CONTROLADORIA-GERAL DA UNIÃO

RELATÓRIO FINAL

AO SENHOR CORREGEDOR-GERAL DA UNIÃO

A Comissão de Processo Administrativo de Responsabilização designada pela Portaria nº 1.095, de 6 de maio de 2021, publicada no DOU nº 85, de 7 de maio de 2021, da lavra do Corregedor-Geral da União da Controladoria-Geral da União, vem apresentar **RELATÓRIO FINAL**, no qual recomenda a aplicação à pessoa jurídica **Sociedade Beneficente Israelita Brasileira - Hospital Albert Einstein, CNPJ 60.765.823/0001- 30,** da **pena de multa no valor de R$ 210.000,00**, nos termos do art. 33, inc. II, da Lei nº 12.527/2011 c/c o art. 66, inc. II, do Decreto nº 7.724/2012, por, comprovadamente, ter permitido o vazamento, por parte de seu preposto, de informações pessoais e médicas de pacientes da rede hospitalar pública e privada, contidos em sistemas internos do Ministério da Saúde, incidindo, assim, nas irregularidades tipificadas nos arts. 31, § 2º, e 32, IV, da Lei nº 12.527/2011 – LAI c/c arts. 65, IV, e 66 do Decreto nº 7.724/2012, de acordo com as razões de fato e de direito a seguir expostas.

I – INTRODUÇÃO

1. Preliminarmente, consideramos conveniente traçarmos algumas linhas acerca da LAI (Lei de Acesso à Informação), que regulamentou um importante direito previsto no artigo 5º da nossa Constituição Federal, que informa que todos podem solicitar informações dos órgãos públicos de interesse particular ou de interesse da coletividade.
2. O acesso à informação contribui para aumentar a eficiência do Poder público, diminuir a corrupção e elevar a participação social.
3. No entanto, a própria Lei nº 12.527/2011 estabelece limites e reservas quanto às informações dos órgãos públicos e, a fim de garantir o devido sigilo de determinados dados, estabelece obrigações, responsabilidades e penalidades àqueles que os manuseiam ou os acessem.
4. Importante destacar que tal norma inclui dentro do seu escopo, não apenas as informações de posse dos órgãos e entidades da Administração Pública, mas também a "informação produzida ou custodiada por pessoa física ou entidade privada decorrente de qualquer vínculo com seus órgãos ou entidades, mesmo que esse vínculo já tenha cessado" (art. 7º, III).
5. Nesse sentido, a norma prescreve ainda disposições específicas para as entidades privadas no tocante à guarda e fornecimento de informações públicas, a saber:

"Art. 26. As autoridades públicas adotarão as providências necessárias para que o pessoal a elas subordinado hierarquicamente conheça as normas e observe as medidas e procedimentos de segurança para tratamento de informações sigilosas.

Parágrafo único. A pessoa física ou entidade privada que, em razão de qualquer vínculo com o poder público, executar atividades de tratamento de informações sigilosas adotará as providências necessárias para que seus empregados, prepostos ou representantes observem as medidas e procedimentos de segurança das informações resultantes da aplicação desta Lei.

[...]

Art. 33. A pessoa física ou entidade privada que detiver informações em virtude de vínculo de qualquer natureza com o poder público e deixar de observar o disposto nesta Lei estará sujeita às seguintes sanções:

I - advertência;

II - multa;

III - rescisão do vínculo com o poder público;

IV - suspensão temporária de participar em licitação e impedimento de contratar com a administração pública por prazo não superior a 2 (dois) anos; e

V - declaração de inidoneidade para licitar ou contratar com a administração pública, até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade.

Art. 34. Os órgãos e entidades públicas respondem diretamente pelos danos causados em decorrência da divulgação não autorizada ou utilização indevida de informações sigilosas ou informações pessoais, cabendo a apuração de responsabilidade funcional nos casos de dolo ou culpa, assegurado o respectivo direito de regresso.

Parágrafo único. O disposto neste artigo aplica-se à pessoa física ou entidade privada que, em virtude de vínculo de qualquer natureza com órgãos ou entidades, tenha acesso a informação sigilosa ou pessoal e a submeta a tratamento indevido."

6. Assim, com base na estrutura jurídica brasileira em relação ao acesso à informação, precipuamente na referida Lei nº 12.527/2011 e no Decreto nº 7.724/2012, buscamos analisar os atos relacionados ao vazamento de informações cuja publicização é vedada.

II – BREVE HISTÓRICO

7. Em apertada síntese, a pessoa jurídica A. Einstein, de acordo com a Nota Técnica nº 1301/2021/COREP (SEI 1937318) e demais documentação constante dos autos, teria, por meio do Sr. Wagner Maurício Nunes dos Santos, preposto da mencionada instituição, permitido o vazamento de informações pessoais e médicas relativas a 16 milhões de pacientes da rede hospitalar pública e privada, contidos em sistemas internos do Ministério da Saúde e concernentes a diagnósticos suspeitos ou confirmados de Covid-19, que teriam ficado passíveis de acesso por terceiros não autorizados, uma vez que os logins e respectivas senhas para tal acesso teriam sido expostos durante quase um mês, irregularidade esta disposta nos arts. 26, § único; 31, § 2º; e 32, IV, da Lei nº 12.527/2011 – LAI c/c arts. 65, IV, e 66 do Decreto nº 7.724/2012.
8. Conforme se pode verificar nos autos, após notícias quanto ao vazamento em comento, esta Corregedoria-Geral da União buscou elementos, provas e dados a fim de avaliar a viabilidade e plausabilidade de se instaurar um Processo de Apuração de Responsabilidade em face da pessoa jurídica A. Einstein.
9. Assim, por meio do Despacho CRG (SEI 1937166), o Senhor Corregedor-Geral determinou a instauração de Investigação Preliminar Sumária, o que se deu através do Despacho DIREP (SEI 1937316).
10. A Nota Técnica nº 1.301/2021/COREP (SEI 1937318), já mencionada acima, concluiu tal Investigação Preliminar Sumária com proposta de deflagração do presente PAR e, em seguida aos Despachos COREP (SEI 1937351), DIREP (SEI 1937352) e CRG (SEI 1937355), foi publicada a Portaria nº 1.095, de 06/05/2021 (SEI 1957576), que instaurou o presente PAR, para que fosse apurada a suposta conduta irregular da pessoa jurídica A. Einstein, prevista nos arts. 26, § único; 31, § 2º; e 32, IV, da Lei nº 12.527/2011 – LAI c/c arts. 65, IV, e 66 do Decreto nº 7.724/2012, em face do vazamento de informações pessoais e médicas relativas a 16 milhões de pacientes da rede hospitalar pública e privada, contidos em sistemas internos do Ministério da Saúde e concernentes a diagnósticos suspeitos ou confirmados de Covid-19, que teriam ficado passíveis de acesso por terceiros não autorizados, uma vez que os logins e respectivas senhas para tal acesso teriam sido expostos durante quase um mês.

III – RELATO

11. Em 07/05/2021, houve a instauração do PAR (SEI 1957576).
12. Em 25/06/2021, a CPAR concluiu o Termo de Indiciação (SEI 2004210), que foi devidamente encaminhado à empresa, em obediência ao art. 16 da Instrução Normativa CGU nº 13/2019.
13. Em 28/07/2021, a pessoa jurídica A. Einstein. apresentou a defesa escrita (SEI 2043928) e respectivos anexos.
14. Em 11/08/2021 foi realizada videoconferência com a participação dos advogados, de representante do Hospital A. Einstein e dos membros da comissão para fins de esclarecimentos dos pontos tratados na defesa escrita, conforme solicitado pela defendente.

IV – INSTRUÇÃO

15. Em relação à instrução do processo nº 00190.103948/2021-69, esta CPAR registra que não produziu provas.
16. O conjunto probatório e fático trazido, em sede de juízo de admissibilidade, pela Nota Técnica nº 1.031/2021/COREP – ACESSO RESTRITO/COREP/CRG (SEI 1937318), foi considerado suficiente para a instauração de comissão de processo administrativo de responsabilização, o que ocorreu com a publicação da anteriormente mencionada Portaria nº 1.095 (SEI 1957576).
17. Considerando, ainda, principalmente, as informações trazidas pelos documentos "Despacho DATASUS/SE/MS de 04/02/21 (SEI 1834587)", "Ofício nº 156/2020/DATASUS/SE/MS, de 01/12/2020", "e-mail de 01/03/2021 (SEI 1937061)", "Petição do Hospital Albert Einstein datada de 12/03/21", "Cópia do Processo 25000.028646/2018-10-Projeto de Apoio Albert Einstein x Ministério da Saúde (SEI 1867317)", "Publicação no DOU de 20/07/18 (Seção 3, p. 99) do EXTRATO DE AJUSTE/Termo de Ajuste (PROADI-SUS) Nº 001/2017", "Relatório elaborado em 11/03/21 pela equipe de Segurança da Informação do Hospital Albert Einstein" e "Laudo Pericial externo assinado em 18/02/21 pelo expert da empresa Ventura Enterprise Risk Management (Ventura) Domingo Montanaro", foi instaurado o presente PAR para apuração do ato irregular praticado pela pessoa jurídica ora tratada, qual seja, o vazamento de informações pessoais e médicas relativas a 16 milhões de pacientes da rede hospitalar pública privada, contidos em sistemas internos do Ministério da Saúde e concernentes a diagnósticos suspeitos ou confirmados de Covid-19, que teriam ficado passíveis de acesso por terceiros não autorizados, uma vez que os logins e respectivas senhas para tal acesso teriam sido expostos durante quase um mês.

V – INDICIAÇÃO, DEFESA E ANÁLISE

V.1 – Indiciação

18. A CPAR indiciou a empresa A. Einstein, conforme, como já destacado, nos termos da "Nota Técnica nº 1.031/2021/COREP" (SEI 1937318) e demais documentação mencionada, que demonstraram, de forma inequívoca, a conduta irregular praticada pela referida pessoa jurídica, dispostos nos arts. 26, § único; 31, § 2º; e 32, IV, da Lei nº 12.527/2011 – LAI c/c arts. 65, IV, e 66 do Decreto nº 7.724/2012.
19. Nos documentos intitulados "Despacho DATASUS/SE/MS de 04/02/21 (SEI 1834587)", "Ofício nº 156/2020/DATASUS/SE/MS, de 01/12/2020", "e-mail de 01/03/2021 (SEI 1937061)", "Petição do Hospital Albert Einstein datada de 12/03/21", "Cópia do Processo 25000.028646/2018-10-Projeto de Apoio Albert Einstein x Ministério da Saúde (SEI 1867317)", "Publicação no DOU de 20/07/18 (Seção 3, p. 99) do EXTRATO DE AJUSTE/Termo de Ajuste (PROADI-SUS) Nº 001/2017", "Relatório elaborado em 11/03/21 pela equipe de Segurança da Informação do Hospital Albert Einstein" e "Laudo Pericial externo assinado em 18/02/21 pelo expert da empresa Ventura Enterprise Risk Management (Ventura) Domingo Montanaro" constam todas as evidências consideradas suficientes para o indiciamento da empresa.
20. Tal ato irregular foi consubstanciado no vazamento, por parte do preposto da empresa investigada, de

informações pessoais e médicas de pacientes da rede hospitalar pública e privada, contidos em sistemas internos do Ministério da Saúde.

V.2 – Defesa e Análise

21. A pessoa jurídica A. Einstein, de acordo com os termos da defesa escrita (SEI 2043928), requereu a declaração de sua inocência e consequente absolvição no PAR, conforme os argumentos que seguem. Esta comissão processante, conforme o disposto na Lei nº 12.527/2011, entende que diversos dos argumentos apresentados pelo A. Einstein não são capazes de eximi-la de responsabilidade, senão vejamos.

- argumento 1: manutenção da defesa em regime de sigilo até a publicação do ato decisório (Art. 29 da Instrução Normativa Nº 13, de 8 de agosto de 2019 – CGU).

análise 1: a comissão, em respeito aos ditames legais, mantém sob sigilo todo processo, de forma que o pedido da defesa foi acatado;

- argumento 2: não houve exposição indevida dos dados pessoais de 16 milhões de cidadãos brasileiros suspeitos de ou contaminados pela COVID-19, o que houve foi a exposição de credenciais de acesso a dois sistemas do Ministério da Saúde (e-SUS-VE e SIVEP-Gripe). E, desta exposição, uma jornalista acessou a referida base de dados e realizou a divulgação pontual de resultados positivos de testes de COVID-19 de três autoridades públicas brasileiras, os quais já eram de conhecimento da população em geral.

análise 2: de fato, não há elementos que comprovem a exposição dos dados pessoais de 16 milhões de cidadãos brasileiros suspeitos de ou contaminados pela COVID-19 à população em geral, no entanto, resta demonstrado que a jornalista obteve acesso a tais dados e que publicou apenas as informações de 3 (três) autoridades públicas por mera liberalidade sua, isto é, tem-se que a repórter, a instituição na qual exerce suas atividades ou o profissional/técnico da área de informática que a teria assessorado na interação com os mencionados sistemas possuem (ou poderiam possuir) tais dados e, oportunamente, podem (ou poderiam) fazer uso deles. Assim, a referida divulgação pontual não pode ser garantida pela pessoa jurídica, uma vez que o acesso a todos os dados dos 16 milhões de brasileiros foi dado a quem o encontrasse e restou comprovado tal acesso pelo menos à referida repórter. Finalmente, não é porque as informações das aludidas autoridades públicas já fossem de conhecimento da população em geral que o vazamento deixa de ser uma infração a LAI. E, além disso, segundo a reportagem do Estadão (SEI 1936753), entre as pessoas que tiveram a privacidade violada, com exposição de informações como CPF, endereço, telefone e doenças pré-existentes, estão o presidente Jair Bolsonaro e familiares; o ministro da Saúde, Eduardo Pazuello; outros seis titulares de ministérios, como Onyx Registros têm informações médicas confidenciais, como histórico clínico e remédios usados no paciente Lorenzoni e Damares Alves; o governador de São Paulo, João Doria (PSDB), e mais 16 governadores, além dos presidentes da Câmara, Rodrigo Maia (DEM-RJ), e do Senado, Davi Alcolumbre (DEM-AP). Diante do exposto, a comissão decide por não acatar o argumento em tela;

- argumento 3: há um laudo técnico, elaborado pela Ventura Enterprise Risk Management (SEI 1937299), que identificou um acesso para fins jornalísticos, haja vista que essa utilização pontual teria ocorrido fora do padrão das atividades, com acesso via *browser*, o que não foi comumente constatado no resto do período. O referido laudo não identificou qualquer acesso adicional fora do padrão e/ou não autorizado.

análise 3: primeiramente, cumpre anotar que esta comissão decidiu por considerar os termos do laudo técnico, uma vez que não há qualquer documento ou informação nos autos que o desabone ou traga suspeita sobre ele. No entanto, importa consignar que o dito laudo não assevera (ou garante) que apenas a repórter que publicou as informações das autoridades públicas teve acesso aos dados e sistemas, mas somente emite uma opinião no sentido de "acreditar" nisso e, ainda, que o fato de não ter sido constatado outros acessos via *browser* no período observado "indica" que esse acesso não teria ocorrido novamente. Em sentido oposto ao

que tenta expor a defesa, o Presidente da SaferNet Brasil pondera que "e*sse arquivo com logins e senhas foi colocado no GitHub, a maior plataforma mundial de desenvolvimento colaborativo de softwares. A quantidade de pessoas que usam essa plataforma é imensa. Muito provavelmente esse arquivo foi visto por outras pessoas, que fizeram cópias, acessaram os dados e muito provavelmente copiaram esses dados. Os dados da população não estão seguros e esse incidente é a prova disso*" (SEI 1936784). Dessa forma, não é possível concluir no sentido de que inexiste qualquer vazamento das informações dos sistemas;

- argumento 4: o Termo de Indiciação, de modo errôneo e contraditório, imputa ao Hospital Albert Einstein "o vazamento de informações pessoais e médicas relativas a 16 milhões de pacientes da rede hospitalar pública privada" (SEI 2004210), ao passo que, em seguida, reconhece que os "logins e respectivas senhas para tal acesso, teriam sido expostas".

análise 4: não há qualquer contradição no Termo de Indiciação. Ora, o vazamento de informações está comprovado com a reportagem jornalística que mencionou o Presidente da República, a Primeira-Dama e o Governador do Estado de São Paulo. E, para se obter referidos dados, certamente a repórter teve acesso aos dados dos sistemas, que, por sua vez, só foi possível em razão dos logins e senhas para tal acesso terem sido expostos. Desse modo, não há falar em contradição no mencionado indiciamento. Cumpre lembrar ainda que a conduta tipificada pela norma prescreve quatro tipos de conduta: divulgar; permitir a divulgação; acessar; ou permitir acesso indevido à informação pessoa. No caso específico, a conduta da pessoa jurídica permitiu justamente a divulgação e o acesso indevido de informações pessoais.

- argumento 5: o Termo de Indiciação concluiu pelo enquadramento legal do Hospital Albert Einstein na conduta tipificada no art. 26, parágrafo único, da LAI. No entanto, tal dispositivo tem a *mens legis* de obrigar os entes públicos (e privados que tratam dados do poder público) a instruir seus subordinados e representantes com relação à observância da norma. O Hospital Albert Einstein, em conjunto com o Ministério da Saúde, cumpriu referido artigo em sua integralidade, pois a referida pessoa jurídica tomou todas as medidas possíveis para que o sr. Wagner declarasse sua plena ciência com relação à necessidade de manter absoluto sigilo das informações a ele repassadas em razão do exercício de sua função. A primeira delas foi a menção expressa no contrato de trabalho para que (i) observasse o absoluto sigilo; (ii) não procedesse à transferência de informações; (iii) atendesse às políticas internas da companhia, em especial às Normas de Segurança (doc. 01). Ademais, o colaborador Wagner Maurício Nunes dos Santos firmou Termo de Compromisso (SEI 1937105) com o Ministério da Saúde por meio do qual comprometia-se a manter sob sigilo quaisquer informações às quais obtivesse acesso em razão de sua função e na prestação de serviços. Assim, o enquadramento dos fatos apurados em Investigação Preliminar Sumária não pode ensejar responsabilização do Hospital Albert Einstein em razão de desídia com relação ao dever se informar seus colaboradores quanto às normas de segurança da informação.

análise 5: de fato, o Hospital A. Einstein cumpriu o disposto no parágrafo único do art. 26 da Lei nº 12.527/2011, uma vez que há documentação comprobatória nos autos quanto à ciência do seu colaborador em relação à necessidade de executar as atividades de tratamento de informações sigilosas com observância de medidas e procedimentos de segurança das informações. Assim, a comissão decidiu por considerar tais cuidados da empresa e retirar a imputação procedida no indiciamento. Nada obstante, o cumprimento do disposto no referido artigo não afasta à imputação das condutas tipificadas na norma.

- argumento 6: o fato ilícito apurado nos autos tem como origem a exposição indevida de credenciais de acesso aos sistemas e-SUS-VE e SIVEP-Gripe pelo Sr. Wagner e o art. 31, § 2º, da LAI, por outro lado, prevê a responsabilização de agentes que fizerem uso indevido de informações pessoais. O Sr. Wagner jamais fez uso indevido de informações pessoais constantes nas bases de dados do Ministério da Saúde. O que restou incontroverso nos autos foi a exposição de credenciais de acesso, em nenhum momento comprovando-se o uso de dados pessoais dos cidadãos suspeitos ou diagnosticados com COVID-19 para qualquer fim indevido, seja pelo sr. Wagner, por algum colaborador do Hospital Albert Einstein ou qualquer terceiro mal-intencionado. Ademais, a exposição indevida de credenciais de acesso não implica automaticamente acesso indevido às bases de dados do Ministério da Saúde, inclusive, não há qualquer indício nos autos que possa indicar acesso indevido a essa base de dados, conforme relatório juntado ao processo. Nesse mesmo sentido foi o entendimento do Ministério da Saúde, que ressaltou não haver "qualquer evidência material de que os dados do e-SUS Notifica

tenham sido, de fato, expostos. Além disso, não há indícios de invasão (acesso indevido) ao ambiente interno do Ministério da Saúde, não comprometendo, assim, a segurança dos dados" (SEI 19405933), motivo pelo qual os fatos apurados não podem ser subsumidos ao art. 31 da LAI, haja vista que não houve tratamento inadequado de quaisquer informações pessoais. O laudo elaborado pela Ventura Enterprise Risk Management (SEI 1937299) concluiu que "nada foi observado que indique ter havido um acesso massivo ou *download* de quantidades significativas de dados" e o expert informou que o único acesso identificado está potencialmente ligado "à própria repórter e/ou alguém de sua confiança, justamente nos momentos que antecedem à publicação da matéria, tendo em vista que os acessos constatados nas análises periciais são circunstancialmente relevantes, pois ocorrem no dia anterior da publicação da matéria, com poucas horas de diferença entre os eventos (acessos e publicação online)". Se houvesse acesso indevido às bases de dados, a visualização ficaria restrita às pessoas que detêm conhecimentos informáticos avançados, haja vista que a possibilidade de visualização e manuseio de dados via *browser* é remota. Para manuseio e/ou visualização dos dados, seria necessário operar uma rotina automatizada alcançável por meio de programação computacional avançada. Dessa forma, considerando que as credenciais de acesso disponibilizadas na plataforma do GitHub não têm a natureza de dados pessoais, deve ser repelida qualquer incidência do art. 31 da LAI ao caso concreto e, consequentemente, o enquadramento legal do art. 31, § 2º, da LAI, conferido à conduta do Sr. Wagner, não pode prosperar.

análise 6: a argumentação não merece prosperar, pois a exposição de credenciais de acesso se subsome perfeitamente ao previsto no dispositivo legal em comento. Ora, foi exatamente em razão da referida exposição de logins e senhas que se deu o vazamento das informações publicadas na já mencionada reportagem jornalística, isto é, sem a ação realizada pelo colaborador do A. Einstein não haveria se tornado públicas informações retiradas dos sistemas do Ministério da Saúde. Dessa maneira, a comissão entendeu por manter a imputação em tela. No que tange à conclusão do laudo elaborado pela Ventura Enterprise Risk Management no sentido de que "nada foi observado que indique ter havido um acesso massivo ou *download* de quantidades significativas de dados" e o expert informou que o único acesso identificado está potencialmente ligado "à própria repórter e/ou alguém de sua confiança, justamente nos momentos que antecedem à publicação da matéria, tendo em vista que os acessos constatados nas análises periciais são circunstancialmente relevantes, pois ocorrem no dia anterior da publicação da matéria, com poucas horas de diferença entre os eventos (acessos e publicação online)", tem-se que a comissão a considerou para efeito de dosimetria da pena sugerida, pois, caso houvesse elementos que indicassem uma publicização maior das informações vazadas, o dano seria completo e, consequentemente, a penalidade mais grave. Lado outro, o Presidente da SaferNet Brasil traz importante ponderação quanto ao tema ao responder sobre a extensão do vazamento "*são dados sensíveis, de saúde, extremamente valiosos porque são confiáveis, obtidos através de exames de laboratórios e preenchimentos de formulários. Eles têm, por exemplo, valor para uma seguradora. Uma informação de que determinado usuário fez um teste de covid, tem comorbidade ou doença preexistente, é extremamente valiosa para alimentar sistemas de precificação de risco. O usuário pode sentir isso, por exemplo, na recusa de um plano de saúde ou se tiver dificuldade de fazer um seguro de vida. É o maior vazamento de dados sensíveis do País.*" – destaquei - (SEI 1936784).

- argumento 7: as credenciais de acesso que foram divulgadas na plataforma GitHub fogem da definição de informação sigilosa ou de informação pessoal conferida pelo art. 4º, III e IV, da Lei de Acesso à Informação. Considerando que a conduta do ex-colaborador limitou-se à exposição das credenciais de acesso aos sistemas do Ministério da Saúde, as quais não foram utilizadas por terceiros para acessar dados pessoais ou informações sigilosas constantes na base de dados da referida Pasta, as credenciais não permitiram o acesso indevido a informação classificada em grau de sigilo ou a informação pessoal, com exceção daquele acesso realizado para fins jornalísticos, que culminou na publicação da referida matéria jornalística. Assim, não se pode responsabilizar o agente (público ou privado) caso haja mera constatação de vulnerabilidade em sistema informático. A responsabilização somente poderia ocorrer caso a vulnerabilidade fosse explorada de maneira mal-intencionada por terceiros. Outrossim, o homem médio não poderia acessar as informações constantes nas bases de dados do Ministério da Saúde sem conhecimentos informáticos avançados.

análise 7: primeiramente, cumpre registrar que a alegação de que "a conduta do ex-colaborador limitou-se à

exposição das credenciais de acesso aos sistemas do Ministério da Saúde, as quais não foram utilizadas por terceiros para acessar dados pessoais ou informações sigilosas constantes na base de dados da referida Pasta, as credenciais não permitiram o acesso indevido a informação classificada em grau de sigilo ou a informação pessoal, com exceção daquele acesso realizado para fins jornalísticos, que culminou na publicação da referida matéria jornalística", é contraditória. Num momento inicial argumentou-se que as credenciais não foram utilizadas para acessar dados pessoais ou informações sigilosas do Ministério da Saúde e logo depois já se apontou o caso comprovado de vazamento. Desse modo, apresenta-se incontroverso que houve a exposição das informações pessoais para terceiros em virtude da conduta do Sr. Wagner, motivo pelo qual a comissão rejeita tal fundamentação. No que se refere ao alegado no sentido de haver necessidade de conhecimentos informáticos avançados para acesso à base de dados do Ministério da Saúde, a comissão entendeu que tal fato é indiferente para a responsabilização ou não da empresa, o que restou comprovado nos autos é que a jornalista teve acesso às informações sigilosas em comento e publicou parte delas.

- argumento 8: caso sejam superados os óbices para a responsabilização administrativa do Hospital Albert Einstein por atos praticados por seu ex-colaborador, devem ser fixados critérios objetivos para aplicação de eventuais reprimendas administrativas, previstas nos arts. 33 da LAI e 66 do Decreto nº 7.724/2012. Por exclusão, o Hospital Albert Einstein entende que o art. 33, III, da LAI não poder ser aplicado ao caso concreto, haja vista que o vínculo com o Ministério da Saúde, no âmbito do projeto para "Utilização de técnicas avançadas de análise de dados (Big Data) e inovação para apoio ao planejamento e desenvolvimento de políticas em saúde" encerrou-se em 31/12/2020. Portanto, eventual rescisão do termo de ajuste firmado entre as partes não possuiria qualquer eficácia. Ademais, o art. 33, V, da LAI tem sua aplicação restrita a casos nos quais haja dolo ou reiteração de falhas do profissional ou da empresa que detém vínculo com o poder público. Caso seja aplicada sanção, será a primeira vez na qual o Hospital Albert Einstein terá incorrido em conduto considerada ilícita pelo poder público no âmbito da Lei de Acesso à Informação. Ainda, destaca-se que não houve dolo na conduta do Hospital Albert Einstein, tampouco de seu ex-colaborador, no momento da exposição de credenciais de acesso aos sistemas do Ministério da Saúde. Restaria, portanto, a possibilidade de aplicação das seguintes reprimendas do art. 32 da LAI: a advertência (inc. I), multa (inc. II) e/ou suspensão temporária de participar em licitação e impedimento de contratar com a administração pública por prazo não superior a dois anos (inc. IV). Para aplicação de uma das reprimendas, deve ser considerada a natureza da infração, sua gravidade, os danos que dela provieram para o serviço público, as circunstâncias agravantes ou atenuantes dos fatos danosos e eventuais incidentes nas infrações administrativas. Também deve ser levado em consideração a presteza e transparência do Hospital Albert Einstein para identificar a falha de seu colaborador e tomar todas as medidas necessárias para a imediata remoção das informações disponibilizadas no Github, comunicando imediatamente o Ministério da Saúde para assegurar a proteção de suas bases de dados e a imediata mudança das credenciais de acesso comprometidas, além da busca por diligência pelo time técnico e independente de peritos da Ventura Enterprise Risk Management, para emissão de parecer sobre os impactos e possíveis danos do episódio. Some-se a isso o fato narrado de que as credenciais expostas permitiam acesso pelas Secretarias de Saúde aos sistemas do Ministério da Saúde utilizados no âmbito do PROOADI-SUS e realização de consultas que ocorriam primordialmente de forma automatizada, sendo esse fluxo dificilmente conhecido por um homem médio, demandando conhecimento específico para utilização das credenciais com a finalidade de acessar os sistemas do Ministério da Saúde, o que minimizou os riscos de acesso e exposição de informações. Ademais, conforme relatório elaborado pelo Hospital Albert Einstein (SEI 1937289), não foi identificada qualquer exposição de dados pessoais e/ou dados sensíveis de cidadãos brasileiros no ambiente da internet, reforçando o apurado de ausência de utilização indevida das credenciais para obtenção de dados de usuários. Além disso, as credenciais de acesso aos sistemas do Ministério da Saúde foram fornecidas ao Sr. Wagner mediante supervisão direta do Ministério da Saúde, haja vista que o ex-colaborador estava alocado fisicamente em Brasília e executava atos e tarefas a ele atribuídas por representantes do Ministério da Saúde. Ainda, importante destacar que o Hospital Albert Einstein jamais aferiu qualquer vantagem, seja ela econômica ou imaterial, decorrente da exposição de credenciais pelo seu ex-colaborador. Pelo contrário: a exposição indevida de credenciais de acesso levou à publicação de inúmeras matérias jornalísticas que publicizaram a reprovabilidade da conduta do Sr. Wagner e diminuíram a reputação do Hospital Albert Einstein com relação às suas políticas de segurança da informação. De igual modo, o Hospital Albert Einstein incorreu em diversas despesas para a apuração do ocorrido e para a elucidação dos fatos, tais quais a contratação de peritos de tecnologia da informação para inspecionar

os sistemas do Ministério da Saúde e verificar eventual indício de acesso indevido. Nessa inspeção, como já visto, o Laudo Pericial elaborado pela Ventura Enterprise Risk Management não identificou acesso não autorizado, com exceção daquele realizado para elaboração de matéria jornalística. Por fim, destaca-se a ausência de qualquer dano, seja aos cidadãos diagnosticados ou com suspeita de COVID-19, seja ao Ministério da Saúde, haja vista que não há nos autos qualquer elemento que indique que as base de dados tenham sido acessadas por terceiros mal-intencionados. Apesar de todos os esforços do Hospital Albert Einstein e do Ministério da Saúde (Termo de Compromisso - SEI 1937105) o Sr. Wagner praticou ato voluntário e culposo, ciente da sensibilidade das informações a ele incumbidas, publicando de maneira errônea dados de acesso aos sistemas do Ministério da Saúde. Descritas todas essas situações fáticas, considerando que os fatos apurados na Investigação Preliminar Sumária (exposição de credenciais) não resultaram em qualquer dano aos cidadãos brasileiros suspeitos e/ou diagnosticados com COVID-19, bem como a diligência do Hospital Albert Einstein para sanar o problema da maneira mais célere e efetiva possível, caso a comissão atribua responsabilidade ao Hospital, requer seja sua sanção limitada à advertência.

análise 8: resta devidamente comprovado nos autos que o Sr. Wagner expôs as senhas e logins dos 16 milhões de pacientes no sistema GitHub, possibilitando que terceiros tivessem acessos aos referidos dados sigilosos. A sanção recomendada decorre da referida conduta incontroversa. As alegações relacionadas à dosimetria da pena serão comentadas no Capítulo VII do presente relatório. No entanto, cumpre, de pronto, registrar que o pedido de limitação da pena à advertência restou rejeitada pela comissão, que entendeu pela aplicação de multa em razão, principalmente, da gravidade da infração cometida, considerando a sensibilidade dos dados que foram expostos.

22. Diante de todo exposto, tem-se que a responsabilização da empresa se mantém e aqui cumpre tecer alguns comentários em face dos apontamentos e ponderações levantados pela defendente em sua peça ora em comento,. Na Lei nº 12.846/2013 a responsabilidade da pessoa jurídica é objetiva, diferentemente da estrutura de responsabilização da Lei nº 12.527/2011, que é subjetiva. Para elucidar a questão a comissão se valeu de trechos da obra Responsabilização Administrativa de Pessoas Jurídicas à Luz da Lei Anticorrupção Empresarial, de Márcio Aguiar Ribeiro, que também trata de responsabilidade subjetiva de empresas:

"Mesmo sob a influência dos paradigmas tradicionais do Direito Administrativo Sancionador, baseada fundamentalmente na tese da responsabilidade subjetiva, a doutrina especializada já reconhecia a dificuldade de se aplicar integralmente os postulados da culpabilidade e pessoalidade da pena às pessoas jurídicas infratoras, evidenciando a necessidade de uma verdadeira adaptação dos institutos principais.

Sobre o tema assim se manifestou Fábio Medina Osório: ´A pessoa jurídica, dotada de personalidade jurídica criada pelo direito, não possui, naturalmente, vontade ou consciência, circunstância que lhe afasta o alcance da culpabilidade, pessoalidade da pena, exigências de dolo ou culpa, e mesmo individualização da sanção, nos moldes tradicionais. Tais princípios resultam ligados a uma específica capacidade humana de obrar, tendo por pressupostos atributos exclusivamente humanos, na sua evolução histórica consolidada na dogmática tradicional.´

Por isso, em relação à responsabilização de pessoas jurídicas, não se pode sustentar a integral aplicabilidade dos princípios em tela na mesma medida e extensão em que dispensadas às pessoas humanas. Não sem antes considerar a existência de diversos mandamentos igualmente constitucionais, que orientam e condicionam a atuação institucional das pessoas jurídicas."

23. Ademais, o Código Civil, no Capítulo I do Título IX, ao estabelecer regras de responsabilização, deixa evidente que as pessoas jurídicas respondem pelos atos de seus empregados, senão vejamos:

"Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.

Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.

[...]

Art. 932. São também responsáveis pela reparação civil:

[...]

III - o empregador ou comitente, por seus empregados, serviçais e prepostos, no exercício do trabalho que lhes competir, ou em razão dele;

[...]

Art. 933. As pessoas indicadas nos incisos I a V do artigo antecedente, ainda que não haja culpa de sua parte, responderão pelos atos praticados pelos terceiros ali referidos."

24. Finalmente, esclarece-se que, além dos argumentos acima expostos, foi solicitado pela defesa o agendamento de videoconferência com a participação dos advogados, de representante do Hospital A. Einstein e dos membros da comissão para fins de esclarecimentos dos pontos tratados na defesa escrita, o que foi autorizado pela comissão. Tal reunião foi realizada por meio da plataforma *Teams* às 15:00 horas do dia 11/08/2021.

VI – RESPONSABILIZAÇÃO LEGAL

25. A CPAR recomenda a aplicação, à pessoa jurídica **Sociedade Beneficente Israelita Brasileira - Hospital Albert Einstein**, da pena de multa no valor de R$ 210.000,00, nos termos do art. 33, inciso II, da Lei nº 12.527/2011 e art. 66, inciso II e § 2º, inciso II, do Decreto nº 7.724/2012, por ter permitido, por meio do Sr. Wagner Maurício Nunes dos Santos, preposto da mencionada instituição, o vazamento de informações pessoais e médicas relativas a 16 milhões de pacientes da rede hospitalar pública e privada, contidos em sistemas internos do Ministério da Saúde e concernentes a diagnósticos suspeitos ou confirmados de Covid-19, que teriam ficado passíveis de acesso por terceiros não autorizados, uma vez que os logins e respectivas senhas para tal acesso teriam sido expostos durante quase um mês, incidindo, assim, nas irregularidades tipificadas nos arts. 31, § 2º, e 32, IV, da Lei nº 12.527/2011 – LAI c/c arts. 65, IV, e 66 do Decreto nº 7.724/2012.

VII - PENA

26. A multa foi calculada com base no § 2º do art. 22 da LINDB, uma vez que a Lei nº 12.527/2011 e o Decreto nº 7.724/2012 não estabelecem os parâmetros para dosimetria, exceto os valores mínimo e máximo, que estão previstos no inciso II do § 2º do art. 66 do referido decreto.
27. Cumpre registrar aqui a utilidade da LINDB no caso concreto, já que, conforme mencionado no item anterior, as normas aplicáveis ao tipo de infração em tela não estipulam o caminho para se estabelecer a dosimetria e, além disso, a referida lei, que se presta a regular a aplicação das leis em todo território nacional no tempo e no espaço, é expressa, principalmente, nos artigos 22 a 27 quanto a sua observância pelos órgãos controladores quando da aplicação de sanções.
28. Nesse sentido, para se estabelecer o valor da multa entre os R$ 5.000,00 e R$ 600.000,00 consignados no Decreto nº 7.724/2012, esta comissão considerou a natureza e a gravidade da infração cometida, os danos dela decorrentes, as circunstâncias agravantes e atenuantes e, finalmente, os antecedentes da empresa em eventuais casos relacionados à LAI.
29. De maneira a tornar a mensuração da pena o mais objetiva possível, conforme determina a LINDB, estabeleceu-se a seguinte ponderação:

- Natureza e gravidade da infração: 0 a 25%;
- Danos que provieram da irregularidade: 0 a 25%;
- Agravantes e atenuantes: 0 a 25%;
- Antecedentes: 0 a 25%:

30. Com a soma dos percentuais tem-se que 0% seria cabível a multa mínima de R$ 5.000,00 e 100% aplicável a multa máxima de R$ 600.000,00.
31. Considerando a natureza e gravidade da irregularidade, esta comissão entendeu como razoável a aplicação de 20%, uma vez que os dados vazados eram sensíveis e a quantidade de pessoas que tiveram suas informações pessoais e médicas relacionadas à Covid-19 era alta (cerca de 16 milhões).
32. No que tange aos danos decorrentes da infração, conforme restou demonstrado nos presentes autos, aplicou-se 10%, tendo em vista que houve um potencial dano (abstrato) pelo período de disponibilização dos dados durante quase um mês em plataforma aberta ao público.
33. Sobre os aspectos agravantes e atenuantes, foi levado em consideração questões como: i) elementos indicadores de má ou boa-fé do infrator; ii) adoção de medidas para reparar os danos da infração; iii) eventual conhecimento e/ou consentimento da cúpula da pessoa jurídica em relação à irregularidade em comento; iv) existência de programa de *compliance* com o propósito de evitar ofensas a LAI; v) valor do contrato entre a Administração Pública e o ente privado.
34. Considerando que: i) não há elementos que indicam má-fé da empresa infratora (0%); ii) o Hospital A. Einstein agiu com rapidez na adoção de medidas para solucionar a questão (0%); iii) não há elementos que indiquem a participação da diretoria e/ou dos órgãos de gestão superior da pessoa jurídica na irregularidade (0%); iv) a empresa juntou aos autos documentos que demonstraram a adoção de medidas no sentido de informar seu colaborador quanto a necessidade de manter sigilosa as informações tratadas (0%); v) o valor do contrato ser na casa de R$ 32 milhões, isto é, de alta monta (5%), e que, portanto, a empresa deveria agir com maior esmero e cuidado em sua execução, esta comissão entendeu por estabelecer o percentual de 5% para esse item.
35. E, finalmente, como não foram encontrados outros casos de desrespeito à LAI pela empresa processada, foi considerado 0% no que se refere a antecedentes.
36. Dessa forma, somando-se os percentuais acima, esta comissão chegou a 35%, o que levou à conclusão de que, em consonância aos ditames da LINDB e da LAI, a multa recomendada à pessoa jurídica A. Einstein, pela infração em tela, é de R$ 210.000,00.

V – CONCLUSÃO

37. Em face do exposto, com fulcro no art. 33, inciso II, da Lei nº 12.527/2011 e art. 66, inciso II e § 2º, inciso II, do Decreto nº 7.724/2012 c/c arts. 22 a 27 da LINDB e art. 22 da Instrução Normativa CGU nº 13/2019, a Comissão decide:

- recomendar a aplicação à empresa A. Einstein, da pena de multa no valor de R$ 210.000,00;
- encerrar os trabalhos;
- encaminhar o PAR à autoridade instauradora.

Documento assinado eletronicamente por **DASO TEIXEIRA COIMBRA**, **Presidente da Comissão**, em 24/08/2021, às 16:53, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **GILMAR RODRIGUES POSSATI JUNIOR**, **Membro da Comissão**, em 24/08/2021, às 17:03, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.cgu.gov.br/conferir informando o código verificador 2077574 e o código CRC 6B6698E6