da transparência ativa significa que não só as atividades de tratamento de dados, mas, sobretudo, os seus detalhes técnicos devem ser publicados. Isso se traduz por uma gestão "transparente"[30] do que é feito com os dados pessoais como ponto de sustentação para as ações de combate à COVID-19.

O princípio da transparência já está vigente no quadro jurídico brasileiro (e.g., art. 37 da Constituição Federal; art. 31, caput, da Lei de Acesso à Informação, art. 7º, III, do MCI e, também, no artigo 4º, caput, do CDC), tendo sido reforçado pela LGPD em seu artigo 6º, VI: "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial".

O princípio da transparência ativa significa que entidades privadas e do poder público devem ser proativas em prestar informações claras, adequadas e facilmente acessíveis sobre quais informações são utilizadas, para quais finalidades e sobre quais agentes envolvidos na cadeia de tratamento de dados. Enquanto o poder público deve tornar públicas tais ações e os respectivos contratos de uso compartilhado de dados em portais de transparência, o setor privado deve manter, preferencialmente na internet, não só a listagem das iniciativas, mas, também, os termos dos seus protocolos de cooperação.

Princípio 10: *Preferência por Aplicativos e Tecnologias de Código Aberto*

O princípio da preferência por aplicativos e tecnologias de código aberto implica que o governo deve privilegiar soluções sem códigos proprietários – ou seja, que não sejam de propriedade de nenhum agente privado específico e que estejam acessíveis de forma abera. O ideal é que as soluções tecnológicas e novos aplicativos sejam geridos e supervisionados por um grupo civil com experiência em código aberto.

Experiências internacionais, mostram a importância de uma política de abertura de dados. Nesse caso, foi construído a partir de uma maratona de oito dias de programação, e hoje é

[30] Art. 31, caput, da Lei de Acesso à Informação: "Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais".

utilizado por 1 a cada 5 residentes de Singapura para políticas de *contact tracing.* O código-base genérico chama-se OpenTrace e pode ser implementado em sistemas iOS e Android. O protocolo BlueTrace, a partir do qual OpenTrace e TraceTogether operam, também foi inteiramente disponibilizado em código aberto. Conforme anunciado pelo governo de Singapura, "a base de código do OpenTrace será mantida por um grupo de ativistas de código aberto. Como órgão governamental, a GovTech decidiu colocar o código em código-fonte aberto para que quaisquer melhorias no OpenTrace estejam sempre disponíveis gratuitamente para que outros possam implantar e melhorar. Ele também permite que os usuários evoluam a base de código para se adequar ao contexto local"[31].

Preferencialmente, com o objetivo de facilitar o escrutínio público, deve-se adotar tecnologias de código aberto para que a comunidade possa avaliar tais ferramentas e, sobretudo, contribuir para o seu aprimoramento. Ainda, deve-se adotar padrões interoperáveis de compartilhamento de dados, para tornar o uso por atores diversos mais eficiente e menos custoso.

RECOMENDAÇÃO PARA O PASSO 5: Medidas de transparência não só permitem o controle social como, também, a colaboração da própria sociedade em pensar e aperfeiçoar medidas de combate à COVID-19. No caso do poder público, tal transparência deve ser proativa mediante a publicação de quais são as ações, dados gerados e arranjos contratuais de uso compartilhado em seus portais de transparência, por exemplo. Além disso, as soluções adotadas pelos setores público e privado devem ser, preferencialmente, de código aberto, a fim de diminuir custos de operação, aumentar eficiência dos programas e permitir o escrutínio público da tecnologia.

IV - CONCLUSÕES E RECOMENDAÇÕES FINAIS

Independentemente da vigência da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018), o Regulamento Sanitário Internacional (Decreto 10.212/2020) e a Lei da Quarentena já trazem regras claras sobre proteção de dados aplicáveis às medidas tomadas no contexto do combate à pandemia do COVID-19. Essas disposições devem ser interpretadas de acordo com a Constituição Federal, e demais leis e regulamentos existentes no Brasil e aplicáveis à matéria, a fim de informar a tomada de decisão sobre compartilhamento de dados pessoais entre agentes privados e o Poder Público.

Se internalizados e bem implementados os princípios e boas práticas de proteção de dados recomendados, aumentar-se-á a probabilidade de eficiência dessas medidas de enquanto também garantida a sua legitimidade, além de gozarem de maior confiança por parte da sociedade. A utilização de dados pessoais é apenas uma das medidas de contenção à pandemia do COVID-19, que deve ser concebida como tal para que seja, de fato, uma medida de contenção e não de ampliação dos danos experimentados por tal epidemia**. O conjunto de recomendações acima deixa claro que a proteção de dados não rivaliza com tal propósito, mas sim permite que o Estado seja eficiente no combate à epidemia e o faça com respeito**

[31] 6 things about OpenTrace, the open-source code published by the TraceTogether team, GovTech Singapore, 09 de abril de 2020. Disponível em: https://www.tech.gov.sg/media/technews/six-things-about-opentrace.

aos direitos e garantias fundamentais da população. Assim, o Relatório destaca quais são os princípios que devem ser seguidos pelos reguladores no âmbito desses processos de tomada de decisão.

A crise da COVID-19 certamente passará, mas os efeitos das escolhas feitas por governos e empresas hoje podem ter efeitos duradouros. Nesse sentido, o uso da tecnologia e dos dados deve se dar de maneira a não comprometer os direitos fundamentais, em especial a privacidade e a proteção de dados pessoais.

Diante da não vigência da LGPD (que pode assumir, nesse contexto, o papel de vetor da base principiológica aplicável), as partes envolvidas em acordos do compartilhamento-acesso de dados pessoais e (pseudo)anonimizados possuem o dever de incorporar salvaguardas e mecanismos de mitigação de riscos a liberdades públicas e direitos fundamentais, seguindo a legislação já em vigor que informa o presente trabalho.

Neste Relatório, foi apresentado um desdobramento concreto dessa legislação, na forma de cinco passos a serem seguidos pelos gestores públicos diante de tais acordos, aos quais se aplicam um total de 10 princípios. As recomendações extraídas dessa metodologia podem ser implementadas por gestores públicos, sociedade civil (terceiro setor e academia) ou internalizadas por profissionais de empresas privadas que lideram iniciativas de uso de dados para análise cartográfica, *contact tracing*, índices de isolamento social e outras técnicas discutidas mundialmente para contenção da COVID-19.

Recomenda-se, para autoridades e agentes públicos do Governo Federal e dos Governos Estaduais e Municipais com competência para atuar nas matérias de que considere esse Relatório para:

- A criação de protocolos a partir dos cinco passos apresentados no Relatório:

  Passo 1: Avaliação da necessidade da elaboração de política de saúde centrada em dados
  Passo 2: Definição da finalidade e necessidade do tratamento de dados
  Passo 3: Definição do ciclo de vida e descarte
  Passo 4: Definição de salvaguardas específicas para direitos fundamentais
  Passo 5: Garantia de publicidade, transparência e participação

- A observação dos 10 princípios apresentados neste Relatório, que se expressam nas formulações abaixo destacadas:

  Princípio 1 - Motivação fundamentada: há evidências científicas que demonstram a importância de implementar essa técnica de análise de dados para combate a COVID-19?
  Princípio 2 - Amparo em autorização legal-infralegal: existe definição clara de quem é a autoridade sanitária e identificação das normas jurídicas que amparam a política?

Princípio 3 - Formalização em instrumento jurídico: existe instrumento jurídico ou congênere de direito administrativo para instrumentalizar a prática de compartilhamento de dados?

Princípio 4 - Definição de finalidade específica de forma expressa: há definição clara sobre de que modo os dados serão usados e para qual fim específico?

4.1. Vedação do uso com finalidades lucrativas e discriminatórias abusivas: o acordo veda a utilização de dados para fins não lucrativos e de combate à COVID-19, bem como para fins não discriminatórios ou abusivos?

Princípio 5 - Limitação ao mínimo necessário: a equipe técnica avaliou se há formas menos invasivas de produzir informação estratégica, coletando o mínimo de dados pessoais?

Princípio 6 - Definição do ciclo de vida dos dados: houve definição de um plano com detalhamento das técnicas aplicadas, tempo de vida e formas de descarte?

6.1. Limitação temporal: há definição clara de limitação temporal e evidências científicas sobre extensão do tempo de uso para estudos?

6.2. Exclusão posterior ao uso adequado: há acordo sobre exclusão dos dados de forma segura após o uso específico para a política pública?

6.3. Qualidade dos dados: há protocolos para manter a exatidão e atualização dos dados?

Princípio 7 - (Pseudo)anonimização controlada pelos pares: as técnicas de (pseudo)anonimização foram validadas pela comunidade técnica e científica de forma a garantir baixos riscos de reidentificação de pessoas?

7.1. Priorização da informação: foram testadas formas de análise da informação sem necessidade de compartilhamento de dados brutos e bases de dados originárias?

7.2. Agregação de bases de dados e recipientes confiáveis: No caso de agregação de bases de dados, há condições de identificação de recipientes confiáveis que atuem como intermediários?

7.3. Compromisso de não reidentificação: Há por parte de quem terá acesso aos dados o compromisso em não aplicar engenharia para tentar reverter o processo de anonimização?

7.4. Não divulgação da identidade dos recuperados, infectados e suspeitos: as técnicas de *contact tracing* e de monitoramento individual são restritas a pessoas infectadas pela COVID-19?

Princípio 8 - Garantia de segurança da informação: há protocolos de segurança da informação, minimizando riscos de incidentes de segurança?

Princípio 9 - Transparência ativa: há publicidade dos documentos técnicos e ampla transparência sobre as técnicas de tratamento de dados e *design* de sistema?

Princípio 10 - Preferência por aplicativos e tecnologias de código aberto: é possível a adoção de soluções de código aberto, garantindo maior participação e segurança?

Recomenda-se, para o Poder Executivo Federal, Estadual e Municipal:

A elaboração de Nota Técnica, a ser publicada por Portaria Ministerial ou Interministerial ou congênere, com incorporação dos 10 Princípios como forma de interpretar, de forma

sistemática, a legislação aplicável a eventuais acordos sobre compartilhamento-acesso de dados (seja entre órgãos da administração pública, seja entre agentes privados).

Recomenda-se ao Poder Legislativo dos entes da federação a adoção dos 10 princípios, idealmente de forma expressa, nos textos legislativos aprovados que se direcionem às matérias de proteção de dados e às medidas adotadas no âmbito do combate à pandemia do COVID-19.

Recomenda-se aos agentes do setor privado e da sociedade civil (academia e terceiro) envolvidos em processos decisórios ou em celebração de acordos de compartilhamento de dados a adoção voluntária das práticas e princípios listados neste documento.

REFERÊNCIAS:

6 things about OpenTrace, the open-source code published by the TraceTogether team, GovTech Singapore, 09 de abril de 2020. Disponível em: https://www.tech.gov.sg/media/technews/six-things-about-opentrace.

An EU coalition of techies is backing a 'privacy-preserving' standard for COVID-19 contact tracing, TechCrunch, 1o de abril de 2020. Disponível em: https://techcrunch.com/2020/04/01/an-eu-coalition-of-techies-is-backing-a-privacy-preserving-standard-for-covid-19-contacts-tracing/.

Future of Privacy. City of Seattle: Open data risk assessment, 2018. Disponível em: https://fpf.org/wp-content/uploads/2018/01/FPF-Open-Data-Risk-Assessment-for-City-of-Seattle.pdf.

Resolución 01/20. Pandemia y Derechos Humanos en las Américas. Comisión Interamericana de Derechos Humanos. Disponível em: http://oas.org/es/cidh/decisiones/pdf/Resolucion-1-20-es.pdf

With Knesset Oversight in Place, High Court Greenlights COVID-19 Surveillance, JNS, 26 de março de 2020. Disponível em: https://www.algemeiner.com/2020/03/26/with-knesset-oversight-in-place-high-court-greenlights-covid-19-surveillance/.

ALAGGAN, Mohammed; GAMBS, Sébastien; MATWIN, Stan, TUHIN, Mohammed. Sanitization of Call Detail Records via Differentially-Private Bloom Filters. 29th IFIP Annual Conference on Data and Applications Security and Privacy (DBSEC), Jul 2015, Fairfax, VA, United States. pp.223-230, ff10.1007/978- 3-319-20810-7_15ff. ffhal-01745827

BIONI, Bruno. Compreendendo o conceito de anonimização e dado anonimizado. Cadernos Jurídicos, São Paulo, ano 21, nº 53, p. 191-201, Janeiro-Março/2020. Disponível em: https://api.tjsp.jus.br/Handlers/Handler/FileFetch.ashx?codigo=118902

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Grupo Editorial Nacional, 2020 (2a edição).

BLACK, Julia. The Rise Fall and Fate of Principles Based Regulation. LSE Law, Society and Economy Working Papers, n. 17, 2010.

KENDALL, Jake; KERRY, Cameron F. e MONTJOYE, Alexandre de. Enabling Humanitarian use of Mobile Phone Data. *Technology* Innovation, Novembro de 2014. Disponível em: <http://www.brookings.edu/~/media/research/files/papers/2014/11/12-enablinghumanitarian-mobile-phone-data/brookingstechmobilephonedataweb.pdf.

MCDONALD, Sean Martin. Ebola: A Big Data Disaster - Privacy, Property, and the Law of Disaster Experimentation. CIS Papers 2016.1.

NIELES, Michael, DEMPSEY, Kelley L., PILLITTERI, Victoria Y. An Introduction to Information Security. Special Publication (NIST SP). Disponível em: https://www.nist.gov/publications/inoduction-information-security.

PEREIRA, Jane Reis Gonçalves. *Interpretação Constitucional e Direitos Fundamentais*. Saraiva: São Paulo, 2018.

SILVA, Virgílio Afonso da. Princípios e regras: mitos e equívocos acerca de uma distinção. *Revista Lationamericana de Estudos Constitucionais*. v. 1, 2003.

SUNDFELD, Carlos Ari. Motivação do ato administrativo como garantia dos administrados. *Revista de direito público*, nº 75, 1985.

TSCHORSCH, Florian, VON VOIGT, Saskia Nuñez. RRTxFM: Probabilistic Counting for Differentially Private Statistics. Disponível em: https://eprint.iacr.org/2019/805.pdf

UBINSTEIN, Ira S. e HARTZOG, Woodrow. Anonymization and Risk. *New York University Public Law and Legal Theory Working Papers 530*, 2015.

WEBER, Griffin M. YU, Yun William. HyperMinHash: MinHash in LogLog space. Journal of Latex Class Files, Vol. 14, no. 8, August 2015. Disponível em: https://arxiv.org/pdf/1710.08436.pdf

ZETTER, Kim. Anonymized Phone Location Data Not So Anonymous, Researchers Find. 2013. Disponível em: https://www.wired.com/2013/03/anonymous-phone-location-data/.