EXCELENTÍSSIMO(A) SENHOR(A) PROCURADOR(A) DA REPÚBLICA - PROCURADORIA REGIONAL DA REPÚBLICA DOS DIREITOS DO CIDADÃO - SÃO PAULO

IDEC – INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR, associação de consumidores sem fins lucrativos e de utilidade pública federal, legalmente constituída desde 1987 (**DOCS. 1 e 2)**, inscrita no CNPJ sob o nº 58.120.387/0001-08, com sede na Rua Dr. Costa Júnior, 543, São Paulo/SP, CEP 05002-000, endereço eletrônico coex@idec.org.br, por meio de sua Representante Legal, Coordenadora Executiva, Teresa Donato Liporace (**DOCS. 3 e 4**), vem respeitosamente, perante Vossa Excelência, com base nos arts. 127 e 129 da Constituição Federal (CRFB/88), no art. 12, da Lei Complementar nº 75/1993 e na Lei 7.347/1985, apresentar **NOTÍCIA DE FATO**, em face do **HOSPITAL ALBERT EINSTEIN**, pessoa jurídica de direito privado, inscrita no CNPJ/MJ sob o nº 60.765.823/0001-30, sediado na Av. Albert Einstein, nº 627, São Paulo/SP, CEP 05652-900 e, em face da **UNIÃO FEDERAL,** pessoa jurídica de direito público, representada pela Advocacia Geral da União, considerando os fatos e fundamentos jurídicos a seguir indicados.

I. Introdução: Relevância do tema e competência da Procuradoria Regional dos Direitos do Cidadão em São Paulo para conhecer e processar a presente notícia de fato

1. O comunicante é pessoa jurídica de direito privado, representante da Sociedade Civil[1]. A República Federativa do Brasil apoia sua existência na Democracia, onde se proclama que "todo o poder emana do povo" (art. 1º, § único, CF/1988).

2. A delegação deste poder ao Estado não retira da Sociedade Civil o poder de exercer seus direitos plenamente, especialmente o de solicitar a apuração de atos e fatos ilegais, quem quer que os tenha cometido.

3. Ao longo de suas três décadas de existência, este instituto consolidou forte atuação nas esferas judicial e extrajudicial para a proteção dos direitos dos usuários de serviços de

[1] A missão institucional do Idec é promover a educação, a conscientização, a defesa dos direitos do consumidor e a ética nas relações de consumo, com total independência política e econômica (Art. 1º, parágrafo único e art. 2º, do Estatuto do Idec, Documento Anexo).

saúde, sejam estes no âmbito da saúde suplementar, sejam estes no âmbito do Sistema Único de Saúde (SUS).

4. Ao fazê-lo, a entidade subscritora opta pelo encaminhamento desses fatos à sólida e competente Instituição do Ministério Público Federal (art. 128, I, "a" c/c 129, III, CF/1988), dadas suas atribuições e a natureza dos fatos aqui colocados.

5. O endereçamento de postulações da sociedade civil é uma ferramenta democrática que, para muito além de uma mera opinião pública, vocaliza o verdadeiro anseio da principal peça-chave de uma República: Seu Povo.

6. A LC n. 75/1993 dispõe sobre a competência do Ministério Público Federal (e, consequentemente, da Justiça Federal) e sua atribuição de promover a responsabilidade de autoridades públicas da União por atos ilegais que tenham cometido (art. 6º, incisos VII, alíneas "a" e "c"; X; XIV, alíneas "a", "c", "e", "f"; XVII, "a" e XX).

7. O Ministério Público Federal é instituição que age de ofício ou por impulso da população. A Resolução 174/2017-CNMP disciplina que qualquer instituição pode demandar a atuação do Parquet para que, em sua atividade fim, promova suas atribuições legais (LC 75/1993) e constitucionais (art. 129, CF/1988).

8. Ademais, também é atribuição ministerial a expedição de recomendações para a melhoria da prestação de serviços públicos e/ou de relevância pública, como também o respeito nos direitos envolvidos no âmbito destes serviços, podendo fixar, ainda, um prazo razoável para a adoção das medidas e providências adequadas. É o que se entende da exegese do art. 6º, inciso XX da LC 75/1993.

9. A LC 75/1993, ainda, prevê a criação de uma unidade especial das Procuradorias Regionais, visando à defesa de direitos constitucionalmente previstos, dando-se especial destaque à saúde, à intimidade e à vida privada. Trata-se da Procuradoria dos Direitos do Cidadão, que, zelará pelo respeito e pleno exercício dos direitos indicados por aqueles que auxiliam na prestação de serviços públicos. *In verbis*, esta é a previsão da Lei Complementar:

> Art. 11. A defesa dos direitos constitucionais do cidadão visa à garantia do seu efetivo respeito pelos Poderes Públicos e pelos prestadores de serviços de relevância pública.
>
> Art. 12. O Procurador dos Direitos do Cidadão agirá de ofício ou mediante representação, notificando a autoridade questionada para que preste informação, no prazo que assinar.

10. Da leitura do capítulo referente à exposição dos fatos, verifica-se que a exposição de dados sensíveis e os danos à privacidade ocorreram em virtude do tratamento de dados governamentais sensíveis por uma pessoa jurídica de direito privado, localizada em São Paulo, no âmbito de uma programa governamental para ampliar acesso ao SUS, nos termos da Lei nº 12.101/2009.

11. Portanto, é inquestionável as atribuições institucionais *ratione loci* e *materiae* que detém a Procuradoria Regional da República em São Paulo, conforme a Lei Orgânica Ministerial, para receber e processar a presente notícia de fato.

12. É dentro deste contexto que o Idec, cumprindo com sua missão institucional de defesa do consumidor, tem acompanhado com total atenção as notícias que dão conta de um episódio gravíssimo, consistente no vazamento de dados e informações pessoais de, aproximadamente, 16 milhões (dezesseis milhões) de brasileiros com diagnósticos confirmados ou não de covid-19, conforme se passa a expor.

II. Dos fatos noticiados submetidos à apreciação do MPF

13. De acordo com informações constantes em jornais de grande visibilidade, no âmbito da parceria existente entre o Hospital Albert Einstein e SUS, ocorreu o vazamento de senhas que concediam acesso a bases de dados governamentais com informações de 16 milhões de pessoas, distribuídas por todo o país, com diagnóstico ou suspeita de covid-19[2].

14. Vale apontar que a parceria existente entre o Hospital Albert Einstein e o Ministério estaria localizada no âmbito do Programa de Apoio ao Desenvolvimento Institucional do Sistema Único de Saúde (PROADI-SUS), iniciativa que contempla cinco hospitais privados no país para o desenvolvimento de projetos específicos[3].

[2] Informações sobre o ocorrido podem ser verificadas nos seguintes endereços eletrônicos, anexos também a presente representação: **Vazamento de senha do Ministério da Saúde expõe dados de 16 milhões de pacientes de covid -** Disponível em <https://saude.estadao.com.br/noticias/geral,vazamento-de-senha-do-ministerio-da-saude-expoe-dados-de-16-milhoes-de-pacientes-de-covid,70003528583>. **Vazamento expõe dados de 16 milhões de pacientes de Covid-19**. Disponível em <https://www.istoedinheiro.com.br/vazamento-expoe-dados-de-16-milhoes-de-pacientes-de-covid-19/>. **Vazamento de senhas do Ministério da Saúde expõe informações de pacientes de Covid-19, diz jornal**. Disponível em <https://g1.globo.com/bemestar/coronavirus/noticia/2020/11/26/ vazamento-de-senhas-do-ministerio-da-saude-expoe-informacoes-de-pessoas-que-fizeram-testes-de-covid-19-diz-jornal.ghtml>. Todos os acessos em 26 nov. 2020.

[3] Disponível em: <https://hospitais.proadi-sus.org.br/sobre-o-programa>

15. O Programa envolve parcerias entre o Ministério da Saúde e entidades de interesse social de excelência, certificadas de acordo com a Lei 12101/09, o Decreto nº 8.242/14 e a Portaria GM/MS nº 3.362/2017.

16. As reportagens indicam que as senhas estavam armazenadas em uma plataforma chamada "github" por aproximadamente um mês. Com estas, por sua vez, concedia-se autorização de acesso a duas plataformas eletrônicas públicas federais, em que são registrados dados sobre a situação de saúde de pessoas com contaminação suspeita ou confirmada pela covid-19, tais sejam, a **E-SUS-VE,** em que se noticia casos leves e moderados e o **Sivep-Gripe**, em que se noticia casos de Síndrome Respiratória Aguda (SRAG).

17. Além da exposição dos dados relacionados à covid propriamente dita, também permaneceram expostos números de CPF, endereço, telefone e até mesmo **dados do prontuário médico e de diagnósticos de doenças ou lesões preexistentes**[4].

18. É o que se lê, por exemplo, do jornal Estadão, conforme segue:

> "Ao menos 16 milhões de brasileiros que tiveram diagnóstico suspeito ou confirmado de covid-19 ficaram com seus **dados pessoais e médicos expostos na internet durante quase um mês por causa de um vazamento de senhas de sistemas do Ministério da Saúde**.
> [...]
> A exposição de dados não foi causada por ataque hacker nem por falha de segurança do sistema. Eles ficaram abertos para consulta após um funcionário do Hospital Albert Einstein divulgar uma lista com usuários e senhas que davam acesso aos bancos de dados de pessoas testadas, diagnosticadas e internadas por covid nos 27 Estados. Conforme o Einstein, o hospital tem acesso aos dados porque está trabalhando em um projeto com o ministério.
>
> **Com essas senhas, era possível acessar os registros de covid-19 lançados em dois sistemas federais: o E-SUS-VE, no qual são notificados casos suspeitos e confirmados da doença quando o paciente tem quadro leve ou moderado, e o Sivep-Gripe, em que são registradas todas as internações por Síndrome Respiratória Aguda Grave (SRAG), ou seja, os pacientes mais graves**.
>
> [...]

[4] Termo técnico que designa as doenças de que o usuário sabe ser portador no momento de uma determinada consulta médica ou contratação de serviço ou plano de saúde de saúde.

> Os bancos de dados do ministério trazem, além das informações pessoais dos pacientes, detalhes considerados confidenciais sobre o histórico **clínico, como a existência de doenças ou condições pré-existentes, entre elas diabete, problemas cardíacos, câncer e HIV**". (sem grifos no original).

19. Vê-se, portanto, a **gravidade dos fatos narrados**. **Em plena pandemia**, estima-se que milhões de pessoas tiveram seus dados pessoais e de saúde tratados sem o devido cuidado e proteção, estando à disposição de acesso a quem tivesse contato com as senhas, em total desrespeito à Lei Geral de Proteção de Dados Pessoais e ao Código de Defesa do Consumidor, o que denota a especial atenção desta Procuradoria para atuar no caso.

III. Da violação à Lei Geral de Proteção de Dados e ao Código de Defesa do Consumidor: inobservância dos princípios da segurança e prevenção e a direitos básicos do consumidor

20. No Brasil, não há dúvidas de que a proteção de dados pessoais é um direito decorrente dos direitos fundamentais à vida privada e intimidade, conforme definido no artigo 5º, caput e inciso X, ambos da Constituição Federal.

21. Recentemente, o Supremo Tribunal Federal referendou esse entendimento, ao julgar medida liminar em face da Medida Provisória (MP) nº 954, de 2020, por meio da qual autorizou-se o compartilhamento de dados pessoais de consumidores de serviços de telefonia com o IBGE (Instituto Brasileiro de Geografia e Estatística) para fins de "produção estatística oficial". Em face da referida MP, foram propostas cinco Ações Diretas de Inconstitucionalidade, tendo sido deferida a medida liminar pela Relatora dos casos, Ministra Rosa Weber, em decisão que foi confirmada pela maioria do Plenário do STF.

22. Em sua decisão liminar, a Min. Relatora Rosa Weber defendeu que as informações "relacionadas à identificação – efetiva ou potencial – de pessoa natural, configuram dados pessoais e integram, nessa medida, o âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII).". A Relatora enfatizou que é necessário respeitar os preceitos fundamentais de liberdade individual, privacidade e livre desenvolvimento da personalidade individual.

23. A Lei Geral de Proteção de Dados (Lei nº 13.709/2018), ao descrever os princípios, regras gerais e direitos disponíveis aos titulares de dados, estabelece uma série de definições para o resguardo e controle dos cidadãos brasileiros sobre suas informações pessoais.

24. Com o intuito de garantir maiores critérios de segurança e prevenção a informações que tivessem a capacidade de oferecer maiores riscos aos titulares de dados, a Lei criou a categoria dos **dados sensíveis**. Estes, descritos no Art. 5º, II, da LGPD, abrangem qualquer "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, **dado referente à saúde** ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

23. A gravidade do incidente ainda surpreende pela ausência de cuidados básicos relacionados à segurança das informações armazenadas.

24. Primeiro, chama atenção o fato de existir uma tabela com todos os *logins*, usuários e senhas de funcionários autorizados para operar um banco de dados sensíveis com milhões de brasileiros. Senhas, conforme qualquer especialista em segurança da informação[5], não devem ser deixadas escritas. Ou seja, já se trata de antemão de uma negligência dos responsáveis deixar isso exposto a qualquer funcionário.

25. Em segundo lugar, surpreende o fato de medidas de segurança relacionadas ao acesso ao banco de dados não terem sido adotadas. A autenticação em dois fatores tem sido utilizada já em larga escala, mesmo para acesso a aplicações básicas como e-mail. Com isso, seria possível evitar que um terceiro tivesse acesso a esse banco de dados sem que antes sua identidade fosse checada pelo sistema. Trata-se, mais uma vez, de um recurso de segurança simples, cuja ausência evidencia a falta de cuidados e prudência relacionada ao tratamento dessas informações.

26. É grave o fato de que nenhum outro critério de segurança rigoroso tenha sido adotado, especialmente considerando-se a sensibilidade dos dados e os riscos de exposição relacionados. Destaca-se, aqui, a ausência de mecanismos como a criptografia dessas informações ou mesmo a anonimização dos dados, o que evitaria a exposição de nomes e números de registros civis.

27. A reiterada ausência de preocupação com mecanismos de segurança aplicáveis ao armazenamento dos dados revela que houve, inegavelmente, falha com relação ao atendimento de garantias básicas e negligência por parte dos responsáveis pelo tratamento desses dados.

---

[5] Tal informação é sugerida pela nota do Ministério da Saúde sobre o ocorrido, divulgada em diferentes veículos de imprensa, por exemplo, como na notícia disponível no link a seguir, que também discrimina a nota na íntegra.: <https://g1.globo.com/bemestar/coronavirus/noticia/2020/11/26/vazamento-de-senhas-do-ministerio-da-saude-expoe-informacoes-de-pessoas-que-fizeram-testes-de-covid-19-diz-jornal.ghtml>

28. Tais garantias básicas encontram respaldo legal, como já repisado, tanto na Lei Geral de Proteção de Dados Pessoais, como também no Código de Defesa do Consumidor (CDC).

29. A Lei Geral de Proteção de Dados descreve, no artigo 6º, os seguintes princípios:

> VII - **segurança**: 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;
>
> VIII - **prevenção**: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

30. Ainda, a segurança é direito básico do consumidor, como afirmado pelo artigo 6º, inciso I, do CDC. Entende-se que a segurança neste caso não compreende apenas a integridade física dos consumidores, mas também a segurança informacional, isto é, a integridade de suas informações e dados pessoais.

31. A ausência de medidas técnicas e administrativas aptas a proteger esses dados, somada à ausência de medidas capazes de prevenir a ocorrência desse dano, gerou um cenário de descaso. O resultado foi a vulnerabilidade de dados sensíveis de milhões de cidadãos brasileiros, que hoje ficam expostos a quaisquer possibilidades de práticas ilícitas e maliciosas de terceiros sob posse dessas informações. Os requisitos legais - o respeito ao princípio da prevenção e à segurança como direito básico dos cidadãos - não foram observados, ficando assim evidente a violação cometida pelas representadas.

32. Vale lembrar, neste sentido, que a vulnerabilidade é pressuposto das relações de consumo (art. 4º, inciso I, CDC). E a vulnerabilidade, no presente caso, ganha especial relevo pela exposição de dados em testilha ter ocorrido em plena pandemia, momento de instabilidade sanitária em que as pessoas já passam por inúmeras dificuldades.

33. E não há que se olvidar, ainda, que existem outros direitos básicos do consumidor a serem protegidos no que se refere à proteção de dados, tais como o direito à informação expressa e adequada, assim como a efetiva reparação pelos danos materiais e morais, individuais e coletivos, sofridos. É o que estabelece o art. 6º, incisos III e IV, do CDC.

34. Por fim, é importante mencionar que tanto a LGPD quanto o CDC preveem a modalidade de responsabilidade dos agentes envolvidos **nas formas objetiva e solidária** quando ocorrer violação a qualquer um dos diplomas mencionados. É o que se extrai dos arts. 42 a 45 da LGPD, e dos arts. 7º, parágrafo único, 12, 14 e 18 do CDC.

35. No entendimento da organização representante, existem elementos suficientes para que seja apurada a responsabilidade, objetiva e solidária, de todos os envolvidos na exposição indevida de dados, não só diante da previsão constante na LGPD, mas também no próprio texto constitucional.

36. Isto porque, sabe-se que a responsabilidade civil do Estado independe de prévia previsão contratual, uma vez que decorre, naturalmente, da própria atividade estatal. Em sua essência, corresponde à obrigação de indenizar danos causados a terceiros por ocasião do desenvolvimento dos serviços públicos e das atividades típicas do Estado. É o que prevê o **art. 37, § 7º, da CFRB/88**.

37. Vê-se, portanto, os fatos ora noticiados correspondem à violação de normas básicas de proteção ao consumidor, a seus dados e informações pessoais, de modo que, além ser analisada a violação da norma em si, é imperiosa a investigação quanto à responsabilidade de todos os agentes envolvidos nos procedimentos de segurança e dos agentes envolvidos no tratamentos destes dados, para se apure sua eventual responsabilização e o consequente dever de indenizar os lesados pela exposição de seus dados.

IV. Da exposição de dados sensíveis e dos danos à privacidade dos cidadãos

38. No caso noticiado, **não há dúvida sobre o caráter sensível das informações disponibilizadas e deixadas expostas pelo incidente de segurança aqui descrito, posto que milhões de pessoas tiveram dados relacionados ao seu estado atual de saúde, condições e doenças pré-existentes divulgadas.**

39. Tais dados, também informam **detalhes relacionados ao tratamento oferecido a cada um e medicamentos que foram administrados ao longo do período de contágio com a Covid-19 e foram deixados expostos junto ao nome e número de CPF de cada um dos cidadãos**. Pela abrangência do incidente e natureza das informações, não é exagero afirmar que se trata de um dos casos mais graves de vazamento de dados já ocorrido no Brasil.

40. **A notória exposição desses dados já deixa os cidadãos sob uma situação grave de hipervulnerabilidade**. E as possibilidades de grave lesão de direitos a partir disso são inúmeras!

41. Sob esse enfoque, de posse dessas informações sensíveis, terceiros poderiam **expor pessoas acometidas de situações graves de saúde**, com chantagens e até mesmo práticas injuriosas. Seria possível, por exemplo, que pessoas com HIV - uma infecção

sexualmente transmissível com elevado estigma sobre as pessoas que a possuem -, fossem indevidamente expostas, e que isso até mesmo impactasse em possibilidades e oportunidades futuras, como locais de estudo e emprego.

42. Além disso, **é enorme o risco de utilização desses dados para fraudes**. Tem sido crescentes os casos em que pessoas têm o seu CPF reiteradamente utilizado de maneira ilegal por terceiros. Tais práticas fraudulentas ocorrem justamente devido a vazamentos como esse e, não raras vezes, o problema não ocorre apenas uma vez, sendo que em muitos casos medidas judiciais recorrentes são necessárias.

43. O vazamento dos dados também possibilita ataques fraudulentos que, comumente, se utilizam de informações deixadas expostas como maneira de "capturar" uma pessoa e enganá-la. Chamada de ***phishing***, essa prática simula uma situação real - um e-mail com uma promoção, por exemplo - e leva cidadãos a compartilharem informações confidenciais como senhas e número de cartões de crédito.

44. O acesso a essas informações é de **evidente interesse econômico por parte de sociedades empresárias do mercado de saúde**, especialmente operadoras de saúde. Dentro do mercado de saúde suplementar, essas informações poderiam ser usadas para mapear potenciais consumidores, inclusive seguida de estratégia de marketing direcionado, e para a recusa de eventual cobertura, por doenças pré-existentes. Por mais que muitas dessas práticas sejam ilegais, é flagrante como o simples acesso de operadoras a informações pessoais desse tipo acerca dos consumidores lesados, coloca-os em situação de vulnerabilidade extrema, aptas a dar ensejo não só a mais práticas abusivas, como também, a ver esvaídas suas mínimas chances de conseguir um convênio médico ou um tratamento adequado para sua doença.

45. A exposição e vazamento desses dados, assim, configura dano moral presumido (*in re ipsa*) causado a todos os cidadãos impactados pelo incidente. Houve indiscutivelmente lesão à honra e dignidade, independentemente de prova que ateste a ofensa moral ou material, uma vez que a conduta negligente dos responsáveis pelo incidente evidencia a falta de prudência no tratamento dessas informações.

46. Neste sentido, vale ressaltar que o Superior Tribunal de Justiça (STJ) também entende que resta presumido o dano moral, assim como a responsabilidade do gestor de banco de dados, quando a disponibilização e a comercialização de dados pessoais não é corretamente informada ao consumidor. Confira-se:

> RECURSO ESPECIAL. FUNDAMENTO NÃO IMPUGNADO. SÚM. 283/STF. AÇÃO DE COMPENSAÇÃO DE DANO MORAL. BANCO DE DADOS. COMPARTILHAMENTO DE INFORMAÇÕES PESSOAIS. DEVER DE

> INFORMAÇÃO. VIOLAÇÃO. DANO MORAL IN RE IPSA. JULGAMENTO: CPC/15.
> [...]
> O fato, por si só, de se tratarem de dados usualmente fornecidos pelos próprios consumidores quando da realização de qualquer compra no comércio, não afasta a responsabilidade do gestor do banco de dados, na medida em que, quando o consumidor o faz não está, implícita e automaticamente, autorizando o comerciante a divulgá-los no mercado; está apenas cumprindo as condições necessárias à concretização do respectivo negócio jurídico entabulado apenas entre as duas partes, confiando ao fornecedor a proteção de suas informações pessoais. (REsp 1.758.799/MG, 3ª Turma, Rel. Min. Nancy Andrighi, j. 12/11/2019, DJe 19.11.2019)

47. É inegável, portanto, a ocorrência de danos à vida privada e à intimidade das pessoas que tiveram seus dados pessoais expostos, sendo necessária a averiguação dos fatos narrados e sua consequente responsabilização pelos eventuais danos materiais e presumidamente morais sofridos.

V. Da necessidade de medidas de aperfeiçoamento da segurança digital no âmbito no Ministério da Saúde

48. Vale destacar que casos como este, por sua gravidade, já justificariam por si só a revisão completa da estratégia do Ministério da Saúde para proteção de dados pessoais, bem como a formulação de uma política robusta e completa de tratamento de dados pessoais que contemplasse a mitigação desse risco. Ainda assim, é importante lembrar que essa não é a primeira vez em tempos recentes que a administração federal do SUS passa por episódios semelhantes de vazamento de dados.

49. Em fevereiro de 2020, o Idec notificou a Agência Nacional de Vigilância de Sanitária (ANVISA), autarquia especial ligada ao Ministério da Saúde, pelo vazamento de endereços eletrônicos de usuários cadastrados nos sistemas de agência para uso terapêutico de medicamentos à base de cannabis[6]. Há poucos dias, já em novembro de 2020, o Ministério da Saúde foi vítima de um ataque hacker, que também propiciou acesso indevido a terceiros a informações internas da entidade[7].

50. Esse conjunto de fatos aponta para a extrema necessidade de que a União adote uma política de proteção de dados pessoais consistente e adequada aos riscos e exigências jurídicas contemporâneas, como a adequação à LGPD.

[6]Disponível em: <https://idec.org.br/zhomologacao/idec-na-imprensa/idec-notifica-anvisa-sobre-email-vazado-de-paciente-de-cannabis>
[7]Disponível em: <https://noticias.uol.com.br/saude/ultimas-noticias/redacao/2020/11/13/apos-possivel-ataque-hacker-ministerio-da-saude-faz-alerta-sobre-golpes.htm>

51. O caso do Ministério da Saúde é especialmente delicado, em relação a outros entes da administração pública, seja pelo conjunto de dados sensíveis sob seu controle, seja especialmente pelas informações sobre condições de saúde individuais e, também, porque qualquer instabilidade pode implicar em graves consequências para a prestação do serviço de saúde, podendo impactar até em perda de vidas.

52. Além disso, o vazamento aqui em discussão revela a enorme **importância de transparência em torno das parcerias entre o SUS e entidades privadas**, seja no âmbito do PROADI-SUS seja no âmbito de outros acordos, como contratos de gestão com Organizações Sociais.

53. O tema, apesar de antigo no campo jurídico em torno do SUS, agora adquire nova dimensão com a transferência de dados pessoais entre o setor público e entes privados no âmbito desses contratos. **É fundamental que se evidencie quais dados são compartilhados e como são tratados pelos contratantes privados.**

54. Soma-se a essas considerações que o Ministério, neste momento, está em vias de estabelecer sua nova versão da Política Nacional de Informática e Informação em Saúde (PNIIS), bem como instrumentos ainda mais sustentados no uso de dados pessoais, como a Rede Nacional de Dados em Saúde (RNDS) e a implementação do prontuário eletrônico, inclusive com projetos inseridos também no âmbito do já mencionado PROADI-SUS[8], inclusive com o Hospital Albert Einstein.

55. Sendo assim, **urge que a União estabeleça uma política com conjunto de princípios e medidas, que incluem a adequação da entidade à LGPD,** a definição de padrões elevados de segurança digital que mitiguem o risco de vazamentos, intencional ou não, como, entre outras, a autenticação em dois fatores, a definição de parâmetros e a divisão precisa de responsabilidades em contratos que envolvam compartilhamento de dados com outros entes públicos ou privados.

VI. Pedidos

56. Diante do exposto, o Instituto Brasileiro de Defesa do Consumidor pede ao Ministério Público Federal que seja realizado o protocolo e respectivo recebimento da presente Representação, assim como **a abertura de inquérito civil público,** nos termos do art. 8º, § 1º da Lei 7.347/85, requerendo a oitiva, no curso do inquérito civil, do Ministério da Saúde

[8] Cita-se como exemplo, o Regula Mais, desenvolvido em parceria com o Hospital Sírio-Libanês (informações disponíveis em: <https://hospitais.proadi-sus.org.br/projetos/114/regula-mais-brasil>) e Projeto de Telemedicina desenvolvido em parceria com o Hospital Albert Einstein (informações disponíveis em: <https://hospitais.proadi-sus.org.br/projetos/18/telemedicina>).

e do Hospital Albert Einstein, para apuração de responsabilidade frente ao vazamento das informações de saúde de usuários do sistema público e da saúde suplementar.

57. O Idec também requer que os representados sejam instados a esclarecer os seguintes aspectos do episódio:

a. Descrição da parceria que permitiu ao Hospital Albert Einstein o manejo destas informações, inclusive os atos administrativos que estabeleceram o projeto em questão, dentro ou não do âmbito do PROADI-SUS, e descrição dos dados a que o Hospital privado teve acesso.
b. Descrição da política de segurança para manejo desses dados tanto do Ministério da Saúde quanto do Hospital Albert Einstein, incluindo medidas protetivas e preventivas adotadas.
c. Medidas tomadas para contenção de danos e reparação imediata dos usuários atingidos pelo vazamento, conforme preconiza a LGPD, por exemplo, aviso dos titulares dos dados.

58. Considerando, ademais, a gravidade dos fatos narrados, relacionados aos dados mais sensíveis dos cidadãos brasileiros, é urgente a atuação do Ministério Público Federal para obtenção das informações supra expostas, de modo a resguardar os interesses e direitos dos usuários.

59. Frente à necessidade de se evitar a repetição no futuro da violação à privacidade dos usuários do sistema de saúde, o Idec requer que o I. *Parquet* adote, nos termos do art. 5º, §6°, da Lei n° 7.347/1985, do art. 20 e seguintes, da Resolução n° 87/2006, do Conselho Superior do Ministério Público Federal, e do art. 14 da Resolução n° 23/2007, do Conselho Nacional do Ministério Público as medidas necessárias para adequar a conduta dos representados à Lei Geral de Proteção de Dados, em especial art. 6º, VII e VIII, e ao Código de Defesa do Consumidor.

60. Por fim, a entidade noticiante também requer:

a) qualquer que seja a análise procedida, **seja feito exame das condutas noticiadas à luz de toda a legislação acima mencionada, inclusive, se for o caso, apuração de responsabilidades à luz da CF/1988, assim como da Lei nº 8.429/1992**.

b) Qualquer que seja a análise procedida **da(s) jurisdicionada(s), que a mesma seja realizada não só à luz do exame de conformidade, mas**

também sob a ótica do desempenho/eficiência (art. 37, *caput*, CF/1988).

c) Que as diligências a serem adotadas no âmbito do MPF, para além das vias investigativas, sejam acompanhadas da adoção de todas as medidas urgentes quanto bastem para obstar os prejuízos imediatos e gravíssimos experimentados pelos brasileiros.

d) Sua habilitação como interessado em eventual procedimento que vier a ser instaurado, requerendo a intimação dos resultados desta promoção para as providências de estilo.

e) que seja a entidade subscritora comunicada de seu encaminhamento/resultado, fundamentadamente.

São Paulo, 26 de novembro de 2020.

IGOR RODRIGUES BRITTO
Diretor de Relações Institucionais
OAB/DF nº 54.565

ANA CAROLINA NAVARRETE
Coordenadora do Programa de Saúde

DIOGO MOYSES
Coordenador do Programa
de Telecomunicações e Direitos Digitais

CHRISTIAN TÁRIK PRINTES
Coordenador Jurídico
OAB/SP nº 316.680

MATHEUS ZULIANE FALCÃO
Pesquisador do Programa de Saúde

MARINA ANDUEZA PAULLELLI
Advogada do Idec
OAB/SP 365.516

BÁRBARA PRADO SIMÃO
Pesquisadora do Programa
de Telecomunicações e Direitos Digitais