



OS DADOS E O VÍRUS INFORME #6

Passaporte da Imunidade: a melhor estratégia para controle da COVID-19 ou arma de discriminação e outros problemas para a sociedade? Governo brasileiro cria mais de 130 serviços públicos em plataformas digitais durante a pandemia. GDPR completa 2 anos e especialistas questionam sua eficácia. Contact tracing: como andam as discussões sobre a tecnologia e aplicação pelo mundo. Você fica por dentro desta e de outras notícias no quinto informe do projeto “Os Dados e o Vírus”.

Passaporte da Imunidade: o que pensam os especialistas e quais seus riscos para a privacidade e proteção dos dados da população mundial

O que você precisa saber...

- Empresas criam Passaportes de Imunidade para países como Estados Unidos e Reino Unido
- Estônia está testando documento especial para cidadãos imunizados
- União Americana pelas Liberdades Civis (ACLU) demonstrou preocupações sobre tais passaportes
- Revista Nature listou 10 motivos para a não implantação do Passaporte da Imunidade pelo mundo

Assunto em alta há alguns meses em diversos países do mundo, o chamado “Passaporte da Imunidade” segue como alternativa para alguns governos, como evidenciou [matéria](#) da CNN na última semana.

Seja via exames de sangue que determinem se o indivíduo possui os anticorpos necessários para o retorno às atividades profissionais ou por meio de documentos e aplicativos, o tema tem ganhado discussão nos maiores veículos de imprensa, além de ONGs e grupos de pesquisas.

De acordo com uma [publicação](#) da Forbes, uma startup chamada FaceFirst, situada na Califórnia, Estados Unidos, está promovendo a ideia do “registro de imunidade a Coronavírus”. A tecnologia se baseia num banco de dados alimentado pelo sistema de saúde informando o status de imunidade dos cidadãos. Para acessar os dados sobre exames feitos, carga viral recebida e outras possíveis informações sobre contato com o vírus, o usuário deverá desbloquear o sistema com o reconhecimento facial.

O CEO da companhia, Peter Trepp, acredita que a medida pode trazer muitos benefícios em diversos lugares e momentos. “Eu acredito que, coletivamente, os dados podem ser úteis para determinar como você enche um avião, por exemplo. Você pode preencher um voo com pessoas livres do vírus e outro com passageiros já imunes”, explicou.



Trepp também acredita que o “Passaporte da Imunidade” será importante para o momento em que a vacina for descoberta, trazendo a prioridade para aqueles que não tiveram contato com a COVID-19.

No Reino Unido, a empresa Onfio tem proposto um [projeto semelhante](#), um sistema para cidadãos, convidados e funcionários terem provas de imunidade para comprovar seu estado de saúde. Neste caso, eles devem realizar o reconhecimento facial, mas sem a necessidade de compartilhar demais informações pessoais.

“A tecnologia é utilizada para vincular um ser humano à sua identidade digital, usando apenas uma foto e um vídeo formato selfie. Os resultados dos exames serão vinculados à imagem e o certificado digital poderá ser exibido, como cartões de embarques para smartphones”, contou Husayn Kassai, CEO da Onfio.

Enquanto países ainda discutem a possibilidade e viabilidade do documento, a Estônia já começou os testes de seu passaporte digital, conforme [matéria](#) da agência de notícias Reuters.

Taavet Hinrikus, fundador da Transferwise e membro da Back to Work, organização não governamental que desenvolve o passaporte, disse à publicação que o documento tem como objetivo diminuir os medos e estimular as sociedades de todo o mundo a seguir com suas vidas em meio à pandemia.

Apesar dos esforços para mostrar os pontos positivos por parte de empresas de tecnologias e governos, é clara a ansiedade sobre a possibilidade do monitoramento dos registros médicos de qualquer indivíduo.

Na última semana, a União Americana pelas Liberdades Civis (ACLU) [demonstrou](#) preocupações sobre tais passaportes, afirmando que certamente a nova infraestrutura de vigilância em saúde põe em risco os direitos à privacidade.

A Organização ainda observou que tal medida dividirá a população entre imunes e não imunes. “Pessoas não imunizadas dificilmente terão vantagens quando estiverem disputando uma vaga de emprego com alguém com anticorpos, por exemplo”, alertou.

Quem também se [mostrou contrária](#) à criação do Passaporte da Imunidade foi a Organização Mundial da Saúde. Entre seus principais motivos está o fato de que ainda não está comprovado cientificamente que os infectados com a COVID-19 de fato estão imunes à doença.

A Revista Nature também falou sobre o assunto em [artigo](#) e listou dez motivos pelos quais a criação de um documento seria impraticável, injusto e inseguro para a população em geral. Além da incógnita sobre o comportamento do Coronavírus no corpo humano está a não confiabilidade dos

testes existentes, já que boa parte dos exames que detectam anticorpos apresentam altas taxas de falsos positivos e negativos.

A falta de testes para os cidadãos também foi fator importante, já que boa parte das pessoas ainda não foi testada. A publicação afirmou que, caso apenas os imunes passem a ser liberados para retomar a economia, por exemplo, o número não seria o bastante para trazer eficácia ao plano.

"A baixa taxa de atingidos pela doença combinada com a capacidade limitada de teste, sem mencionar testes altamente não confiáveis, significa que apenas uma pequena fração de qualquer população seria certificada como livre para trabalhar", escreveram.

A Nature ainda aponta o monitoramento como fator de comprometimento da privacidade, podendo causar a marginalização dos não infectados ou até mesmo maior segregação racial ou social. Tais fatores podem gerar infecções intencionais de pessoas que não desejam ser rotuladas como vulneráveis e sofrer possíveis discriminações.

"Os passaportes de imunidade de hoje podem se tornar os passaportes biológicos abrangentes de amanhã", finalizaram.

Governo cria mais de 130 serviços públicos em plataformas digitais e dados pessoais podem estar em risco

O que você precisa saber...

- Desde o início da pandemia do novo Coronavírus, mais de 130 serviços públicos foram lançados em plataformas digitais
- Segundo Internetlab, os aplicativos não possuem garantias de privacidade e proteção de dados pessoais
- Idec publica lista com boas práticas de utilização de dados pessoais

Home office, reuniões por videoconferência, calls e toda uma transformação digital que aconteceria em anos, mas precisou ser antecipadas para meses. Essa foi a realidade do mundo inteiro nos últimos meses e, claro, no Brasil.

Somente durante o período da pandemia do novo coronavírus, o governo federal divulgou a criação de 130 serviços digitais até o momento, segundo [matéria](#) da Agência Brasil. Os aplicativos e serviços online criaram facilidades para uma parte da população, mas também trouxeram exclusão da parte não conectada e colocaram em cheque a proteção dos dados pessoais.

Entre os serviços mais procurados estão o auxílio emergencial, a solicitação do seguro desemprego, abono salarial, emissão do comprovante do Cadastro Único e obtenção da carteira de trabalho.



Lançado para evitar contágio e trazer informações sobre a doença, o aplicativo coronavírus-SUS já atingiu o número de 14 milhões de acessos únicos, de acordo com [site especial](#) feito pelo Ministério da Saúde.

O Centro de Pesquisa em Internet e Sociedade Internetlab [analisou](#) diversos aplicativos, inclusive do Governo Federal, investigando aspectos ligados à privacidade e proteção de dados.

A organização identificou exposição alta a riscos, incluindo nos aplicativos coronavírus-SUS e auxílio emergencial, em relação a garantias definidas na legislação.

“Se os aplicativos analisados não informam a respeito do tratamento que realizam para os objetivos do app, também não o fazem quanto a um eventual tratamento posterior dos dados, isto é, para outras finalidades além daquelas que o usuário consentiu. Considerando o potencial que os dados coletados têm de fornecer informações e qualificar o debate público e pesquisas a respeito da pandemia, esses novos usos deveriam ser considerados”, informaram os autores do estudo.

E não são apenas os aplicativos públicos que causam bastante preocupação em relação à privacidade e segurança dos dados pessoais.

O Instituto Brasileiro de Defesa do Consumidor (Idec) também se manifestou em relação aos riscos de exposição dos dados pessoais de milhões de usuários, tanto em aplicativos do governo como em diversos outros, como e-commerces e etc.

A pandemia intensificou a utilização de dados pessoais e os rastros digitais coletados pelos telefones celulares. Além do cadastro dos usuários nas plataformas, um dos dados mais relevantes neste período é o de geolocalização, bastante utilizado como possível ferramenta de contenção da COVID-19.

A publicação ressaltou o atraso da vigência da Lei Geral de Proteção de Dados no país e o atraso na criação da Autoridade Nacional de Proteção de Dados (ANPD). “É importante ressaltar que princípios relacionados ao direito à privacidade e a proteção de dados estão presentes em leis nacionais muito anteriores à LGPD, como o Código de Defesa do Consumidor, a Lei de Acesso à Informação, o Marco Civil da Internet e a Lei Geral de Telecomunicações, bem como a Constituição Federal”, acrescentou.

A organização elencou, num artigo, cinco recomendações básicas para o compartilhamento seguro de dados de geolocalização e orientações para evitar violações de direitos. Entre eles estão a transparência na utilização de dados, anonimização, descarte e não discriminação. Confira a [lista completa](#).

O coordenador da Associação Data Privacy Brasil de Pesquisa Rafael Zanatta falou sobre o risco da má utilização de dados pessoais e também sobre a importância da Lei Geral de Proteção de Dados na garantia da privacidade da população no país. Confira a [entrevista](#) para a TV Senado.

Confira, também, a [entrevista](#) de Rafael Zanatta sobre os riscos da vigilância na pandemia.

Em meio à pandemia, GDPR completa dois anos de desafios, sob questionamentos e longo caminho a percorrer

O que você precisa saber...

- No dia 25 de maio, a General Data Protection Regulation (GDPR) completou dois anos.
- a ONG Privacy Internacional publicou balanço sobre a lei, suas vitórias e suas falhas.
- A European Digital Rights (EDRi) publicou carta aberta aos regulamentadores da lei.
- A None of Your Business (NOYB) fez ponderações sobre a GDPR, colocando o foco em “como” criar tecnologia de acordo com a lei para combater a COVID-19.

O dia 25 de maio foi marcado pelo [2º aniversário](#) da General Data Protection Regulation (GDPR). Há dois anos, a lei tinha como objetivo punir práticas invasivas e utilização abusiva de dados pessoais por parte de grandes empresas e do setor público. Ao longo desse período a lei tem se mostrado presente, mesmo que, por vezes, sofra de falta de fiscalização, financiamento insuficiente e recursos limitados.

A lei ficou ainda mais em evidência com a chegada da pandemia do novo Coronavírus e, por consequência, a criação de aplicativos e tecnologias que visam conter o vírus, utilizando-se de extensas base de dados pessoais para tanto.

A ONG Privacy International fez um [balanço](#) da GDPR desde sua criação, passando por vitórias alcançadas e também o longo caminho que a lei ainda precisa percorrer. A publicação citou diversas empresas, o Facebook e até mesmo as eleições e o caso do Cambridge Analytica.

A organização revelou preocupação com a falta de fiscalização e falta de responsabilização das companhias. “Essas infrações não apenas exacerbam ainda mais a opacidade em torno do ecossistema de dados online, mas também constituem um grande obstáculo ao exercício efetivo dos direitos dos titulares de dados, minando efetivamente a proteção oferecida pela GDPR e a confiança das pessoas na lei para proteger seus direitos fundamentais”, acrescentou.

Acerca da aplicação da lei sobre as tecnologias criadas para combater a COVID-19, a Privacy International demonstrou desapontamento, afirmando que, infelizmente, a atenção para a transparência e finalidade não tem surtido efeito no Reino Unido e países que constituem a União Europeia.



“A GDPR é um projeto de longo prazo. Os últimos dois anos mal nos dão uma ideia se esse projeto será bem sucedido”, disse Eduardo Ustaran, que lidera a prática de privacidade no escritório de advocacia de Londres Hogan Lovells International, em [matéria publicada](#) pelo Estadão.

A European Digital Rights (EDRi), para celebrar a data comemorativa, escreveu uma [carta aberta](#) à GDPR. Nela, evidencia uma série de falhas, bem como falta de recursos e, inclusive, aponta ineficiência da aplicação da lei em casos de abuso do consentimento, falha no acesso a perfis comportamentais e falta de transparência das empresas.

Enquanto algumas publicações mostram dúvidas sobre a eficácia da lei nesse período e também seu papel durante a pandemia, o The New York Times publicou uma [matéria](#) afirmando que a GDPR é um ótimo “cão de guarda” para a população, mantendo em segurança - ou no caminho de - os dados pessoais e a transparência das empresas.

A None of Your Business (NOYB), [publicou um estudo](#) sobre a GDPR em meio à pandemia do novo Coronavírus e também fez um artigo especial, falando sobre a falta de compreensão entre a possibilidade da aplicação da lei em tecnologias ao combate da COVID-19 e a ilegalidade da apresentação de alguns aplicativos, sinalizando que a questão correta a ser debatida não é “se” mas “como” fazer isso da forma correta.

Max Schrems, presidente honorário da noyb, [relatou](#): “A GDPR prevê explicitamente o processamento de dados na luta contra epidemias. As leis de proteção de dados não devem, portanto, ser 'rejeitadas', mas simplesmente observadas”.

Contact Tracing: o que pensam as ONGs e especialistas da área de Proteção de Dados

O que você precisa saber...

- Países em todo o mundo buscam na tecnologia o controle do novo Coronavírus.
- ONGs acreditam que o trabalho digital deve ser atrelado a planos de saúde manuais e governamentais.
- Apesar do papel forte durante a pandemia, Apple e Google ainda são alvos de dúvidas e críticas.
- Transparência dos dados é o ponto mais preocupante na utilização do Contact Tracing, além de sua real eficácia.

O mundo segue na corrida tecnológica para descobrir a melhor forma de combater o novo Coronavírus. Enquanto empresas pelo mundo correm para descobrir o meio correto e mais eficiente,



população se torna cada vez mais receosa e especialistas mais preocupados com as consequências de produtos que desrespeitem a privacidade e com a utilização desenfreada de dados pessoais.

Sobre o assunto, a ONG Privacy International escreveu um [extenso artigo](#) sobre a “bagunça” que se tornou o Contact Tracing pelo mundo. A publicação fala sobre a urgência dos governos em descobrir uma fórmula rápida para o combate a COVID-19, sem depender da ciência para criação de vacinas, medicamentos ou necessidade de criação de hospitais e outros gastos elevados.

“Não está claro se alguns dos dados gerados pelos telefones celulares são úteis; e eles não serão tão confiáveis quanto o rastreamento manual de contatos. Tornar os aplicativos obrigatórios aumentará a desigualdade. Nenhum governo jamais soube tanto de você quanto pode estar prestes a fazê-lo”, afirmou a organização.

Apesar disso, membros do exército suíço, funcionários de hospitais e funcionários públicos podem instalar o aplicativo SwissCovid antes de uma implantação mais ampla planejada no país, segundo [reportagem](#) da BBC.

A tecnologia escolhida pela Suíça foi a desenvolvida pela parceria Apple-Google e envolve o rastreamento de contatos para detectar quando duas pessoas ficam próximas e se existe risco de contágio entre elas.

Assim como a Suíça, a Letônia também já [iniciou seus testes](#) com a plataforma das gigantes mundiais. A tecnologia é conhecida como descentralizada, ou seja, não fornece os dados pessoais para governos em uma base centralizada. Porém, ainda assim gera desconforto por parte de especialistas.

Em publicação recente, a Privacy International questionou se a reputação da Apple e do Google durante os tempos da COVID-19 seria suficiente para que todo seu passado fosse apagado. A publicação ainda [citou fato recente](#), em que um ex-colaborador da Apple afirmou ser possível ouvir gravações dos usuários da marca por meio da Siri.

A organização acrescentou: “Nossos dados pessoais, incluindo dados sobre nossa saúde, estão no cerne do modelo de negócios dessas empresas, pois são uma entrada essencial para o treinamento de modelos de IA, incluindo resultados de mecanismos de pesquisa. Nossos dados são o produto que eles comercializam. E dada a crescente importância dos dados em todos os setores da economia, essa concentração está se expandindo para outros setores, como a saúde.”

Neste cenário, países como o Reino Unido, França e algumas regiões dos Estados Unidos optaram pela criação dos próprios aplicativos, a fim de reter todas as informações dos usuários. Porém, a maioria deles já apresentaram algum tipo de falha, seja na política de privacidade ou no vazamento de dados pessoais.



De acordo [com o site](#) The Independent, o Care19, criado para a Dakota do Sul e do Norte tem vendido dados para companhias externas, apesar de não evidenciar isso na sua política de privacidade.

Isso traz ainda mais insegurança para seus usuários. De acordo com a Check Marx, mais da [metade da população](#) norte-americana não está disposta a aderir ao Contact Tracing como meio de combate à pandemia.

A ONG Algorithm Watch [publicou](#) uma série de observações sobre o assunto, ponderando a utilização dos aplicativos como “salvadores” da COVID-19 e alertando para outras frentes necessárias.

“A COVID-19 não é um problema tecnológico. Análises das respostas reais ao surto mostram que intervenções bem-sucedidas são sempre fundamentadas em políticas de saúde pública mais amplas. Cingapura, Coreia do Sul e Taiwan, frequentemente citadas como exemplos para manter a epidemia sob controle, todos tinham planos, a maioria deles projetados após o surto de SARS em 2003. A preparação para uma epidemia vai além das soluções técnicas: significa ter recursos, competências, planos, legitimidade política e vontade de implantá-los rapidamente quando necessário.”

LICENÇA DO DOCUMENTO

Este documento possui uma licença **Creative Commons CC-BY-NC 2.5**. Você pode reproduzi-lo, modificá-lo, reutilizá-lo livremente, desde que seja mencionada a autoria do documento e desde que seja para uma finalidade não comercial.

EQUIPE

Projeto “Os dados e o vírus”. Associação Data Privacy Brasil de Pesquisa. **Coordenação:** Rafael Zanatta & Bruno Bioni. **Equipe de pesquisa:** Mariana Rielli, Gabriela Vergili, Iasmine Favaro e Carolina Pain. **Apoio:** AccessNow.

IMPRENSA

Para contato com assessoria de imprensa e pedidos de colaboração (entrevistas e podcasts), favor enviar e-mail para imprensa@dataprivacybr.org. Informações sobre o projeto constam em dataprivacybr.org