inloco

Meios de Controle à Pandemia da COVID-19 e a Inviolabilidade da Privacidade

Por Raíssa Moura com a colaboração de Lara Ferraz[1]

Sumário

[1] Raíssa Moura é Head of Data Privacy e Lara Ferraz é Data Privacy Intern na In Loco.

O controle à Pandemia da COVID-19

O surgimento de uma pandemia, como a que estamos vivendo com a COVID-19, doença infecciosa causada pelo novo coronavírus, tem o potencial de transformar o mundo que conhecemos em um curto período de tempo.

O distanciamento social é o modelo de controle de infecção recomendado pela OMS[2] e adotado por muitos países até o presente momento. Com esse modelo, pesquisadores e órgãos de saúde acreditam ser possível controlar a velocidade de disseminação do vírus, a fim de manter o número de enfermos sempre menor do que a capacidade do sistema de saúde de cada país.

Na prática, é muito difícil garantir que toda a população - exceto pessoas que exercem serviços essenciais - permanecerá em casa durante o tempo necessário e, entre tantos desafios urgentes, é de suma importância que as autoridades públicas tenham uma forma eficaz de se comunicar com a população, enviar alertas e informações educativas, controlar aglomerações e até mesmo permitir que especialistas, órgãos de pesquisas e epidemiologistas possam entender o fluxo de deslocamento de pessoas, visitas a estabelecimentos e locais públicos, percentagem de pessoas em quarentena e monitoramento da efetividade de medidas como o isolamento social, por exemplo.

O uso tecnologias de geolocalização como medida de controle ao COVID-19

As tecnologias de geolocalização embarcadas em *smartphones* estão sendo utilizadas por países do mundo todo para assegurar a proteção das pessoas e evitar a propagação do vírus, conforme exemplificaremos abaixo[3].

A **Coreia do Sul** está rastreando telefones de indivíduos e criando um mapa publicamente disponível para permitir que outros cidadãos verifiquem se podem ter cruzado com pacientes

[2] Disponível em: https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public. Acessado em 23/03/20.
[3] Disponível em: https://www.businessinsider.com/countries-tracking-citizens-phones-coronavirus-2020-3#the-uk-isnt-tracking-yet-but-is-considering-it-11. Acessado em 24/03/20.

contaminados pelo coronavírus. Os dados de rastreamento que entram no mapa não se limitam aos dados de telefones celulares; registros de cartão de crédito e até mesmo entrevistas pessoais com pacientes estão sendo usados para criar um mapa retroativo de onde eles estiveram. Não apenas o mapa está lá para os cidadãos verificarem, mas o governo sul-coreano está usando-o para enviar proativamente mensagens de texto regionais, alertando as pessoas de que podem ter entrado em contato com alguém portador do vírus.

O governo do **Irã** criou um aplicativo de diagnóstico do coronavírus que coletava dados de localização em tempo real dos usuários. Em 3 de março, uma mensagem foi enviada a milhões de cidadãos iranianos pedindo para instalar o aplicativo, chamado AC19, antes de ir para um hospital ou centro de saúde. O aplicativo foi muito criticado e, recentemente, removido da loja do Google Play.

O Primeiro Ministro de **Israel,** Benjamin Netanyahu, aprovou uma série de medidas de vigilância da população, e, com isso, a Agência de Segurança de Israel passou a rastrear os telefones dos cidadãos israelenses. Em discurso para a nação, Netanyahu afirmou: “Implementaremos medidas que anteriormente implementamos contra terroristas. Algumas delas serão invasivas e violarão a privacidade das pessoas afetadas”.

Taiwan criou uma tecnologia chamada de "cerca eletrônica", que rastreia dados de telefones celulares e alerta as autoridades quando alguém que deveria ficar em quarentena está saindo de casa. "O objetivo é impedir que as pessoas circulem e espalhem a infecção", disse Jyan Hong-wei, chefe do Departamento de Segurança Cibernética de Taiwan.

A maior operadora de rede de telecomunicações da **Áustria,** a Telekom Austria AG, anunciou, em 17 de março, que estava compartilhando dados de localização anonimizados com o governo. Embora os dados sejam agregados, a medida tem causado muita preocupação pela possibilidade da companhia de telecomunicação reidentificar seus usuários e fornecer ao governo a capacidade de rastrear o movimento de grande parte de seus cidadãos no futuro.

O governo da **Polônia** anunciou, em 20 de março, o lançamento de um novo aplicativo chamado "Quarentena doméstica". O objetivo do aplicativo é garantir que as pessoas que deveriam ficar em quarentena por 14 (catorze) dias fiquem no lugar. Para usar o aplicativo pela primeira vez, os poloneses precisam registrar uma selfie e, em seguida, o aplicativo envia

solicitações periódicas para selfies geolocalizadas. Se o usuário não cumprir dentro de 20 minutos, a polícia é alertada. "As pessoas em quarentena têm uma escolha: receber visitas inesperadas da polícia ou fazer o *download* deste aplicativo", disse um porta-voz do Ministério Digital da Polônia. O governo polonês está gerando automaticamente contas para pacientes com suposta ordem de quarentena, incluindo pessoas que retornam do exterior.

O governo da **Bélgica** aprovou, em 11 de março, a utilização de dados anonimizados de empresas locais de telecomunicações. A **Alemanha** também adotou medida similar, na qual a empresa de telefonia Deutsche Telekom passou a compartilhar dados de deslocamento das pessoas por todo o país, a nível estadual e até comunitário.

A **Itália,** que foi particularmente afetada pela disseminação do coronavírus, também assinou um acordo com as operadoras de telecomunicações para coletar dados de localização anonimizados. Em 18 de março, a Itália havia acusado 40.000 cidadãos de violar suas leis de lockdown, de acordo com o The Guardian[4].

As operadoras de celulares na Europa estão se unindo à Comissão Europeia para compartilhar dados de localização dos usuários. O objetivo, segundo o grupo, é monitorar o avanço do coronavírus no continente, onde estão localizados países com dezenas de milhares de casos confirmados da Covid-19, como Itália, Espanha, Alemanha e França[5].

Outros países como **Estados Unidos, Reino Unido** e **Brasil** estão considerando adoção de medidas similares, conversando com gigantes da tecnologia, startups e empresas de telecomunicação para estudar a viabilidade do uso de geolicação no combate à COVID-19.

Meios de controle à COVID-19 e o Direito à Privacidade

Os esforços para a utilização de tecnologias capazes de monitorar a população e controlar a disseminação do vírus são legítimos, no entanto, se as medidas de controle que os países vêm

[4]Disponível em: https://www.theguardian.com/world/2020/mar/18/italy-charges-more-than-40000-people-violating-lockdown-coronavirus. Acessado em 23/03/20.

[5] Disponível em: https://tecnoblog.net/331251/operadoras-na-europa-vao-rastrear-localizacao-de-celulares-para-combater-covid-19/. Acessado em: 26/03/20

aplicando não observarem as melhores práticas de proteção de dados pessoais, muitos direitos humanos universais e garantias fundamentais poderão sofrer consequências irremediáveis no presente e, principalmente, no futuro pós-pandêmico que nos aguarda.

A situação é urgente, mas toda medida tomada deve ser proporcional à emergência e causar o menor dano possível a longo prazo. Gideon Lichfield, em seu distópico artigo para o MIT Technology Review, argumenta que, ao fim da pandemia, "a vigilância intrusiva será considerada um pequeno preço a pagar pela liberdade básica de estar com outras pessoas."[6]

Para Lichfield, isso acontecerá porque, em meio à pandemia, Estados estão coletando dados pessoais, como históricos de saúde, condições financeira e de higiene, localizações e outras **informações diretamente associadas aos indivíduos,** visando minimizar os danos da doença. Richfield acredita que, em um futuro próximo, quando a COVID-19, ainda que controlada, continuar sendo uma ameaça, tais políticas de vigilância poderão mudar a forma como nos organizamos em sociedade, minar oportunidades de emprego de pessoas mais vulneráveis e dificultar, ainda mais, a entrada de imigrantes e refugiados em um país ou de ex-presidiários no mercado de trabalho.

O escritor e historiador israelense Yuval Harari, alertou, no dia 20 de março de 2020, em artigo publicado no Financial Times:

> "A humanidade agora está enfrentando uma crise global. Talvez a maior crise da nossa geração. As decisões tomadas pelas pessoas e pelos governos nas próximas semanas provavelmente moldarão o mundo nos próximos anos. Eles moldarão não apenas nossos sistemas de saúde, mas também nossa economia, política e cultura. Devemos agir de forma rápida e decisiva. Também devemos levar em consideração as consequências a longo prazo de nossas ações. Ao escolher entre alternativas, devemos nos perguntar não apenas como superar a ameaça imediata, mas também que tipo de mundo habitaremos quando a tempestade passar. Sim, a tempestade passará, a humanidade sobreviverá, a maioria de nós ainda estará viva - mas habitaremos um mundo diferente"[7].

[6] Disponível em: https://www.technologyreview.com/s/615370/coronavirus-pandemic-social-distancing-18-months/. Acessado em 23/03/20.
[7] Disponível em: https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75. Acessado em 24/03/20.

É evidente que em um estado de calamidade global muitos direitos são relativizados, normas são flexibilizadas e todo o esforço deverá estar concentrado em preservar o máximo de vidas. Entretanto, a "escolha de Sofia" não deve estar centrada no dilema "controle da pandemia x privacidade", sob pena de instituirmos governos autoritários. Mais do que nunca, a discussão sobre privacidade, tão debatida pelo mundo antes da eclosão da pandemia, deve permanecer sob holofotes.

O próprio Harari afirma que, nas últimas semanas, alguns dos esforços mais bem-sucedidos para conter a epidemia do coronavírus foram orquestrados pela Coréia do Sul, Taiwan e Cingapura. Os referidos países fizeram uso de aplicativos de rastreamento, mas confiaram também em testes extensivos, em relatórios honestos e na cooperação voluntária de um público bem informado[8].

É em um momento como esse que a tecnologia deve servir aos seres humanos e, para tanto, devem ser utilizados os recursos desenvolvidos pensando em privacidade por design, ou seja, desde a concepção dos produtos e serviços até sua efetiva entrega, conceito desenvolvido por Ann Cavoukian, especialista em privacidade e proteção de dados e "Information and Privacy Commissioner" da província de Ontário, Canadá, entre os anos de 1997 e 2014.

O *Privacy by Design* é um princípio geral, composto por 7 princípios fundamentais mais específicos, que tem como objetivo antecipar as situações que podem ferir a privacidade das pessoas e evitar que elas aconteçam. Foi adotado em 2010 pela International Assembly of Privacy Commissioners and Data Protection Authorities, difundido no mundo todo, e incorporado tanto pelo regulamento europeu de proteção de dados como pela Lei Geral de Proteção de Dados brasileira. Sob este princípio, é possível desenvolver tecnologias que protegem a privacidade das pessoas de forma preventiva, não corretiva[9].

Portanto, antes de adotar tecnologias de monitoramento da pandemia, é imprescindível que os governos busquem aquelas que cumpram os princípios de *privacy by design* e mantenham os mais elevados padrões de proteção de dados pessoais e segurança da informação. Seria irremediável para a humanidade a adoção de tecnologias intrusivas por natureza ou a

[8] Idem.
[9] Disponível em: https://content.inloco.com.br/hubfs/Privacidade%20-%20eBooks/Ebook-Descomplicando-PrivacyByDesign%2002.pdf?hsLang=pt-br. Acessado em 23/03/20

adaptação de serviços que não foram criados com a finalidade de entender o comportamento das pessoas respeitando a sua privacidade.

O serviços de telecomunicação e muitas empresas gigantes de tecnologia, por exemplo, detém dados cadastrais e de identificação civil de milhões de pessoas no mundo todo, incluindo a sua geolocalização. Portanto qualquer esforço para anonimizar esses dados, técnica utilizada para que o dado perca a possibilidade de associação direta ou indireta a um indivíduo, é reativo e não proativo, podendo cair na armadilha da reidentificação ao cruzá-los com as informações que as próprias empresas detém. É muito difícil garantir a anonimização completa, por isso, os governos que adotaram essas soluções estão sendo alvo de tantas críticas.

Ao mesmo tempo, inúmeros editais públicos estão sendo abertos ao redor do mundo, buscando contratar startups e pesquisadores com ideias e tecnologias capazes de ajudar no combate ao coronavírus, como, por exemplo, a iniciativa do Ministério Público de Pernambuco (MPPE), que por meio de seu Laboratório de Inovação Tecnológica e de Negócios (MPlabs), e a Secretaria Estadual de Saúde de Pernambuco (SES-PE) lançaram, no dia 17 de março, por meio do Porto Digital, o Desafio Covid-19[10], ciclo de inovação aberta no qual a solução da In Loco foi classificada como uma das vencedoras. A iniciativa teve como objetivo o desenvolvimento de soluções tecnológicas para auxiliar na contenção da pandemia no Brasil, que tenham alto impacto e possam ser implementadas em curto prazo. Ou, ainda, o edital expresso do Ministério da Tecnologia da Itália para diagnóstico e monitoramento do coronavírus (SARS-CoV-2), buscando a contratação de tecnologias para produção de máscaras/respiradores, kits de diagnóstico e ferramentas de geolocalização[11].

De fato, o modelo de negócio das startups é baseado na busca de solução para problemas do mundo e, em geral, essas empresas são capazes de se mover de forma muito rápida, utilizando metodologias ágeis para desenvolver tecnologias proprietárias inovadoras que consigam amenizar a maior crise global das últimas décadas. Não há dúvidas que os governos estão no caminho certo ao buscar essas iniciativas, contudo, precisam estar atentos, uma vez que, mesmo diante do interesse público, os princípios que regem os regulamentos e leis de

[10] Disponível em: https://desafiocovid19.mppe.mp.br/resultado. Acessado em 27/03/20.
[11] Disponível em: https://innovaperlitalia.agid.gov.it/#/call-for-action. Acessado em 24/03/20.

proteção de dados, como a transparência com o titular do dado, a minimização dos dados, confidencialidade, limitação da finalidade e segurança dos dados, por exemplo, devem ser aplicados e respeitados.

No combate ao inimigo invisível que parou o mundo e está mudando completamente muitas das nossas estruturas sociais, precisamos fortalecer os direitos fundamentais para que, ao final da crise, em nome de um interesse que atualmente é legítimo, governos e corporações não excedam seu poder de vigilância e controle sobre a vida das pessoas, colocando em risco tudo que construímos em termos de garantias individuais, como o direito das pessoas expressarem livremente sua opinião e personalidade, não serem discriminadas, não serem manipuladas, controlar a própria reputação e terem segundas chances.

Privacidade não é um tema novo. George Orwell e Aldous Huxley, por exemplo, publicaram obras na primeira metade do século passado sobre a perda da privacidade e a manipulação feita por entes dotados de controle sobre as informações pessoais da sociedade, e antes deles, a Harvard Law Review publicou o emblemático artigo "*The Right to Privacy*", em 1890. Nos últimos tempos, os debates sobre o exercício do direito à privacidade se intensificaram de maneira exponencial com o uso de tecnologias disruptivas e as frequentes notícias de vazamentos ou usos indevidos de dados pessoais[12].

"Mas se eu não tenho nada a esconder, por que devo preservar minha privacidade?" costuma ser o questionamento mais recorrente. Essa será, sem dúvida, a razão pela qual milhões de pessoas no mundo todo vão compartilhar seus dados pessoais em nome da preservação da sua saúde, sem questionar se as empresas que estão coletando esses dados respeitam diretrizes mínimas de proteção de dados e segurança da informação ou o que poderão fazer com esses dados.

É muito perigoso que uma parte seleta da sociedade tenha o poder de controlar todas as outras pessoas. A violação da privacidade por meio do controle de informações pessoais de

[12] Disponível em: https://content.inloco.com.br/hubfs/Estudos%20-%20Conte%C3%BAdo/Privacidade/5-razoes-PT.pdf?hsLang=pt-br. Acessado em 24/03/20.

forma não autorizada e não transparente pode ser um desses instrumentos de controle, capaz de manipular pensamentos, atitudes e decisões[13].

Harari argumenta: "Pedir às pessoas que escolham entre privacidade e saúde é, de fato, a própria raiz do problema. Porque esta é uma escolha falsa. Podemos e devemos desfrutar de privacidade e saúde"[14].

A In Loco pode ajudar no combate ao COVID-19 com respeito à privacidade

É possível utilizar a tecnologia como aliada no combate ao coronavírus sem a necessidade de uma política de vigilância e violação da privacidade por parte de qualquer instituição pública ou privada. Por isso, a In Loco decidiu disponibilizar sua tecnologia, desenvolvida pensando em privacidade desde a concepção, para desenvolver algumas soluções que podem ser utilizadas por prefeituras, governos, secretárias de saúde, universidades e quaisquer outros interessados que queiram se aliar a nós no combate à pandemia.

Até então, temos funcionalidades capazes de implementar os seguintes projetos:

- **Integração do nosso módulo de software (Software Development Kit; "SDK") a aplicativos do poder público**

  Oferecemos a integração da nossa tecnologia a aplicativos do poder público, a fim de coletar dados sem identificação do usuário, que poderão auxiliar instituições para (i) **gerar métricas de isolamento social por bairro**; (ii) **monitorar áreas de risco**; (iii) **estabelecer uma comunicação direta com a população**, para enviar notificações informativas e educativas sobre o distanciamento social, isolamento social e quarentena, e sobre a suspensão das atividades de estabelecimentos.

- **Análise de visitas a hospitais, postos de saúde e serviços essenciais**

[13] Idem.
[14] https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

Excepcionalmente, no combate à COVID-19, utilizaremos um conjunto probabilístico (HyperLogLog) para fazer contagens de visitas com maior precisão, com o objetivo de analisar a capacidade de hospitais e postos de saúde, a fim de evitar superlotação e possibilitar que órgãos responsáveis aloquem profissionais de saúde e pacientes ede forma distribuída e inteligente. Estes dados serão armazenados separadamente e eliminados ao fim da crise da COVID-19. Além disso, coletaremos visitas a locais que oferecem serviços essenciais, como farmácias e supermercados, para evitar aglomeração e distribuir consumidores.

- **Índice de deslocamento de pessoas por bairro/estado**

  Enviaremos, ao órgão interessado, dados anonimizados, estatísticos e cartográficos para verificar o índice de deslocamento por bairro ou por estado. Não haverá qualquer análise individualizada, apenas um índice com o percentual dos bairros/estados que tiveram maior ou menor deslocamento de pessoas, para mapear focos de aglomeração, áreas de risco e a efetividade das medidas de distanciamento e isolamento social. A ação já foi iniciada com a Prefeitura da Cidade do Recife e está em andamento com outros municípios e governos estaduais.

- **Índice de isolamento por residência (agrupado por bairro)**

  Enviaremos, ao órgão interessado, dados anonimizados, estatísticos e cartográficos para verificar o índice de isolamento por bairro ou por estado. Não haverá qualquer compartilhamento individualizado, apenas um índice com o percentual dos bairros/estados que tiveram maior ou menor isolamento de pessoas em região próxima a suas residências estatisticamente inferidas, para mapear a efetividade das medidas de distanciamento e isolamento social.

- **Índice de isolamento e propagação de pessoas para fins de pesquisa**

  Fornecemos, a pesquisadores interessados, análises de isolamento por bairro, movimentação por Estado e propagação de pessoas a partir de determinada localização (um aeroporto, por exemplo), de forma agregada e não individualizada. A

ação foi realizada para pesquisa e produção de artigo científico junto a professores da Universidade de São Paulo, em processo de revisão para publicação.

- **Estudo de propagação de visitas**

  Mapearemos o impacto de um grupo de pessoas-chave (frequentadores do Aeroporto Internacional de Guarulhos em um dia, por exemplo) por meio de uma "propagação de visitas". Esta iniciativa própria da In Loco funcionará como uma simulação de infecções, em que será considerado que pessoas (não identificadas) que visitaram lugares próximos em um determinado período de tempo estiveram em contato, podendo ocorrer propagação da infecção por coronavírus, caso alguma já estivesse contaminada. No entanto, as informações utilizadas neste estudo serão anonimizadas a partir da degradação da localização, em que coordenadas exatas são substituídas por aproximadas, restando apenas as informações de contato entre pessoas, sem identificá-las diretamente ou localizá-las com precisão.

- **Análise de visita a estabelecimentos**

  Mapearemos locais de serviços não essenciais que não estejam cumprindo as recomendações de suspensão das atividades, como shoppings, restaurantes e casas de show, por meio de uma análise de fluxo de visitas a estes estabelecimentos com atualização diária, em que será computado apenas o movimento nestes locais, de forma agregada ou não individualizada.

- **Mapeamento de focos de aglomeração**

  Mapearemos focos de aglomeração de pessoas (hotspots) através de uma análise de visitas que considera "aglomeração" um grande número de dispositivos no mesmo local e instante, sem identificação direta de indivíduos.

Com o dever de prestar contas à sociedade, é importante esclarecer que a tecnologia da In Loco respeita o artigo 5º da Constituição Federal, o artigo 21 do Código Civil, os artigos 4º, caput e inciso IV, 6º, inciso III do Código de Defesa do Consumidor e o artigo 7º, inciso IX, do Marco Civil da Internet, bem como o artigo 12 da Declaração Universal dos Direitos Humanos.

Em recente decisão de promoção de arquivamento de inquérito civil público movido pela Unidade Especial de Proteção de Dados e Inteligência Artificial - ESPEC do Ministério Público do Distrito Federal e Territórios, o Promotor de Justiça Frederico Meinberg Ceroy concluiu que "o modelo de negócio da empresa In Loco é legal, em face do arcabouço normativo existente atualmente, afinal não ocorre a coleta de dados que permita a vinculação direta ao titular dos dados pessoais. Diferente do serviço Vivo Ads, da empresa Telefônica, que detém os dados cadastrais e geolocalização dos titulares dos dados pessoais, a In Loco, em tese, não consegue relacionar as informações de geolocalização com pessoa natural identificada ou identificável."[15].

A In Loco criou sua tecnologia de modo a impedir o acesso a informações que de alguma forma permitissem fazer o rastreamento individualizado e identificado dos usuários, mesmo com o seu consentimento. Assim, a In Loco não acessa os identificadores estáticos e únicos dos dispositivos (IMEI e MAC) nem contas associadas ao dispositivo (e-mail e telefone). Esse foi um dos primeiros e mais importantes passos para criar a In Loco, que tem como um dos principais objetivos estar à frente do seu tempo em questões relativas à privacidade.

Ao ser *privacy by design*[16], a In Loco não coleta, acessa, armazena ou trata - de qualquer outra forma - dados pessoais de identificação civil, como nome, RG, CPF. A empresa também não cruza ou agrega os dados coletados com qualquer outra base externa, e utiliza todos os meios adequados para manter os dados que coleta de forma anônima.

O compromisso de não coletar informações que possam identificar diretamente uma pessoa nem cruzar os dados coletados com bases externas se mantém, neste momento, tão crucial para a humanidade, posto que o combate ao coronavírus se faz imperioso, ao mesmo tempo que não devemos, em hipótese alguma, relativizar o direito à privacidade e proteção dos dados pessoais.

---

[15] Disponível em: https://porta23.blogosfera.uol.com.br/2020/02/21/mp-arquiva-inquerito-contra-a-startup-inloco-por-coleta-indevida-de-dados/. Acessado em: 23/03/20.

[16] Disponível em : https://content.inloco.com.br/hubfs/Privacidade%20-%20eBooks/Ebook-Descomplicando-PrivacyByDesign%2002.pdf?hsLang=pt-br. Acessado em: 23/03/20

A preocupação em garantir o anonimato dos consumidores está presente desde a origem da empresa, quando os fundadores partiram da pergunta inicial de como a solução poderia aumentar a privacidade de algum segmento que já adotasse boas práticas, ou de como a In Loco poderia criar soluções voltadas à proteção de dados em mercados que, de diversas formas, vão na contramão dessa busca por privacidade. Na In Loco, privacidade é um valor desde o primeiro dia da empresa.

Ter a privacidade como um dos valores da cultura organizacional garante que todos os produtos e soluções da empresa sejam rigorosamente concebidos com foco na privacidade dos titulares de dados. Afinal, na In Loco, a cultura é o *framework* de tomada de decisão, o que permite assegurar que todos estejam alinhados com a visão da empresa e também que a empresa negue toda e qualquer proposta que contrarie sua missão focada em privacidade[17].

Reforçando o compromisso público de respeito à privacidade assumido pela In Loco com a sociedade, desde a sua fundação, há 10 (dez) anos, elencamos abaixo os principais esclarecimentos sobre o tratamento dos dados que poderão ser coletados pela In Loco no controle à pandemia da COVID-19:

a. **Como os dados serão coletados**

A In Loco disponibiliza a seus parceiros e clientes um módulo de software chamado Software Development Kit (SDK), o qual é integrado aos aplicativos que estes parceiros e clientes desenvolvem, sendo que no combate à pandemia da COVID-19, poderá ser integrado também a aplicativos de prefeituras, governos e órgãos públicos.

Indivíduos interessados nas aplicações desenvolvidas por estes parceiros e clientes, por sua vez, instalam voluntariamente estes aplicativos em seus dispositivos móveis. Uma vez instalado o aplicativo e as permissões necessárias serem dadas pelo usuário, o SDK detecta quando o dispositivo móvel permanece por períodos prolongados em determinada localidade e envia os dados de geolocalização para os servidores da In Loco. Os dados são armazenados após aplicação de hash com segredo e criptografia. Não há coleta de dados que permita vinculação direta da geolocalização à identidade de um indivíduo usuário do aplicativo.

[17] Disponível em: https://www.inloco.com.br/pt/about. Acessado em 25/03/20.

Tais dados são, então, agrupados em clusters[18], sem qualquer indicação direta da identidade dos usuários. Todos estes aplicativos são obrigados contratualmente a apresentar a Política de Privacidade da In Loco em seus respectivos Termos de Uso e/ou Políticas de Privacidade e solicitar o consentimento dos seus usuários para o tratamento de dados pela In Loco.

Para fins da colaboração com o controle da pandemia, a In Loco está utilizando as mais avançadas técnicas de anonimização para compartilhar os dados com o poder público, sem identificação direta ou indireta dos titulares de dados.

Embora a LGPD não esteja em vigor, a In Loco respeita todos os seus princípios. Assim, caso os aplicativos não atendam o princípio da transparência, previsto no artigo 6º, IV, da LGPG, que consiste na garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, a In Loco reserva-se ao direito de desinstalar o seu SDK e descontinuar a parceria com o órgão público responsável.

b. **Como os dados serão armazenados**

Os dados serão armazenados em "*object storage"* ou base de armazenamento de objetos (*Simple Storage Service*, ou S3) hospedadas em ambientes tecnológicos **geridos única e exclusivamente pela In Loco** por meio de uso de plataforma de nuvem pública fornecida pela *Amazon Web Services* (AWS).

O armazenamento em nuvem (*cloud computing*) é o padrão da indústria, pois simplifica a operação da tecnologia, gera escalabilidade e aumenta o nível de segurança de todos os serviços que o utilizam. A AWS adere a padrões, regulamentações e certificações internacionais de segurança da informação[19], como por exemplo ISO 27001, ISO 27017, ISO 27018, ISO 9001, SOC 1/ISAE 3402, SOC 2, SOC 3, FISMA, DIACAP, FedRAMP, PCI DSS Level 1 e Cloud Security Alliance.

[18]"Clusterização de dados" ou "análise de agrupamentos" é uma técnica de mineração de dados que agrupa automaticamente os dados de uma base em clusters ou agrupamentos não previamente definidos. Distingue-se, portanto, da "classificação", técnica de mineração de dados com classes predefinidas de agrupamento e, sobretudo, com uma dinâmica de perfilhamento individualizada.

[19] Disponível em: https://aws.amazon.com/compliance/programs/. Acesso em: 31.10.2019.

c. Como os dados serão utilizados

A tabela a seguir representa o máximo de dados que podem ser coletados de determinado dispositivo nas condições técnicas atuais. Nem todos os aplicativos que utilizarem a tecnologia da In Loco coletarão todos esses dados. A lista é fornecida de forma completa para maior transparência aos usuários dos aplicativos que usarem nossas tecnologias.

Tipo de dado	Descrição	Finalidades
Localização	GPS Sinais de Wi-Fi Sinais de Bluetooth-LE Sinais de telefonia Atividade (correndo, andando, dirigindo)[20]	Envio de notificação push com campanhas educativas para reforçar a comunicação com a população, enviando alertas e informações educativas sobre o distanciamento social, áreas de risco e a suspensão de atividades de estabelecimentos.
		Índice de deslocamento de determinada região. Ex: Fornecer informações sobre como a população está respondendo às recomendações para permanência em casa.
		Identificação de áreas de risco. Ex: Possibilitar a órgãos responsáveis enviem alerta de proximidade a locais de risco
		Contagem de visitas anonimizadas a hospitais, clínicas e postos de saúde. Ex: Possibilitar que órgãos responsáveis aloquem de forma inteligente pacientes e profissionais de saúde, evitando superlotação.
Performance	Cliques Visualizações	Métricas de performance de uma notificação. Ex: Quantos visualizações/ cliques teve uma notificação?
Identificador	Identificadores de mídia[21] (armazenados após aplicação de hash com segredo e criptografia).	Segmentação e contagem de usuários únicos. Ex.: Quantos usuários visualizaram notificação A? Quantos usuários únicos visitaram local B?
Dispositivo	Modelo dos aparelhos Sistema operacional Versão do SO Métricas de performance do SDK IP (sendo os últimos 4 dígitos ignorados para remover precisão) Tipo de rede (3G, 4G, Wi-Fi) Provedor de rede Resolução da tela	Depuração e monitoramento do nosso SDK com intuito de melhorá-lo e consumir menos recurso (CPU, memória, rede, bateria, etc.). Ex.: Quanto recurso nosso SDK está consumindo? A funcionalidade X está funcionando como deveria?
		Segmentação para excluir informações de regiões que não serão analisadas
		Otimização de recursos de rede. Ex.: Para um aparelho com resolução mais baixa ou pior qualidade de rede, podemos enviar anúncios mais leves.
		Pesquisas estatísticas. Ex.: Como usuários de app X estão distribuídos no país? Que tipo de estabelecimentos eles continuam frequentando durante as medidas de isolamento social e quarentena?

[20] O Google Play Services fornece para os dispositivos Android uma forma de consultar este dado diretamente pelo sistema operacional chamada de activity recognition.

[21] Disponível em: https://inloco.com.br/pt/privacy-policy#section9. Acesso em: 31.10.2019.

	Apps instalados	
Dados de Apps	Sessão de apps (quando o app é aberto e quanto tempo ele passa aberto) Eventos definidos pelos desenvolvedores dos apps (uso de determinadas funcionalidades)	Bloquear coleta de dados de menores de idade (<18 anos).
		Inteligência sobre o uso dos apps e avaliação das comunicações através de notificações push no uso de determinadas funcionalidades.
		Inteligência sobre o uso dos apps e avaliação das comunicações através de notificações push na recorrência de uso do aplicativo. Ex.: Locais nos quais os usuários mais usam o app; tempo gasto no aplicativo.

d. **Compartilhamento de dados**

Como regra geral, a In Loco não compartilhará os dados pessoais dos usuários com as autoridades públicas, **apenas dados anonimizados.** Dessa forma, as autoridades públicas que utilizarem a tecnologia da In Loco no combate à COVID-19 não terão acesso a históricos de visitas individualizados ou a qualquer dado que possa identificar uma pessoa física direta ou indiretamente. O monitoramento será realizado de maneira agregada, por cidades e bairros, com dados anônimos, ou seja, não haverá compartilhamento de qualquer dado individualizado.

e. **Retenção de dados**

Os dados pessoais dos usuários serão armazenados enquanto durarem as medidas de quarentena e isolamento social decorrentes da pandemia ou o estado de calamidade pública decretado. Em hipótese alguma a In Loco utilizará as informações coletadas durante este período para qualquer finalidade que não seja o combate à COVID-19, nem agregará ao seu banco de dados para outras finalidades de negócio. Os contratos celebrados com os órgãos públicos terão duração de 02 (dois) meses, podendo ser prorrogados por igual período. Após o fim do estado de calamidade pública, a In Loco realizará a eliminação segura dos dados.

A In Loco também poderá reter dados anonimizados (que não são capazes de identificar o titular nem direta, nem indiretamente) para realizar análises estatísticas, por tempo indeterminado.

f. **Segurança de dados**

Aplica-se técnica avançada de pseudonimização do *Advertising* ID (identificador de publicidade) dos usuários, sendo que o dado original é removido da base e substituído por dados criptografados e hasheados, como descrito na Política de Privacidade da In Loco[22], que terá uma versão atualizada para as ações de combate à pandemia antes da integração do SDK nos aplicativos dos governos e órgãos públicos.

Esses dois identificadores (*hashed ID* e o ID encriptado) são suficientes para suprir os serviços da In Loco e não permitem a identificação direta dos titulares dos dados. Eles também reduzem, ou até mesmo eliminam, o risco de o *Mobile Advertising ID* ser capaz de identificar qualquer titular de dados no caso de eventual acesso indevido a esses dados ou cruzamento com base de dados de terceiros que contenha o mesmo ID atrelado a outros dados pessoais, como CPF, e-mail, dentre outros.

Assim, na hipótese de qualquer acesso não autorizado ao *hashed ID* e ao ID encriptado, não será possível o terceiro associar diretamente qualquer titular a tais dados, evitando riscos de danos aos usuários titulares e também aplica técnicas de assinatura criptográfica, que permitem a detecção de quaisquer alterações realizadas nos dados que compõem a sua base.

A In Loco tem uma equipe de pesquisa e desenvolvimento estudando e prototipando técnicas de pseudonimização e anonimização com destaque para agregações, privacidade diferencial, criptografia homomórfica, private data join e k-anonymity.

g. **Sensibilidade dos dados**

Embora a LGPD não esteja em vigor, observamos que artigo 5º, inciso II, da LGPD cita os seguintes dados como sendo pessoais sensíveis: dados sobre “origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado[s] referente[s] à saúde ou à vida sexual, dado[s] genético[s] ou biométrico[s], quando vinculado[s] a uma pessoa natural”.

[22] Disponível em: https://www.inloco.com.br/pt/privacy-policy.. Acessado em 26/03/20.

Dada esta definição, a In Loco não trata de nenhuma forma, dados pessoais sensíveis dos usuários. A In Loco ainda bloqueia o armazenamento e outros tratamentos dos dados de visita quando associados a qualquer tipo de identificador pessoal das seguintes categorias de locais: hospitais, clínicas, consultórios odontológicos, laboratórios médicos, cemitérios, mortuárias, creches, sedes de partidos políticos, locais relacionados a religiões (templos religiosos, igrejas, mesquitas, dentre outros), penitenciárias, estabelecimentos relacionados a atividades sexuais. Por último, aplicativos relacionados a qualquer dado sensível não estão em nossa base e são automaticamente bloqueados, conforme destacado no Código de Ética da In Loco[23]. Não se conhece outras tecnologias que tratam dados de localização que façam esse tipo de bloqueio, demonstrando a postura inovadora e proativa da In Loco com relação à proteção da privacidade.

Contudo, diante da pandemia do coronavírus e o compromisso da In Loco em servir à população com sua tecnologia de localização proprietária, a In Loco poderá coletar informações de visitas a hospitais e postos de saúde, utilizando-se de máxima transparência com o titular e apenas com o seu consentimento livre, expresso, informado, conforme disposição do art. 7º, VII, do Marco Civil da Internet[24],[25] e sem conhecer a identidade do titular do dado.

Nesse caso, utilizaremos um conjunto probabilístico (HyperLogLog) para fazer contagens de visitas com maior precisão, com o objetivo de analisar a capacidade de hospitais e postos de saúde, a fim de evitar superlotação e possibilitar que órgãos responsáveis aloquem profissionais de saúde e pacientes de forma distribuída e inteligente. Estes dados serão armazenados separadamente e eliminados ao fim da crise da COVID-19.

[23] Disponível em: https://www.inloco.com.br/pt/code-of-ethics. Acessado em: 25.03.20.
[24] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acessado em 25.03.20.
[25] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acessado em: 25.03.20.

h. Controle dos indivíduos sobre seus dados

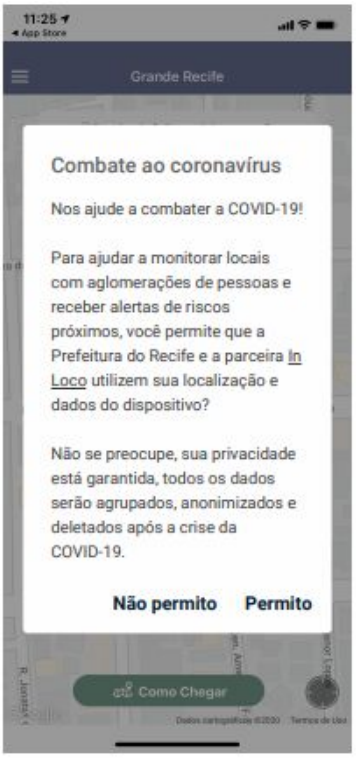
Atualmente, existem três mecanismos que permitem aos indivíduos o controle sobre seus dados. São eles:

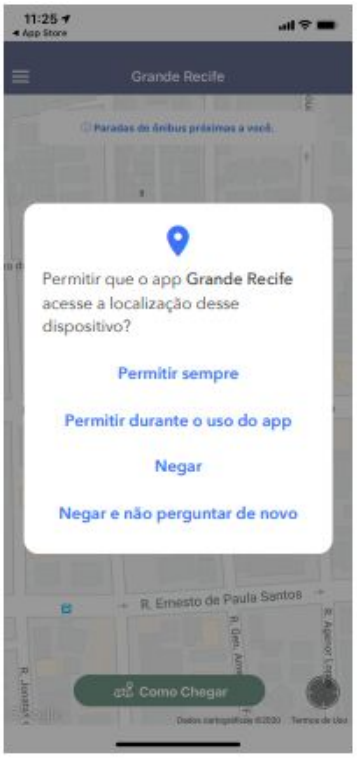
Consentimento

Atualmente, existe uma exigência contratual para que os aplicativos parceiros façam referência expressa ao uso da tecnologia da In Loco e também para que mencionem e ofereçam um link para a Política de Privacidade da In Loco, solicitando o consentimento dos seus usuários.

A coleta do consentimento é de responsabilidade dos aplicativos parceiros, e a In Loco monitora automaticamente, através de um crawler (software que rastreia e analisa conteúdo de websites), se os termos de uso ou políticas de privacidade dos aplicativos parceiros de fato mencionam a In Loco e sua política de privacidade. Além disso, a In Loco disponibiliza aos aplicativos a funcionalidade de consentimento inequívoco durante a jornada do usuário no aplicativo. É uma medida que extrapola a exigência legal de "cláusulas contratuais destacadas", conforme exemplo abaixo[26]:

[26] As finalidades apresentadas neste consentimento são meramente exemplificativas. Cada aplicativo tem um texto adaptado de acordo com a finalidade pela qual os dados estão sendo coletados.





E como parte deste esforço de transparência, a In Loco está lançando também um **aplicativo para comunicação direta com os usuários.**

Mudança na configuração de permissões no dispositivo móvel

Por padrão, os sistemas operacionais dos dispositivos móveis (Android[27] e iOS[28]) proveem mecanismos para ativar ou desativar o acesso das aplicações aos serviços de localização. Portanto, mesmo que o usuário de aplicativo tenha dado o consentimento explícito, ele ainda pode escolher desativar essa funcionalidade numa granularidade por aplicação.

Além disso, o usuário pode optar por desligar os serviços de localização do dispositivo móvel, o que também encerraria a coleta de dados de localização de todas as aplicações que

[27] Disponível em: https://support.google.com/accounts/answer/3467281?hl=pt-BR. Acesso em: 06.11.2019.

[28] Disponível em: https://support.apple.com/pt-br/HT207092. Acesso em: 06.11.2019.

porventura façam uso dessa funcionalidade, sejam elas provenientes de parceiros e clientes da In Loco ou não.

Oposição

A In Loco disponibiliza, em seu website institucional, um link para requisição de "opt-out"[29], com instruções claras para usuários das plataformas para as quais a In Loco disponibiliza seu SDK. Quando o usuário exercita seu direito de "opt-out", a In Loco interrompe a coleta de novos dados deste usuário. O titular do dado também pode entrar em contato com a In Loco através do e-mail dpo@inloco.com.br, disponível em nossa política de privacidade[30].

i. Questões de interesse público e de toda sociedade

A Constituição Federal determina em seu art. 196 que a saúde é direito de todos e dever do Estado e deve ser garantido mediante políticas sociais e econômicas que visem à redução do risco de doença e de outros agravos e ao acesso universal e igualitário às ações e serviços para sua promoção, proteção e recuperação.

Portanto, principal questão atual de interesse público no Brasil é a preservação do direito à saúde concretizado na criação de políticas públicas para o combate à pandemia ocasionada pelo coronavírus, que provocou a decretação do estado de calamidade pública aprovado pelo Congresso Nacional. Além do mais, é dever do Estado preservar a dignidade da pessoa humana e a inviolabilidade da privacidade[31] frente às novas tecnologias.

A iniciativa da In Loco vai contribuir com medidas mais acertadas pelo Poder Público, que poderá tomar decisões com base em dados estatísticos, evitando a disseminação do vírus, bem como a reavaliação das medidas de isolamento social adotadas ao mesmo tempo que preserva a privacidade das pessoas.

[29] Disponível em: https://inloco.com.br/pt/opt-out. Acessado em: 26.03.20.

[30] Disponível em: https://www.inloco.com.br/pt/privacy-policy. Acessado em: 26.03.20

[31] O direito à privacidade, estabelecido pelo artigo 12 da Declaração Universal de Direitos Humanos de 1948, constitui-se, também, como direito fundamental pelo artigo 5º, inciso X, da Constituição Federal.

Estatísticas públicas, cumprem papel fundamental no dimensionamento de questões sociais latentes na sociedade que, vocalizadas adequadamente, podem entrar na agenda prioritária de governo e têm sido fundamentais na formulação de políticas públicas nos três níveis de governo, ao permitirem a elaboração de diagnósticos socioeconômicos com abrangência temática, detalhe territorial e comparabilidade histórica[32].

Para o Regulamento Geral de Proteção de Dados europeu (GDPR), normativa mais especializada no tema, tal processamento de dados é legítimo e lícito, conforme demonstra o item 46 do seu preâmbulo:

> (...) Alguns tipos de tratamento podem servir tanto importantes interesses públicos como interesses vitais do titular dos dados, por exemplo, se o tratamento for necessário para fins humanitários, incluindo a monitorização de epidemias e da sua propagação ou em situações de emergência humanitária, em especial em situações de catástrofes naturais e de origem humana. (Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho)

Mas esse interesse não é apenas do nosso país, uma vez que a pandemia atinge escalas globais. Segundo o *European Data Protection Board*[33] *(EDPB)* **"a luta contra doenças transmissíveis é uma meta valiosa compartilhada por todas as nações e, portanto, deve ser suportada da melhor maneira possível. É do interesse da humanidade coibir a disseminação de doenças e usar técnicas modernas na luta contra os flagelos que afetam grande parte do mundo".** Portanto, as regras de proteção de dados não impedem as medidas tomadas na luta contra o pandemia do COVID-19, mas devem ser observadas com cuidado.

É importante atentar para as disposições que o *EDPB* criou proativamente para responder às dúvidas quanto a utilização de dados de localização no combate a COVID-19, conforme colacionado abaixo:

---

[32] : Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-30982018000100551&lng=en&nrm=iso. Acessado em: 26.03.20.

[33] https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en

> Os governos dos Estados-Membros podem usar dados pessoais relacionados aos telefones celulares nos seus esforços para monitorar, conter ou mitigar a disseminação da COVID-19?
> Em alguns Estados-Membros, os governos consideram o uso de dados de localização de dispositivos móveis como uma maneira possível de monitorar, conter ou mitigar a disseminação da COVID-19. Isso implicaria, por exemplo, a possibilidade de geolocalizar indivíduos ou enviar mensagens de saúde pública a indivíduos em uma área específica por telefone ou mensagem de texto. **As autoridades públicas devem primeiro tentar processar dados de localização de maneira anônima (ou seja, processamento de dados agregados de forma que os indivíduos não possam ser identificados novamente), o que poderia permitir gerar relatórios sobre a concentração de dispositivos móveis em um determinado local ("cartografia")**. As regras de proteção de dados pessoais não se aplicam a dados que foram adequadamente anonimizados. (...) O princípio da proporcionalidade também se aplica. **As soluções menos invasivas devem sempre ser preferidas, levando em consideração o objetivo específico a ser alcançado.** Medidas invasivas, como o "rastreamento" de indivíduos (ou seja, processamento de dados históricos locais não anônimos) podem ser consideradas proporcionais em circunstâncias excepcionais e dependendo das modalidades concretas do processamento. No entanto, deve ser sujeito a um maior escrutínio e salvaguardas para garantir o respeito a princípios de proteção de dados (proporcionalidade da medida em termos de duração e escopo, limitações de retenção de dados e limitação de finalidade). (tradução nossa)

A In Loco adota medidas concretas para a proteção da privacidade dos indivíduos em seu modelo de negócio. Em atendimento ao princípio da necessidade (art. 6º, inciso III, LGPD) e minimização (art. 5, 1, c, do GDPR), coleta apenas os dados mínimos necessários e proporcionais ao cumprimento de suas finalidades, e não coleta nenhum dado que identifique diretamente o indivíduo, como nome, CPF, RG, e-mail, dentre outros. Além disso, utiliza técnicas avançadas de pseudonimização e compartilhará com as autoridades públicas somente dados anonimizados, evitando que os indivíduos sejam identificados. Com isso, possibilita a obtenção segura de dados essenciais ao monitoramento e controle da pandemia, sem precisar associar diretamente esses dados as pessoas.

É importante reforçar que a privacidade é o maior valor da In Loco, que investe continuamente no aperfeiçoamento de processos, controles e medidas, para não somente se manter em conformidade com a legislação vigente, como também com a Lei Geral de Proteção de Dados que tem previsão para entrar em vigor em agosto de 2020.

A In Loco não poderia se furtar do dever de contribuir com o a população num momento tão difícil. Entendemos que a situação é urgente e que só com solidariedade poderemos minimizar danos, salvar vidas e combater esta crise. Por isso, disponibilizamos a instituições interessadas, sem cobrar a licença de software, o uso da nossa tecnologia, além de treinamento remoto e painéis de controle (*dashboards*) para acompanhamento de dados. Somente os custos incorridos com o aumento de processamento de dados em nosso ambiente de armazenamento em nuvem (*cloud computing*) serão repassados a estas instituições. As análises compartilhadas com os órgãos públicos serão agregadas, sem dados individualizados e sem tráfego de dados para a nuvem do governo. Os órgãos públicos terão acesso apenas a um *painel de controle* com visualizações de dados agrupados por cidades e bairros.

A In Loco está trabalhando incansavelmente para abreviar o sofrimento dos brasileiros, contribuir para mitigação, controle e erradicação da pandemia com base em dados seguros, além de garantir que a privacidade das pessoas seja preservada. O Estado Democrático de Direito conquistado pelo Brasil não deverá, em hipótese alguma, ser ameaçado. Durante e ao final desta crise, no que depender dos esforços empregados pela In Loco, nenhum cidadão brasileiro terá os seus direito fundamental à privacidade violado. Possivelmente, o Brasil será o primeiro país a utilizar uma tecnologia *privacy by design* no combate à pandemia.