# Privacidade e Segurança Nacional: o combate da pandemia do Covid-19 através da tecnologia.

Danielle Jacon Ayres Pinto
Arthur Corrêa Maziero

Atualmente não é possível negar a capacidade que a pandemia causada pelo Sars-CoV-2, popularmente conhecida como “novo coronavírus”, tem de colapsar os sistemas de saúde dos mais diversos Estados se não for meticulosamente combatida. A transmissão, o número de infectados e o número de mortos aumenta exponencialmente em um curto período de tempo. Para confirmarmos estes fatos basta olhar a quantidade de número de mortos em um único dia na cidade de Nova York. Dados obtidos desde março até o dia 23 de abril confirmam o total de 10.290 mortos pelo Covid-19 e 141.754 infectados (PREFEITURA DA CIDADE DE NOVA YORK, 2020).

Nesse sentido, se faz necessário políticas públicas para combater o vírus. A principal política aplicada em maior parte do mundo é o isolamento social, a qual pode ou não evoluir para uma quarentena. Por sua vez, o Estado para garantir que as pessoas cumpram esta orientação ou determinação fazem uso da tecnologia disponível. A qual também é utilizada para identificar possíveis focos de contágio ou possíveis contagiados, seu histórico de contato com outras pessoas e suas movimentações.

É possível identificar duas maneiras pelas quais o Estado pode atuar. Por um lado, temos o exemplo da China exerce uma profunda vigilância em massa de sua população. Por exemplo, há câmeras instaladas em estações de trem capazes de verificar a temperatura corporal de cada pessoa. Se a temperatura é mais alta que o normal ela é automaticamente levada pelos funcionários a um isolamento e testada para o vírus. Caso teste positivo, as pessoas que estiveram em contato com ela na mesma estação receberão mensagens notificando o ocorrido. É importante destacar aqui, que a mesma empresa que forneceu estas câmeras trabalha para adicionar a capacidade de reconhecimento facial, mesmo se a pessoa estiver utilizando uma máscara. A China obtém a localização geográfica da população através dos celulares para garantir o isolamento. (YUAN, 2020)

Por outro lado, o governo de Cingapura desenvolveu o aplicativo "TradeTogether". O qual é utilizado por mais de um milhão de pessoas. Ele não utiliza e não necessita de sua localização geográfica. Além do mais, não é necessário colocar seus dados pessoais. O aplicativo salvará apenas seu número de telefone e gerará um número de identificação aleatório. A ideia principal do aplicativo é através da conexão *bluetooth* que o próprio usuário seja notificado se esteve próximo a alguém que estava com o Covid-19. É importante destacar aqui que o Ministério da Saúde de Cingapura pode obter acesso aos seus dados e também ao seu histórico dentro do aplicativo. No entanto, conforme avisam os desenvolvedores no próprio site, isto apenas acontecerá caso o usuário permita. E, não será informado entre os usuários a identidade do infectado. O Ministério da Saúde é, também, o único que pode decodificar o usuário (GOVERNO DE SINGAPURA, 2020).

Estes são alguns dos exemplos que o Estado se utiliza da tecnologia disponível para enfrentar a pandemia. A partir desta utilização, o debate sobre a privacidade em tempos de espaço cibernético ganha mais enfoque, pois de um lado temos o exemplo do Estado chinês com pouca ou nenhuma preocupação em prestar contas à população e do outro lado o governo de Cingapura que tenta utilizar a tecnologia sem uma grande perda da privacidade dos usuários. Acerca deste debate algumas perguntas surgem: Esse tipo de tecnologia deve ser utilizado no combate da pandemia? Qual a real efetividade da utilização deste tipo de tecnologia? Qual o nível de acesso aos nossos dados é permitido aos Estados? O que acontece/acontecerá com os dados que são e serão salvos? Como garantir o sigilo destes dados e a transparência de todo o processo? Estas perguntas se encaixam em um amplo debate de Privacidade versus Segurança Nacional e devido ao espaço curto deste artigo não é a sua intenção responde-las por completo, mas sim instigar o leitor.

A privacidade é um direito humano reconhecido pela Organização das Nações Unidas (ONU). Em dezembro de 2013, após os escândalos que envolveram os EUA e a vigilância em massa de pessoas em todo o mundo, foi adotada uma resolução que além de reafirmar esse direito o estendia ao mundo digital. E pede para que os Estados "Respeitem e protejam o direito à privacidade, incluindo o contexto da comunicação digital; " (GA UM, 2013, p. 2, tradução nossa). [1]

[1] "To respect and protect the right to privacy, including in the context of digital communication;"

Apesar da privacidade não ser um assunto novo, o que é considerado privado ou público mudou ao decorrer do tempo. Antes da Internet e dos novos aparatos tecnológicos, o entendimento de privacidade girava em torno da não invasão da propriedade privada, das escutas em linhas telefônicas etc. Atualmente, no entanto, com a massiva utilização da Internet em todos os aspectos da vida social, dos aparelhos de telefonia móvel, dos computadores, das câmeras de vigilância, a diferença entre o público e privado entra em uma área nublado, sem clareza de até que ponto a privacidade se estende no campo digital. Esta diferenciação se torna mais difícil quando é necessário utilizar-se do espaço cibernético para combater crimes ou auxiliar no combate de uma pandemia. Nesse sentido, Bauman et al (2014, p. 136, tradução nossa) afirma que "[…] evidências recentes sugerem que uma erosão ainda mais sustentada de tais distinções e do direito presumido das agências estatais para entrar profundamente dentro do mundo do dia-a-dia da sociedade civil e da vida privada. ". [2]

Em um cenário normal com a ausência de ameaças evidentes para a Segurança Nacional e da sociedade é difícil imaginar que as pessoas aceitariam voluntariamente e de bom grado ceder a sua privacidade. No entanto, uma vez que se inicia a narrativa da Segurança Nacional, se inicia também a narrativa de que excepcionalmente é 'aceitável' ceder a privacidade e receber em troca o aumento da segurança, pois o cenário pede que todos os esforços e sacrifícios sejam tomados. É neste sentido que o termo guerra pode ser interpretado, quando utilizado nos discursos políticos sobre o Covid-19. É uma tentativa de através do discurso exercer práticas excepcionais que não seriam aceitas em outro contexto.

O problema em relação ao discurso de guerra e do cenário de exceção é que ele pode virar a norma. O filósofo italiano Giorgio Agamben (2018), se utilizando do exemplo do terrorismo, defende esta ideia. Por exemplo, através da justificativa do terrorismo se aceitou o grande número de dispositivos de segurança em aeroportos e o grande número de câmeras de vigilâncias nas ruas e estabelecimentos. É este processo que os pensadores Byung Chul Han (2020) e Yuval Noah Harari (2020) temem, que as políticas de vigilância em massa da população se tornem a norma e não mais uma exceção. Nesse sentido, Harari (2020) defende, em uma entrevista ao

[2] "[…] recent evidence suggests an even more sustained erosion of such distinctions and the presumed right of state agencies to penetrate deeply into the everyday worlds of civil society and private life."

jornal alemão Deutsche Welle (DW) que a vigilância é uma via de mão dupla, ou seja, quando aumentada do lado dos cidadãos deve ser aumentada no lado do governo, através da prestação de contas.

A vigilância em massa da população pode inibir elementos essenciais para uma democracia, como a liberdade de expressão e de livre associação. Se assumirmos a necessidade da tecnologia para enfrentar esta pandemia, é necessário criarmos maneiras de a população garantir que o governo preste contas sobre o que é feito com seus dados e de quem os acessam. Pois, esta prestação de contas é algo central para a viabilidade de uma democracia. (SOLOVE, 2011) É necessário tomar cuidado com as falácias do argumento do 'tudo ou nada' quando se trata da Segurança Nacional versus Privacidade. Uma vez que um não é excludente do outro e também que não há garantias de que a segurança aumentará ao ceder totalmente a privacidade. Por último, é importante destacar que há possiblidades do uso da tecnologia sem que o Estado invada a privacidade do cidadão, como bem demonstra o exemplo de Cingapura. Todavia, para isso acontecer é preciso um compromisso ético e legal por parte das instituições do Estado, com a proteção dos dados dos cidadãos e a garantia que tais informações não serão utilizadas no futuro para dar ao Estado um conhecimento adicional que poderá vir a controlar a vida desse indivíduo de acordo com a vontade do agente público.

A tecnologia tem milhares de funções e estamos vendo isso claramente na busca por proteção efetiva da população frente a pandemia de COVID-19. Todavia, o Estado ainda continua sendo o mesmo ente utilitarista em relação aos seus interesses e é nessa dicotomia que todo cuidado deve ser redobrado para que a violação dos direitos humanos, em especial os ligados à privacidade, não se torne "o novo normal" no período pós-pandemia em nome de uma falsa sensação de segurança.

Bibliografia

AGAMBEN Giorgio. Giorgio Agamben 'O estado de exceção se tornou norma'. O pensador italiano, que publica no Brasil 'O Fogo e o Relato', fala de filosofia, de arte, de poesia e da tendência política do mundo atual. Entrevista concedida a Francesc Arroyo, **El País**, 30 de abr. de 2018. Disponível em: https://brasil.elpais.com/brasil/2016/04/19/cultura/1461061660_628743.html; Acesso em: 23 de abr. de 2020.

BAUMAN, Zygmunt et al, After Snowden: Rethinking the Impact of Surveillance, **International Political Sociology**, v. 8, n. 2, p. 121–144, 2014.

GENERAL ASSEMBLY OF UNITED NATIONS, **68/167. The right to privacy in the digital age**, [s.l.: s.n.], 2013.

GOVERNO DE SINGAPURA. 2020. Disponível em: https://www.tracetogether.gov.sg/common/privacystatement; Acesso em: 20 de abril de 2020;

HAN, Byung-Chul. O coronavírus de hoje e o mundo de amanhã, segundo o filósofo Byung-Chul Han. Países asiáticos estão lidando melhor com essa crise do que o Ocidente. Enquanto lá se trabalha com dados e máscaras, aqui se chega tarde e fecham fronteiras. **El País**, 22 de mar. de 2020; Disponível em; https://brasil.elpais.com/ideas/2020-03-22/o-coronavirus-de-hoje-e-o-mundo-de-amanha-segundo-o-filosofo-byung-chul-han.html; Acesso em; 23 de abr. de 2020.

HARARI, Yuval Noah. Yuval Noah Harari on COVID-19: 'The biggest danger is not the virus itself'. A crisis can be a turning point for a society. Which way will we go now? Professor Yuval Noah Harari, whose company donated $1 million to WHO, explains how the decisions we make today on COVID-19 will change our future. Entrevista concedida a Anna Carthaus, DW, 22 de abr. 2020. Disponível em; https://www.dw.com/en/virus-itself-is-not-the-biggest-danger-says-yuval-noah-harari/a-53195552; Acesso em; 23 de abr. 2020.

PREFEITURA DA CIDADE DE NOVA YORK. 2020. Disponível em: https://www1.nyc.gov/site/doh/covid/covid-19-data.page; Acesso em 23 de abril de 2020;

SOLOVE, Daniel J., **Nothing to Hide: The False Tradeoff between Privacy and Security**, New Haven & London: Yale University Press, 2011.

YUAN, Shawn. How China is using AI and big data to fight the coronavirus. Authorities in China step up surveillance and roll out new artificial intelligence tools to fight deadly epidemic. **AlJazeera**, 1 de mar. de 2020. Disponível em: https://www.aljazeera.com/news/2020/03/china-ai-big-data-combat-coronavirus-outbreak-200301063901951.html; Acesso em 19 de abril de 2020;