Panorama Setorial da Internet

Número 4
Dezembro, 2021
Ano 13

Privacidade e proteção de dados durante a pandemia

Proteção de dados pessoais em tempos de pandemia: novos paradigmas para o compartilhamento e o uso secundário de dados no poder público[1]

Por Miriam Wimmer[2]

O alastramento do novo coronavírus pelo planeta acarretou o rápido surgimento de estratégias para o monitoramento e a contenção de sua disseminação, caracterizando-se a atuação dos governos por dois importantes aspectos: de um lado, pelo uso inédito, em termos de intensidade, de tecnologias digitais e de dispositivos móveis de comunicação nos processos de detecção, notificação e investigação da doença; de outro, pela veloz escalada na coleta, análise e compartilhamento de dados pessoais entre atores públicos e privados, assim como entre diferentes órgãos e entidades governamentais.

No Brasil, tais acontecimentos reacenderam o debate acerca dos limites e das possibilidades de tratamento de dados pessoais no setor público, reavivando a discussão sobre os critérios para seu compartilhamento e uso secundário, isto é, a utilização de dados pessoais para finalidades distintas daquelas que justificaram a sua coleta original. Trata-se de questão controversa, visto que as normas de proteção de dados pessoais incluem a ideia de que o tratamento deve ser realizado para propósitos específicos informados ao titular dos dados, sem que, em regra, seja possível efetuar um tratamento posterior de forma incompatível com os objetivos inicialmente estabelecidos. Conhecido como "princípio da finalidade", esse fundamento foi também consagrado na legislação brasileira sobre proteção de dados pessoais[3].

Ainda que a temática do compartilhamento de dados pessoais envolvendo o poder público já tivesse sido tratada pelo Supremo Tribunal Federal (STF), o ano de 2020 caracterizou-se pelo amadurecimento desse debate por parte do órgão, com o reconhecimento de um novo direito fundamental à proteção de dados pessoais[4] e a aplicação de tal compreensão em um julgamento subsequente sobre o compartilhamento de dados no âmbito do poder Executivo. A partir desse cenário, considerando-se a intensificação da utilização de dados pessoais decorrente da pandemia COVID-19 e as recentes manifestações do STF sobre o tema, este artigo busca investigar possíveis critérios e parâmetros capazes de balizar de modo legítimo o compartilhamento e o uso secundário de dados pessoais no poder público, tendo como referência a interpretação do princípio da finalidade.

---

[1] Versão editada do artigo "Limites e possibilidades para o uso secundário de dados pessoais no poder público: lições da pandemia", publicado originalmente na *Revista Brasileira de Políticas Públicas*, vol. 11, n. 1 (2021).
Disponível em: https://www.publicacoes.uniceub.br/RBPP/article/view/7136

[2] Doutora em Comunicação pela Universidade de Brasília (UnB) e mestre em Direito Público pela Universidade do Estado do Rio de Janeiro (Uerj), é professora da Faculdade de Direito do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP) em Brasília.

[3] Conforme o artigo 6º, inciso I, da Lei n. 13.709, de 2018: "finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades". Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[4] Muito embora a Constituição Federal já reconhecesse e assegurasse a proteção à intimidade e à vida privada, o STF reconheceu em 2020 um direito fundamental à proteção de dados pessoais que transcende tal preceito. O direito à proteção de dados não se refere apenas a dados íntimos ou privados, tampouco se confunde com o direito ao sigilo, mas se pauta pela ideia de autodeterminação informativa, com base no direito fundamental à dignidade da pessoa humana.

Foto: Diego Canabarro

Miriam Wimmer
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP).

A pandemia COVID-19 e o compartilhamento de dados no poder público: iniciativas e reações

Uma consequência indiscutível da pandemia COVID-19 foi a intensificação do compartilhamento de dados pessoais. Globalmente, as iniciativas de combate à crise sanitária fizeram uso expressivo de ferramentas tecnológicas com vistas ao monitoramento, à contenção e à mitigação da disseminação do vírus. Dada a possibilidade técnica de utilizar os dados de geolocalização oriundos de terminais celulares, diversos países criaram "mapas de calor" a partir de dados anonimizados e agregados, com o objetivo de identificar locais com aglomeração de pessoas, observar padrões de deslocamento e estimar o nível de isolamento social da população. Foram adotadas também estratégias para controlar de maneira individualizada a observância da quarentena por parte de pessoas infectadas ou com suspeitas de infecção, além de medidas voltadas ao uso de aplicativos de rastreamento de contato com base na emissão de sinais Bluetooth.

Também no Brasil esse fenômeno pôde ser observado. Diversos estados da federação entabularam parcerias com empresas de tecnologia e prestadoras de serviços de telecomunicações para monitorar os índices de isolamento social e definir estratégias de combate ao coronavírus a partir da análise de dados de localização anonimizados e agregados. Os questionamentos judiciais a medidas desse tipo acabaram por não prosperar, entendendo o poder Judiciário que nesse caso não havia risco aos direitos dos cidadãos por estes não serem passíveis de identificação individual.

No entanto, os impactos da pandemia global quanto à escalada na coleta, análise e compartilhamento de dados pessoais não se limitaram estritamente às ações para o seu enfrentamento. De fato, a crise sanitária forçou a súbita migração de inúmeras atividades para o ambiente digital e a aceleração de projetos de transformação digital que já estavam em curso. Tais mudanças foram sentidas de modo bastante intenso pelo próprio poder público, que se viu compelido a intensificar esforços para a digitalização de seus serviços com vistas à continuidade do exercício de suas atribuições legais.

No Brasil, iniciativas de governo digital vinham sendo desenvolvidas há anos. Não existem dúvidas, entretanto, de que a pandemia imprimiu novo ritmo e sentido de urgência à transformação digital, inclusive por conta da necessidade de viabilizar o pagamento do auxílio emergencial instituído pela Lei n. 13.982, de 2020[5]. Como não poderia deixar de ser, a migração de serviços e processos para o ambiente digital veio acompanhada de crescentes demandas por coleta, análise, compartilhamento e cruzamento de dados pessoais no âmbito do poder público.

Nesse contexto, a implementação de soluções tecnológicas de enfrentamento à COVID-19 foi recebida com cautela por entidades voltadas à proteção de dados pessoais, incluindo muitos casos de questionamentos judiciais. Autoridades de proteção de dados pessoais de diversos países europeus e o próprio Comitê Europeu para a Proteção de Dados[6] indicaram não haver incompatibilidade entre proteção de dados pessoais e medidas de combate à pandemia, sendo o arcabouço normativo da Europa suficientemente flexível para assegurar a possibilidade de compartilhamento dos

[5] A Lei em questão instituiu medidas excepcionais de proteção social a serem adotadas durante a pandemia, incluindo o pagamento de um auxílio financeiro no valor de R$600,00, durante três meses, a cidadãos de baixa renda.

[6] Em abril de 2020, a organização, que reúne representantes das autoridades de proteção de dados dos países da Europa, adotou as "Diretrizes 4/2020 sobre a utilização de dados de localização e meios de rastreio de contactos no contexto do surto de COVID-19". Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_pt.pdf

dados relevantes ao efetivo enfrentamento da situação emergencial. Por outro lado, sublinharam a importância de que critérios de adequação, necessidade e proporcionalidade fossem observados, de maneira a limitar as ferramentas adotadas à sua finalidade específica e ao período de tempo estritamente necessário, excluindo-se a possibilidade de tratamento posterior dos dados coletados para finalidades não relacionadas com a gestão da crise sanitária.

No entanto, quando se trata das iniciativas dedicadas à aceleração da migração de serviços e processos públicos rotineiros para o ambiente digital – fruto indireto da pandemia –, a discussão assume nuances distintas. De fato, a transformação digital de serviços de governo costuma ser concebida como um "caminho sem volta". Assim, elementos como a limitação temporal do tratamento de dados pessoais ao período da pandemia e a utilização desses dados apenas para a finalidade específica de combate à COVID-19 são passíveis de questionamento, especialmente quando se verifica que os dados coletados e os compartilhamentos realizados podem ser úteis para outras finalidades públicas, diferentes daquelas que justificaram o tratamento original.

Renovação dos paradigmas: um novo direito fundamental e o reconhecimento de limites aos fluxos de dados pessoais no poder público

As demandas por compartilhamento de dados pessoais associadas à pandemia COVID-19 acabaram por precipitar uma discussão judicial sobre o tema no âmbito do STF, com impactos duradouros para a proteção de dados pessoais no Brasil. Ainda que o STF já tivesse se debruçado sobre o assunto de maneira menos aprofundada, o caso mais importante, sem dúvida, foi o da decisão do órgão de suspender os efeitos da Medida Provisória n. 954, de 2020, que determinava o compartilhamento de dados detidos pelas operadoras de serviços de telecomunicações com o Instituto Brasileiro de Geografia e Estatística (IBGE) para a produção estatística oficial.

Em razão da impossibilidade de realizar entrevistas de modo presencial por conta da crise sanitária, o IBGE decidiu conduzir as atividades por telefone. Para isso, seria necessário ter acesso a uma base de dados telefônicos confiável e suficientemente representativa. Assim, foi editada a referida Medida Provisória, determinando que, no contexto específico da situação de emergência de saúde pública, as empresas de telecomunicações em telefonia fixa e móvel disponibilizassem ao IBGE, em meio eletrônico, a relação dos nomes, números de telefone e endereços de seus consumidores, pessoas físicas ou jurídicas. A despeito dos cuidados de que buscou se cercar, a Medida Provisória foi prontamente contestada por cinco Ações Diretas de Inconstitucionalidade (ADIs)[7] movidas por diferentes partidos políticos e pelo Conselho Federal da Ordem dos Advogados do Brasil (OAB).

O julgamento tornou-se paradigmático porque, ao argumentar a respeito da inconstitucionalidade da Medida Provisória, o STF articulou a ideia de um direito fundamental autônomo à proteção de dados pessoais, derivado do direito à dignidade da pessoa humana e pautado na noção de autodeterminação informativa (Mendes, 2020). Ao longo do julgamento, discutiu-se também o fato de que a nova finalidade de tratamento dos dados pessoais não havia sido suficientemente especificada. Como

As demandas por compartilhamento de dados pessoais associadas à pandemia COVID-19 acabaram por precipitar uma discussão judicial sobre o tema no âmbito do STF, com impactos duradouros para a proteção de dados pessoais no Brasil.

[7] Ação judicial que visa obter uma decisão declarando a incompatibilidade de determinada norma com a Constituição Federal. A competência para julgar tais ações é do STF.

(...) a despeito dos objetivos em geral meritórios e legítimos para o compartilhamento e o uso secundário de dados pessoais no poder público, a forma concreta de (re)utilização dos dados pode ensejar consequências negativas (...)

se depreende do Acórdão, o STF entendeu que, por não definir de maneira apropriada como e para que seriam utilizados os dados coletados das operadoras de telecomunicações, a Medida Provisória não permitia considerar a adequação e a necessidade do compartilhamento, ou seja, avaliar "a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades"[8].

Embora tenha salientado a insuficiente especificação da finalidade do compartilhamento na Medida Provisória, a decisão do STF não chegou a aprofundar a análise sobre uma eventual incompatibilidade de finalidades decorrente do uso secundário dos dados. Ainda assim, ao fixar o entendimento de que a proteção de dados pessoais é um direito passível de controle diretamente em face da Constituição Federal, criou as bases para uma avaliação mais detalhada do tema em um julgado subsequente, que envolveu o compartilhamento da base de dados do Departamento Nacional de Trânsito (Denatran) com a Agência Brasileira de Inteligência (ABIN).

Nesse segundo caso, muito embora o ato autorizativo do compartilhamento tenha sido revogado antes do julgamento, o voto do Ministro Relator fez inúmeras referências à problemática da alteração da finalidade do tratamento. Destacou-se o entendimento de que não há uma permissão irrestrita no ordenamento jurídico brasileiro ao livre fluxo e compartilhamento de dados no poder público e a noção de que a incidência do princípio da finalidade nessas relações deve levar em conta elementos como: (i) as expectativas razoáveis[9] do titular dos dados; (ii) a natureza dos dados processados; e (iii) os possíveis prejuízos a serem suportados pelo titular.

Riscos e benefícios do uso secundário de dados pessoais no poder público

As decisões do STF reacenderam o debate acerca dos benefícios e riscos das atividades de coleta, análise e compartilhamento de dados pessoais entre os setores privado e público, bem como entre diferentes órgãos e entidades governamentais. Tal discussão suscita duas perspectivas de difícil conciliação. A primeira afirma que o amplo compartilhamento de dados propicia a oferta de melhores serviços públicos, a eficiência e a desburocratização, além do combate a fraudes na distribuição de benefícios sociais e fiscais. De outro lado, um segundo ponto de vista chama atenção para os riscos decorrentes dessas iniciativas.

Sob o prisma da proteção de dados pessoais, é preciso considerar que, a despeito dos objetivos em geral meritórios e legítimos para o compartilhamento e o uso secundário de dados pessoais no poder público, a forma concreta de (re)utilização dos dados pode ensejar consequências negativas, decorrentes da quebra de confiança entre o titular dos dados e a organização que os coletou, da frustração das expectativas do titular quanto ao tratamento que justificou determinada coleta e da sensação de insegurança em relação à forma como os dados pessoais serão utilizados no futuro (Solove, 2006).

Há ainda questões mais complexas ligadas ao *design* institucional, associadas, de um lado, aos riscos ampliados de danos morais ou materiais por conta do aumento da exposição e circulação dos dados; e, de outro, à possibilidade de desequilíbrio indesejável do poder social ou institucional, diante de uma distribuição inadequada de informações sobre os indivíduos entre órgãos públicos com diferentes atribuições. No âmbito nacional, existe considerável incerteza em torno da questão, visto que a Lei Geral de Proteção de

[8] Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754358567

[9] Aqueles tratamentos de dados pessoais que os indivíduos podem razoavelmente esperar que sejam realizados, levando-se em consideração o contexto do tratamento e a natureza da relação entre as partes.

Dados Pessoais (LGPD)[10] limita-se a enunciar de maneira bastante vaga que o uso compartilhado de dados pessoais pelo poder público deve atender a finalidades específicas de execução de políticas públicas e de atribuição legal pelos órgãos e entidades, respeitados os princípios de proteção de dados pessoais elencados na própria Lei (Artigo 26).

Muito embora a LGPD não detalhe como os princípios de proteção de dados pessoais podem impactar o fluxo dos dados dentro do Estado, não há dúvidas de que o debate sobre compartilhamento e uso secundário de dados pessoais remete fortemente à interpretação do princípio da finalidade, pilar fundamental das normas de proteção de dados pessoais presente também na LGPD. Como mencionado, tal princípio é capaz de estabelecer importantes restrições ao uso secundário de dados pessoais, uma vez que condiciona a realização do tratamento a propósitos específicos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

Com base nesse significativo princípio, parte importante da doutrina argumenta que o Estado não deve se configurar como uma "unidade informacional", ou seja, um ambiente de desimpedida circulação de informações sobre os cidadãos. Pelo contrário, o compartilhamento de dados entre órgãos públicos precisa considerar a necessidade de que os dados pessoais sejam tratados em conformidade com as funções do órgão e com a finalidade específica que justificou sua coleta (Simitis, 1987). Por outro lado, o princípio da finalidade não significa um impedimento absoluto ao uso secundário de dados pessoais, mas impõe a observância de que eventual nova finalidade seja, em regra, compatível com a original.

A ideia de "compatibilidade" decerto possui uma enorme abertura conceitual, requerendo elaboração adicional no campo da doutrina e da regulamentação no Brasil. Nessa linha, conforme indicam Doneda e Viola (2009) em trabalho publicado quase uma década antes da aprovação da LGPD, a compatibilidade entre o motivo da coleta e a utilização do dado pessoal pode ser verificada por meio do princípio da proporcionalidade. Nos casos concretos, isso permite avaliar se: (i) a utilização do dado é abusiva; (ii) tal uso secundário ultrapassa os limites razoavelmente cogitados pelo titular ao fornecer o dado; e (iii) há interesses relevantes que sugerem a necessidade de elasticidade e tolerância em relação a utilizações mais amplas de dados pessoais.

Alguns parâmetros adicionais podem ser depreendidos da experiência europeia. O Regulamento Geral de Proteção de Dados[11], por exemplo, estabelece que, para fins de arquivo de interesse público, fins estatísticos, fins de investigação científica ou histórica, o tratamento posterior não é considerado incompatível com as finalidades iniciais. Para os demais casos, define critérios que permitem avaliar a compatibilidade de tratamento de dados pessoais para uma finalidade distinta da original. São eles: a existência de vínculos entre as finalidades original e nova; o contexto em que os dados pessoais foram coletados, em particular no que se refere ao relacionamento entre o titular dos dados e a organização que realiza ou determina a realização do tratamento; a natureza dos dados pessoais; as possíveis consequências do tratamento adicional dos dados para o titular; e a existência de salvaguardas apropriadas, que podem incluir o uso de criptografia ou pseudonimização[12].

O conceito de compatibilidade de finalidades como condição para usos secundários de dados pessoais tem sido reiterado em diversas manifestações de autoridades de proteção de dados, colocando ênfase no atendimento às razoáveis expectativas dos indivíduos quanto à forma como seus dados são tratados e compartilhados. No Brasil, Bioni

(...) o compartilhamento de dados entre órgãos públicos precisa considerar a necessidade de que os dados pessoais sejam tratados em conformidade com as funções do órgão e com a finalidade específica que justificou sua coleta.

[10] Lei n. 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[11] Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE

[12] Técnicas que possibilitam desidentificar dados pessoais de maneira reversível (pseudonimização) ou irreversível (anonimização).

(...) quando se trata das relações entre indivíduo e Estado, o uso da base legal do consentimento para fundamentar o tratamento de dados pessoais pode ser considerado problemático em alguns aspectos, dada a assimetria de forças entre os atores, o que dificulta a obtenção de um consentimento livre, informado e inequívoco.

(2019) utiliza a ideia de privacidade contextual para refletir sobre o tema. Segundo o autor, a elasticidade do conceito, amparado nas expectativas legítimas dos titulares no que se refere às características contextuais da relação estabelecida entre controlador[13] e titular, permite governar os usos secundários de dados que não podem ser previamente especificados nem verificados de maneira rígida.

Portanto, um grande desafio que se apresenta para o setor público ao compartilhar dados pessoais entre diferentes órgãos e entidades está não apenas em verificar a existência de uma base legal para o tratamento dos dados, mas também em aferir se a nova finalidade específica que justifica o compartilhamento possui compatibilidade com a finalidade original. Tais preocupações são particularmente relevantes no contexto do poder público por conta da natureza assimétrica, não facultativa e continuada das relações entre indivíduos e Estado. Além disso, outra questão se coloca: caso se constate que determinado uso secundário no âmbito do Estado é, de fato, incompatível com a finalidade original, seria possível "remediar" tal incompatibilidade? Se sim, de que forma?

Apesar das controvérsias que circundam o tema, é possível identificar no cenário internacional certa consistência de entendimentos. Segundo estes, a incompatibilidade de finalidades pode ser superada por meio do consentimento do titular ou com base em previsão legal específica, necessária e proporcional, observando-se o pleno respeito aos demais princípios e direitos associados à proteção de dados pessoais. Nesse sentido, ganha importância o dever de transparência perante o titular, uma condição objetiva para o exercício de direitos e para a possibilidade de contestar o novo tratamento.

Cabe recordar que, quando se trata das relações entre indivíduo e Estado, o uso da base legal do consentimento para fundamentar o tratamento de dados pessoais pode ser considerado problemático em alguns aspectos, dada a assimetria de forças entre os atores, o que dificulta a obtenção de um consentimento livre, informado e inequívoco. Além disso, como mostram a experiência internacional e o debate doméstico sobre o tema, uma previsão normativa genérica para autorizar o compartilhamento de dados pessoais parece carecer dos elementos necessários para legitimar usos secundários de dados pessoais no âmbito do Estado. É preciso prever finalidade suficientemente especificada que permita avaliar o interesse público a ser atingido, assim como a necessidade e a adequação de tal medida.

Por fim, o reconhecimento do profundo impacto que a circulação de dados pessoais no âmbito do Estado pode ensejar para a esfera de direitos dos indivíduos impõe que os usos secundários dos dados estejam acompanhados não apenas da identificação de uma base legal apropriada, mas também de uma avaliação sobre as consequências das novas utilizações para os direitos e as liberdades do titular, estabelecendo-se com transparência as políticas e salvaguardas adequadas para a mitigação de eventuais riscos identificados.

Conclusão: consequências para o debate brasileiro

Conforme este artigo buscou demonstrar, a pandemia COVID-19 intensificou e acelerou as iniciativas de compartilhamento de dados pessoais com o poder público, bem como entre seus órgãos e entidades, precipitando discussões judiciais que acabaram por estabelecer novos paradigmas. Assim, uma situação extraordinária deixou um legado inesperado: a fixação definitiva na jurisprudência de parâmetros interpretativos

[13] Segundo a LGPD, o controlador dos dados é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

sobre o tratamento de dados pelo Estado, com efeitos duradouros e estruturantes para o debate nacional. A partir do reconhecimento pelo STF de um direito fundamental à proteção de dados pessoais, uma decisão subsequente fixou o entendimento de que não há autorização irrestrita no ordenamento jurídico brasileiro ao livre fluxo e compartilhamento de dados no poder público. Indicou ainda que eventuais usos secundários de dados pessoais, a partir do compartilhamento entre diferentes órgãos e entidades, devem considerar elementos como as expectativas razoáveis do titular e a natureza dos dados processados. Os julgados em questão são de enorme importância e impõem tanto para a doutrina quanto para o próprio poder Executivo a necessidade de aprofundar o debate sobre os critérios capazes de viabilizar o legítimo compartilhamento de dados no âmbito estatal.

Com base na experiência internacional e à luz do texto da LGPD, é possível vislumbrar que não haveria impedimentos a *priori* para o compartilhamento de dados visando ao tratamento de dados pessoais para finalidades compatíveis com aquelas que justificaram a coleta original, desde que observadas as regras procedimentais e, principalmente, os princípios aplicáveis ao tratamento de dados pessoais, tais como necessidade, adequação e transparência. Por outro lado, a indeterminação e a abertura do conceito de "compatibilidade" mostram a urgência do desenvolvimento de parâmetros mais objetivos para sua aferição nos casos concretos.

No âmbito do Estado, quando se trata de usos secundários incompatíveis com a finalidade original, coloca-se a questão de saber se isso significa a exclusão definitiva da possibilidade do tratamento pretendido ou se novas bases legais podem ser invocadas para superar tal incompatibilidade. Embora o assunto seja controverso, a experiência internacional indica que uma nova autorização do titular ou a previsão legal específica podem fundamentar esses tratamentos, com a condição de que sejam garantidos os princípios de proteção de dados e, em especial, a adequada informação ao indivíduo afetado. No caso de usos secundários no âmbito do poder público, a assimetria de forças e o caráter não voluntário da relação entre cidadão e Estado exigem cautela adicional na utilização da base legal do consentimento para legitimar novos tratamentos.

De ambas as decisões descritas é possível extrair a ideia de que, ainda que se admita em determinadas circunstâncias o compartilhamento de dados pessoais no âmbito do poder público com uma mudança das finalidades que justificaram sua coleta, não basta apenas conferir um verniz de legalidade para embasar formalmente tal uso secundário. É necessário estabelecer mecanismos de proteção substantivos e procedimentais, bem como observar todo o conjunto de direitos e princípios associados à proteção de dados pessoais, deixando claro o interesse público específico a ser atingido diante dos parâmetros protetivos conferidos pelos princípios constitucionais que asseguram a liberdade individual, a privacidade e o livre desenvolvimento da personalidade. Definir a maneira concreta pela qual tal exercício de equilíbrio pode ser realizado com segurança e legitimidade, à luz das disposições da LGPD e da Constituição Federal, é tarefa a ser enfrentada no campo normativo e doutrinário.

(...) eventuais usos secundários de dados pessoais, a partir do compartilhamento entre diferentes órgãos e entidades, devem considerar elementos como as expectativas razoáveis do titular e a natureza dos dados processados.

Referências

Bioni, B. R. (2019). *Proteção de dados pessoais: A função e os limites do consentimento*. Forense.

Doneda, D., & Viola, M. (2009). Risco e informação pessoal: O princípio da finalidade e a proteção de dados no ordenamento brasileiro. *Revista Brasileira de Risco e Seguro*, *5*(10), 85–102.

Mendes, L. S. (2020, Maio 10). Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais. *Portal Jota*.

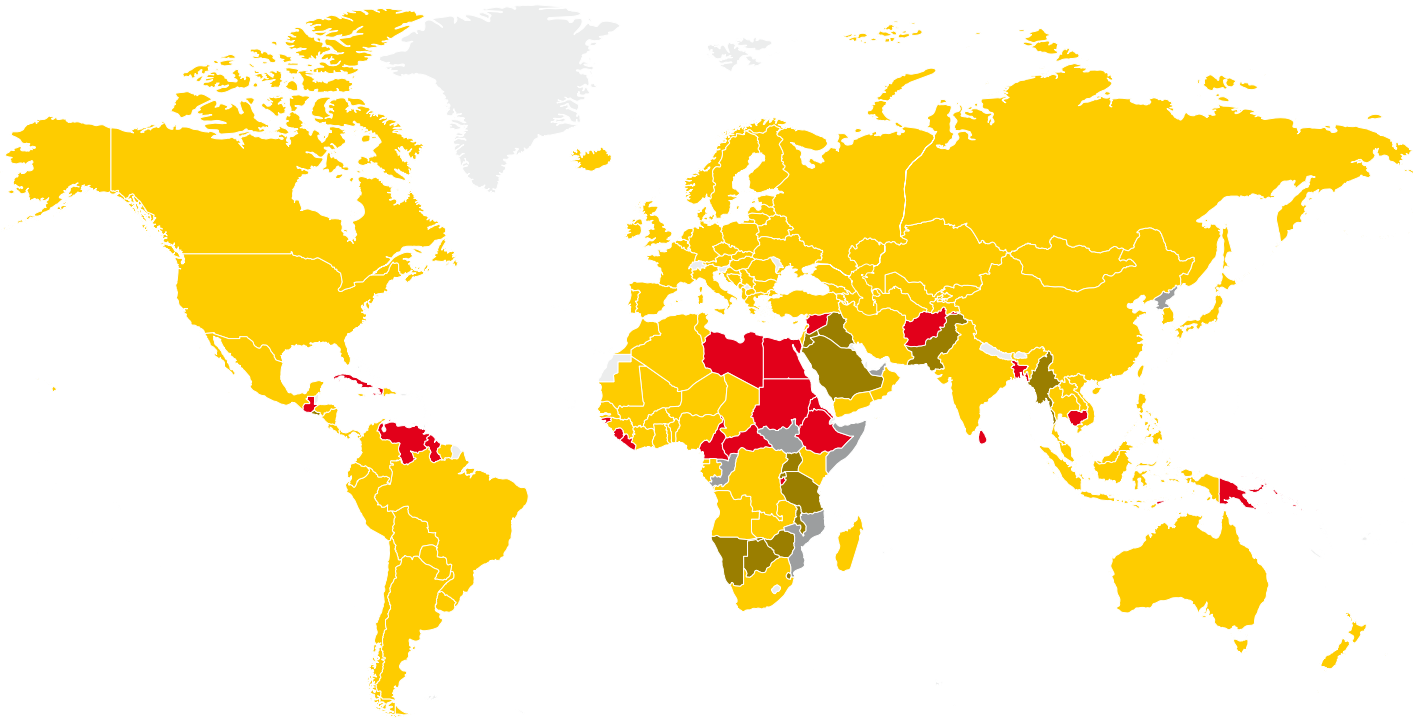
Simitis, S. (1987). Reviewing privacy in an information society. *University of Pennsylvania Law Review*, *135*, 707–46.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, *154*(3), 477–560.

BOX 1

Legislação de privacidade e de proteção de dados no mundo[14]

A digitalização crescente e o uso intensivo das tecnologias têm ampliado a relevância e a atenção em torno do tema da privacidade e da proteção de dados em nível global. A existência de uma legislação específica para lidar com tais questões é um indicativo da adoção de medidas regulatórias em cada país. Veja a seguir um mapa da existência de normas jurídicas sobre privacidade e proteção de dados no mundo.



Total de países (%)

- Possui legislação – 66%
- Possui projeto de legislação – 10%
- Não possui legislação – 19%
- Sem informação – 5%

[14] Adaptado de texto elaborado por UNCTAD. Publicado orignalmente em: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide. Última atualização em 25 de novembro de 2021.

Entrevista I

Bertrand de La Chapelle é diretor executivo da Internet & Jurisdiction Policy Network (I&JPN), organização multissetorial que aborda as tensões entre a Internet transfronteiriça e as jurisdições nacionais. Nesta entrevista, ele fala sobre como conciliar a proteção de dados com o uso de tecnologias digitais no combate à pandemia COVID-19, o que é governança de dados e como promover essa agenda internacional.

Bertrand de La Chapelle
Diretor executivo da Internet & Jurisdiction Policy Network (I&JPN).

Panorama Setorial da Internet (P.S.I.)_ As tecnologias digitais adotadas no combate à pandemia COVID-19 aumentaram intensamente a coleta e o uso de dados pessoais. De que forma as preocupações relativas à proteção de dados podem ser conciliadas com os benefícios dos dados coletados para as políticas de prevenção de contágio?

Bertrand de La Chapelle (B.C.)_ Diferentes aplicativos foram desenvolvidos e implementados por múltiplos países no contexto da pandemia COVID-19, e é provável que seu uso tenha variado mesmo internamente em cada nação. Além disso, as populações locais reagiram de diferentes maneiras quanto ao uso dessas ferramentas, em especial no que concerne à confiança nas autoridades. Alguns governos conseguiram que os aplicativos fossem endossados e adotados pelos cidadãos por terem um processo bastante transparente, com uma eficiência provavelmente maior do que países com um histórico ruim, em que havia preocupação da população com a vigilância e o uso indevido de dados. Em suma, ao buscar conciliar objetivos concorrentes, a reputação e a confiança acumuladas pelo poder público contribuem muito quando se trata de implementar uma inovação que exige esforço, mas cujos benefícios são claros e visíveis. A proteção da privacidade não é um direito absoluto. Há casos em que as limitações são aceitáveis, desde que se mostrem necessárias e que a proteção da privacidade seja considerada no marco referencial geral. Portanto, acredito que a conciliação deve considerar a proporcionalidade e as circunstâncias que justificam as limitações desse direito. Costumo me referir à ideia de conciliar objetivos aparentemente conflitantes, de modo que não seja compreendido como um jogo de soma zero – há situações em que de fato é possível proteger a privacidade e combater a pandemia COVID-19 ao mesmo tempo, sem necessariamente precisar sacrificar uma em prol da outra.

P.S.I._ Quais medidas podem ser tomadas para mitigar os riscos relacionados à privacidade e à proteção de dados no uso de tecnologias digitais para enfrentar a pandemia?

B.C._ Há uma ampla gama de medidas concretas que podem ser adotadas quanto à quantidade de dados coletados, à anonimização dos dados, à granularidade dos dados comunicados, entre outros aspectos. Nesse sentido, a I&JPN elaborou em abril de 2020 um documento de referência[15] com uma lista de critérios para avaliar quando um aplicativo está funcionando corretamente ou como implementar ferramentas que respeitem os princípios definidos.
A primeira medida é avaliar quem cria o aplicativo e quem são seus beneficiários: destina-se principalmente ao Estado, ao setor de Saúde ou aos próprios usuários? São situações bastante diferentes. A segunda pergunta é: qual a finalidade do com-

[15] Disponível em: https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-20-103-User-Data-Access-COVID-19.pdf

"A localização dos dados parece ser uma questão fundamental, mas devemos prestar ainda mais atenção a quem coleta esses dados, de quem eles provêm, quem os acessa e qual a finalidade do seu processamento."

partilhamento de dados? Mapear o movimento de grandes populações, fazer rastreamento de contatos, verificar se as pessoas estão respeitando o isolamento social ou receber alertas em situações de exposição?
Outros dois elementos a serem considerados são os tipos de dados coletados e as modalidades de coleta. São dados de geolocalização, de proximidade dos usuários? Quem fornece esses dados, o provedor de infraestrutura ou os próprios usuários? Qual é o grau de agregação, anonimização e granularidade dos dados? No que se refere às proteções, qual é o tempo de acesso a esses dados? Limita-se ao período de emergência? Existe certo nível de consentimento? Se sim, qual? E, por fim, quais são os mecanismos de supervisão empregados para garantir que não haja violações?

P.S.I._ O que é governança de dados e quais são os principais aspectos dessa agenda em nível internacional?

B.C._ Há inúmeras definições para governança de dados. Sabemos que hoje os dados não apenas sustentam a maior parte das atividades humanas, como também as refletem em muitos aspectos. Indivíduos, empresas e governos deixam rastros, e uma grande coleção de dados tem surgido e crescido em um ritmo impressionante. Pensar como criamos valor social e econômico por meio desses dados é de extrema relevância, e é exatamente disso que trata a governança de dados.
Existem diversas situações em que se pode aumentar tanto o valor social quanto o econômico. No entanto, há circunstâncias em que se tenta ampliar o valor econômico e se criam externalidades negativas na esfera social, ou vice-versa, que, na verdade, diminuem o valor global. Assim, a governança de dados diz respeito à maneira como podemos maximizar a criação de valor nos dois âmbitos de forma suficientemente equitativa e que reduza as desigualdades ou, pelo menos, não as aumente. Essa seria uma definição geral de governança de dados quanto aos objetivos.
Além disso, muitos dos debates internacionais sobre o tema – especialmente entre governos –, giram em torno dos locais de armazenamento e processamento dos dados. A localização dos dados parece ser uma questão fundamental, mas devemos prestar ainda mais atenção a quem coleta esses dados, de quem eles provêm, quem os acessa e qual a finalidade do seu processamento. Em termos de governança de dados, essas questões são certamente mais importantes do que a localização dos dados. Em suma, trata-se de maximizar a criação de valor dos dados e focar nos mecanismos que permitem às pessoas coletá-los, processá-los e usá-los, independentemente de sua localização.

P.S.I._ De que maneira é possível estabelecer um debate equilibrado entre o livre fluxo de dados, a soberania e a proteção de dados?

B.C._ Há um extenso debate sobre o livre fluxo de dados nas agendas internacionais. Por um lado, sabemos que a infraestrutura técnica da Internet se baseia no fluxo livre e indiscriminado de dados – ela apenas transporta pacotes, razão pela qual essa arquitetura é tão flexível. Dito isso, seria irreal desconsiderar as preocupações legítimas sobre as consequências desse fluxo livre e absoluto. Na esfera econômica, a concentração de riqueza e de poder na economia de dados gera um ambiente desigual em rápido crescimento. Existem também questões de segurança que justificam a restrição do acesso ou a retirada de determinados dados do território. Com relação aos direitos humanos, há preocupações legítimas como a proteção da privacidade.
A questão principal é: como lidar com essas apreensões e construir confiança? O conceito de soberania de dados é a resposta apropriada? Certamente não é a panaceia que muitos atores sugerem. Em primeiro lugar, existe uma série de desafios

diferentes, não sendo possível resolver todos eles com uma só medida. O foco no armazenamento de dados, por exemplo – um dos elementos-chave da soberania de dados –, é muito limitado para lidar com a variedade de questões mencionadas. Além disso, há uma conexão fundamental da soberania com o território dos Estados-nações. O problema é que, tanto para os dados quanto para a maioria dos aspectos de política digital, as questões são transnacionais. Não apenas as interações atravessam fronteiras, mas as medidas nacionais relacionadas à soberania de dados costumam impactar outros países. Dessa forma, a extraterritorialidade torna-se um elemento do exercício da soberania de dados; se um Estado exerce a extraterritorialidade, está inevitavelmente infringindo a soberania de outro país. Assim, é muito provável que a soberania de dados fortaleça os desequilíbrios de poder entre os diferentes atores, porque aqueles que podem impor suas normas além das fronteiras defenderão essa medida, enquanto aqueles que sofrem com a soberania de dados alheia conhecerão uma história diferente. Alem disso, várias das saídas propostas – que, novamente, concentram-se primariamente na localização dos dados, e não em sua finalidade – apresentam grandes armadilhas de implementação e consequências não intencionais. Portanto, quando analisamos o livre fluxo de dados e a soberania de dados, o elemento fundamental é que nenhum deles deve ser considerado como algo absoluto. Um fluxo de dados livre e irrestrito não é a solução para tudo, mas precisamos habilitar o compartilhamento de dados porque é assim que se cria valor. Por outro lado, uma resposta de base territorial e de curto prazo é totalmente contrária aos objetivos de compartilhamento de dados, o que pode acabar fazendo dela algo pior do que o desafio que tentamos resolver. O ecossistema de dados envolve uma infinidade de atores, o que impede que um país sozinho promulgue medidas capazes de resolver seu problema, muito menos o problema que todos temos em comum.

P.S.I._ Quais são as principais recomendações para avançar na agenda de governança de dados e promover a cooperação internacional em direção a uma Datasfera comum?

B.C._ A principal recomendação é que precisamos de uma discussão global sobre dados[16]. Muitas vozes não são ouvidas nesse debate, particularmente os países do Sul, as empresas menores e as comunidades não representadas. Também deve ser uma discussão multissetorial, pois um debate conduzido apenas entre Estados não resolverá o problema – em geral, os esforços de governos nacionais não são coordenados, e no momento não há uma tendência forte para a cooperação intergovernamental internacional. O terceiro elemento é que a maioria dessas questões está sendo tratada em nichos. Há um número substancial de organizações que trabalham o tema de forma legítima, mas sob perspectivas bastante particulares (como proteção de dados, comércio, segurança cibernética), e em uma abordagem econômica ou de direitos humanos. Portanto, a primeira recomendação é que o debate seja global, multissetorial, intersetorial e transdisciplinar, porque há interdependências entre todas essas áreas: se solucionarmos apenas uma dimensão, talvez haja impactos negativos em outra. Essas questões são inéditas devido à escala e à dimensão transnacional. Nesse sentido, o elemento mais importante das recomendações é a necessidade de inovar nas ferramentas, nos tipos de marcos referenciais básicos que desenvolvemos e nos conceitos que utilizamos. As ferramentas podem ser técnicas, novas estruturas, fiduciários de dados, *data trusts*, entre outras. Marcos referenciais são relevantes porque

"A principal recomendação é que precisamos de uma discussão global sobre dados. Muitas vozes não são ouvidas nesse debate, particularmente os países do Sul, as empresas menores e as comunidades não representadas."

[16] Saiba mais: https://www.internetjurisdiction.net/uploads/pdfs/We-Need-to-Talk-About-Data-Framing-the-Debate-Around-the-Free-Flow-of-Data-and-Data-Sovereignty-Report-2021.pdf

não é possível resolver esses problemas apenas por meio da autorregulação ou de tratados internacionais cuja elaboração leva anos – precisamos de iniciativas governamentais e de instrumentos que organizem os compromissos mútuos dos diferentes atores. O mais importante, porém, é que carecemos de novos conceitos, justamente o motivo de introduzirmos a concepção sobre a Datasfera. É necessária uma mudança de perspectiva para enfrentar os desafios da governança de dados de uma forma transnacional e transetorial, que observe a governança a partir da própria Datasfera, e não dos territórios.

A Datasfera corresponde ao triângulo de interações entre: toda a coleção de dados e bases de dados produzidas; a multiplicidade de grupos humanos até a humanidade como um todo; e as regras e contratos relativos ao acesso, processamento ou uso desses dados. Não se trata apenas de uma mudança conceitual de perspectiva, mas também comportamental, com o objetivo positivo de construir um regime de governança da Datasfera que maximize o bem-estar de todos. Isso é extremamente necessário, pois a forma como organizamos a governança da Datasfera é crítica para abordar a maioria dos problemas centrais que enfrentamos – a pandemia COVID-19, as mudanças climáticas, as desigualdades –, bem como para alcançar os Objetivos de Desenvolvimento Sustentável (ODS). É, portanto, um desafio fundamental, e somente por meio da cooperação podemos endereçá-lo. Essa discussão levou à criação da *Datasphere Initiative*, que a Internet & Jurisdiction Policy Network incuba no momento[17].

Artigo II

Entre a urgência e a vigilância: análise do uso de tecnologias durante a pandemia COVID-19 na América Latina[18]

Por Jamila Venturini[19]

Desde que a pandemia COVID-19 foi declarada pela Organização Mundial da Saúde (OMS), em 11 de março de 2020, multiplicaram-se tentativas de utilizar tecnologias digitais para auxiliar no combate à propagação do vírus. Entre outros objetivos, tais iniciativas prometiam entregar informações confiáveis ao público, apoiar o monitoramento da evolução dos casos e dos padrões de mobilidade da população durante períodos de isolamento social, bem como melhorar as capacidades de acompanhamento de pessoas expostas à doença cumprindo com as regras de quarentena. Para isso, requeriam a coleta e o processamento de uma grande quantidade de dados pessoais e sensíveis, o que levantou preocupações por parte de ativistas e especialistas de direitos humanos em todo o mundo.

[17] A *Datasphere Initiative* é uma rede global que promove diálogos de sensibilização, pesquisa e um laboratório para identificar ações inovadoras que proponham medidas, normativas e tecnológicas, para a governança de dados.
Saiba mais: https://www.thedatasphere.org

[18] Versão editada do relatório "Informe Observatorio COVID-19 del Consorcio Al Sur: un análisis crítico de las tecnologías desplegadas en América Latina contra la pandemia", publicado pelo Consórcio Al Sur em 2021. A autoria é de: Jamila Venturini e Maria Paz Canales (Derechos Digitales), Morena Schatzky e Agustina del Campo (Centro de Estudios en Libertad de Expresión y Acceso a la Información – CELE), Olga Lucía Camacho e Carolina Botero (Fundación Karisma), e Bárbara Simão (InternetLab). Disponível em: https://www.alsur.lat/reporte/informe-observatorio-covid-19-consorcio-al-sur-un-analisis-critico-tecnologias-desplegadas

[19] Jornalista pela Universidade de São Paulo (USP) e mestra em Ciências Sociais com foco em Educação pela Faculdade Latino-Americana de Ciências Sociais (Flacso Argentina), é doutoranda no Programa de Ciências Sociais da Universidade Estadual de Campinas (Unicamp) e membro da Rede Latino-Americana de Estudos sobre Vigilância, Tecnologia e Sociedade (Lavits). É diretora executiva da Derechos Digitales, organização latino-americana de defesa e proteção dos direitos humanos no ambiente digital.

Jamila Venturini
Derechos Digitales.

Na América Latina, medidas desse tipo foram promovidas por agentes públicos e privados a partir da chegada do novo coronavírus à região[20], seguindo a tendência mundial. Em sua maioria, tratou-se de aplicativos de celular e *chatbots*, às vezes acompanhados ou complementados por portais *web*. A velocidade com que esses sistemas foram implementados gerou apreensão em relação aos critérios de segurança e privacidade utilizados, em um contexto em que muitos países da região carecem de marcos normativos e instituições robustas para a adequada proteção de dados pessoais.

Alguns governos serviram-se do cenário da pandemia para flexibilizar suas responsabilidades referentes à entrega de informações públicas e avançar na coleta de dados sensíveis sem as devidas garantias de proteção. Partindo desse diagnóstico, o Consórcio Al Sur, formado por 11 organizações latino-americanas de proteção de direitos digitais[21], concentrou esforços em mapear e analisar como iniciativas de uso de tecnologias para o combate à crise sanitária na região observaram critérios internacionais de direitos humanos[22]. Os resultados foram publicados no Observatório COVID-19 do Consórcio Al Sur (OCCA), um repositório público e aberto com fichas detalhadas de 16 sistemas (14 aplicativos e dois *chatbots*) de 14 países[23].

Este artigo busca resumir as principais tendências observadas a partir da análise dessas iniciativas. Embora o ápice de seu lançamento e uso tenha ocorrido em 2020, novas estratégias de digitalização associadas ao contexto da pandemia se apresentam, agora com foco na vacinação. Espera-se que os dados e as reflexões apresentados sirvam de alerta para discussões futuras sobre os potenciais impactos desse tipo de tecnologia para o exercício de direitos fundamentais.

Tendências regionais

As respostas das autoridades à COVID-19 variaram significativamente de um país a outro na América Latina, o que influiu na maneira como cada governo empregou as tecnologias para o combate à pandemia. Na Argentina e no Chile, onde foram implementadas quarentenas estritas por longos períodos, essas ferramentas cumpriram um importante papel no controle da mobilidade da população. No Uruguai, o aplicativo nacional foi parte de uma estratégia mais ampla de identificação e rastreamento de casos da doença.

As tecnologias identificadas na região foram implementadas por agentes públicos, privados ou, na maioria dos casos, por uma associação entre ambos. Em países como a Costa Rica, soluções preexistentes foram adaptadas ou expandidas para novos usos. E enquanto alguns países se dedicaram à promoção de uma ferramenta principal de alcance nacional, em outros – como Bolívia, Brasil e México – multiplicaram-se iniciativas de caráter local. Algo similar aconteceu em relação às aplicações: parte dos países buscou concentrar uma série de funcionalidades em um só aplicativo ou portal, enquanto outros – como o Brasil, por exemplo – propagaram soluções diversas de acordo com a área de implementação. As várias experiências têm em comum a dependência do acesso e do processamento de dados para sua operação – seja pela coleta direta via os

[20] O aplicativo uruguaio foi lançado em fevereiro de 2020, mês em que se registrou o primeiro caso de COVID-19 na América Latina. Em abril do mesmo ano, a maioria dos países já contava com ao menos um aplicativo nacional.

[21] São elas: Asociación por los Derechos Civiles (Argentina), CELE (Argentina), Coding Rights (Brasil), Derechos Digitales (América Latina), Fundación Karisma (Colômbia), Hiperderecho (Peru), Instituto Brasileiro de Defesa do Consumidor – Idec (Brasil), Instituto Panameño de Derecho y Nuevas Tecnologías (Panamá), InternetLab (Brasil), Red en Defensa de los Derechos Digitales (México) e TEDIC (Paraguai). Saiba mais: https://www.alsur.lat/

[22] O estudo se baseia em uma metodologia padronizada que permitiu a análise comparada dos aplicativos móveis e *chatbots* investigados. Foram coletadas informações como: dados contextuais do país de implementação (inclusive sobre acesso à Internet); características da iniciativa; termos de uso e políticas de privacidade; características de segurança, transparência, financiamento e efetividade. A coleta se deu a partir de entrevistas, pedidos de acesso à informação, notícias oficiais ou publicadas na imprensa, entre outras fontes. A pesquisa incluiu ainda uma análise do marco legal de cada país e das mudanças realizadas durante o período da pandemia.

[23] Dados detalhados de cada país estão disponíveis em: https://covid.alsur.lat/pt/

aplicativos, seja pela disponibilidade prévia em bancos de dados públicos ou privados cujo uso foi redirecionado. O primeiro caso é mais frequente, mas há pouca transparência sobre como essas informações coletadas pelos aplicativos podem ser associadas a outros dados.

As estratégias de implementação das iniciativas foram bastante heterogêneas. Houve casos de promoção tímida das tecnologias, como na Bolívia e no Brasil. Outros discursos foram marcados por um otimismo tecnológico que superestimou o papel das ferramentas dentro da estratégia sanitária, como na Colômbia e no Equador, onde elas foram apresentadas como capazes de "salvar vidas". Ao argumento de utilidade para a cidadania somou-se muitas vezes outro relacionado à gestão pública: a coleta de dados por meio da funcionalidade de autodiagnóstico serviria para auxiliar no mapeamento de casos e orientar as políticas de combate à pandemia. Tal retórica dialoga com um cenário de escassez de testes que afetou gravemente a região.

É inegável que o uso de dados pessoais tem um relevante interesse público em contextos como o da pandemia COVID-19 e que as tecnologias digitais podem auxiliar os governos no desenho de estratégias de resposta. No entanto, a efetividade dessas ferramentas e os riscos associados a um eventual uso indevido ou abusivo dependem das estruturas normativas, técnicas e de governança por trás de sua operação. Como ressaltam especialistas da Organização das Nações Unidas (ONU), os Estados têm de respeitar os direitos humanos em seus esforços de enfrentamento à crise sanitária, que em qualquer caso devem ser proporcionais, necessários e não discriminatórios[24].

A Comissão Interamericana de Direitos Humanos (CIDH) é ainda mais específica em sua orientação. De acordo com a Resolução 1/2020, o uso de ferramentas de vigilância digital na resposta à pandemia deve ser estritamente limitado em termos de propósito e de tempo, assim como tem de proteger com rigor os direitos individuais, o princípio de não discriminação e as liberdades fundamentais[25]. Além disso, é preciso que os Estados sejam transparentes em relação às tecnologias de vigilância utilizadas e à sua finalidade, e também que implementem mecanismos de supervisão independentes para analisar seu uso, de um lado, e canais seguros para a recepção de denúncias e reclamações, de outro.

A seguir, analisamos de que maneira as diretrizes dos organismos internacionais de direitos humanos foram ou não observadas na implementação de tecnologias para o combate à COVID-19 na América Latina, com foco nos aspectos de legalidade, necessidade, proporcionalidade e transparência.

Tabela 1 – INICIATIVAS ANALISADAS E CARACTERÍSTICAS PRINCIPAIS

NOME	PAÍS	VOLUNTARIEDADE	TAXA DE ADESÃO (% DA POPULAÇÃO)[26]	NATUREZA	DADOS COLETADOS	CONSENTIMENTO LIVRE, ESPECÍFICO E INFORMADO
Cuidar	Argentina	Sim	22,12	Público-privada	Documento de identidade, nome, idade, gênero, endereço, localização, sintomatologia, doenças preexistentes	Sim
Bolivia Segura	Bolívia	Sim	0,43	Pública	Documento de identidade, nome, idade, endereço, localização, sintomatologia	Não
Salud en Cochabamba	Bolívia	Sim	Não se aplica	Público-privada	Documento de identidade, nome, idade, gênero, endereço, localização, sintomatologia, doenças preexistentes	Sim

[24] "COVID-19: States should not abuse emergency measures to suppress human rights", de 16 de março de 2020. Disponível em: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25722&LangID=E

[25] Disponível em: https://www.oas.org/pt/cidh/decisiones/pdf/Resolucao-1-20-pt.pdf

[26] Dados calculados a partir de fontes oficiais ou informações disponíveis sobre *downloads* em lojas de aplicativos até dezembro de 2020. Considera apenas aplicativos para dispositivos móveis e iniciativas de alcance nacional (não se aplica aos *chatbots* nem ao aplicativo boliviano Salud en Cochabamba).

NOME	PAÍS	VOLUNTARIEDADE	TAXA DE ADESÃO (% DA POPULAÇÃO)	NATUREZA	DADOS COLETADOS	CONSENTIMENTO LIVRE, ESPECÍFICO E INFORMADO
Dr. Sammy Bot	Bolívia	Sim	Não se aplica	Público-privada	Documento de identidade, localização, sintomatologia, doenças preexistentes	Não
Coronavírus-SUS	Brasil	Sim	0,47	Pública	Localização, sintomatologia	Não
CoronApp	Chile	Sim	0,52	Pública	Documento de identidade, nome, idade, gênero, endereço, localização, sintomatologia, doenças preexistentes	Sim
CoronApp	Colômbia	Sim	21,62	Pública	Documento de identidade, nome, localização, sintomatologia	Não
EDUS	Costa Rica	Sim	10,27	Pública	Documento de identidade, nome, idade, gênero, endereço, localização, sintomatologia, doenças preexistentes	Não
ASÍ Ecuador	Equador	Sim	2,83	Público-privada	Idade, gênero, localização	Não
SIVI	El Salvador	Sim	Não se aplica (*chatbot*)	Público-privada	Nome, idade, sintomatologia	Não
Alerta Guate	Guatemala	Sim	1,68	Público-privada	Localização	Não
COVID-19MX	México	Sim	0,4	Pública	Nome, idade, gênero, endereço, localização, sintomatologia, doenças preexistentes	Sim
Protégete con salud	Panamá	Sim, com exceção de pessoas estrangeiras ingressando no país	0,06	Público-privada	Documento de identidade, nome, idade, gênero, endereço, localização, sintomatologia, doenças preexistentes, fotografia	Não
Covid-19 PY	Paraguai	Sim	0,08	Pública	Documento de identidade, nome, idade, gênero, endereço, localização, sintomatologia, doenças preexistentes	Não
Perú en tus manos	Peru	Sim	3,03	Público-privada	Documento de identidade, nome, idade, gênero, localização, sintomatologia, doenças preexistentes	Sim
Coronavirus UY	Uruguai	Sim, mas determinados grupos foram orientados a utilizá-la, como pessoas ingressando no país	17,73	Público-privada	Documento de identidade, nome, idade, gênero, endereço, sintomatologia, doenças preexistentes	Sim

Fonte: Elaboração própria a partir de dados do Observatório COVID-19 do Consórcio Al Sur (OCCA).

(...) sem informações suficientes sobre as condições de coleta e processamento dos dados, a possibilidade de um consentimento significativo fica seriamente comprometida.

Urgência, opacidade e vigilância

Todas as iniciativas analisadas foram implementadas de maneira administrativa, sem que passassem por discussões legislativas antes ou depois de seu lançamento. Com raras exceções, não foram encontradas normas específicas que estabelecessem marcos para orientar sua operação, seja em relação ao potencial impacto nos direitos fundamentais distintos do direito à saúde, seja no que se refere à criação de mecanismos de controle, metas e objetivos para avaliar sua eficiência. A maioria das ferramentas foi resultado de iniciativas público-privadas decorrentes de interações diretas entre governos e empresas.

Ainda que a cooperação de diferentes setores seja bem-vinda, especialmente em um contexto extremo como o da pandemia COVID-19, ela deve ocorrer de forma transparente. No entanto, o que se viu nos casos analisados foi o contrário: a divulgação, quando ocorreu, foi feita depois de consumadas as alianças, sem que o público soubesse ou pudesse opinar sobre os termos e as próprias condições de acesso que as empresas teriam a dados pessoais e sensíveis da população.

A ausência de debate público a respeito da adoção de sistemas tecnológicos destinados a auxiliar no combate à COVID-19 reproduziu uma tendência observada na aquisição de sistemas de vigilância na América Latina. Do mesmo modo não foram encontradas evidências de que as tecnologias implementadas tenham passado por uma avaliação prévia relativa a possíveis efeitos no exercício de direitos e, especificamente, na privacidade. A prática contraria a recomendação da CIDH de que, ao contratar sistemas privados, o Estado garanta a realização de uma auditoria externa e independente para identificar potenciais impactos nos direitos humanos[27].

Entre as funcionalidades oferecidas pelas tecnologias estão a entrega de informações de interesse público, autodiagnóstico, alertas de exposição ao coronavírus, telemedicina e passaportes de mobilidade e de trabalho, que implicam a coleta de dados pessoais sensíveis sobre gênero, saúde e localização. O processamento desses e de outros dados permite inferir uma série de informações adicionais sobre hábitos íntimos e igualmente sensíveis, como preferências políticas e religiosas. Seu tratamento deve estar sujeito aos mais elevados critérios de proteção, segurança e transparência.

Nesse contexto, a transparência deve ser entendida não só a partir da perspectiva do acesso a informações públicas sobre as características das iniciativas – que, como apontado, sofreu importantes limitações –, mas também em relação ao tratamento e uso dos dados pessoais coletados por cada sistema. Trata-se de um princípio fundamental para o exercício da autonomia das pessoas usuárias sobre como serão utilizados seus dados, conforme estabelecem os padrões internacionais e diversas normas nacionais de proteção de dados. Em outras palavras, sem informações suficientes sobre as condições de coleta e processamento dos dados, a possibilidade de um consentimento significativo fica seriamente comprometida.

[27] Disponível em: https://www.oas.org/es/cidh/decisiones/pdf/Resolucion-4-20-es.pdf

Diversos problemas se apresentam em relação a esse aspecto. Como mostra a Tabela 1, menos da metade das iniciativas cumpre com o critério estabelecido para um consentimento expresso, livre e informado, falha que se deve a vários motivos. No caso do aplicativo brasileiro Coronavírus-SUS, por exemplo, foram identificadas inconsistências entre as informações presentes na Política de Privacidade e os dados efetivamente coletados. Enquanto a maioria das ferramentas solicita o consentimento de maneira ativa, três o assumem apenas pelo uso. Além disso, sete (referentes a Bolívia, Brasil, Colômbia, Guatemala e Panamá) não explicitam em suas políticas os mecanismos para a retirada de consentimento após ele ser concedido.

Muitos dos sistemas analisados permitem o acesso de outras instituições governamentais aos dados coletados. Algumas iniciativas explicitam essa possibilidade nos contratos de adesão, enquanto em outras só é possível compreender o que ocorre ao revisar as normas aplicáveis e eventuais alterações vigentes durante a pandemia. Por conta disso, nem sempre é fácil entender quais são os órgãos com autorização e condições para acessar os dados. A Política de Privacidade do aplicativo brasileiro, por exemplo, afirma que o consentimento cobre apenas o tratamento de dados pelo Ministério da Saúde, mas a legislação prevê uma série de hipóteses para o compartilhamento[28]. No caso do Panamá, os dados podem ser acessados por uma força-tarefa criada no contexto da pandemia e que inclui a polícia nacional – situação similar à do aplicativo paraguaio.

Nenhuma das iniciativas analisadas – aplicativos de celular ou *chatbots* incorporados em outros aplicativos – oferece informações detalhadas sobre as estratégias de segurança adotadas. No máximo, indica-se o compromisso de zelar pela segurança dos dados coletados ou a tomada de medidas "adequadas" para tal. Somente no caso argentino uma página *web* associada ao aplicativo menciona a adesão a normas ISO específicas. Apenas metade dos sistemas possibilita o controle efetivo das pessoas titulares sobre o uso de seus dados, o que se reflete nos direitos de acesso, correção, eliminação e oposição ao tratamento de dados. Ainda assim, em muitos casos as formas de exercício desses direitos são pouco explícitas, especialmente nos países que não possuem uma autoridade de proteção de dados estabelecida.

Para além do tecnossolucionismo

A análise desenvolvida pelo Consórcio AI Sur aponta para uma série de riscos ao exercício de direitos fundamentais colocados pelo uso de tecnologias dirigidas à cidadania no contexto de combate à pandemia COVID-19. Além das fragilidades mencionadas em termos de transparência, segurança e privacidade, a situação se agrava quando consideramos que nem todos os países da América Latina contam com marcos normativos adequados e atualizados para o acesso à informação e a proteção de dados ou com instituições independentes devidamente capacitadas para supervisionar a implementação desse tipo de tecnologia.

Muitos dos sistemas analisados permitem o acesso de outras instituições governamentais aos dados coletados.

[28] As hipóteses de compartilhamento de dados sensíveis (como os de saúde) estão previstas no Decreto n. 10.046/2019 e nos seguintes artigos da Lei Geral de Proteção de Dados Pessoais (LGPD): artigo 11, inciso II; artigo 13; e artigo 26. Disponíveis em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm e http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

(...) diante da pandemia, diversos países flexibilizaram suas regras de proteção de dados, ampliando a possibilidade de acesso e compartilhamento de dados de saúde sem a necessidade de consentimento das pessoas titulares.

Cabe ressaltar que, diante da pandemia, diversos países flexibilizaram suas regras de proteção de dados, ampliando a possibilidade de acesso e compartilhamento de dados de saúde sem a necessidade de consentimento das pessoas titulares. Em alguns casos, as já precárias estruturas de controle existentes tiveram sua operação limitada devido às restrições da quarentena. O mesmo ocorreu em relação às normas de transparência, ainda que, em países como o Brasil, as tentativas de diminuir a responsabilidade estatal na entrega de informações públicas tenham sido contestadas[29].

Além do enorme potencial discriminatório desse tipo de informação, contextos marcados por autoritarismo, polarização e perseguição política trouxeram preocupações adicionais sobre como os dados coletados pelos chamados "COVID *apps*" poderiam ser utilizados. Um exemplo é a Bolívia, que enfrentou os primeiros meses da pandemia sob um governo interino que tentou criminalizar de forma ambígua e preocupante a difusão de informações que afetassem a saúde pública. O resultado foi a acusação de ao menos 781 pessoas e 273 processos penais somente no mês de abril de 2020, segundo organizações da sociedade civil locais[30].

De acordo com a avaliação do Consórcio Al Sur, o direito à proteção de dados é o mais afetado pelas iniciativas identificadas, seguido do direito à privacidade, diretamente conectado ao primeiro. Enquanto a proteção de dados se refere à capacidade de autodeterminação informativa das pessoas titulares de dados – ou seja, a capacidade de exercer um controle efetivo sobre o uso de suas informações pessoais –, a privacidade diz respeito ao direito de não intrusão na intimidade por parte de terceiros ou autoridades públicas. Abusos à privacidade podem acarretar a violação de uma série de outros direitos, como à liberdade de expressão, à livre associação e à não discriminação.

É certo que nenhum direito é absoluto, e um contexto de pandemia exige medidas em favor da saúde da população. No entanto, os critérios de legalidade, necessidade, proporcionalidade e transparência são cruciais para uma intervenção equilibrada, bem como para diferenciar uma política pública responsável do mero tecnossolucionismo que tem marcado o uso de tecnologias pelos Estados latino-americanos. Nesse sentido, cabe analisar se essas iniciativas de fato cumprem com seus objetivos. Como vimos, não houve um cuidado por parte dos governos em estabelecer metas e mecanismos de avaliação, o que, por si só, parece sintomático de uma confiança cega no poder das tecnologias. O que sabemos é que a adesão da população foi extremamente limitada devido às profundas desigualdades no acesso às tecnologias, o que ficou ainda mais evidente durante a pandemia.

Importante ressaltar que a inclusão digital não se restringe ao acesso a equipamentos ou à conectividade, mas também diz respeito às habilidades

[29] Saiba mais: https://ok.org.br/noticia/so-venceremos-a-pandemia-com-transparencia/

[30] Saiba mais: https://www.derechosdigitales.org/14611/in-support-of-freedom-of-expression-in-bolivia-we-request-the-abrogation-of-the-ds-4231/

de uso das tecnologias e à qualidade da conexão. Dessa forma, as barreiras impostas por um acesso que se dá majoritariamente via dispositivos móveis e planos de dados limitados impactam na penetração dos aplicativos e, em consequência, na sua efetividade. No caso de alertas de exposição ao coronavírus, por exemplo, estudos indicam que a eficácia dessa funcionalidade depende de uma adoção de 40% a 60% da população[31]. Na América Latina, em 2020, somente a Argentina, a Colômbia e o Uruguai chegaram perto dos 20%, locais onde o uso dos aplicativos estava associado ao acesso a determinados serviços, à possibilidade de circulação ou de trabalho. Nos demais países, a taxa ficou em torno de 3%.

É preocupante que, na busca por soluções tecnológicas que auxiliem no combate à pandemia, os Estados falhem em oferecer uma perspectiva integral de atenção aos direitos humanos – segundo orientam organismos internacionais – e descumpram suas obrigações de proteger esses direitos, tornando-os mais frágeis na maioria dos casos. Conforme observado, em termos gerais, fatores como desigualdades de acesso, análises de impacto e evidências de efetividade não foram considerados no planejamento das iniciativas analisadas. A tendência é de passividade dos governos diante de tecnologias que representam riscos reais de restrição aos direitos da população.

Seja no contexto da pandemia COVID-19 ou além, o uso de tecnologias pelos Estados deve estar acompanhado de medidas rígidas de transparência, participação e prestação de contas. É inaceitável que iniciativas com grande potencial de abusos aos direitos não contem com justificativas sólidas para sua implementação. Por parte do Consórcio Al Sur, espera-se que essa análise sirva de ponto de partida para oportunidades de melhoria das práticas de uso de tecnologias no enfrentamento à pandemia, bem como para uma reflexão coletiva sobre o papel que elas podem cumprir no futuro.

Seja no contexto da pandemia COVID-19 ou além, o uso de tecnologias pelos Estados deve estar acompanhado de medidas rígidas de transparência, participação e prestação de contas.

[31] Luca Ferretti et al., "Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing", *Science* (2020). Disponível em: https://science.sciencemag.org/content/early/2020/03/30/science.abb6936/tab-pdf. Ver também Patrick Howell O'Neill, "No, coronavirus apps don't need 60% adoption to be effective", *MIT Techonology Review* (2020). Disponível em: https://www.technologyreview.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percent-download/

BOX 2

Guia do PNUD sobre privacidade, proteção de dados e dimensões mais amplas de direitos humanos no uso de tecnologias digitais para combater a COVID-19[32]

Diante da extensa resposta digital à pandemia COVID-19 e dos desafios relacionados aos direitos de privacidade, o Programa das Nações Unidas para o Desenvolvimento (PNUD) propôs uma série de princípios e orientações práticas para seus escritórios regionais.

Principais desafios de privacidade e de proteção de dados na resposta digital à COVID-19

- Falta de oportunidades para a deliberação pública durante a crise;
- Falta de normas gerais de privacidade e de proteção de dados.

Orientação digital específica a respeito da COVID-19

PRINCÍPIOS GERAIS A SEREM CONSIDERADOS

- Abordagem baseada nos direitos humanos;
- Abordagem participativa;
- Consentimento do usuário;
- Anonimização/pseudonimização de dados pessoais;
- Natureza temporária do "rastreamento" digital e das medidas de vigilância;
- Diretrizes para a coleta, uso e duração do armazenamento de dados;
- Proteção de violações baseadas em gênero;
- Proteção a populações vulneráveis;
- Direito de reparação de danos causados pela coleta, processamento e uso de dados pessoais.

RECOMENDAÇÕES AO CRIAR OU USAR TECNOLOGIAS PARA AÇÕES RELACIONADAS À COVID-19

- Na ausência de normas gerais de proteção de dados, adotar marcos referenciais regionais ou internacionais, bem como normas de privacidade de dados de saúde;
- Criar um marco referencial que estabeleça regras claras sobre quem pode coletar, acessar, e utilizar quais tipos de dados, em quais momentos e para qual finalidade;
- Definir e implementar práticas com propósito definido e minimização de dados;
- Incluir privacidade e participação na fase de *design*;
- Garantir as melhores práticas durante o processo de aquisição das tecnologias ou serviços digitais;
- Enfatizar códigos de conduta de privacidade para detentores comerciais de dados;
- Realizar o licenciamento cuidadoso de inovações digitais do setor privado;
- Conduzir processos obrigatórios de devida diligência de direitos humanos e privacidade para todas as parcerias e aquisições públicas;
- Fomentar debates sobre a necessidade de regulamentação geral de proteção de dados;
- Considerar questões que vão além do rastreamento e da vigilância digitais.

[32] Adaptação de texto elaborado por PNUD. Disponível em: https://www.sdg16hub.org/content/covid-19-guidance-undp-country-offices-privacy-data-protection-and-digital-technologies

Entrevista II

Nina da Hora é pesquisadora do Centro de Tecnologia e Sociedade da Escola de Direito da Fundação Getulio Vargas (CTS/FGV) e conselheira de Segurança Digital do TikTok Brasil. Nesta entrevista, ela fala sobre riscos à privacidade e à segurança digital, implicações da coleta de dados biométricos e caminhos para a garantia de direitos digitais mais acessíveis.

Nina da Hora
Pesquisadora do CTS/FGV e conselheira de Segurança Digital do TikTok Brasil.

Panorama Setorial da Internet (P.S.I.)_ No atual contexto de intensa adoção das tecnologias digitais para o enfrentamento da pandemia COVID-19, quais são os principais riscos associados à privacidade? Como eles podem ser minimizados?

Nina da Hora (N.H.)_ No Brasil, mesmo antes da COVID-19, as tecnologias digitais já eram usadas para o enfrentamento de problemas estruturais da sociedade, como na Saúde e em outras áreas. A pandemia intensificou esse uso, assim como os riscos relacionados à privacidade, o que contribuiu para a vigilância digital que vem acontecendo há bastante tempo. Nesse contexto, as pessoas cedem seus dados para ter acesso a direitos fundamentais. Ao mesmo tempo, não leem as políticas de privacidade e termos de uso das tecnologias por serem longos e de difícil compreensão. No entanto, temos enormes problemas quando relacionamos dados e Inteligência Artificial (IA), e hoje, com a ideia de que precisamos estar conectados a tudo e a todos, enfrentamos cada vez mais desafios associados à segurança digital.
Por outro lado, casos emblemáticos de falhas na segurança de dados envolvendo ataques *hackers*, clonagens de aplicativos e vazamento de dados – cobertos intensamente pela imprensa – ampliaram o alerta das pessoas acerca dos dados que compartilham, seja no meio digital ou fora dele (por exemplo, quando passam a questionar o fornecimento do número do CPF para a realização de compras). A preocupação com a proteção aparece, assim, como consequência das falhas encontradas no ambiente digital. Não que estas não ocorressem antes da pandemia, mas a questão, até então restrita a especialistas e acadêmicos, ganhou visibilidade e atenção. O caminho é longo, mas precisamos repensar toda a estrutura de dados. Vejo a educação digital como um pilar capaz de gerar informação e questionamentos por parte da sociedade a respeito das ferramentas que estão sendo utilizadas.

P.S.I._ Considerando as desigualdades existentes na sociedade brasileira, como garantir o direito à privacidade e a proteção de dados pessoais a parcelas mais vulneráveis da população?

N.H._ No sistema atual é muito difícil pensar como garantir o direito à privacidade e à proteção de dados, uma vez que estamos cada vez mais ligados a bases de dados utilizadas de forma intensa para diversos fins. O Brasil ainda tem uma parcela muito grande de pessoas sem acesso à Internet ou a serviços digitais, e precisamos identificar como proteger seus dados também. Existem, por exemplo, muitas pessoas em situação de rua sem documentos de identificação, e não sabemos quantas delas tiveram seus dados *hackeados* para usos indevidos.

"Além da anonimização dos dados sensíveis, é fundamental o estabelecimento de regras de transparência, no sentido de explicitar para o usuário o que é coletado, com qual propósito e que uso será feito disso, o que deve ser adaptado a cada contexto."

Pensando nas tecnologias digitais, cedemos e armazenamos nossos dados em empresas privadas, sem haver transparência das condições e do processamento dessas informações. Além da anonimização dos dados sensíveis, é fundamental o estabelecimento de regras de transparência, no sentido de explicitar para o usuário o que é coletado, com qual propósito e que uso será feito disso, o que deve ser adaptado a cada contexto. A adoção de ferramentas digitais de *software* livre também pode contribuir para a educação digital e o desenvolvimento de um pensamento crítico acerca das tecnologias, já que a abertura dessas ferramentas pressupõe entender e documentar o que acontece com os dados, como se dão a coleta e o processamento, bem como as possíveis aplicações e resultados, incluindo questões éticas. Na minha opinião, são esses os caminhos para construirmos um direito à privacidade e à proteção de dados mais acessível para a população.

P.S.I._ Quais são as possíveis implicações da coleta de dados sensíveis por soluções tecnológicas adotadas em ações de apoio emergencial à população durante a pandemia, como a coleta de dados biométricos para o reconhecimento facial?

N.H._ A coleta de dados biométricos não é novidade, já que utilizamos a digital há bastante tempo. Essa prática foi naturalizada por se colocar como o método mais seguro, mas não necessariamente evitou fraudes. O problema no uso de reconhecimento facial e de outros reconhecimentos biométricos remotos é que estes permitem a vigilância em massa, discriminatória e enviesada. O reconhecimento facial é ainda mais prejudicial porque identifica a pessoa, permitindo seu rastreamento individualizado. Muitos cidadãos não brancos estão sendo diretamente afetados por essas ferramentas, que são capazes de reconhecer, seguir, destacar e rastrear indivíduos em todos os lugares, minando direitos humanos básicos como o direito à privacidade, à proteção de dados, à igualdade, à não discriminação e mesmo à liberdade de expressão (levando à criminalização de protestos, por exemplo).
Cada inovação tecnológica gera vulnerabilidades a serem descobertas ao longo do caminho, que são menos ligadas às ferramentas em si do que às estratégias e aos contextos de uso. Há diversos problemas potenciais na aceleração do uso de IA, por exemplo, como as técnicas desenvolvidas para clonar rostos e criar *deepfakes*. Quando rostos são armazenados sem que nós saibamos o que será feito com essas informações, há riscos. Embora alguns aplicativos de reconhecimento facial e biométrico sejam promovidos como um mecanismo para aumentar a segurança digital e incentivar sua adoção na sociedade, há formas alternativas que permitem assegurar segurança e privacidade. Em todas essas situações, o dano aos direitos ocorre independentemente da anonimização dos dados, o que, a meu ver, vai contra o que se entende por direitos humanos e democracia.

P.S.I._ Quais estratégias podem ser adotadas para ampliar o conhecimento e o engajamento da população no debate sobre os possíveis impactos negativos das tecnologias digitais, em especial no que se refere à coleta e ao tratamento de dados pessoais?

N.H._Sempre parto da ideia da educação. Primeiro, precisamos tornar esses temas acessíveis e repensar os exemplos usados para explicá-los, de modo que se adaptem aos diferentes contextos brasileiros. Para isso, o debate da diversidade

e da inclusão tem de acontecer, principalmente nos grupos que hoje promovem as discussões sobre essas questões. Outro ponto é realizar esse processo de forma gradual. A Internet e a tecnologia estão conectadas com todas as áreas e todas as pessoas, pois mesmo aquelas que não têm acesso estão "rastreadas" no sistema. Logo, trata-se de um processo de longo prazo. A meu ver, não é o solucionismo tecnológico que irá nos ajudar, ou seja, a tendência de colocar a tecnologia para enfrentar problemas – inclusive tecnológicos – que não serão resolvidos com mais tecnologia. Vieses raciais, de gênero ou de qualquer outro tipo, por exemplo, não serão corrigidos com mais dados, mas sim com reflexão e pensamento crítico, pois se tratam de vieses humanos encontrados na sociedade.
Como é possível resolver a problemática da democracia no Brasil e no mundo usando tecnologias monitoradas, pensadas e criadas somente por um grupo social, normalmente empresas privadas, às quais a sociedade civil não tem acesso? É necessário fomentar políticas públicas e promover um debate mais plural e aberto a diversos setores, não só o setor público, mas também o setor privado e a sociedade civil, incluindo organizações e ativistas de diferentes pautas e contextos. As tomadas de decisão precisam estar acessíveis à população para que ela possa participar desse processo. Trata-se realmente de uma abordagem abrangente de educação e informação para impulsionar o entendimento acerca desses temas.

"É necessário fomentar políticas públicas e promover um debate mais plural e aberto a diversos setores, não só o setor público, mas também o setor privado e a sociedade civil (...)"

Relatório de Domínios

A dinâmica dos registros de domínios no Brasil e no mundo

O Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), departamento do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), monitora mensalmente o número de nomes de domínios de topo de código de país (ccTLD, do inglês, *country code Top-Level Domain*) registrados entre os países que compõem a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e o G20[33]. Considerados os membros de ambos os blocos, as 20 nações com maior atividade somam mais 89,75 milhões de registros. Em novembro de 2021, os domínios registrados sob .de (Alemanha) chegaram a 17,10 milhões. Em seguida, aparecem China (.cn), Reino Unido (.uk) e Países Baixos (.nl), com, respectivamente, 9,83 milhões, 9,70 milhões e 6,21 milhões de registros. O Brasil teve 4,85 milhões de registros sob .br, ocupando a sexta posição na lista, como mostra a Tabela 1[34].

[33] Grupo composto pelas 19 maiores economias mundiais e a União Europeia. Saiba mais: https://g20.org/

[34] A tabela apresenta a contagem de domínios ccTLDs segundo as fontes indicadas. Os valores correspondem ao registro publicado por cada país, tomando como base os membros da OCDE e do G20. Para países que não disponibilizam uma estatística oficial fornecida pela autoridade de registro de nomes de domínios, a contagem foi obtida em: https://research.domaintools.com/statistics/tld-counts. É importante destacar que há variação no período de referência, embora seja sempre o mais atualizado para cada localidade. A análise comparativa de desempenho de nomes de domínios deve considerar ainda os diferentes modelos de gestão de registros ccTLDs. Assim, ao observar o *ranking*, é preciso atentar para a diversidade de modelos de negócio existentes.

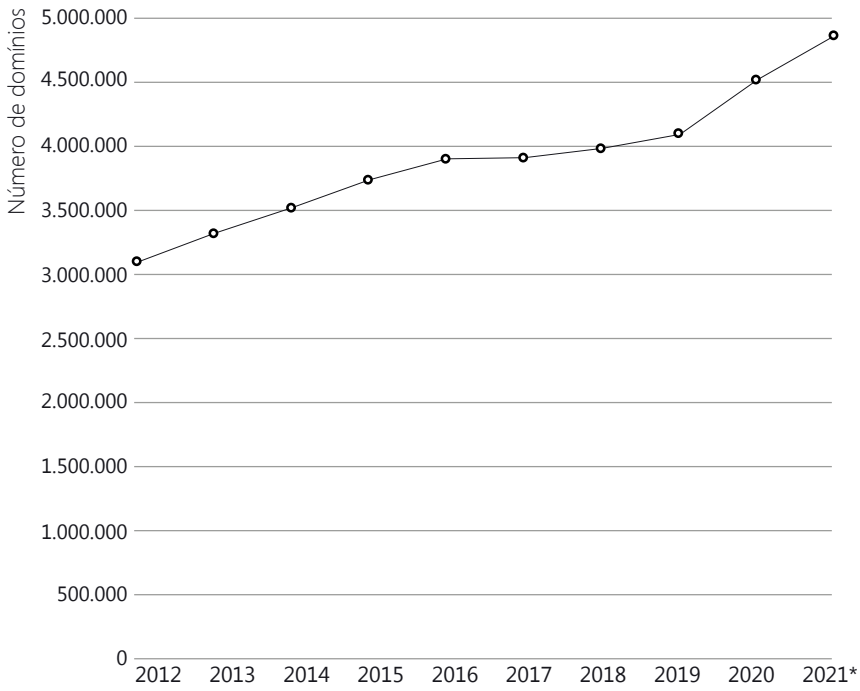
Tabela 1 – TOTAL DE REGISTROS DE NOMES DE DOMÍNIOS ENTRE OS PAÍSES DA OCDE E DO G20

Posição	País	Número de domínios	Data de referência	Fonte (*site*)
1	Alemanha (.de)	17.109.697	30/11/2021	https://www.denic.de
2	China (.cn)	9.837.644	30/11/2021	https://research.domaintools.com/statistics/tld-counts/
3	Reino Unido (.uk)	9.703.171	01/06/2021	https://www.nominet.uk/news/reports-statistics/uk-register-statistics-2021/
4	Países Baixos (.nl)	6.219.806	30/11/2021	https://api.sidn.nl/rest/counters/domains
5	Rússia (.ru)	5.025.335	30/11/2021	https://cctld.ru
6	**Brasil (.br)**	**4.858.768**	**30/11/2021**	**https://registro.br/dominio/estatisticas/**
7	França (.fr)	3.874.717	30/11/2021	https://www.afnic.fr/en/observatory-and-resources/statistics/
8	União Européia (.eu)	3.666.151	30/11/2021	https://research.domaintools.com/statistics/tld-counts/
9	Itália (.it)	3.456.471	30/11/2021	http://nic.it
10	Austrália (.au)	3.401.599	30/11/2021	https://www.auda.org.au/
11	Canadá (.ca)	3.214.548	30/11/2021	https://www.cira.ca
12	Colômbia (.co)	3.186.901	30/11/2021	https://research.domaintools.com/statistics/tld-counts/
13	Índia (.in)	2.586.097	30/11/2021	https://research.domaintools.com/statistics/tld-counts/
14	Polônia (.pl)	2.521.965	30/11/2021	https://www.dns.pl/en/
15	Suíça (.ch)	2.459.804	15/11/2021	https://www.nic.ch/statistics-data/domains_ch_monthly.csv
16	Espanha (.es)	1.980.363	25/10/2021	https://www.dominios.es/dominios/en
17	Bélgica (.be)	1.735.833	30/11/2021	https://www.dnsbelgium.be/en
18	Estados Unidos da América (.us)	1.735.153	30/11/2021	https://research.domaintools.com/statistics/tld-counts/
19	Japão (.jp)	1.674.481	30/11/2021	https://jprs.co.jp/en/stat/
20	Suécia (.se)	1.508.386	30/11/2021	https://internetstiftelsen.se/en/domain-statistics/growth-se/?chart=active

Data de coleta: 30 de novembro de 2021.

O Gráfico 1 apresenta o desempenho do .br desde o ano de 2012.

Gráfico 1 – TOTAL DE REGISTROS DE DOMÍNIOS DO .BR – 2012 a 2021*



*Data de coleta: 30 de novembro de 2021.
Fonte: Registro.br
Recuperado de: https://registro.br/dominio/estatisticas/

Em novembro de 2021, os cinco principais domínios genéricos (gTLD, do inglês *generic Top-Level Domain*) totalizaram mais de 189,52 milhões de registros. Com 158,41 milhões de registros, destaca-se o .com, conforme apontado na Tabela 2.

Tabela 2 – TOTAL DE REGISTROS DE DOMÍNIOS DOS PRINCIPAIS gTLD

Posição	gTLD	Número de domínios
1	**.com**	158.418.426
2	**.net**	13.289.632
3	**.org**	10.523.459
4	**.info**	3.828.293
5	**.xyz**	3.467.440

Data de coleta: 30 de novembro de 2021.
Fonte: DomainTools.com
Recuperado de: research.domaintools.com/statistics/tld-counts

APLICATIVOS E DADOS PESSOAIS NA PANDEMIA: O QUE PENSA A POPULAÇÃO BRASILEIRA?

As estratégias de adoção das tecnologias digitais no enfrentamento à pandemia ampliaram a coleta e o uso de dados pessoais. Veja a seguir dados[35] sobre a propensão da população usuária de Internet[36] no Brasil a baixar aplicativos relacionados à COVID-19, bem como suas percepções sobre os benefícios e os riscos da disponibilização de dados pessoais.

DONWLOAD DE APLICATIVOS DO GOVERNO COM INFORMAÇÕES SOBRE SINTOMAS E FORMAS DE TRATAMENTO

Entre usuários de Internet com 16 anos ou mais

20% BAIXARAM

19% NÃO BAIXARIAM

MOTIVOS PARA NÃO BAIXAR APLICATIVOS[37]

Entre os que não baixariam aplicativos

42%

- Não acha que ajuda a conter a pandemia
- Se preocupa que o governo possa vigiar a população após a pandemia

39%

- Não quer que o governo tenha acesso à sua localização
- Não acredita que o aplicativo não irá identificá-lo

PERCEPÇÃO DOS BENEFÍCIOS E RISCOS DE DISPONIBILIZAR SEUS DADOS PESSOAIS PARA O USO DE EMPRESAS OU GOVERNOS

Entre usuários de Internet com 16 anos ou mais

54% Mais riscos do que benefícios

16% Nem benefícios nem riscos

13% Mais benefícios do que riscos

17% Não sabe

O Núcleo de Informação e Coordenação do Ponto BR (NIC.br) e o Comitê Gestor da Internet no Brasil (CGI.br) possuem materiais informativos relacionados ao tema da privacidade e da proteção de dados pessoais. São eles:

• CARTILHA DE SEGURANÇA PARA INTERNET:

FASCÍCULO PRIVACIDADE (2020)

FASCÍCULO PROTEÇÃO DE DADOS (2021)

cartilha.cert.br/fasciculos/#privacidade | cartilha.cert.br/fasciculos/#protecao-de-dados

• SEMINÁRIOS DE PROTEÇÃO À PRIVACIDADE E AOS DADOS PESSOAIS:

seminarioprivacidade.cgi.br

[35] Dados do Painel TIC COVID-19, pesquisa *web* sobre o uso da Internet no Brasil durante a pandemia do novo coronavírus, do Cetic.br|NIC.br. Disponível em: https://www.cetic.br/pt/tics/tic-covid-19/painel-covid-19/2-edicao/

[36] Considera-se "usuária" a pessoa que utilizou a Internet pelo menos uma vez nos três meses que antecederam a entrevista.

[37] Refere-se a aplicativos que informem sintomas e formas de obter tratamento para a COVID-19 ou que avisem do contato com pessoas diagnosticadas com a doença.

/Créditos

REDAÇÃO

ARTIGO I
Miriam Wimmer
(Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP)

ARTIGO II
Jamila Venturini
(Derechos Digitales)

RELATÓRIO DE DOMÍNIOS
José Márcio Martins Júnior
(Cetic.br|NIC.br)

INFOGRAFIA E DIAGRAMAÇÃO
Giuliano Galves,
Klezer Uehara e
Maricy Rabelo
(Comunicação|NIC.br)

TRADUÇÃO PARA O PORTUGUÊS

ENTREVISTA I
Letralia

EDIÇÃO DE TEXTO EM PORTUGUÊS
Mariana Tavares

COORDENAÇÃO EDITORIAL
Alexandre F. Barbosa,
Tatiana Jereissati,
Javiera F. M. Macaya e
Luciana P. B. Lima
(Cetic.br|NIC.br)

AGRADECIMENTOS
Bertrand de la Chapelle e
Lorrayne Porciuncula
(Internet & Jurisdiction Policy Network)
Jamila Venturini
(Derechos Digitales)
Miriam Wimmer (IDP)
Nina da Hora (CTS/FGV)
Scarlett Fondeur Gil e
Torbjorn Fredriksson (Unctad)

*As ideias e opiniões expressas nos textos dessa publicação são as dos respectivos autores e não refletem necessariamente as do NIC.br e do CGI.br.

Organização das Nações Unidas para a Educação, a Ciência e a Cultura

cetic.br
Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação sob os auspícios da UNESCO

nic.br
Núcleo de Informação e Coordenação do Ponto BR

cgi.br
Comitê Gestor da Internet no Brasil

POR UMA INTERNET CADA VEZ MELHOR NO BRASIL

CGI.BR, MODELO DE GOVERNANÇA MULTISSETORIAL

www.cgi.br

nic.br cgi.br

FOTOS: RICARDO MATSUKAWA E SHUTTERSTOCK