OS DADOS E O VÍRUS
INFORME #5

Apesar de Medida Provisória, Senado aprova vigência de Lei Geral de Proteção de Dados para agosto deste ano. O Comitê Gestor da Internet no Brasil publica nota sobre tratamentos de dados pessoais durante pandemia. Microsoft e UnitedHealth lançam aplicativo de rastreamento de COVID-19 para retorno ao trabalho. Contact Tracing: como andam as experiências pelo mundo com a utilização da tecnologia. Você fica por dentro desta e de outras notícias no quinto informe do projeto "Os Dados e o Vírus".

Senado retoma decisão e mantém início da LGPD para agosto deste ano

O que você precisa saber...

- Votação do Senado retoma agosto de 2020 como data para a vigência da Lei Geral de Proteção de Dados no Brasil.
- Simone Tebet, relatora da matéria, afirmou que o texto foi feito por especialistas e pode entrar em vigor na data previamente definida.
- MP de Jair Bolsonaro, que adiava a vigência da LGPD para maio de 2021, ainda não foi apreciada pelo Congresso Nacional e pode caducar.

A Lei Geral de Proteção de Dados (LGPD) no Brasil contou com um novo capítulo de sua história na noite do dia 19 de maio. Após ter sido aprovada pelo Senado Federal para começar a vigorar no país em janeiro de 2021, com a aplicação das sanções previstas no Projeto de Lei 1.179/2020 a partir de agosto de 2021, a LGPD retoma o texto original e volta a valer a partir de agosto deste ano.

Davi Alcolumbre escreveu sobre a decisão logo após a sessão em sua conta do Twitter: "O @SenadoFederal aprovou, agora à noite, a antecipação da vigência para este ano ainda da Lei Geral de Proteção de Dados (LGPD), principal legislação na prevenção e combate aos ataques criminosos promovidos pelas Fake News no país. O Congresso continuará atento ao tema."

No início do mês, o presidente Jair Bolsonaro, por meio da Medida Provisória 929/2020, havia adiado a vigência da lei de proteção de dados para maio de 2021.

A relatora da matéria, a senadora Simone Tebet (MDB-MS), defendeu a manutenção do texto original de Antonio Anastasia (PSD-MG), aprovado pelo Senado ainda em Abril. Ela argumentou que a MP ainda não foi apreciada pelo Congresso Nacional e que seu conteúdo pode vir a ser rejeitado integralmente, pode ter o dispositivo referente à data da entrada em vigor suprido ou ainda caducar por não ser aprovado dentro do prazo constitucional.

"É bom lembrar que esse projeto foi feito por especialistas, com participação da Universidade de São Paulo e tribunais superiores. Foi construído um texto com amplo consenso entre os senadores", ressaltou Simone Tebet.

Apesar da afirmação, o texto passou por mais uma alteração no Senado. O senador Weverton (PDT-MA) destacou que a LGPD passe a valer em agosto deste ano, com a ressalva de que os artigos que tratam das sanções só entrarão em vigor em agosto de 2021. O senador acredita que a mudança será importante para o tratamento das *fake news*. O destaque foi aprovado, com 62 votos a 15.

"A Medida Provisória 959 vai caducar, porque foi feita para auxiliar no auxílio emergencial e isso já está sendo feito. Já falei com vários líderes e a Câmara vai deixar caducar. Portanto, se os senadores que querem ajudar a combater *fake news*, algo importante, afinal estamos em ano eleitoral, estamos em meio a uma pandemia, ela deve vigorar agora", disse o senador Wewerton.

GCI emite Nota Pública sobre tratamento de dados pessoais e vigilância durante a pandemia do COVID-19

O que você precisa saber...

- Comitê Gestor da Internet no Brasil afirmou que a privacidade e a proteção de dados pessoais são valores que devem ser preservados.
- GCI pediu transparência sobre utilização de dados, armazenamento e descartes em aplicativos desenvolvidos para combater o Coronavírus
- Comitê reafirmou que toda tecnologia deve ser analisada antes de ser colocada em desenvolvimento e utilização do público.

No dia 19 de maio, o Comitê Gestor da Internet no Brasil (GCI.br) emitiu uma Nota Pública sobre vigilância e a utilização dos dados pessoais no combate ao Coronavírus e todos os cuidados que devem ser tomados em diferentes tecnologias.

O Comitê iniciou a publicação baseando-se no uso das atribuições que lhe confere o Decreto nº 4.829/2003, bem com o inc. I, do art. 24, da Lei 12.965/2014, e também com base no Decálogo de Princípios de Governança da Internet.

A nota foi dividida em seis pontos, sendo o primeiro a reafirmação da importância da internet e de outras tecnologias digitais no enfrentamento da COVID-19 com garantia aos direitos humanos fundamentais.

O CGI também afirmou entender que a manutenção da saúde da população, a privacidade e a proteção de dados pessoais dos indivíduos são valores que devem ser igualmente preservados em nossa sociedade.

O GCI alertou que a transparência e a segurança dos dados devem ser asseguradas, bem como a divulgação dos procedimentos de tratamento, guarda, compartilhamento e seu descarte. Além disso, prevê o acesso a auditorias independentes como certificador de segurança.

Por fim, reafirmou: "a eventual instalação de aplicativos de acompanhamento de casos de coronavírus SARS-COV-2 deve ser previamente informada a todos, de maneira ostensiva, observando-se os princípios estabelecidos pela Lei 12.965/2014, pelo Decreto 8.771/2016, bem como pela Lei 13.709/2018. Seu uso não deve se prestar à estigmatização ou discriminação de qualquer segmento da população".

A entidade teve papel central na formulação da LGPD e na organização dos Seminários de Privacidade, como destacado no projeto Memória da LGPD.

Microsoft e UnitedHealth Group lançam aplicativo para a retomada ao trabalho e rastreamento de sintomas do COVID-19

O que você precisa saber...

- Microsoft e UnitedHealth utilizarão coletas de dados e Inteligência Artificial em novo aplicativo.
- Empresas poderão controlar a segurança do ambiente de trabalho por meio de informações enviadas pelos colaboradores para o aplicativo.
- Microsoft garantiu que os dados serão responsabilidade da UnitedHealth Group, não tendo acesso a nenhum dado identificável.

A Microsoft anunciou a criação de um novo aplicativo com a parceria do UnitedHealth Group. O ProtectWell™ tem como objetivo atuar no retorno ao local de trabalho dos usuários, bem como apresentar espaços seguros de tráfego e empresas seguindo todas as normas.

O aplicativo, segundo releases das empresas, incorpora as diretrizes dos Centros de Controle e Prevenção de Doenças (CDC, em inglês) e os estudos referentes ao vírus. Assim como em outros aplicativos lançados pelo mundo, o usuário informa sintomas e a tecnologia estabelece diretrizes para apoiar a saúde e segurança da força de trabalho, bem como do espaço físico profissional.

A parceria entre as duas marcas combina os recursos clínicos e de análise de dados do UnitedHealth Group, com a liderança tecnológica da Microsoft. O ProtectWell™ é desenvolvido com as soluções Microsoft Azure, Inteligência Artificial e soluções analíticas, além do serviço já existente Healthcare Bot - coletando dados para triagem de sintomas do Coronavírus.

No dia-a-dia, o app funciona da seguinte forma: o usuário faz o download no próprio aparelho celular e responde uma série de perguntas. Caso o risco de infecção seja indicado, as empresas podem direcionar seus funcionários para um processo de teste simplificado do COVID-19. Além

disso, o App dá diretrizes e recursos para apoiar o ambiente de trabalho, como regras de distanciamento social, saneamento e etc.

“Enquanto planejamos um retorno seguro e cuidadoso ao local de trabalho, os empregadores precisam de diretrizes claras para garantir um ambiente seguro e um processo robusto para que os funcionários examinem seus sintomas de COVID-19”, disse Ken Ehlert, diretor científico do UnitedHealth Group.

Segundo a Microsoft, os dados pessoais e de saúde coletados pelo aplicativo serão gerenciados por meio da aceitação e consentimento de seus usuários. A UnitedHealth será a responsável pelos mesmos, sendo que a gigante da tecnologia não terá acesso a informações identificáveis compartilhadas pelo App.

A Microsoft vai implantar o serviço para o retorno de seus colaboradores nos Estados Unidos.

Dados privados e aplicativos de rastreamento: o que sabemos até o momento sobre sua segurança?

O que você precisa saber...

- Governo Chinês pede que cidadãos coloquem dados pessoais, incluindo fotos, em seus aplicativos de rastreamento e combate ao Coronavírus.
- Testes do Reino Unido não são conclusivos e NHS é questionada sobre segurança e privacidade dos dados coletados.
- Nature lança artigo sobre Contact Tracing e questiona sua eficácia.

Além da Microsoft, diversas outras empresas e governos estão investindo em aplicativos de Contact Tracing ou outras tecnologias, a fim de monitorar casos de Coronavírus, coletar dados de infectados e tentar controlar a pandemia.

Na China, por exemplo, os aplicativos estão por toda parte e para as mais diferentes finalidades. As autoridades coletam e armazenam grandes quantidades de informações de seus cidadãos, que não possuem a liberdade de escolher entre usar ou não, já que funcionam nos aparelhos mesmo sem consentimento dos mesmos.

Assim como em outros lugares do mundo, parte da população não tem se preocupado com a captação de dados pessoais por parte desses aplicativos e governos. “A epidemia é um contexto particular. A vida humana é a coisa mais importante”, disse uma funcionária pública que vive em Xangai à AFP.

São diversos aplicativos por todo o país, sendo alguns baseados em geolocalização, outros contact tracing e também alguns que analisam histórico de saúde de usuários. O que todos têm em comum é que, depois do download, é necessário digitar nome, número de identidade, endereço, telefone e, por vezes, uma foto.

“No final, quem tem acesso a esses dados? Estão à mercê de um hacker? Sabemos que o estado não venderá as informações, mas sempre existe o risco de um funcionário fazer isso em benefício próprio”, afirmou Cui Xiaohui, professor do Centro de Pesquisa de Metadados e Inteligência Artificial da Universidade de Wuhan, cidade onde o novo coronavírus apareceu.

A mesma preocupação existe no Reino Unido. No dia 18 de maio, advogados especialistas em privacidade de dados cobraram do Serviço Nacional de Saúde (NHS, em inglês) transparência sobre o armazenamento de dados do aplicativo de Contact Tracing que está prestes a ser lançado em todos os países que compõem as terras da Rainha Elizabeth.

"As emergências exigem respostas rápidas, mas essas respostas também devem ser apropriadas, legais e justas. É improvável que o plano atual do NHS de construir um armazenamento de dados COVID-19 em grande escala atenda a esses princípios. Entendemos a necessidade de melhores informações sobre saúde, mas reiteramos que o público deve ser consultado durante a finalidade do armazenamento de dados e ser capaz de obter informações adequadas sobre os acordos de compartilhamento de dados em vigor", afirmou, em carta aberta, um grupo composto por membros da sociedade civil, advogados e organizações direcionadas à proteção de dados.

O Centro Nacional de Segurança Cibernética (NCSC) do Serviço de Inteligência britânico disse à BBC, em entrevista publicada no dia 19 de maio, que já está ciente da maioria das questões levantadas e está no processo de resolvê-las.

A NHS, desde o início dos testes da Ilha de Wight, afirmou tratar os dados dos usuários de forma segura e seguindo especificações. Apesar disso, até mesmo os testes na região escolhida ainda são inconclusivos.

No dia 19 de maio, a revista científica Nature publicou um artigo sobre a segurança da tecnologia de Contact Tracing e também sua eficácia. Dentre os assuntos discutidos, a publicação ressalta a necessidade humana para captação de dados, informações e também atendimento durante todo o processo de identificação de um infectado. Bem como a necessidade de aderência da população para que a tecnologia seja, de fato, mais eficaz.

“O importante entender de tudo isso é que: tudo pode virar lixo. Pode ser que nada disso funcione. Mas, ainda assim temos que tentar. Não sabemos nada concreto”, disse Matthew Green, um criptógrafo da Universidade Johns Hopkins, em Baltimore, Maryland. “Temos que tentar. Nós simplesmente não sabemos. "

A publicação ressalta a diferença entre ter um aplicativo centralizado - quando o próprio governo cria a plataforma e cuida dos dados pessoais dos usuários - e o sistema descentralizado, este desenvolvido por uma empresa que garanta o tratamento e privacidade dos mesmos.

A Nature ainda parabenizou os esforços das empresas Apple e Google - parceria chamada Gapple - e sua preocupação com a criptografia de dados e protocolos de segurança.

LICENÇA DO DOCUMENTO

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