Vigilância governamental e a pandemia da Covid-19: Aplicativos de rastreamento de contato e privacidade de dados

Sofia Bordin Rolim
Graduada em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul e servidora do Tribunal de Contas do Município de São Paulo

Resumo: O presente artigo se propõe a examinar o uso de aplicativos de rastreamento de contatos durante a pandemia da Covid-19, em um contexto de vigilância governamental e autoritarismo digital crescentes. Através de uma perspectiva de proteção de dados, consideramos atributos chaves desses aplicativos, como sua arquitetura de sistema e gerenciamento de dados, examinando as principais implicações para privacidade. Exploramos brevemente alguns dos métodos de vigilância empregados ao redor do mundo e refletimos sobre suas implicações para as liberdades individuais e a democracia. Por fim, nós examinamos os resultados de uma revisão sistemática sobre a eficácia do rastreamento de contato automatizado para a prevenção da propagação do novo coronavírus.

Palavras-chave: Proteção de dados. Vigilância governamental. Rastreamento de contato. Privacidade. Autoritarismo digital.

Abstract: This article aims to examine the use of contact tracing apps during the Covid-19 pandemic in a context of rising government surveillance and digital authoritarianism. Through a data protection perspective, we will consider key attributes of these softwares such as system architecture and data management, and examine their main privacy implications. We briefly explore some of the surveillance methods employed around the world and reflect on its implications for individual freedoms and democracy. At last, we examine the findings of a systematic review

of the effectiveness of automated contact-tracing for preventing the spread of the novel coronavirus.

Keywords: Data protection. Government surveillance. Contact tracing. Privacy. Digital authoritarianism.

1 Os dados importam: vigilância e autoritarismo digital

Em 2018, o escândalo de dados da Cambridge Analytica (CA) revelou como, através do Facebook, a empresa vinha coletando dados dos usuários sem seu consentimento e os utilizando para influenciar o voto das pessoas e os resultados das eleições. Um aplicativo de propriedade da CA foi oferecido no Facebook a milhares de usuários, que foram pagos para responder a uma pesquisa online e consentiram que seus dados fossem coletados para "fins acadêmicos". Embora a Política da Plataforma da rede social proíba a coleta de dados de amigos dos usuários para fins comerciais ou publicitários[1], a CA foi capaz de coletar dados de 87 milhões de usuários do Facebook, embora apenas 270 mil pessoas tenham baixado o aplicativo.[2] Essa informação foi então usada para microssegmentação (*microtargeting*) política online, removendo o debate político da esfera pública e impondo, assim, uma ameaça de manipulação e supressão eleitoral, e também facilitando a disseminação de desinformação.[3] O caso da Cambridge Analytica desvelou não apenas um único caso de coleta ilegal e uso político de dados, mas também expôs como os governos e a sociedade civil têm pouco controle e conhecimento sobre a forma como as empresas privadas coletam, armazenam e compartilham os dados dos cidadãos.

O debate sobre como a *Big Tech*[4] se beneficia economicamente, e até estrutura seus modelos de negócios com base na coleta agressiva dos dados de seus usuários, tem ocupado especialistas em privacidade, ativistas de direitos digitais, filósofos políticos e cientistas sociais preocupados com o declínio democrático, e até mesmo economistas liberais, empresários e advogados que defendem o fim das *Big Four*, argumentando que o monopólio sufoca a inovação e a competição.[5] Para Shoshana Zuboff, professora da Escola de Negócios da Universidade de Harvard, nos Estados Unidos, a abordagem contemporânea da *Big Tech* e das empresas privadas em relação aos dados do usuário instituiu uma "nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais ocultas de extração, previsão e vendas"[6], que ela nomeia *capitalismo de vigilância*. Zuboff desvenda como, através do *machine learning*, os dados são usados para fabricar produtos de previsão – isto é, previsões do comportamento futuro do usuário – que são extremamente lucrativos. Na busca competitiva por dados comportamentais cada vez mais preditivos, as empresas perceberam a eficiência de direcionar o comportamento do consumidor para resultados que garantam lucros ainda maiores. Isso produziu uma mudança "na qual os processos automatizados não apenas conhecem nosso comportamento, mas também moldam nosso comportamento em escala"[7].

Ainda, a ameaça do autoritarismo digital – o uso da vigilância digital para rastrear e suprimir dissidência política – está presente em países situados em diferentes pontos do espectro democrático.[8] De acordo com a *Freedom House*, a pandemia da Covid-19 acelerou um processo já acentuado de declínio da liberdade na internet em todo o mundo:

> [...] autoridades [governamentais] citaram a covid-19 para justificar a expansão dos poderes de vigilância e a implantação de novas tecnologias antes vistas como demasiadamente intrusivas. A crise de saúde pública criou uma oportunidade para a digitalização, coleta e análise dos dados mais íntimos das pessoas, sem proteções adequadas contra

> abusos. Governos e entidades privadas estão aumentando seu uso de inteligência artificial (IA), vigilância biométrica e ferramentas de big data para a tomada de decisões que afetam os direitos econômicos, sociais e políticos dos indivíduos. Crucialmente, os processos envolvidos frequentemente tem carecido de transparência, de supervisão independente e possibilidades de reparação. Essas práticas aumentam a perspectiva de um futuro distópico em que empresas privadas, agências de segurança e cibercriminosos tenham acesso fácil não apenas a informações confidenciais sobre os lugares que visitamos e os itens que compramos, mas também a nossos históricos médicos, padrões faciais e de voz, e até mesmo nossos códigos genéticos.[9]

Nos tópicos a seguir, abordaremos esse processo de aumento da vigilância e coleta de dados especificamente no que diz respeito ao desenvolvimento e promoção de aplicativos que dependem de monitoramento de localização para rastrear casos de possível exposição ao vírus Sars-CoV-2.

2 O surgimento da Covid-19 e o rastreamento de contatos

Em dezembro de 2019, médicos e pesquisadores de Wuhan, capital da província de Hubei, na China central, se esforçavam para identificar a origem da doença semelhante à pneumonia que rapidamente infectara dezenas de residentes da cidade.[10] Em 3 de janeiro de 2020, o Instituto Nacional de Controle e Prevenção de Doenças Virais identificou o primeiro genoma completo do vírus posteriormente designado como Sars-CoV-2[11] nas amostras de fluidos de um paciente[12]; 16 dias depois, havia 198 casos confirmados em Wuhan, com casos reportados no Japão, Coreia do Sul, Tailândia e em outros lugares da China.[13]

Em 5 de janeiro, 121 contatos próximos dos pacientes infectados haviam sido identificados e colocados sob observação médica;[14] antes do final do mês, um rigoroso bloqueio (*lockdown*) foi estabelecido em Wuhan, que ficou completamente isolada do resto do país.[15] Em 30 de janeiro de 2020, quando pacientes com o vírus haviam sido diagnosticados em 18 países para além da China, a Organização Mundial da Saúde (OMS) declarou o novo surto de coronavírus uma emergência de saúde pública de interesse internacional sob o Regulamento Sanitário Internacional.[16] À medida que mais informações sobre o vírus e sua doença foram sendo descobertas, a rápida identificação de casos e o rastreamento de contatos logo se tornaram estratégias essenciais para uma política de saúde pública. Com um período médio de incubação de 3 a 9 dias[17] e evidência de transmissão pré-sintomática,[18] isolar indivíduos potencialmente infectados antes que eles continuem a disseminar a doença tornou-se um desafio complexo para autoridades de saúde pública e governos em todo o mundo.

São muitos os desafios do rastreamento de contatos "analógico". Primeiramente, o processo de conduzir entrevistas individuais é demorado e, em contextos nos quais o número de casos diários está aumentando, pode rapidamente sobrecarregar as autoridades de saúde. Em segundo lugar, as informações prestadas pelos entrevistados sobre os locais que visitaram e as pessoas com quem estiveram em contato em um determinado período de tempo estão sujeitas a imprecisões diversas por conta de lapsos de memória.[19] Ainda, por motivos variados, as pessoas podem mentir ou omitir informações sobre seu paradeiro e encontros, ou podem não querer se apresentar para realizar uma entrevista de rastreamento de contatos. A Coreia do Sul foi confrontada com esse desafio em maio de 2020, quando um surto do vírus no bairro boêmio de Itaewon, em Seul, em bares e clubes conhecido por atender a população LGBTQ +, infectou mais de 200 pessoas.[20] Devido ao estigma enfrentado por essa comunidade, muitos sul-coreanos ficaram relutantes em fazer o teste

de Covid-19 e relatar que haviam estado nos estabelecimentos noturnos do bairro, receosos que isso pudesse levar a especulações sobre sua sexualidade. O prefeito de Seul garantiu o anonimato de todos aqueles que solicitassem testagem em conexão com o *cluster* de Itaewon, mas a população permaneceu apreensiva com a possibilidade de violações de privacidade.[21]

Tornou-se cada vez mais evidente a importância da detecção rápida de novos casos nos primeiros momentos de um surto, para evitar que *clusters* de pequena escala evoluíssem para um cenário de transmissão comunitária sustentada. De acordo com a OMS, a "vigilância, equipes de resposta rápida e investigação de casos" é um dos principais pilares na preparação e planejamento da resposta à Covid-19.[22] Enquanto milhares de pessoas foram contratados para trabalhar como rastreadoras de contatos,[23] muitos países também recorreram à tecnologia e vigilância em busca de uma solução. Aplicativos de rastreamento de contatos desenvolvidos para smartphones irão rastrear a localização de seus usuários e prometem alertá-los quando eles entrarem em contato próximo com alguém infectado pelo vírus; assim, indivíduos potencialmente expostos poderiam rapidamente realizar o teste de contaminação e prevenir contágio posterior.

3 Aplicativos de rastreamento de contatos e questões de privacidade

Aplicativos de rastreamento de contatos já foram lançados por dezenas de países ao redor do mundo, com arquiteturas e abordagens variadas para privacidade de dados. Enquanto a maioria dos países têm tentado encorajar seus cidadãos a instalarem os softwares, governos com inclinações mais autoritárias tornaram seu download obrigatório. Algumas das principais questões de privacidade a serem consideradas são a possibilidade de que terceiros obtenham acesso às Informações de Identificação Pessoal (IIP) e localização dos cidadãos, e as maneiras com que esses dados podem ser usados pelos governos quando a pandemia acabar, ou para outros fins que não o controle epidemiológico. Abordaremos, resumidamente, alguns aspectos sobre arquitetura de sistema e gerenciamento de dados para indicar possíveis implicações para a privacidade dos usuários.

A essência do rastreamento de contato automatizado são os dados de localização, que são coletados por meio de uma série de tecnologias diferentes que podem identificar a localização absoluta ou relativa do usuário. Os sistemas baseados em dados de localização absoluta (coletados por meio de localização GPS, pontos de acesso a WiFi ou torres de celular) monitoram o movimento dos usuários constantemente e são amplamente considerados mais intrusivos em termos de privacidade pessoal; entretanto, embora ofereçam uma visão ampla dos padrões de mobilidade dos indivíduos, os dados gerados podem não ser suficientemente precisos para determinar um contato próximo para fins epidemiológicos. Por outro lado, dados de localização relativa obtidos por meio do emparelhamento de dois dispositivos com tecnologia *Bluetooth* podem oferecer informações mais precisas, mas exigem que uma grande porcentagem da população instale o aplicativo para serem eficazes.[24] Além disso, a estimativa da distância pode variar a depender do nível de potência da transmissão do sinal *Bluetooth*, que varia em telefones diferentes; ainda, os padrões de transmissão de um mesmo dispositivo podem ser afetados pelo uso de uma capa de proteção do aparelho, ou pela orientação da antena do celular.[25] Sobre a eficiência dos aplicativos de rastreamento de contato em relação à estimativa de proximidade, Ahmed *et al.* concluíram que:

> Afirmações sobre uma precisão "garantida" na ordem de 1 metro por qualquer aplicativo atual devem, portanto, ser consideradas com algum ceticismo. [...] com as técnicas usadas pelos aplicativos atuais para estimativa de proximidade, ainda haveria muitos falsos

positivos e falsos negativos. A estimativa de proximidade pode indicar um contato próximo quando o contato real está distante, ou indicar erroneamente que está distante quando está próximo. Da mesma forma, um contato próximo percebido pela estimativa de distância nem sempre se traduz em um cenário de exposição, pois pode haver uma parede ou obstrução entre os dois indivíduos (por exemplo, dois apartamentos adjacentes), ou o contato pode ser ocorrido em um espaço ao ar livre, onde as chances de infecção são mais baixas. No entanto, obter falsos positivos não é tão desastroso, resultando apenas em testes adicionais para esses casos falsos. Os falsos negativos são um problema mais significativo, pois são considerados uma oportunidade perdida de registrar contato com um caso positivo.[26]

Os tipos de arquitetura de sistema mais comumente adotados para a coleta desses dados são as abordagens centralizada, descentralizada e híbrida, que exploraremos brevemente. A principal característica da arquitetura centralizada é o servidor central que armazena Informações de Identificação Pessoal criptografadas, gera identificações temporárias que preservam a privacidade (TempID) para cada dispositivo registrado, realiza análise de risco e notifica contatos próximos de um indivíduo infectado.[27] Os dados armazenados pelo servidor central, portanto, incluem informações pessoais dos usuários como seus nomes, números de telefone, faixa etária e CEP, bem como as suas TempIDs e também os contatos próximos de cada um dos casos positivos.[28] Um ataque ao servidor, portanto, pode colocar em risco a privacidade de todos os usuários e seus respectivos contatos.[29]

A arquitetura descentralizada visa prevenir vazamentos de dados evitando o acúmulo de responsabilidades em um único servidor. Nesse modelo, as atribuições são deslocadas para o dispositivo pessoal do usuário, que irá gerar um identificador anônimo e processar as notificações de exposição e a análise de risco.[30] Nesse cenário, os únicos dados armazenados pelo servidor são as *seeds* (ou "sementes") enviadas voluntariamente por usuários diagnosticados com o vírus.[31] Os smartphones, no entanto, tendem a ser menos seguros do que um servidor, e o usuário fica vulnerável a ter o seu dispositivo roubado ou ser coagido a conceder a terceiros acesso aos dados armazenados. Além disso, ataques maliciosos podem conseguir desanonimizar a informações pessoais dos usuários e, baixando as *seeds* enviadas ao servidor, identificar os usuários positivos para a Covid-19, se invasores obtiverem acesso a dados coletados a partir de informações de contexto de um canal paralelo.[32]

Por fim, o modelo híbrido compartilha as tarefas entre o servidor e o dispositivo do usuário: enquanto a geração e o gerenciamento dos identificadores temporários permanecem descentralizados, o processo de rastreamento em si (ou seja, análise de risco e notificação) é realizado pelo servidor.[33] Os dados armazenados pelo servidor incluem a identificação do dispositivo, *tokens* de encontro privado recebidos voluntariamente de casos positivos, metadados de casos positivos e *tokens* de encontro privado carregados por outros usuários para que o servidor realize uma análise de risco.[34] Contra o risco de desanonimização, o sistema híbrido "adota métodos avançados adicionais de aprimoramento de privacidade, como compartilhamento de segredo, problema decisional de Diffie-Hellman (DDH) e interseção de conjunto privado".[35]

Os aplicativos de rastreamento de contatos atualmente em desenvolvimento, ou já em uso, fizeram escolhas variadas no que se refere à arquitetura do sistema e outros recursos. Aplicativos como *TraceTogether*, implantado pelo governo de Singapura; *CovidSafe*, lançado pelo governo da Austrália; o aplicativo francês *Stop-Covid*; e *Aarogya Setu*, cujo download foi tornado obrigatório pelo governo indiano para certos segmentos da população[36], são todos

baseados na arquitetura centralizada.[37] Por outro lado, o sistema de notificação de exposição desenvolvido pela Apple e pelo Google adota um modelo descentralizado, assim como o aplicativo israelense *HaMagen*.[38]

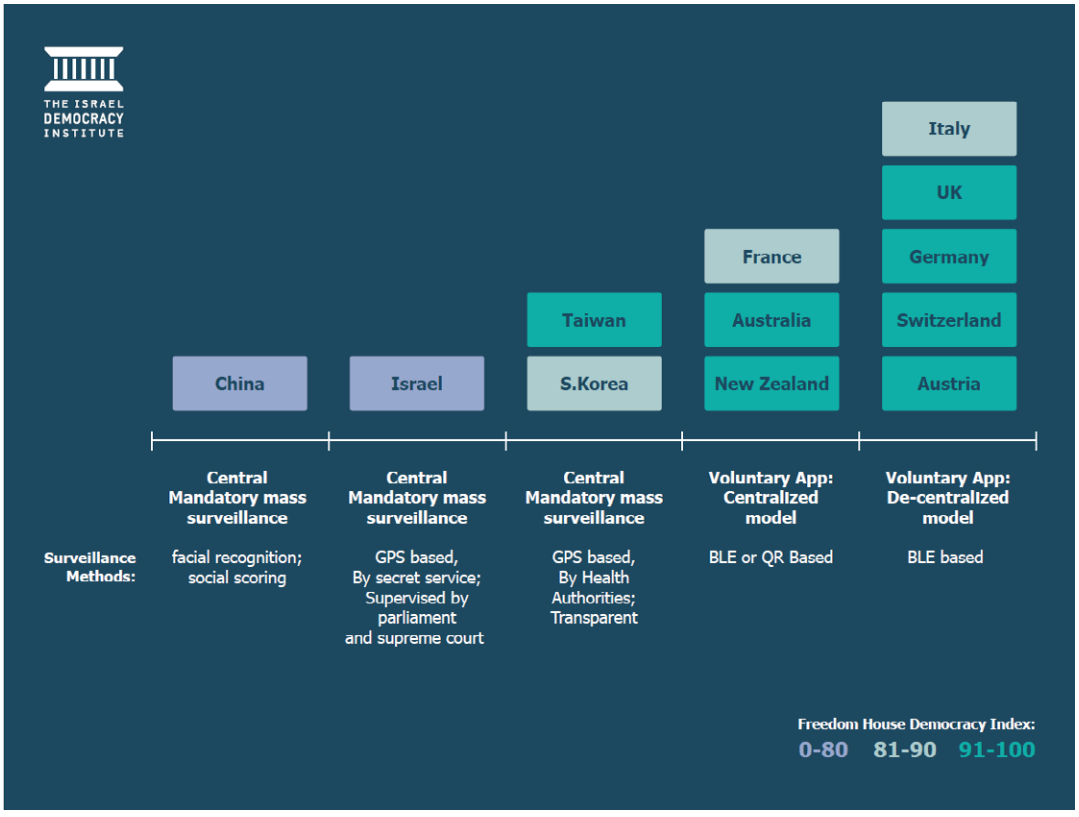
Outra questão relevante é a falta de transparência verificada na grande maioria dos aplicativos de rastreamento de contatos ativos atualmente, para os quais Ahmed *et al* sugerem duas abordagens principais. Primeiramente, o código fonte do aplicativo deve ser aberto e sujeito a revisões periódicas e auditorias externas e, em segundo lugar, a realização de uma Avaliação de Impacto na Proteção de Dados deve ser um requisito básico para todos os aplicativos em funcionamento.[39]

4 Métodos de vigilância e ameaças à privacidade do usuário

Embora qualquer tipo de coleta e armazenamento de dados apresente algum grau de risco para a privacidade de dados e liberdades individuais devido à impossibilidade de eliminar totalmente ameaças de vazamentos, ataques maliciosos ou uso indevido, é evidente que as ferramentas de vigilância empregadas por alguns países excedem a quantidade de monitoramento necessária para fins estritamente epidemiológicos. Abaixo, reproduzimos um gráfico produzido por Tehilla Shwartz Altshuler e Rachel Aridor Hershkovitz, pesquisadoras do Israel Democracy Institute, que lista uma variedade de métodos de vigilância, classificados de mais intrusivos a menos, adotados por vários países, apontando como esses estados se classificam no Índice de Democracia da *Freedom House*.

O gráfico apresenta variações, indo desde a vigilância centralizada, obrigatória e em massa da China, onde provedores de telecomunicações compartilham dados de usuários com autoridades e câmeras de reconhecimento facial identificam

Gráfico 1 – Índice de Democracia da *Freedom House*



Fonte: Israel Democracy Institute[40]

pedestres e medem sua temperatura corporal à distância, até os aplicativos descentralizados desenvolvidos por estados europeus, mais estritamente limitados pela legislação de proteção de dados, onde a coleta de dados de localização deve ser vinculada por consentimento ou anonimato.[41] A Coreia do Sul e Taiwan, apesar de serem relativamente bem classificados pela *Freedom House*, implantaram métodos extensivos de vigilância e coletaram dados de localização de maneira obrigatória. A experiência anterior com epidemias como a Sars e a gripe suína deixou um legado de legislação específica para epidemias que, em Taiwan, "autoriza o serviço de saúde a realizar amplos estudos epidemiológicos e impor sanções àqueles que se recusarem a cooperar com ele"[42] e, na Coréia do Sul, "autoriza que as pessoas se recusem a participar de uma investigação epidemiológica, mas [as sujeita] a sanções se essa recusa não for justificada"[43]. Em relação ao sistema chinês de vigilância em massa, o filósofo Byung-Chul Han observa:

> A consciência crítica diante da vigilância digital é praticamente inexistente na Ásia. Já quase não se fala de proteção de dados, incluindo Estados liberais como o Japão e a Coreia. Ninguém se irrita pelo frenesi das autoridades em recopilar dados. Enquanto isso a China introduziu um sistema de crédito social inimaginável aos europeus, que permitem uma valorização e avaliação exaustiva das pessoas. Cada um deve ser avaliado em consequência de sua conduta social. Na China não há nenhum momento da vida cotidiana que não esteja submetido à observação. Cada clique, cada compra, cada contato, cada atividade nas redes sociais são controlados. Quem atravessa no sinal vermelho, quem tem contato com críticos do regime e quem coloca comentários críticos nas redes sociais perde pontos. A vida, então, pode chegar a se tornar muito perigosa. Pelo contrário, quem compra pela Internet alimentos saudáveis e lê jornais que apoiam o regime ganha pontos. Quem tem pontuação suficiente obtém um visto de viagem e créditos baratos. Pelo contrário, quem cai abaixo de um determinado número de pontos pode perder seu trabalho. Na China essa vigilância social é possível porque ocorre uma irrestrita troca de dados entre os fornecedores da Internet e de telefonia celular e as autoridades. Praticamente não existe a proteção de dados. No vocabulário dos chineses não há o termo "esfera privada".[44]

Em Israel, embora o aplicativo HaMagen seja oferecido para download de forma voluntária, o país destacou o *Shin Bet*, seu serviço de segurança doméstica, para rastrear e monitorar a localização de indivíduos, sem seu consentimento, a fim de conter o contágio do vírus. O programa de rastreamento de contatos, que depende da vigilância de telefones celulares, foi interrompido em abril de 2020 pela Suprema Corte do país, que identificou graves violações aos direitos de privacidade.[45] Embora o governo israelense tenha argumentado que as medidas de emergência eram necessárias e que um aplicativo seria inútil para rastrear a comunidade ultraortodoxa do país, que não possui smartphones, a decisão legal determinou que uma alternativa compatível com a privacidade deveria ser produzida.[46] Dois meses depois, o *Knesset*, o Parlamento de Israel, aprovou uma lei autorizando o *Shin Bet* a continuar o rastreamento.[47] O país carece de uma legislação moderna de proteção à privacidade e tem uma "tendência inerente" de recorrer às forças de segurança em situações de emergência[48], o que aumenta a ameaça que a vigilância governamental representa para as liberdades individuais. Entre os países avaliados, agências de inteligência estavam envolvidas na coleta e rastreamento de dados apenas em Israel e na China.[49]

Altshuler e Hershkovitz refletem sobre as motivações e consequências da vigilância em massa empregada por Israel e outros países com tendências autoritárias:

> Países como China e Rússia viram a pandemia como uma oportunidade de ouro para expandir os poderes coercitivos do Estado sobre os cidadãos e usar a tecnologia para identificar, rastrear, adquirir conhecimento e intimidar. Quando a pandemia acabar, eles encontrarão outra desculpa e a vigilância intensificada continuará. Em Israel, também, a insistência obstinada dos tomadores de decisão no uso contínuo do GSS [General Security Service, ou Serviço de Segurança Geral] e rejeição das alternativas corroboram as afirmações sobre a ladeira escorregadia cujo fundo é imprevisível. Além disso, Israel se encontra na companhia de democracias iliberais como a Polônia, Turquia, Bulgária e Hungria, que exploraram o coronavírus para privar as pessoas de seus direitos civis e ignorar seus parlamentos e tribunais.[50]

Além disso, graves falhas de segurança e vigilância altamente intrusiva foram identificadas em outros países. Uma pesquisa recente da Anistia Internacional analisou aplicativos de rastreamento de contatos da Europa, Oriente Médio e Norte da África e realizou uma análise detalhada de softwares da Argélia, Bahrein, França, Islândia, Israel, Kuwait, Líbano, Noruega, Catar, Tunísia e Emirados Árabes Unidos, classificando-os quanto ao respeito pela privacidade dos usuários. A organização internacional destacou a ameaça representada pelas ferramentas de vigilância altamente invasivas empregadas pelos aplicativos *BeAware Bahrain*, desenvolvidos pelo governo bareinita, *Shlonik*, implantados pelo Kuwait, e *Smittestopp*, o aplicativo oficial de rastreamento de contatos da Noruega, todos os quais rastreiam a localização dos usuários em tempo real através do monitoramento GPS carregado em um servidor centralizado.[51] Recentemente, o governo norueguês interrompeu o uso do *Smittestopp*.[52]

A Anistia Internacional também identificou uma grave violação de segurança no aplicativo catari *EHTERAZ*, que "teria permitido que invasores cibernéticos acessassem informações pessoais altamente confidenciais, incluindo nome, identidade nacional, estado de saúde e dados de localização de mais de um milhão de usuários"[53]; após o alerta, o governo corrigiu a falha. A organização criticou os governos por apressar a implantação de aplicativos de rastreamento de contatos que "costumam ser mal projetados e carecem de proteção de privacidade"[54], ecoando as preocupações expressas por pesquisadores e ativistas de privacidade de dados em todo o mundo.

5 Sobre a efetividade dos aplicativos de rastreamento de contatos

Pesquisadores do University College London conduziram uma revisão sistemática[55] para avaliar a efetividade de sistemas de rastreamento de contato automatizados e parcialmente automatizados no controle da disseminação da Covid-19. A revisão sistemática foi publicada online em agosto de 2020 e identificou 4.036 estudos, 110 dos quais foram revisados e 15 dos quais foram incluídos na análise final e avaliação de qualidade. Os indicadores primários e secundários da revisão foram o número ou proporção de contatos (ou casos subsequentes) identificados, e indicadores de controle de surto, adesão, uso de recursos, relação custo-eficácia e lição aprendida.[56] Neste tópico, exploraremos suas principais descobertas.

Primeiramente, os estudos de modelagem mostraram que a eficácia do rastreamento de contato automatizado, como aquele realizado por aplicativos, depende de dois fatores. O primeiro é a adesão por uma parcela grande da população, que deve baixar os softwares e permitir que coletem seus dados; sobre o percentual necessário para garantir a eficácia, as estimativas dos estudos variam entre 56% e 95% da população. O segundo fator é a capacidade de assegurar que pessoas potencialmente expostas sejam postas em isolamento a tempo.[57] Os pesquisadores observam que eventos de falsos

positivos e falsos negativos podem ser influenciados por fatores como o uso de equipamentos de proteção individual, níveis de ventilação e separação por telas ou paredes não identificadas pela tecnologia de monitoramento de localização. São necessários mais dados do mundo real para avaliar a extensão do efeito desses fatores.[58]

Em relação à efetividade das arquiteturas de sistema, Braithwaite *et al.* indicam que:

> Os sistemas descentralizados de rastreamento de contatos automatizado se beneficiam do suporte da Apple e do Google, o que significa que a interoperabilidade entre países com tais aplicativos é provavelmente mais direta do que entre países que usam sistemas centralizados. No entanto, um estudo relatou que os sistemas centralizados avaliam o risco de transmissão com mais precisão (reduzindo o número de pessoas em quarentena), permitem uma melhor otimização, são menos suscetíveis a informes falsos e são avaliados mais prontamente.[59]

Os pesquisadores fazem referência a estudos acadêmicos sobre os riscos em que o rastreamento automatizado de contatos pode incorrer se os dados forem violados ou usados indevidamente, incluindo um aumento da vigilância e erosão da confiança pública, mas alertam que considerações de privacidade e compensações entre privacidade e utilidade não estão no escopo da revisão sistemática.

Além disso, diferentes estudos levantam preocupações sobre a exclusão digital, embora essas questões não estejam bem quantificadas atualmente. Especialmente em países de baixa renda, os grupos vulneráveis que podem estar em maior risco de infecção pela Covid-19 também podem ter menos probabilidade de possuir smartphones do que a população em geral. Os aplicativos de rastreamento de contato seriam, portanto, menos capazes de reduzir os riscos de transmissão nesses círculos, potencialmente ampliando seus riscos.[60] Embora apontem para a escassez de estudos empíricos sobre o rastreamento de contatos totalmente automatizado, os autores não identificaram nenhuma evidência empírica da efetividade do rastreamento de contato automatizado em relação à identificação de contatos ou redução da transmissão. Isso não quer dizer, é claro, que os aplicativos de rastreamento de contatos ou outras formas de rastreamento automatizado de contatos *não* sejam efetivos; mas, simplesmente, que sua efetividade potencial ainda não foi comprovada cientificamente.

Os pesquisadores listam indagações essenciais que devem ser investigadas por cientistas e ponderadas por formuladores de políticas públicas antes de implantar aplicativos de rastreamento de contatos. Essas questões incluem:

> [...] se as preocupações em torno da aceitabilidade e privacidade do público foram tratadas de forma adequada, com consulta pública apropriada; como um sistema automatizado será integrado com outras estratégias de rastreamento de contato e controle de doenças, em consulta com especialistas em saúde pública; e, talvez o mais importante, se é provável que [o sistema automatizado de rastreamento de contatos] seja eficaz, econômico e equitativo nesse contexto.[61]

Além disso, se tais aplicativos ou sistemas forem implantados, é essencial que eles sejam avaliados rigorosamente, "inclusive por meio de estudos prospectivos em grande escala com dimensões técnicas, de efetividade e de equidade", bem como que sejam realizados "estudos qualitativos para melhorar a compreensão sobre as principais questões sociais e dimensões comportamentais do uso do aplicativo e adesão."[62]

6 Conclusão

Neste artigo, examinamos o contexto

atual de crescente vigilância governamental e autoritarismo digital. O capitalismo de vigilância, formulação de Shoshana Zuboff, nos ajuda a entender como os dados e informações pessoais são usados não apenas para prever nossos desejos e necessidades, mas para direcionar o comportamento do usuário para resultados mais lucrativos para as empresas. Além disso, o autoritarismo digital é uma perigosa tendência em ascensão entre os governos, especialmente entre as democracias mais fragilizadas. O monitoramento e a vigilância são frequentemente usados para conter a dissidência e perseguir oponentes políticos, e outras ferramentas tecnológicas são empregadas para prever e tomar decisões em torno de questões sociais, políticas e econômicas relevantes sem a transparência ou consentimento apropriado. No contexto da pandemia do coronavírus, surgiu a necessidade do rastreamento de contatos para prevenir a transmissão do vírus e, frente aos desafios colocados pelo rastreamento de contatos manual ou analógico, os governos têm buscado soluções automatizadas. Uma vez que o processo de rastreamento automatizado de contatos é baseado no monitoramento de localização, essas ferramentas trazem graves implicações para a privacidade dos dados do usuário e para as liberdades individuais.

Examinamos alguns importantes aspectos dos aplicativos de rastreamento de contato, como a arquitetura de sistema e gerenciamento de dados, e oferecemos algumas considerações sobre efetividade e implicações de privacidade. A impossibilidade de produzir uma estimativa de proximidade suficientemente precisa é consistentemente apontada como um grande obstáculo. Baseando-nos em um estudo de Tehilla Shwartz Altshuler e Rachel Aridor Hershkovitz, comentamos sobre a variedade de métodos de vigilância empregados por estados que ocupam diferentes posições no Índice de Democracia da *Freedom House*. Enquanto leis mais rígidas sobre privacidade de dados tendem a desencorajar uma vigilância mais intrusiva na Europa, países como China e Rússia aumentaram a vigilância e o monitoramento durante a pandemia, intensificando as ameaças às liberdades e privacidade individuais. Países como Coreia do Sul e Taiwan também adotaram métodos de vigilância obrigatórios, enquanto Israel recorreu ao seu serviço de segurança nacional para rastrear e monitorar a localização de seus cidadãos, apesar de uma decisão da Suprema Corte que ordenou a suspensão do programa devido a graves violações aos direitos de privacidade.

Uma revisão sistemática conduzida por pesquisadores do University College London, publicada em agosto de 2020, examinou milhares de estudos sobre rastreamento automatizado de contatos para conter a disseminação da Covid-19 e não encontrou qualquer evidência empírica de sua efetividade, até o momento. Mais estudos são necessários para melhor compreendermos o impacto dessas políticas. Qualquer tipo de coleta e armazenamento de dados de localização representará algum grau de risco para a privacidade de dados, e a pressa com que muitos governos implementaram novas tecnologias de monitoramento e vigilância agrava muito esses riscos. Entendemos que mais investimentos em rastreamento automatizado de contatos e suas tecnologias de vigilância e monitoramento não devem ser realizados enquanto sua efetividade para fins epidemiológicos não for clara e a ameaça imposta para a privacidade do usuário, liberdades individuais e fortalecimento democrático for visível e bem documentada.

Referências

AHMED, Nadeem; MICHELIN, Regio A.; XUE, Wanli; RUJ, Sushmita; MALANEY, Robert; KANHERE, Salil S.; SENEVIRATNE, Aruna; HU, Wen; JANICKE, Helge; JHA, Sanjay K. A Survey of COVID-19 Contact Tracing Apps. **IEEE Access**, v. 8, p. 134577 - 134601, 2020.

ALTSHULER, Tehilla Shwartz; HERSHKOWITZ, Rachel Aridor. **Digital contact tracing and the coronavirus: Israeli and comparative perspectives**. Brookings. 2020a. Disponível em https://www.brookings.edu/wp-content/uploads/2020/08/FP_20200803_digital_contact_tracing.pdf

ALTSHULER, Tehilla Shwartz; HERSHKOWITZ, Rachel Aridor. **How Israel's COVID-19 mass surveillance operation works**. Brookings. 2020b. Disponível em https://www.brookings.edu/techstream/how-israels-covid-19-mass-surveillance-operation-works/

AMNESTY INTERNATIONAL. **Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy.** 16 jun 2020. Disponível em https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/

AMNESTY INTERNATIONAL. **Norway: Halt to COVID-19 contact tracing app a major win for privacy.** 15 jun 2020. Disponível em https://www.amnesty.org/en/latest/news/2020/06/norway-covid19-contact-tracing-app-privacy-win/

AMNESTY INTERNATIONAL. **Qatar: Contact tracing app security flaw exposed sensitive personal details of more than one million.** 26 mai 2020. Disponível em https://www.amnesty.org/en/latest/news/2020/05/qatar-covid19-contact-tracing-app-security-flaw/

BORGESIUS, Frederik J. Z.;MÖLLER, Judith; KRUIKEMEIER, Sanne; Ó FATHAIGH, Ronan; IRION, Kristina; DOBBER, Tom; BODO, Balazs; DE VREESE, Claes. Online Political Microtargeting:

Promises and Threats for Democracy. **Utrecht Law Review**, v. 14, n. 1, p. 82 - 96, 2018.

BRAITHWAITE, Isobel; CALLENDER, Thomas; BULLOCK, Miriam; ALDRIDGE, Robert W. Automated and partly automated contact tracing: a systematic review to inform the control of COVID-19. **Lancet Digital Health**, v. 2, n. 11, nov 2020, p. 607- 621.

CADWALLADR, Carole; GRAHAM-HARRISON, Emma. **Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach**. The Guardian. 17 mar 2018. Disponível em https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

GORBALENYA, Alexander E.; BAKER, Susan C.; BARIC, Ralph S. et al. The species Severe acute respiratory syndrome-related coronavirus: classifying 2019-nCoV and naming it SARS-CoV-2. **Nature Microbiology**, v. 5, n.3, p. 536–544, mar 2020.

GALLOWAY, Scott. **The Four: The Hidden DNA of Amazon, Apple, Facebook, and Google**. New York: Random House, 2017, 448 p.

HAN, Byung-Chul. **O coronavírus de hoje e o mundo de amanhã, segundo o filósofo Byung-Chul Han**. El País Brasil. Mar 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

HE, Xi; LAU, Eric H.Y.; WU, Peng; et al. Temporal dynamics in viral shedding and transmissibility of COVID-19. **Nature Medicine**, v. 26, p. 672–675, abr 2020.

HIGGINS, Julian; THOMAS, James (Eds.). **Cochrane Handbook for Systematic Reviews of Interventions**. 2nd ed., New Jersey: Wiley-Blackwell, 2019, 728 p.

KIM, Nemo. **South Korea struggles to contain new outbreak amid anti-gay backlash**. The Guardian. 11 mai 2020. Disponível em https://www.theguardian.com/world/2020/may/11/south-korea-struggles-to-contain-new-outbreak-amid-anti-lgbt-backlash

LAPOWSKY, Issie. **Facebook Exposed 87 Million Users to Cambridge Analytica**. Wired. 4 abr 2018. Disponível em https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/

POLYAKOVA, Alina; MESEROLE, Chris. **Exporting digital authoritarianism: The Russian and Chinese models**. Brookings, 2019. Disponível em https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf

PRIVACY INTERNATIONAL. **India's contact tracing app will be voluntary in theory but mandatory in practice.** Abr 2020. Disponível em https://privacyinternational.org/examples/3769/indias-contact-tracing-app-will-be-voluntary-theory-mandatory-practice

PRIVACY INTERNATIONAL. **Israel's coronavirus surveillance is an example for others - of what not to do**. Mai 2020. Disponível em https://privacyinternational.org/long-read/3747/israels-coronavirus-surveillance-example-others-what-not-do

QIN, Amy; WANG, Vivian. **Wuhan, Center of Coronavirus Outbreak, Is Being Cut Off by Chinese Authorities**. New York Times. 24 jan 2020. Disponível em https://www.nytimes.com/2020/01/22/world/asia/china-coronavirus-travel.html

SIMMONS-DUFFIN, Selena. **States Nearly Doubled Plans For Contact Tracers Since NPR Surveyed Them 10 Days Ago**. NPR. 7 mai 2020. Disponível em https://www.npr.org/sections/health-shots/2020/04/28/846736937/we-asked-all-50-states-about-their-contact-tracing-capacity-heres-what-we-learne

SIORDIA JR, Juan A. Epidemiology and clinical features of COVID-19: A review of current literature. **Journal of Clinical Virology**, v. 127, jun 2020.

TANG, Qiang. Privacy-Preserving Contact Tracing: current solutions and open questions. **arXiv:2004.06818**, p. 1 -18, 2020.

TAN, Wenjie; ZHAO, Xiang; MA, Xuejun et al. Notes from the Field: A Novel Coronavirus Genome Identified in a Cluster of Pneumonia Cases — Wuhan, China 2019-2020. **China CDC Weekly**, v. 2, n. 2, p. 61 - 62, jan 2020.

TEACHOUT, Zephyr. **Break 'Em Up: Recovering Our Freedom from Big Ag, Big Tech, and Big Money**. New York: All Points Books, 2020, 320 p.

THE 2019-NCOV OUTBREAK JOINT FIELD EPIDEMIOLOGY INVESTIGATION TEAM; LI, Qun. Notes from the Field: An Outbreak of NCIP (2019-nCoV) Infection in China — Wuhan, Hubei Province, 2019-2020. **China CDC Weekly**, v. 2, n. 5, p. 79 - 80, jan 2020.

THE KOREA HERALD. **Itaewon cluster grows to 237, six-stage transmission confirmed**. 25 mai 2020. Disponível em http://www.koreaherald.com/view.php?ud=20200525000683

TINDALE, Lauren; COOMBE, Michelle; STOCKDALE, Jessica E.; et al. Evidence for transmission of COVID-19 prior to symptom onset. **eLife**, v. 9, jun 2020

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**. New York: PublicAffairs, 2019, 704 p.

WONG, Julia Carrie; SOLON, Olivia. **US government demands details on all visitors to anti-Trump protest website**. The Guardian, 2017. Disponível em https://www.theguardian.com/world/2017/aug/14/donald-trump-inauguration-protest-website-search-warrant-dreamhost

WORLD HEALTH ORGANIZATION. **Pneumonia of unknown cause – China.** 2020a. Disponível em https://www.who.int/csr/don/05-january-2020-pneumonia-of-unkown-cause-china/en/.

WORLD HEALTH ORGANIZATION. **WHO Director-General's statement on IHR Emergency Committee on Novel Coronavirus (2019-nCoV)**. 2020b. Disponível em https://www.who.int/dg/speeches/detail/who-director-general-s-statement-on-ihr-emergency-committee-on--novel-coronavirus-(2019-ncov).

WORLD HEALTH ORGANISATION. **COVID-19 Strategic Preparedness and Response Plan: Operational Planning Guidelines To Support Country Preparedness And Response**. 2020c. Disponível em https://www.who.int/docs/default-source/coronaviruse/covid-19-sprp-unct-guidelines.pdf?sfvrsn=81ff43d8_4

Notas

1 CADWALLADR, Carole; GRAHAM-HARRISON, Emma. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach**. The Guardian**. 17 mar. 2018.

2 LAPOWSKY, Issie. Facebook Exposed 87 Million Users to Cambridge Analytica. Wired. 4 abr 2018.

3 BORGESIUS, Frederik J. Z.;MÖLLER, Judith; KRUIKEMEIER, Sanne; Ó FATHAIGH, Ronan; IRION, Kristina; DOBBER, Tom; BODO, Balazs; DE VREESE, Claes. Online Political Microtargeting: Promises and Threats for Democracy. **Utrecht Law Review**, v. 14, n. 1, p. 82 - 96, 2018.

4 As empresas dominantes no setor de tecnologia da informação, muitas vezes referidas como *Big Four / Five* em referência à Amazon, Google, Facebook, Apple e às vezes Microsoft.

5 GALLOWAY, Scott. **The Four: The Hidden DNA of Amazon, Apple, Facebook, and Google**. New York: Random House, 2017, 448 p. and TEACHOUT, Zephyr. **Break 'Em Up: Recovering Our Freedom from Big Ag, Big Tech, and Big Money**. New York: All Points Books, 2020, 320 p.

6 Tradução nossa. No original: "new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales". ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**. New York: PublicAffairs, 2019, p. 1.

7 Tradução nossa. No original: "in which automated machine processes not only know our behavior but also shape our behavior at scale". Ibidem, p. 8.

8 POLYAKOVA, Alina; MESEROLE, Chris. **Exporting digital authoritarianism: The Russian and Chinese models.** Brookings, 2019. and WONG, Julia Carrie. Sobre autoritarismo digital nos Estados Unidos, ver SOLON, Olivia. **US government demands details on all visitors to anti-Trump protest website.** The Guardian, 2017.

9 Tradução nossa. No original: "[...] authorities cited COVID-19 to justify expanded surveillance powers and the deployment of new technologies that were once seen as too intrusive. The public health crisis has created an opening for the digitization, collection, and analysis of people's most intimate data without adequate protections against abuses. Governments and private entities are ramping up their use of artificial intelligence (AI), biometric surveillance, and big-data tools to make decisions that affect individuals' economic, social, and political rights. Crucially, the processes involved have often lacked transparency, independent oversight, and avenues for redress. These practices raise the prospect of a dystopian future in which private companies, security agencies, and cybercriminals enjoy easy access not only to sensitive information about the places we visit and the items we purchase, but also to our medical histories, facial and voice patterns, and even our genetic codes." SHAHBAZ, Adrian; FUNK, Allie. **Freedom on the Net 2020: The Pandemic's Digital Shadow.** Freedom House.

10 WORLD HEALTH ORGANIZATION. **Pneumonia of unknown cause – China**. 2020a.

11 GORBALENYA, Alexander E.; BAKER, Susan C.; BARIC, Ralph S. et al. The species Severe acute respiratory syndrome-related coronavirus: classifying 2019-nCoV and naming it SARS-CoV-2. **Nature Microbiology**, v. 5, n.3, p. 536–544, mar 2020.

12 TAN, Wenjie; ZHAO, Xiang; MA, Xuejun et al. Notes from the Field: A Novel Coronavirus Genome Identified in a Cluster of Pneumonia Cases — Wuhan, China 2019□2020. **China CDC Weekly**, v. 2, n. 2, p. 61 - 62, jan 2020.

13 THE 2019-NCOV OUTBREAK JOINT FIELD EPIDEMIOLOGY INVESTIGATION TEAM; LI, Qun. Notes from the Field: An Outbreak of NCIP (2019-nCoV) Infection in China — Wuhan, Hubei Province, 2019□2020. **China CDC Weekly**, v. 2, n. 5, p. 79 - 80, jan 2020.

14 Op. cit. WORLD HEALTH ORGANIZATION, 2020a.

15 QIN, Amy; WANG, Vivian. **Wuhan, Center of Coronavirus Outbreak, Is Being Cut Off by Chinese Authorities**. New York Times. 24 jan 2020.

16 WORLD HEALTH ORGANIZATION. **WHO Director-General's statement on IHR Emergency Committee on Novel Coronavirus (2019-nCoV)**. 2020b.

17 SIORDIA JR, Juan A. Epidemiology and clinical features of COVID-19: A review of current literature. **Journal of Clinical Virology**, v. 127, jun 2020.

18 TINDALE, Lauren; COOMBE, Michelle; STOCKDALE, Jessica E.; et al. Evidence for transmission of COVID-19 prior to symptom onset. **eLife**, v. 9, jun 2020 and HE, Xi; LAU, Eric H.Y.; WU, Peng; et al. Temporal dynamics in viral shedding and transmissibility of COVID-19. Nature Medicine, v. 26, p. 672–675, abr 2020.

19 AHMED, Nadeem; MICHELIN, Regio A.; XUE, Wanli; RUJ, Sushmita; MALANEY, Robert; KANHERE, Salil S.; SENEVIRATNE, Aruna; HU, Wen; JANICKE, Helge; JHA, Sanjay K. A Survey of COVID-19 Contact Tracing Apps. **IEEE Access**, v. 8, p. 134577 - 134601, 2020.

20 THE KOREA HERALD. **Itaewon cluster grows to 237, six-stage transmission confirmed**. 25 mai 2020.

21 KIM, Nemo. **South Korea struggles to contain new outbreak amid anti-gay backlash**. The Guardian. 11 maio 2020.

22 WORLD HEALTH ORGANISATION**. COVID-19 Strategic Preparedness and Response Plan: Operational Planning Guidelines To Support Country Preparedness And Response**. 2020c.

23 SIMMONS-DUFFIN, Selena. **States Nearly Doubled Plans For Contact Tracers Since NPR Surveyed Them 10 Days Ago**. NPR. 7 maio 2020.

24 TANG, Qiang. Privacy-Preserving Contact Tracing: current solutions and open questions. **arXiv:2004.06818.** 2020, p. 6.

25 Op. cit. AHMED, Nadeem *et al*, p. 134586.

26 Tradução nossa. No original: "Claims of "guaranteed" accuracy of order 1m by any current app should therefore be considered with some scepticism. [...] with the techniques used by current apps for proximity estimation, there would still be many false positives and false negatives. The proximity estimate may indicate close contact, whereas the actual contact is far off or erroneously indicates that it is far off when it is nearby. Similarly, a close contact as perceived by distance estimation does not always translate into an exposed case as there may be a wall/obstruction between the two individuals (e.g., two adjacent apartments), or the contact has occurred in open space where chances of infection are lower. However, getting false positives is not as disastrous, as they only result in additional tests for these false cases. False negatives are a more significant issue as these are considered a missed opportunity to register contact with a positive case." Ibid., p. 134586.

27 Op. cit. AHMED, Nadeem *et al*, p. 134584.

28 Ibid.

29 Ibid., p. 134585

30 p. 134580 - 134582

31 p. 134584

32 Ibid., p. 134585

33 p. 134580-134583

34 p. 134584

35 Ibid., p. 134585. Para mais informações sobre os referidos métodos adicionais de aprimoramento de privacidade, ver SHAMIR, A. 'How to share a secret. Commun, ACM, v. 22, n. 11, p. 612–613, Nov. 1979.; BONEH, D.'The decision diffie-hellman problem. Algorithmic Number Theory. Berlin: Springer, p. 48–63, 1998; e DE CRISTOFARO, E.; TSUDIK, G. Practical private set intersection protocols with linear complexity. Proc. Int. Conf. Financial Cryptogr. Data Secur. Springer, pp. 143–159, 2010.

36 PRIVACY INTERNATIONAL. **India's contact tracing app will be voluntary in theory but mandatory in practice**. abr 2020.

37 Op. cit. AHMED, Nadeem *et al*, p. 134590-134592.

38 Ibid., p. 13492 - 134594.

39 Ibid., p. 13497.

40 ALTSHULER, Tehilla Shwartz; HERSHKOWITZ, Rachel Aridor. **Digital contact tracing and the coronavirus: Israeli and comparative perspectives.** Brookings. 2020a.

41 Op. cit. ALTSHULER, Tehilla Shwartz; HERSHKOWITZ, Rachel Aridor, 2020a, p. 7.

42 Ibid, p. 8.

43 Ibid.

44 HAN, Byung-Chul. **O coronavírus de hoje e o mundo de amanhã, segundo o filósofo Byung-Chul Han**. El País Brasil. Mar. 2020.

45 PRIVACY INTERNATIONAL. **Israel's coronavirus surveillance is an example for others - of what not to do**. Mai 2020.

46 ALTSHULER, Tehilla Shwartz; HERSHKOWITZ, Rachel Aridor. **How Israel's COVID-19 mass surveillance operation works**. Brookings. 2020b.

47 STAFF, Toi. **Knesset passes law authorizing Shin Bet tracking of virus carriers until January.** The Times of Israel. Jul. 2020.

48 Op. cit. ALTSHULER, Tehilla Shwartz; HERSHKOWITZ, Rachel Aridor, 2020a, p. 9.

49 Ibid., p. 13.

50 Tradução nossa. No original: "Countries such as China and Russia saw the pandemic as a golden opportunity to expand the state's coercive powers over citizens and to use technology in order to identify, track, acquire knowledge, and intimidate. When the pandemic dies down, they will find some other excuse, and the heightened surveillance will continue. In Israel, too, the decisionmakers' obstinate insistence on continued use of the GSS [General Security Service] and rejection of alternatives corroborate the claims about the slippery slope whose bottom is unpredictable. In addition, Israel finds itself in the company of illiberal democracies such as Poland, Turkey, Bulgaria, and Hungary, which exploited the coronavirus in order to strip people of their civil rights and to ignore their parliaments and courts". Op. cit. ALTSHULER, Tehilla Shwartz; HERSHKOWITZ, Rachel Aridor. 2020a. p. 16 - 17.

51 AMNESTY INTERNATIONAL. **Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy**. 16 jun 2020.

52 AMNESTY INTERNATIONAL. **Norway: Halt to COVID-19 contact tracing app a major win for privac**y. 15 jun 2020.

53 AMNESTY INTERNATIONAL. Qatar: **Contact tracing app security flaw exposed sensitive personal details of more than one million.** 26 mai 2020.

54 Ibid.

55 De acordo com o Cochrane Handbook for Systematic Reviews of Interventions (2011), as revisões sistemáticas "tentam reunir todas as evidências empíricas que se enquadram em critérios de elegibilidade pré-especificados para responder a uma questão de pesquisa específica. Elas usam métodos explícitos e sistemáticos que são selecionados com o objetivo de minimizar o viés, fornecendo, assim, resultados mais confiáveis a partir dos quais podem conclusões podem ser tiradas e decisões, tomadas". Tradução nossa.

56 BRAITHWAITE, Isobel; CALLENDER, Thomas; BULLOCK, Miriam; ALDRIDGE, Robert W. Automated and partly automated contact tracing: a systematic review to inform the control of COVID-19. **Lancet Digital Health**, v. 2, n. 11, nov 2020, p. 607- 621.

57 Ibid.

58 Ibid., p. 618.

59 Ibid., p. 619.

60 Ibid.

61 Tradução nossa. No original: "whether concerns around public acceptability and privacy have been adequately addressed, with appropriate public consultation; how an automated system will be integrated with other contact-tracing and disease control strategies, in consultation with public health experts; and, perhaps most importantly, whether it is likely to be effective, cost-effective, and equitable in that context". Ibid.

62 Ibid.