



LAPIN

Relatório

**Vigilância digital
contra o Covid-19:
*um mal necessário?***

2020

Introdução

O webinar “**Vigilância digital contra o Covid-19: um mal necessário?**”, realizado em 8 de abril de 2020 pelo Laboratório de Políticas Públicas e Internet (LAPIN), abordou a possibilidade de **utilização de dados pessoais como recurso capaz de contribuir no combate à pandemia** do novo coronavírus no Brasil e no mundo. Devotou-se especial atenção para a análise de constituição, ou não, de quadro de vigilância digital, isto é, de situação em que ocorre **uso indevido** de dados pessoais, sob pressuposto de combate à pandemia, para que agentes públicos e ou privados obtenham dados e informações de modo contrário às diretrizes legais de proteção de dados pessoais.

A mesa de debates teve Otávio Mayrink, representante do LAPIN, como mediador, e Giovanna Carloni (CIPL), Carlos Affonso (ITS Rio) e Bruno Bioni (Data Privacy Brasil) como membros debatedores.

O seminário digital foi organizado em **quatro momentos**. No primeiro momento, Otávio Mayrink introduziu a pauta do debate. No segundo momento, cada um dos membros debatedores, expôs seu posicionamento inicial a respeito do tema. No terceiro momento, houve aproximadamente sete rodadas de perguntas, realizadas por espectadores, via plataforma do YouTube. No momento último, os membros debatedores foram convidados a realizar considerações finais e a responder uma última pergunta, formulada pelo mediador.

Considerações preliminares

Otávio Mayrink (mediador): sugere que há **conflito entre a disciplina de dados pessoais e as estratégias de contenção do COVID-19** em todo o mundo. Tomam-se como exemplo **China, Coreia do Sul, Israel e Japão**, que utilizam dados pessoais, tais como os de geolocalização e os de biometria, para (i) alimentar sistemas de inteligência artificial com capacidade preditiva para **antever a disseminação do vírus** e (ii) evitar a formação de aglomerações humanas. Todavia benéficos quando utilizados para o controle da pandemia de novo coronavírus, é factível o **risco** de que esses recursos perdurem para além do período de pandemia, em desacordo com a finalidade para a qual foram obtidos.

Exposição inicial dos debatedores

Giovanna Carloni: Para Carloni, **a tecnologia é forma de combater o coronavírus** e o tratamento de dados pessoais possibilita o mapeamento de focos da pandemia de COVID-19, bem como, quando tratados por sistemas de

inteligência artificial, os dados pessoais servem de **auxílio às buscas por possíveis tratamentos**. Para Giovanna, não é devido que entidades públicas e privadas tratem dados de modo **ilimitado**, mas devem se ater à **necessidade e à finalidade**, visando à proteção de direitos fundamentais tais como a saúde e a vida.

Ações e programas de **governança**, de acordo com o princípio **accountability**, são formas de garantir a observância dessas restrições ao tratamento de dados. Assim será possível estruturar programas de governança e proteção de dados de forma que os diversos setores da sociedade possam utilizar esses dados de **modo transparente e responsável**. Essas medidas consistem em provisão da devida transparência em relação às formas de tratamento de dados e a observância do rol principiológico que compõe a disciplina de tratamento de dados.

Para ilustrar, Giovanna aponta que a França e o Reino Unido já desenvolveram **aplicativos que informam diretamente sobre como ocorre o processamento de dados e até quando essas informações são armazenadas**. Para além do governo, as empresas criam plataformas para combater o vírus, elas também devem aplicar medidas de segurança e elementos de *accountability* à coleta de dados, como exemplo a representante do CIPL aponta para o tratamento de dados agregados sobre localização pela Google. Dessa forma, uso de dados deve se dar de forma responsável.

Carlos Affonso: Para Affonso, é necessário fazer um exercício de "futurologia" para entender os cenários que os países migrarão em um contexto pós coronavírus.

Há, no curso do tempo, **três cenários** que se estabelecem sucessivamente e que caracterizam a forma como as normas de proteção de dados impactam no controle da pandemia. O **primeiro** cenário consiste no reconhecimento da emergência epidemiológica e da necessidade de tomar medidas para controlá-la. O **segundo** cenário é aquele em que se faz necessário aumentar o rigor com o qual governos lidam com a emergência epidemiológica. É nesse momento que há demanda de acesso a dados pessoais para controlar a pandemia. Se ocorrer de modo a configurar uso abusivo ou excessivamente rigoroso de poder, então configura-se o **terceiro** cenário, no qual há reação aos atos governamentais, de modo a causar tensões políticas e sociais.

A depender de como cada cenário se configurar no Brasil, pode-se prospectar situações de maior otimismo ou de maior pessimismo. Como exemplo, Calos evidencia o caso do Kosovo e a situação de um governo com viés autoritário, em que busca silenciar e restringir discursos com a justificativa de combater o coronavírus, principalmente em democracias fracas.

Bruno Bioni: Bioni aponta para a necessidade de que o tratamento de dados pessoais respeite a diretrizes consagradas pela disciplina de proteção de dados, a exemplo dos **princípios de necessidade, de finalidade, de qualidade dos dados e de proporcionalidade, sem embargo de outros**. Desse modo,

não surge a dicotomia entre a proteção de dados pessoais e o uso desses mesmos dados em ações para o controle da pandemia de COVID-19.

Diante do isolamento social e análise de dados agregados, não individualizados, tem-se que a finalidade do uso de uma informação pessoal esclarece especificamente qual dado é necessário para um determinado objetivo, no caso o combate à epidemia. Assim, **com a definição de um objetivo, torna-se possível delinear quais dados são fundamentais e como o governo irá usar de forma eficiente esses dados.**

Para Bruno, é imprescindível a observância dos princípios da finalidade, da necessidade e da adequação. Assim, o governo, a fim de proteger o gestor público e evitar violações de direitos, deve delimitar formas específicas e endereçar instrumentos para alcançar seu objetivo de acabar com o coronavírus e assegurar contexto estável para a saúde pública.

Além dos princípios já evidenciados, o princípio de qualidade determina que deve ser respeitado o ciclo de vida do dado, a informação pessoal entendida diante de uma coleta necessária, tratamento adequado e, quando não mais útil, deve ser descartado ou transformado em estatística. Nessa perspectiva, **Bruno aponta que as bases de dados já utilizadas, as estatísticas, os métodos e as ações devem ter início meio e fim.** Diante da observância dos princípios da proteção de dados, o gestor público está mais capacitado para formular um calendário de ações para combater o vírus.

Dessa forma, **a proteção de dados é reforço para evitar a disseminação do coronavírus.** Ainda, o princípio da transparência, efetivado pelos portais de transparência e pela Lei de Acesso à Informação (LAI), torna a publicação das ações e a modelagem dos dados para combate do vírus mais seguras e responsáveis. **Em um contexto de transparência, a sociedade pode colaborar com as ações de prevenção à disseminação do vírus e a academia pode pesquisar ações que estão sendo realizadas para apontar eficiências e deficiências das medidas implementadas.**

Diante dos problemas causados pelo coronavírus, Bioni destaca que **as normas de proteção de dados pessoais não servem para restringir o uso de dados, mas para possibilitar o uso, desde que adequado, de dados e de informações pessoais.** Assim, o gestor público perceberá que a proteção de dados **não é um obstáculo, mas um catalisador** o qual aponta de forma eficiente a melhor forma de utilizar dados pessoais. Com exemplo, a doença do vírus Ebola também ensejou o controle de dados pessoais e pesquisas a partir dessa experiência afirmam que, em alguma medida, usar dados agregados não foi eficiente. Assim, estudos no contexto pós pandemia podem apontar aspectos os quais foram eficientes e podem ser repetidos em outras situações similares. Com isso, percebe-se quais ações e quais dados vão ser necessários para ações de contenção de uma pandemia.

Como também, Bruno Bioni defende que as regras já vigentes devem fazer *enforcement* e orientar ações dos governos, como o Marco Civil da Internet e a LAI. Assim, ele conclui que **a proteção de dados é forma eficiente de combate o coronavírus.**

Rodadas de perguntas

Pergunta nº 1: “Como regular a coleta de dados por empresas privadas em situação de crise?”

Giovanna: sobre a necessidade de consentimento e a LGPD, ela afirma que **existem outras bases legais que permitem a coleta de dados para fins de saúde sem ser consentimento**. Ainda, talvez o governo e as empresas não atinjam o consentimento de todas as pessoas que vão ter dados tratados. Com isso, algumas medidas protetivas devem ser implementadas para que as pessoas tenham **confiança** de que dados serão tratados de forma correta.

Carlos Affonso: Para Carlos, deve haver **estrita observância do princípio da finalidade**, de modo que quaisquer empresas que colem dados para fins de combate à pandemia de novo coronavírus, seja por meio de parceria governamental ou não, estejam limitadas pelas normas de tratamento de dados. De acordo com o princípio da finalidade, **o tratamento de dados deve ser rigorosamente realizado para atender a um fim previamente determinado e amplamente informado**, de modo a afastar vícios no processo de tratamento de dados.

Bruno Bioni: Bruno Bioni enfatiza o fato de que, **em razão da *vacatio legis* da Lei Geral de Proteção de Dados Pessoais, há insegurança normativa no Brasil**. Isso porque não há previsão normativa ampla das operações de tratamento de dados. Essa forma de tutela, em larga medida, encontra-se limitada à Lei de Acesso à Informação e à Lei de Cadastro Positivo. Isso posto, Bioni considera prejudicial a prorrogação do prazo de *vacatio legis* da LGPD, por entender que o referido dispositivo legal auxilia na recuperação dos danos econômicos e sociais causados pela pandemia de COVID-19.

Pergunta nº 2: “É factível utilizar dados agregados e anonimizados, ou dados pessoais são necessários?” | “Como lidar com tecnologias que monitoram dados de geolocalização para verificar o cumprimento da quarentena?”

Carlos Affonso: Para Affonso, **há risco de que dados agregados sejam identificados, ferindo o caráter anônimo que outrora possuíam**. Se serviços trocam dados com parceiros econômicos, há risco latente de vazamento de informações pessoais para além do consentimento.

Pergunta nº 3: “Caso a LGPD estivesse em vigor, seria possível lançar mão do artigo 4º, III, que diz que a lei não se aplica para fins de segurança pública?”

Bruno Bioni: Para Bruno, **a proteção da saúde não configura “segurança pública” no sentido estrito, bem como há previsão normativa na LGPD para situações de proteção à saúde**. Por isso, considera improvável que a tese do contida na pergunta se prove vitoriosa.

Pergunta nº 4: “Qual a dimensão do prejuízo causado por políticas de privacidade antigas, desatualizadas ou com baixa qualidade técnica?”

Carlos Affonso: Em larga medida, para Affonso, muitas pessoas se colocam em uma posição de fragilidade a fim de obter acesso às prestações estatais que objetivam combater a pandemia, se **sujeitando a termos e a políticas de privacidade e de tratamento de dados de baixa qualidade.**

Bruno Bioni: À tese de Affonso, Bioni acrescenta que **a ausência de poder de barganha por parte de quem depende de sistemas de auxílio social compromete a identificação do consentimento como sendo “livre”.** Pessoas nessas condições não consentem de forma livre, mas de forma condicionada, visto que dependem, por questões de subsistência, do auxílio financeiro fornecido, sem alternativa ou recurso.

Pergunta nº 5: “Quais os riscos provenientes das parcerias governamentais com entidades privadas?”

Bruno Bioni: **Para medir riscos é necessário saber os termos que regem a parceria referida. Não é possível fazê-lo em abstrato.** Por isso, devem-se observar os princípios de *accountability* e de transparência.

Pergunta nº 6: “Qual a influência exercida por instituições como a ICO e a CNIL em relação aos programas de *accountability* adotados na França e no Reino Unido? Quais os obstáculos que o Brasil encontra em razão de não possuir, ainda, a ANPD?”

Giovanna: A representante da CIPL entende que **as autoridades de proteção de dados, mais especificamente ICO e CNIL, têm papel de dar diretrizes e fazer o enforcement das leis de proteção de dados** (min. 56). Ela aponta que essas autoridades possuem poder de influência global, como exemplo o *global privacy assembly*. Assim essas instituições devem coordenar ações para ajudar a combater o coronavírus e restabelecer a economia. Porém, no Brasil ainda não se tem lei nem mesmo uma autoridade de proteção de dados, o que prejudica o país.

Pergunta nº 7: “Com relação ao próprio app do SUS, poderia ser considerado um instrumento de vigilância?”

Giovanna: No que diz respeito ao aplicativo do SUS (min. 47), Carloni entende que **o aplicativo é para fins de saúde pública, se depois da pandemia os dados forem utilizados para outras finalidades não é permitido, mas a própria LGPD possibilita o tratamento de dados para saúde.**

Considerações Finais

Por fim, Carloni entende que **a proteção de dados é uma legislação possibilitadora, não impeditiva. Os dados são necessário para combater o vírus e avançar a economia**, nessa perspectiva, as leis possuem como objetivo possibilitar o tratamento de forma responsável.

Para Affonso, assim como o caso do Edward Snowden e do Cambridge Analytica, **o coronavírus irá compor história da proteção de dados**, mas ainda não se sabe se será mais uma história de grande violação da proteção de dados, tendo um viés negativo diante de um tratamento de dados feito de forma irregular. O representante da ITS Rio afirma que a LGPD permite que se concretizem histórias melhores e de outra natureza, diante da observância dos aspecto principiológicos e procedimentais da lei.

Como provocação final, Bruno analisa que **postergar a LGPD é postergar direitos e diversas possibilidades de novas políticas para proteção de dados**. Por mais que a lei seja prorrogada, a criação de uma autoridade de proteção de dados deve ser feita rapidamente, mesmo que no contexto de contenção de gastos para combater o coronavírus.