Garantir a privacidade de dados na luta contra a COVID-19

14 de abril de 2020

Mensagens principais

- Muitos governos estão adotando medidas sem precedentes para rastrear, monitorar e conter a disseminação do novo coronavírus (COVID-19), recorrendo a tecnologias digitais e estratégias de análises avançadas para coletar, processar e compartilhar dados para obter respostas eficazes na linha de frente.
- Embora as medidas excepcionais implementadas ou previstas em alguns países possam mostrar-se, finalmente, eficazes na limitação da propagação do vírus, algumas abordagens têm se mostrado controversas em termos de risco de violação àprivacidade e outros direitos fundamentais dos cidadãos, especialmente quando essas medidas carecem de transparência ou não são objeto de ampla consulta à população.
- As autoridades responsáveis pela aplicação das normas sobre privacidade geralmente endossam uma abordagem pragmática e contextual em momentos de crise ou estado de emergência, e exercem um poder discricionário, de modo que o respeito aos princípios fundamentais de proteção de dados e privacidade não impeça respostas à COVID-19 que sejam necessárias e proporcionais na linha de frente.
- Os formuladores de políticas, em consulta com as autoridades nacionais de proteção de dados devem avaliar as potenciais soluções de compromisso em matéria de utilização de dados durante esta crise (que equilibre riscos e benefícios), mas devem garantir que quaisquer medidas extraordinárias sejam proporcionais aos riscos e sejam implementadas com total transparência, responsabilidade e compromisso de cessar ou reverter imediatamente usos excepcionais de dados quando a crise terminar.

Algumas respostas digitais à crise precipitaram novos desafios de governança e privacidade de dados

Os governos estão adotando medidas sem precedentes para rastrear e conter a disseminação do novo coronavírus (COVID-19) e estão se beneficiando do poder dos dados para impulsionar soluções digitais. De particular importância para uma resposta eficaz na linha de frente são os dados relativos à disseminação do vírus, relativos, por exemplo, à localização e o número de novos casos confirmados, as taxas de recuperações e mortes e a origem de novos casos (chegadas internacionais ou transmissão intracomunitária). Os dados também são cruciais para avaliar e melhorar a capacidade dos sistemas de saúde e para avaliar a eficácia das políticas de contenção e mitigação que restringem a movimentação de indivíduos. Muitos governos estão recorrendo a tecnologias digitais e estratégias de análises (“analytics”) avançadas para coletar, analisar e compartilhar dados para respostas na linha de frente, em particular, (i) dados de geolocalização derivados de registros de dados de chamadas móveis ou coletados de aplicativos móveis do usuário; e (ii) biometria, particularmente dados de reconhecimento facial.

O acesso e compartilhamento em tempo hábil de dados seguros e confiáveis são, portanto, fundamentais para a compreensão do vírus e sua disseminação, melhorando a eficácia das políticas governamentais e promovendo a cooperação global na corrida para desenvolver e distribuir terapias e vacinas.

No entanto, algumas respostas à crise estão dando origem a novos desafios de governança e privacidade de dados. Por exemplo, as tecnologias de rastreamento de contatos podem ser úteis, pois fornecem informações críticas para limitar a propagação do vírus, mas, se deixadas sem controle, também podem ser usadas para coleta e compartilhamento extensivos de dados pessoais, vigilância em massa, limitando liberdades individuais, desafiando a governança democrática.

Poucos países possuem estruturas para fundamentar as medidas extraordinárias de rastreamento de contatos e vigilância prevista para toda a população

As medidas previstas em alguns países já se mostraram controversas em termos de riscos de violação da privacidade e de outros direitos fundamentais dos cidadãos, especialmente quando essas medidas carecem de transparência e consulta pública. Mesmo quando os dados pessoais são anonimizados, pesquisas recentes sugerem que os indivíduos ainda podem ser identificados por um conjunto limitado de pontos de dados - quatro pontos espaço-temporais podem ser suficientes para identificar univocamente 95% das pessoas no banco de dados de celulares de 1,5 milhão de pessoas e identificar 90% das pessoas em nobanco de dados relativos aos cartões de crédito cartão de crédito de 1 milhão de pessoas.

Poucos países possuem estruturas para fundamentaressas medidas extraordinárias de maneira rápida, segura, confiável, em escala necessária e e em conformidade com os regulamentos de privacidade e proteção de dados existentes. Como resultado, muitos países aprovaram recentemente ou estão prestes a aprovar leis específicas definindo como a coleta de dados pode ser restrita a uma determinada população, por quanto tempo e com que finalidade. Por exemplo:

- O governo italiano publicou um decreto para criar uma estrutura legal especial para coletar e compartilhar dados pessoais relacionados à saúde pelas autoridades de saúde pública e por empresas privadas que fazem parte do sistema nacional de saúde durante o estado de emergência.
- O governo alemão propôs emendar a Lei de Proteção contra Infecções para permitir que o Ministério Federal da Saúde exija que pessoas de "risco" se identifiquem e forneçam informações sobre seu histórico de viagens e detalhes de contato. A proposta original, conferindo autoridade geral para utilizar meios técnicos para identificar possíveis doentes e obter dados de

geolocalização de fornecedores de telecomunicações, foi retirada em parte devido a fortes críticas da autoridade alemão de proteção de dados (Federal Privacy Commissioner).

- Os senadores franceses durante o exame do projeto de lei de emergência propuseram uma emenda para permitir, por um período de seis meses, "qualquer medida" com vistas a a coleta e o processamento de dados de saúde e localização para lidar com a epidemia de COVID-19. A emenda foi rejeitada por ser uma incursão excessiva nos direitos de privacidade.
- Outros governos têm coletado e processado dados de geolocalização relacionados ao COVID-19 sem a necessidade de adotar nova legislação. Por exemplo:
- As autoridades da República da Coréia já têm poderes extraordinários para coletar dados pessoais, se “necessário para prevenir doenças infecciosas e bloquear a propagação da infecção” (Lei de Controle e Prevenção de Doenças Infecciosas, Artigo 76-2).
- Em Cingapura, dados pessoais relevantes podem ser coletados, usados e divulgados sem consentimento durante um surto para realizar o rastreamento de contatos e outras medidas de resposta.
- Em Israel, o governo conta com medidas de emergência que permitem o uso de tecnologia desenvolvida para fins de contraterrorismo para rastrear pessoas infectadas monitorando telefones celulares.

As autoridades de proteção da privacidade têm um papel fundamental a desempenhar, à medida que os governos adotam legislação de emergência e os os responsáveis pelo tratamento de dados buscam segurança jurídica

Apesar da escala dos desafios econômicos e de saúde pública colocados pela pandemia da COVID-19, é crucial que os governos e os atores do setor privado não se afastem dos princípios fundamentais de governança de dados e os princípios de privacidade. As autoridades nacionais de proteção de dados (PEAs em inglês) têm papel fundamental a desempenhar assessorando a elaboração de propostas de novas legislações governamentais proporcionando clareza quanto à aplicação das estruturas existentes de privacidade e proteção de dados. As PEAs pode ser ver na contingência de ter que oferecer soluções inovadoras e prospectivas, principalmente quando se trata de questões importantes de exclusão e retenção de dados pessoais, reversibilidade de novos controles governamentais e o exercício de seus poderes de auditoria e investigação.

Em meados de abril de 2020, as PEAs na Argentina, Austrália, Canadá, Finlândia, França, Alemanha, Irlanda, Nova Zelândia, Polônia, Eslováquia, Suíça e Reino Unido publicaram diretrizes gerais para controladores e processadores de dados sobre a aplicação das suas leis de privacidade e proteção de dados durante a crise. As PEAs geralmente endossam uma abordagem pragmática e contextual e exercem um poder discricionário, deixando claro que o respeito aos princípios fundamentais de proteção de dados e privacidade não atrapalha as respostas na linha de frente ao COVID-19 que sejam necessárias e proporcionais. O Conselho Europeu de Proteção de Dados e o Conselho da Europa divulgaram declarações semelhantes explicando que o Regulamento Geral de Proteção de Dados (RGPD) e a Convenção 108 não impedem as medidas tomadas na luta contra a pandemia, mas exigem que as restrições de emergência às liberdades sejam proporcionais e limitadas ao período de emergência.

Algumas PEAs publicaram orientações específicas, relativas, por exemplo, às quais regras se aplicam ao uso de informações nas mídias sociais para rastrear possíveis portadores (por exemplo, Hong Kong, China) e às ações governamentais relacionadas a fraudes ligadas ao coronavírus e alegações sem fundamento de que determinados produtos poderiam tratar ou prevenir o vírus (por exemplo, na Espanha e nos Estados Unidos).

Em outros casos, as PEAs estão respondendo de maneira inovadora. O Gabinete do Comissário de Informação do Reino Unido, por exemplo, anunciou que reconhecerá o interesse público urgente na aplicação de sua lei de proteção de dados e permitirá que os responsáveis pelo tratamento de dados

equilibrem suas obrigações com sua capacidade de responder a solicitações de acesso dos indivíduos. A Global Privacy Assembly, um consórcio mundial de reguladores de privacidade e proteção de dados, criou um página dedicada que compara as mais recentes orientações e informações de seus membros sobre o tema.

Principais recomendações

As respostas políticas estão evoluindo rapidamente em um ambiente de poucas evidências confiáveis ou oportunidades para consultas internas ou multilaterais sólidas. No entanto, todos os países precisam urgentemente de dados para informar respostas regulatórias e políticas à medida que a crise se desenrola. As considerações a seguir, baseadas nos princípios de governança e privacidade de dados da OCDE, devem orientar essas práticas de coleta e compartilhamento de dados.

- Os governos precisam promover o uso responsável dos dados pessoais . Parece haver uma tendência crescente no sentido de utilizar, em larga escala, meios mais invasivos de coleta, processamento e compartilhamento de dados pessoais de saúde e comportamentais, que envolvem monitoramento direcionado de indivíduos para conter a disseminação da COVID-19. Embora algumas dessas medidas possam ser eficazes para ajudar a conter o surto, os governos devem garantir que essas ferramentas sejam implementadas com total transparência, responsabilidade e um compromisso de cessar ou reverter rapidamente usos excepcionais de dados quando a crise terminar. Os responsáveis pelo tratamento de dados ainda devem ter uma base jurídica e equitativa para coletar e usar dados pessoais.
- Os governos devem consultar as autoridades nacionais de proteção de dados (PEAs) antes de introduzir medidas que correm o risco de infringir os princípios estabelecidos de privacidade e proteção de dados . As PEAs devem ser consultadas nos esforços para definir as respostas na linha de frente para garantir que as incursões nos direitos de privacidade sejam acompanhadas de salvaguardas apropriadas. As PEAs e os governos devem dedicar recursos especializados para permitir essas avaliações.
- As PEAs devem abordar incertezas regulatórias, devendo adotar uma abordagem pragmática e contextual para responder rapidamente a pedidos de aconselhamento e esclarecer como as estruturas de proteção e privacidade de dados em cada jurisdição se aplicam à coleta e compartilhamento de dados pessoais nesta crise. Isso provavelmente promoverá a conformidade com essas estruturas e permitirá fluxos de dados internos e transfronteiriços eficientes.
- Respeitadas as salvaguardas necessárias e proporcionais, os governos devem apoiar a cooperação nacional e internacional para coleta, processamento e compartilhamento de dados pessoais de saúde para pesquisas, estatísticas e outros fins relacionados à saúde na gestão da crise da COVID-19 . Isso inclui a adoção de soluções de preservação da privacidade para acesso e compartilhamento de dados e, quando apropriado, o envolvimento e o aproveitamento de parcerias público-privadas para facilitar o compartilhamento de dados.
- Os governos e responsáveis pelo tratamento de dados devem ser transparentes e responsáveis por todas as ações que tomam em resposta à crise . Os governos devem garantir o engajamento e a participação, principalmente por meio de consulta pública, de uma ampla gama de partes interessadas, com o objetivo de garantir que a coleta, o processamento e o compartilhamento de dados pessoais sirvam ao interesse público e sejam coerentes com os valores da sociedade e as expectativas razoáveis dos indivíduos.

Leitura adicional

OECD (2013), Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188 .

OECD (2017), Recommendation of the Council on Health Data Governance, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0433 .

OECD (2019), Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, OECD Publishing, Paris, https://doi.org/10.1787/276aaca8-en .

OECD (2020), Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics (COVID-19)

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 tema do coronavírus.

Publicado originalmente pela OCDE sob o título: ***Ensuring data privacy as we battle COVID-19***. 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.