SEU NÚMERO DE PROTOCOLO:

25072.010199/2020-13

CÓDIGO DE ACESSO AO PROTOCOLO:

rerx7156

*A **Open Knowledge Brasil (OKBR)**, pessoa jurídica de direito privado, constituída na forma de associação privada sem fins lucrativos, inscrita no CNPJ/MF sob o nº 19.131.243/0001-97, com sede na Avenida Paulista, nº 37, Andar 4, Bairro Bela Vista, Cidade de São Paulo, Estado de São Paulo, CEP 01.311-902, neste ato representada por sua diretora-executiva Fernanda Campagnucci Pereira, brasileira, gestora, RG nº [redacted], CPF nº [redacted], vem apresentar a seguinte DENÚNCIA, com base nos fundamentos abaixo.*

1. Problemas identificados

1.1. Violação da privacidade e da proteção de dados pessoais de todos os brasileiros que tiveram seus dados registrados no sistema e-SUS Notifica, com suspeita ou confirmação de Covid-19.

1.2. Afronta ao Art. 5º, inciso X da Constituição Federal de 1988, que dispõe sobre o direito à privacidade;

1.3. Descumprimento do Art. 6º, inciso III da Lei Federal nº 12.527/2011 (Lei de Acesso à Informação Pública), que determina aos órgãos públicos a obrigação de proteger informação pessoal;

1.4. Descumprimento da Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), em especial de seu Art. 46, que trata das medidas de segurança, técnicas e administrativas, para proteger os dados pessoais.

2. Prováveis responsáveis

2.1. Ministério da Saúde e seus eventuais fornecedores de tecnologia.

3. Descrição do problema

3.1. Na noite de 04/06/2020, identificamos uma grave vulnerabilidade de segurança no e-SUS Notifica, do Ministério da Saúde (https://notifica.saude.gov.br/login). Esse sistema é o canal oficial para o registro das notificações compulsórias de casos de Covid-19 no país, e a referida falha expõe dezenas de informações pessoais e estado de saúde de cada um dos centenas de milhares de indivíduos que foram cadastrados pelos estabelecimentos de saúde de todo o país.

3.2. A falha é a exposição indevida das credenciais (usuário, senha e demais informações) do banco de dados armazenado em “bucket” da Amazon Web Services (local onde os dados são depositados e acessados na nuvem). Pela análise do código disponível a qualquer pessoa na web, trata-se de uma funcionalidade de exportação de relatórios do sistema, que deveria ser acessível somente para gestores com perfil de acesso criteriosamente concedido para acesso seguro por estrita necessidade funcional.

3.3. Causa espanto que a segurança de um sistema dessa importância e magnitude seja tratada com tanto descaso. Expor as credenciais do banco de dados no próprio código do site é um erro primário que sugere inépcia ou imperícia de quem desenvolveu, supervisionou e homologou a implementação do sistema. Equivale a deixar a chave de um cofre na porta do mesmo.

3.4. A exposição das credenciais pode ser verificada no próprio navegador (com a ferramenta “Inspecionar Elemento” presente nos principais navegadores web). Na aba “Network” (ou “Rede”), é possível encontrar o arquivo JavaScript chamado “main-es2015.e34b7d4f2c26ea460510.js”, acessível nesta URL https://notifica.saude.gov.br/main-es2015.e34b7d4f2c26ea460510.js. O arquivo é extenso, mas a ferramenta de localizar palavra-chave na página pode ser usada para facilmente encontrar as credenciais, com o termo “S3_SECRET_KEY_ID”. Naquele trecho, estão exposta as diversas informações que permitiriam a qualquer pessoa na web ter acesso não autorizado a esses dados.

3.5. Tão-logo tomou conhecimento da vulnerabilidade, a Open Knowledge Brasil (OKBR), representada por sua diretora-executiva, registrou o referido trecho em Ata Notarial no 12º Tabelião de Notas da Comarca da Capital do Estado de São Paulo, conforme documento anexo, para que possa ser usada posteriormente como prova da irregularidade ora denunciada. No momento de registro desta denúncia, 07/06/2020, o trecho continua no ar. É possível que tenha ali estado desde o momento de seu lançamento, há meses.

3.6. Houve tentativa, em 07/06/2020, de protocolar esta mesma denúncia na Ouvidoria do SUS, já que o Ministério da Saúde é o controlador legal dos referidos dados. No entanto, um dos campos obrigatórios, “Ouvidoria”, está com defeito e não permite fazer nenhuma seleção para seguir com o protocolo (houve tentativa nos três principais navegadores: Chrome, Firefox e Internet Explorer). Além disso, possui limite de 3 mil caracteres e não permite o envio de anexos, impossibilitando a adequada fundamentação da denúncia.

4. Requerimentos

4.1. Requeremos, diante a gravidade do exposto, e visando proteger informações pessoais e sensíveis de centenas de milhares de cidadãos em situação de vulnerabilidade por motivo de saúde, a RETIRADA IMEDIATA das credenciais do banco de dados que estão expostas no site.

4.2. Requeremos a investigação sobre a possível inexistência ou inobservância de protocolos de segurança para essa e outras bases de dados que contêm informação pessoal no Ministério da Saúde. De acordo com a LGPD, a segurança de bases de dados consiste na “utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (Art. 6º, inciso VII).

4.3. Requeremos que seja realizada auditoria para confirmar a vulnerabilidade e averiguar a extensão dos danos eventualmente provocados, por exemplo, com a verificação de logs do servidor que hospeda o banco de dados para identificar possíveis acessos e usos indevidos dessas informações sensíveis.

4.4. Requeremos que seja apurada a RESPONSABILIDADE administrativa, funcional e civil de agentes públicos ou eventualmente de terceiros contratados sobre o ocorrido.

4.5. Requeremos, nos termos do Art. 5º, XVII, da LGPD, que seja publicizado relatório de impacto à proteção de dados pessoais, documentação que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

5. Documentos Anexos

5.1. Ata Notarial