Rastreamento e monitoramento da COVID: proteção da privacidade e dos dados pessoais na utilização de aplicativos e biometria

23 de abril de 2020

Mensagens principais

- As tecnologias digitais, em particular aplicações móveis e biométricas, estão sendo utilizadas de forma inovadora para melhorar a eficácia das respostas governamentais na linha de frente de combate à COVID-19.
- As informações e tendências resultantes são inestimáveis para os governos que procuram monitorar o surto da COVID-19, alertar comunidades vulneráveis e compreender o impacto de políticas como distanciamento social e confinamento.
- A divulgação de informações pessoais pode permitir que o público identifique mais facilmente possíveis infecções por COVID-19 e acompanhe a propagação ao longo do tempo. No entanto, as soluções digitais atuais para monitoramento e contenção têm implicações variadas para privacidade e proteção de dados.
- Soluções responsáveis e transparentes de preservação da privacidade devem ser implementadas para equilibrar os benefícios e os riscos associados à coleta, processamento e compartilhamento de dados pessoais. Os dados devem ser retidos apenas durante o tempo necessário para servir à finalidade específica para a qual foram coletados.

Os governos estão colaborando com os provedores de serviços de telecomunicações para acessar dados de geolocalização para rastrear movimentos populacionais

Enquanto a COVID-19 continua a tirar vidas e a impactar a economia global, os governos procuram urgentemente ferramentas inovadoras para informar políticas e enfrentar a crise. Soluções digitais baseadas em dados de geolocalização estão surgindo para ajudar as autoridades a monitorar e conter a disseminação do vírus. Algumas são alimentadas por registros de dados de chamadas móveis (*call data records*, CDRs), ou seja, dados produzidos por provedores de serviços de telecomunicações em chamadas telefônicas ou outras operações de telecomunicações, que fornecem informações valiosas sobre os deslocamentos da população. Como as operadoras de rede atendem partes substanciais da população em nações inteiras, os deslocamentos de milhões de pessoas em pequenas escalas espaciais e temporais podem ser medidos em tempo quase real. As informações e tendências resultantes são inestimáveis para os governos que procuram acompanhar o surto da COVID-19, alertar as comunidades vulneráveis e compreender o impacto de políticas como o distanciamento social e o confinamento.

Provedores de telecomunicações em vários países da OCDE começara a compartilhar dados de geolocalização baseados em CDR com os governos em um formato agregado e anônimo. Seguem alguns exemplos:

- O provedor alemão de telecomunicações Deutsche Telekom está fornecendo dados anônimos de "fluxos de movimento" de seus usuários para o Instituto Robert-Koch, um instituto de pesquisa e agência governamental responsável pelo controle e prevenção de doenças.
- O "Plano de Cinco Pontos" adotado pelo Grupo Vodafone para lidar com a COVID-19 contempla fornecimento de grandes conjuntos de dados anônimos (como "mapa de calor", ou *heat map,* agregado e anônimo para a região da Lombardia) para ajudar as autoridades a compreender melhor os movimentos populacionais.
- A Comissão Europeia está atualmente em contato com oito operadoras de telecomunicações europeias para obter dados agregados anônimos de geolocalização móvel, a fim de coordenar medidas de acompanhamento da propagação da COVID-19. Para resolver os problemas de privacidade, os dados serão excluídos quando a crise terminar.

Novos aplicativos móveis para o rastreamento da COVID-19 também estão sendo lançadas

Os aplicativos móveis de aconselhamento em saúde já constituem uma parte importante do ecossistema de saúde móvel e provaram ser eficazes para fins de prevenção, diagnóstico precoce (verificação de sintomas, por exemplo) e para conectar usuários a serviços de saúde locais e unidades de emergência.

Novos aplicativos voltados para o consumidor estão surgindo agora para rastrear a COVID-19. Esses aplicativos estão sendo desenvolvidos, cada vez mais como software de código aberto (open source) e são resultado de parcerias de empresas de tecnologia, universidades, médicos e autoridades públicas, responsáveis pelo seu financiamento, desenvolvimento e implementação. Embora não necessariamente alcancem toda a população (parte da população idosa, por exemplo, pode não ter smartphones ou não ser proficiente no seu uso), nem estejam livres de algumas falhas (quando, por exemplo, não logram distinguir entre pessoas na mesma casa e aquelas em residências vizinhas), esses aplicativos fornecem uma ferramenta para os governos monitorarem e conterem o vírus. Entre os mais citados estão:

- **TraceTogether**: Desenvolvido pela Agência de Tecnologia do Governo de Singapura (GovTech) em colaboração com o Ministério da Saúde, este aplicativo, usando Bluetooth, rastreia indivíduos que foram expostos ao vírus. A informação é usada para identificar usuários que estiveram em contato próximo, baseado na proximidade e a duração dos encontros entre dois usuários. O aplicativo, então, alerta quem tiver tido contato com alguém que testou positivo ou corre alto risco ser portador do coronavírus. Uma vez confirmados o diagnóstico ou a suspeita de infecção, pode-se optar por permitir que o hospital, o Ministério da Saúde e terceiras partes acessem dados no aplicativo para ajudar a identificar contatos próximos. Singapura está considerando transformar em código aberto o protocolo de preservação de privacidade em que se baseia a troca de dados do aplicativo TraceTogether.
- **Pan-European Privacy-Preserving Proximity Tracing:** Mais de 130 cientistas, tecnólogos e especialistas de oito países europeus – incluindo França, Alemanha e Itália – participaram de uma iniciativa sem fins lucrativos que desenvolveu um aplicativo em código aberto que analisa sinais Bluetooth entre telefones celulares para detectar usuários que estão próximos uns dos outros. O aplicativo armazena temporariamente esses dados criptografados localmente e, se os usuários apresentarem resultados positivos para o COVID-19, o aplicativo pode alertar qualquer pessoa que tenha estado perto do indivíduo infectado nos dias anteriores, ao mesmo tempo em que mantém protegidas as identidades dos usuários.
- **Aplicativo de rastreamento da Coréia**: Financiado pelo governo coreano, o aplicativo “Self-quarantine Safety” é usado pelas autoridades públicas designadas para fornecer informações sobre COVID-19, incluindo diretrizes de quarentena, e para evitar possíveis violações de ordens de auto-isolamento. O aplicativo também pode ser usado para autoverificação e para o relato voluntário de contaminação às autoridades de saúde. Os dados coletados não são compartilhados com terceiros.
- **C-19 COVID Symptom Tracker**: O objetivo desse aplicativo, desenvolvido no Reino Unido em uma parceria entre médicos e cientistas do King's College London, uma empresa de ciência de dados em saúde (uma divisão da King's) e o Instituto Nacional de Pesquisa em Saúde dos Hospitais Guy's e St Thomas's, é de retardar o surto de COVID-19 ajudando os pesquisadores a identificar (i) a rapidez com que o vírus se espalha em diferentes áreas, (ii) as áreas de alto risco

no Reino Unido (iii) quem está em maior risco, analisando a correlação entre sintomas e condições de saúde subjacentes. Segundo os pesquisadores, os dados do estudo podem revelar informações essenciais sobre os sintomas e a progressão da infecção em diferentes pessoas. Podem ajudar os pesquisadores a entender, ainda, porque alguns indivíduos desenvolvem sintomas mais graves ou fatais, enquanto outros apresentam apenas sintomas leves devido a COVID-19.

- Adicionalmente, **Apple e Google** lançaram interfaces de programação de aplicativos (application programming interfaces, APIs) para permitir a interoperabilidade entre dispositivos Android e iOS no uso de aplicativos de autoridades de saúde pública. Os usuários poderão baixar esses aplicativos de suas respectivas lojas de aplicativos. As duas empresas também trabalharão juntas para habilitar uma plataforma mais ampla de rastreamento de contatos baseada em Bluetooth, incorporando essa funcionalidade nas plataformas subjacentes. Essa solução permitiria que mais pessoas participassem caso desejassem e poderia melhorar a interação com um ecossistema mais amplo de aplicativos e autoridades de saúde do governo.

Os aplicativos de rastreamento podem incorporar vários graus de privacidade e proteção de dados

O uso de aplicativos de coleta de dados de geolocalização pode permitir o compartilhamento de dados de uma forma que incorpore mecanismos explícitos de proteção de dados e privacidade e que habilite usuários a darem seu consentimento explícito e informado para a coleta e o compartilhamento de seus dados pessoais (supondo que o uso do aplicativo não seja obrigatório). O aplicativo TraceTogether de Singapura, por exemplo, possui várias salvaguardas de privacidade, incluindo o de não coletar ou fazer uso de dados de geolocalização, e o de armazenar os registros de dados de forma criptografada. Para proteger a privacidade de seus usuários, o aplicativo pan-europeu criptografa os dados e torna anônimas as informações pessoais. Além disso, como dois telefones nunca trocam dados diretamente e os codinomes dos utilizadores são alterados frequentemente, é virtualmente impossível revelar a identidade dos usuários.

A variedade de dados pessoais que esses aplicativos coletam, processam e compartilham, no entanto, pode ser muito ampla e de difícil compreensão para os usuários. Em muitos casos, os aplicativos continuam a ser executados em segundo plano, mesmo quando o dispositivo não está em uso. Alguns aplicativos também podem trocar informações com outros aplicativos por meio de APIs, gerando informações mais detalhadas. Embora a Organização Mundial da Saúde (OMS) tenha elogiado as extensas medidas de rastreamento da Coreia, alguns casos de uso dos dados coletados pelo Sistema de Apoio à Investigação Epidemiológica nos movimentos de pessoas com casos confirmados pelas autoridades locais designadas levantaram preocupações sobre a privacidade. Em resposta, o governo coreano publicou recentemente orientações relacionadas à divulgação dos deslocamentos de pessoas com casos confirmados com base na Lei de Controle e Prevenção de Doenças Infecciosas, aprovada em 2015, que veda a divulgação de qualquer informação específica sobre o indivíduo cujos dados são coletados.

A utilização de dados biométricos gera tanto benefícios quanto desafios

O reconhecimento facial tem sido uma das aplicações de tecnologia biométrica mais usadas em diversos países para monitorar a disseminação da COVID-19. O reconhecimento facial permite que as autoridades reduzam o uso de tecnologias de identificação que exigem contato físico (tais como varreduras de íris e impressões digitais). A biometria pode ser associada a outras tecnologias, como imagens térmicas aprimoradas por inteligência artificial, que contribuem para o melhor rastreamento de cidadãos que podem testar positivo para a COVID-19.

Na Polônia, o governo lançou um aplicativo de smartphone biométrico para confirmar que as pessoas infectadas com COVID-19 permanecem em quarentena. Na República Popular da China (doravante denominada "China"), o reconhecimento facial foi usado para impedir que cidadãos infectados pela COVID-19 viajem. Além disso, empresas na China desenvolveram tecnologia para permitir que o governo identifique pessoas com precisão, ainda que seus rostos estejam parcialmente cobertos por máscaras. Na Federação Russa, os sistemas de reconhecimento facial estão sendo usados para rastrear indivíduos que não respeitam a quarentena obrigatória.

No entanto, o uso da biometria (incluindo o reconhecimento facial) em resposta a COVID-19 levanta várias questões de privacidade e segurança, principalmente quando essas tecnologias são usadas na ausência de orientação específica ou consentimento plenamente informado e explícito. Os indivíduos também podem ter problemas para exercer ampla gama de direitos fundamentais, incluindo o direito de acesso aos seus dados pessoais, o direito de apagar seus dados e o direito de ser informado sobre os objetivos do processamento e com quem esses dados são compartilhados. Os sistemas de reconhecimento facial também podem ter um viés tecnológico intrínseco, como, por exemplo, quando baseados em raça ou origem étnica.

“Privacy-by-design” pode ajudar a lidar com os riscos

O conceito de “privacy-by-design” (que poderia ser traduzido por privacidade desde a concepção) busca assegurar o máximo grau de privacidade, garantindo que, como regra, mecanismos de proteção de dados pessoais sejam inerentes ao sistema. “Privacy-by-design” pode, por exemplo, envolver a previsão de uso de dados agregados, anônimos ou pseudônimos para reforçar a proteção à privacidade ou de exclusão de dados uma vez atendido o objetivo previsto.

O aplicativo COVID-19, desenvolvido pelo Instituto Norueguês de Saúde Pública, por exemplo, foi projetado para armazenar dados de localização por apenas 30 dias. O uso de soluções adicionais de aprimoramento da privacidade (como criptografia homomórfica)[1] podem conferir segurança adicional, assim como o uso de espaços de armazenamento de dados tipo “sandbox”, em que o acesso a dados altamente sensíveis (pessoais) é concedido apenas dentro de um ambiente físico e/ou digital restrito a usuários confiáveis. Um exemplo deste último é o Flowminder, que com a colaboração das empresas de telecomunicações durante o surto de ebola de 2014 a 2016 forneceu aos epidemiologistas acesso seguro

a dados de geolocalização de baixa resolução desidentificados. O Flowminder vem empregando estratégia semelhante para contribuir com a resposta à crise da COVID-19.

Principais recomendações

As tecnologias digitais fornecem ferramentas poderosas para os governos no combate à propagação da pandemia COVID-19, mas suas implicações para a privacidade e a proteção de dados precisam ser reconhecidas. Os aplicativos de rastreamento de contatos devem ser implementados com total transparência, em consulta com as principais partes interessadas, com proteções sólidas de privacidade desde a concepção dos sistemas e por meio de softwares de código aberto (quando apropriado).

Os governos devem considerar:

- A base legal para o uso dessas tecnologias, que varia de acordo com o tipo de dados coletados (pessoais, sensíveis, pseudonimizados, anonimizados, agregados, estruturados ou não estruturados etc.).
- Se o uso dessas tecnologias e a subsequente coleta de dados é proporcional e a forma como os dados são armazenados, processados, compartilhados e com quem (incluindo quais protocolos de segurança e privacidade na concepção do projeto são implementados).
- A qualidade dos dados coletados e sua adequação à finalidade.
- Se o público está bem informado e as abordagens adotadas são implementadas com total transparência e prestação de contas.
- O período dentro do qual tecnologias mais invasivas que coletam dados pessoais podem ser usadas para combater a crise. Os dados devem ser retidos apenas pelo tempo necessário para servir ao propósito específico para o qual foram coletados.

Leitura adicional

OCDE (2019a), Melhorando o acesso e o compartilhamento de dados: reconciliando riscos e benefícios para a reutilização de dados nas sociedades, OCDE Publishing, Paris, https://doi.org/10.1787/276aaca8-en.

OCDE (2019b), Recomendação do Conselho de Inteligência Artificial, OCDE, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

OCDE (2017), Recomendação do Conselho sobre Governança de Dados de Saúde , OCDE, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0433.

OCDE (2015), “Serviços móveis baseados em tecnologia para saúde e bem-estar globais: oportunidades e desafios”, página da web da OCDE, Paris, www.oecd.org/sti/ieconomy/mobile-technology-based-services-for-global- health.htm.

OCDE (2013), Recomendação do Conselho sobre diretrizes para a proteção da privacidade e fluxos transfronteiriços de dados pessoais, OCDE, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.

A OCDE está compilando dados, informações, análises e recomendações sobre os desafios de saúde, econômicos, financeiros e sociais colocados pelo impacto do coronavírus (COVID-19). Visite nossa página dedicada para obter um conjunto completo de informações relacionadas ao coronavírus.

Nota

← 1. Permite o processamento de dados criptografados sem revelar as informações incorporadas.

Publicado originalmente pela OCDE sob o título: *Tracking and tracing Covid: protecting privacy and data while using apps and biometrics.* Traduzido com o apoio da Delegação do Brasil na OCDE. Os textos oficiais são os textos em inglês e/ou francês. A qualidade da tradução e sua coerência com o texto no idioma original são de exclusiva responsabilidade da Delegação do Brasil na OCDE.