PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO

FACULDADE DE DIREITO

GUILHERME BIZARRO DALLA COSTA

Desafios para um diálogo entre proteção e segurança de dados: tratativa de dados sensíveis pelo Conselho Nacional de Saúde.

SÃO PAULO

2022

GUILHERME BIZARRO DALLA COSTA

Desafios para um diálogo entre proteção e segurança de dados: tratativa de dados sensíveis pelo Conselho Nacional de Saúde.

A presente monografia diz respeito ao aluno Guilherme Bizarro Dalla Costa (RA00209475), estudante de Direito. O projeto integra a grande área de ciências sociais aplicadas e a área específica de Direito, sendo orientado pela Professora Juliana Cardoso Ribeiro Bastos, que integra o Departamento de Direito do Estado (V) da Pontifícia Universidade Católica de São Paulo e apresenta a monografia com o título "Desafios para um diálogo entre proteção e segurança de dados: tratativa de dados sensíveis pelo Conselho Nacional de Saúde".

SÃO PAULO

2022

Banca Examinadora

_____

_____

_____

_____

_____

AGRADECIMENTOS

Sinto grande satisfação em chegar ao fim do curso de Direito da Pontifícia Universidade Católica de São Paulo. Foram cinco anos que se passaram muito rápido, mas muito valiosos, com muitos desafios, aprendizados, amizades e alegrias.

Em primeiro lugar, gostaria de agradecer à minha família por todo o apoio financeiro e emocional ao longo desses anos. Meus pais foram os grandes responsáveis por possibilitarem a minha formação com qualidade.

Gostaria de agradecer ao corpo docente da PUC-SP por todo o ensino, em especial à orientadora do presente trabalho, a professora Juliana Cardoso Ribeiro Bastos.

Às minhas queridas amigas Ana Clara, Valentina, Beatriz, Maria Laura, Victoria, Anna e Isabella, que foram uma grande rede de apoio durante todo o curso e, desde o início, estiveram ao meu lado.

Guilherme.

RESUMO

A Lei Geral de Proteção de Dados entrou em vigor recentemente e qualquer pessoa responsável por um tratamento de dados deve estar de acordo com as normas. Dados relativos à saúde são sensíveis e demandam maior rigor em seu tratamento. O problema é que a Lei não tem sido devidamente aplicada nas instituições de saúde pública, o que resulta na necessidade de implementar um programa de compliance. Objetiva-se estudar as diretrizes dadas pela Lei Geral de Proteção de Dados no tratamento de dados e avaliar a melhor política pública a ser implementada no âmbito da saúde pública. A partir do estudo da lei seca e de diversos artigos especializados no tema, o autor deste trabalho concluiu que a melhor forma de se criar um sistema que permita a segurança na tratativa de dados de saúde é a contratação de serviços de compliance, para a criação sistemas tecnológicos que garantam o não vazamento e uso adequado dos dados, em consonância com o conceito de Privacy by Design. Concluiu também que a iniciativa e o investimento nesse setor deve partir do Ministério da Saúde e, mais especificamente, do Conselho Nacional de Saúde.

Palavras-chave: Implementação da Lei Geral de Proteção de Dados. Dados relativos à saúde. Compliance enquanto política pública. Conselho Nacional de Saúde.

ABSTRACT

The brazilian General Data Protection Law has recently come into force and anybody responsible for data treatment is obliged to follow its rules. Health data are considered sensitive personal data and, therefore, require a more rigorous treatment. The main issue is that the Law has not been properly implemented in the public health institutes, which results in the necessity of implementing a compliance program. The aim is to study the personal data treatment guidelines given by the General Data Protection Law in order to evaluate the best public policy to be implemented in the Public Health System. From the study of the Law and various specialized articles, the author of this work has concluded that the best way of creating a system that allows true safety in health related personal data treatment is hiring compliance services to create technological systems that avoid data leak and offer a safe data treatment. Also, by observing the principles of Privacy by Design, the author has also concluded that the Health Ministry and the National Health Council are responsible for the initiative and investment in this area.

Keywords: General Data Protection Law implementation. Health related personal data. Compliance as a public policy. National Health Council.

SUMÁRIO

INTRODUÇÃO

A Lei Geral de Proteção de Dados entrou em vigor no dia 18 de setembro de 2020, porém, as sanções administrativas decorrentes do seu descumprimento passaram a ser exigíveis a partir de 1º agosto de 2021, nos termos da Lei nº 14.010/2020.

Ainda, a Emenda Constitucional nº 115 de 2022 foi responsável por incluir o direito à proteção dos dados pessoais, inclusive nos meios digitais no rol do artigo 5º da Constituição Federal, de modo que esse direito passou a ser considerado fundamental.

As diversas empresas e instituições que fazem o tratamento de dados pessoais tiveram desde a data de publicação da Lei, 14 de agosto de 2018, para se adequarem às suas disposições, todavia, isso não ocorreu.

Em entrevista à CNN[1], o perito em crimes digitais Wanderson Castilho, afirmou que, em 2021, o Brasil ficou no topo de vazamentos de informações no mundo: foram vazados dados de mais de 227 milhões de brasileiros.

A área da saúde foi uma das que mais sofreu com esse episódio: somente atrás do varejo, foi a segunda que mais registrou vazamento de dados, sendo que golpes virtuais na saúde aumentaram 64%.

Dados de saúde são considerados sensíveis pelo artigo 5º, II, Lei Geral de Proteção de Dados[2] e, dessa forma, requerem um tratamento diferenciado conforme disciplina o artigo 11 da LGPD.

Frente à necessidade de um tratamento adequado e mais cauteloso dos dados de saúde nas mais diversas instituições que lidam com essas informações, é imperioso que a Lei seja devidamente implementada, tanto no âmbito privado, como no público.

A Emenda Constitucional nº 115 também incluiu o inciso XXVI ao artigo 21, que previu a competência material da União para organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei[3].

---

[1] Em 2021, Brasil ficou no topo de vazamento de informação no mundo, diz especialista. CNN Brasil, 2021. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/em-2021-brasil-ficou-no-topo-de-vazamento-de-informacao-no-mundo-diz-especialista/>. Acesso em 18 de Agosto de 2022.
[2] BRASIL. Art. 5º, II, Lei 13.709/2018.
[3] BRASIL.Artigo 21, XXVI, da CF/88.

Frente à nova previsão constitucional de competência, na seara da saúde, tem-se que o Ministério da Saúde é o responsável pela organização e fiscalização da proteção e do tratamento de dados pessoais nas diferentes unidades de saúde.

Dentro da organização do Ministério da Saúde, encontra-se o Conselho Nacional da Saúde, que atua na formulação de estratégias e no controle da execução da política de saúde na instância correspondente, inclusive nos aspectos econômicos e financeiros. [4]

Nesse sentido, seria o Conselho Nacional de Saúde, em conjunto com o Ministério da Saúde, os responsáveis pela implementação de políticas públicas no sentido de garantir com que os hospitais e demais unidades de saúde públicas estejam em conformidade com a Lei Geral de Proteção de Dados.

A partir da leitura de diversos artigos e livros sobre o assunto, fica clara a necessidade da contratação de um serviço de compliance, com profissionais especializados em tecnologia e na Lei Geral de Proteção de Dados para criar um sistema virtual seguro e eficaz para o armazenamento de dados e que possibilite um tratamento que vise à segurança além da simples proteção.

Embora a atividade de compliance ainda esteja bastante relacionada à Lei Anticorrupção, a ela não está limitada, de modo que qualquer lei pode ser objeto de compliance em qualquer instituição, público ou privada.

Desse modo, a presente monografia pretende analisar alguns dos aspectos legais e doutrinários sobre a Lei Geral de Proteção de Dados, principalmente no que concerne aos dados de saúde, bem como tentar encontrar uma política pública que garanta uma efetiva segurança no tratamento de dados pelas instituições públicas de saúde.

[4] BRASIL. Art. 1º, §2º, Lei 8.142/1990.

CAPÍTULO 1: O DIREITO DE PRIVACIDADE E A PROTEÇÃO DE DADOS NA CONSTITUIÇÃO FEDERAL DE 1988

1.1 A proteção de dados como direito fundamental

O avanço tecnológico ocorrido nas últimas décadas foi responsável por uma significativa alteração nas relações humanas, inclusive nas relações jurídicas. Cada vez mais são celebrados contratos, prestados serviços e estabelecidos contatos dentro do ambiente virtual.

Consequência direta desse cenário foi a facilitação de captação e de armazenamento de dados pessoais. Para realizar uma compra online, entrar em uma rede social, ou até mesmo baixar um aplicativo, é exigido que o usuário informe seus dados.

Embora seja evidente que a coleta e o uso de dados pessoais não tenha surgido apenas com o advento da internet, tal fenômeno impulsionou essa prática de maneira exponencial, o que acarretou em uma insegurança por parte dos indivíduos sobre qual seria a destinação dada aos seus dados e de que forma eles seriam usados.

Durante um bom tempo, a legislação brasileira não contemplava especificamente a matéria dos dados, mas, com o avanço da preocupação mundial sobre o tópico e o surgimento de legislações internacionais sólidas para proteção de dados, o Brasil, hoje, prevê a proteção dos dados pessoais como direito fundamental.

Por meio da Emenda Constitucional nº 115 de 2022, foi incluído ao artigo 5º, o inciso LXXIX na Constituição Federal, que passou a prever o direito à proteção dos dados pessoais, inclusive nos meios digitais, nos termos da Lei Geral de Proteção de Dados. Tal alteração foi bastante importante, vez que o direito de privacidade e de proteção de dados pessoais atingiu o patamar de direito fundamental, ou seja, se tornou garantia com o objetivo de promover a dignidade humana e de proteger os cidadãos.

Não obstante, em leitura combinada com o artigo 60, §4º, IV, da CF/88, verifica-se que o direito à proteção de dados se tornou cláusula pétrea, de modo que não pode ser objeto de Emenda Constitucional tendente a aboli-lo, o que garante a sua manutenção no ordenamento jurídico.

Outra alteração trazida pela Emenda de nº 115 foi a inclusão do inciso XXVI ao artigo 21, que previu a competência material da União para organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei[5], bem como a do inciso XXX no artigo 22, que determinou a competência privativa da União para legislar sobre a proteção e o tratamento de dados pessoais.

Em comento à aprovação da Emenda, o presidente Rodrigo Pacheco realçou a importância dela para o fortalecimento das liberdades públicas. Ele avaliou que o novo mandamento constitucional reforça a liberdade dos brasileiros e a privacidade do cidadão, além de favorecer os investimentos em tecnologia no país.[6]

De fato, é clara a relação entre as novas garantias constitucionais de proteção de dados pessoais e o direito de privacidade, tanto que, com o avanço tecnológico ao longo dos anos, o próprio conceito de privacidade passou a abarcar os dados pessoais.

1.2 A relação do Direito de Proteção de Dados com o Direito de Privacidade.

O artigo 5º, inciso X da carta constitucional considera "invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação".

Embora o texto una a intimidade e a vida privada no mesmo inciso, é importante estabelecer uma distinção entre a intimidade e a privacidade e esclarecer porque a proteção de dados está inserida na segunda.

O direito à intimidade está relacionado ao íntimo, ao confidencial. Segundo Felix Ruiz Alonso, a intimidade refere-se ao âmbito interior da pessoa, aos seus pensamentos e desejos, sendo assim inacessível a terceiros. Para ele, a pessoa baseia sua vida relacionada à sua intimidade. Já a privacidade, para o mesmo autor, refere-se a "tudo o que não pertença ao âmbito da intimidade, mas que, por sua vez, não transparece à esfera pública."[7]

---

[5] BRASIL. Artigo 21, XXVI, da CF/88.

[6] Promulgada emenda constitucional de proteção de dados. Agência Senado, 2022. Disponível em: <https://www12.senado.leg.br/noticias/materias/2022/02/10/promulgada-emenda-constitucional-de-protecao-de-dados>. Acesso em 05 de outubro de 2022.

[7] ALONSO, Felix Ruiz. **Direito à privacidade**. Porto Alegre: Síntese, 2004. p. 457

O direito à privacidade, que abarca um espectro mais amplo, está relacionado à garantia das pessoas de terem uma vida íntima sem que sejam expostas de forma arbitrária e sem intervenções ilegais do Governo ou empresas.

Historicamente, a proteção à privacidade na doutrina era definida com características de direito negativo, de modo que, para ser garantida, exigia-se absoluta de abstenção do Estado na esfera privada individual. Apenas no século XX, com a revolução tecnológica e a transformação da função do Estado, o sentido de direito à privacidade alterou para passar a ser considerado uma garantia de controle do indivíduo sobre as próprias informações e um pressuposto para qualquer regime democrático[8].

A autora Garrido Gómez conceitua o direito à privacidade como a "(...) *libertad de ejercer un derecho de control sobre los datos referidos a la persona, que hayan salido ya de la esfera própria para convertirse en elemento de un archivo electrónico*"[9], de modo a relacioná-lo diretamente aos dados pessoais.

É possível dizer, então, que, embora tais direitos não se confundam, a proteção de dados é um dos instrumento para garantir o direito de privacidade.

A partir do momento em que a tecnologia passa a permitir o armazenamento e o processamento rápido e eficiente de dados pessoais, dá-se a associação entre proteção à privacidade e informações pessoais disponibilizadas ao controlador. Nesse contexto, além de uma alteração no conteúdo do direito à privacidade, há também no seu léxico, com o surgimento das denominações privacidade informacional, proteção de dados pessoais, autodeterminação informativa, entre outros.[10]

No âmbito da tratativa dos dados pessoais, então, não se busca a privacidade na acepção histórica. Fala-se em autodeterminação informativa, pois o objetivo é que os cidadãos continuem fornecendo seus dados, mas que eles saibam por onde estes dados

---

[8] MENDES, Laura S. Série IDP - Linha de pesquisa acadêmica - Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental, 1ª Edição, São Paulo: Editora Saraiva, 2014. E-book. ISBN 9788502218987. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502218987/. Acesso em: 08 set. 2022.

[9] GARRIDO GÓMEZ, María Isabel. Art. Cit., p. 82. "Liberdade de exercer um direito de controle sobre os dados pessoais de alguém, que já deixaram a esfera pessoal para se transformar em parte de um arquivo eletrônico"

[10] MENDES, Laura S. Série IDP - Linha de pesquisa acadêmica - Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental, 1ª Edição, São Paulo: Editora Saraiva, 2014. E-book. ISBN 9788502218987. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502218987/. Acesso em: 08 set. 2022.

estão circulando e que sejam utilizados para atividades específicas e que não os prejudiquem direta ou indiretamente.

A própria Lei Geral de Proteção de Dados, nos incisos I e II do artigo 2º, definiu que a disciplina de proteção de dados pessoais tem como fundamentos o respeito à privacidade e a autodeterminação informativa.

Observa-se, assim, a construção de um conceito de privacidade relacionado à proteção de dados, mas que não se confundem entre si.

1.3. Histórico da Lei Geral de Proteção de Dados

Apesar de ser um tema jurídico relativamente recente no Brasil, a proteção de dados é objeto de lei na Alemanha desde 1970. Considerada a primeira lei formal sobre o tema no mundo, a Lei de Proteção de Dados do estado federal de Hesse entrou em vigor em 1970, enquanto que o principal instrumento legal na Alemanha sobre a matéria, a Lei Federal de Proteção de Dados ("Bundesdatenschutzgesetz", BDSG), entrou em vigor em 1979.[11]

Com a expansão do debate sobre o tema no continente europeu, em 2012, surge na Europa o Regulamento Geral sobre a Proteção de Dados ou **GDPR** (*General Data Protection Regulation*), que entrou em vigor em 2018 e teve como objetivo harmonizar as leis de privacidade de dados pela Europa.

Tão influente foi esse movimento que outros países ao redor do mundo passaram a criar o seu próprio regulamento de proteção de dados, inclusive o Brasil, com a Lei Geral de Proteção de Dados.

No entanto, durante a primeira década do século XXI, o Brasil já vislumbrou a necessidade de regulamentações sobre os dados pessoais. Em 2010, ocorreu a primeira consulta pública sobre a proteção de dados e, nos anos seguintes, surgiram leis relevantes tangentes ao tema, como a Lei de Acesso à Informação (Lei nº 12.527/2011) e a Lei Carolina Dieckmann (Lei nº 12.737/2012).

---

[11] Alemanha – Informações sobre a Regulamentação da Internet. Disponível em: <http://pensando.mj.gov.br/marcocivil/wp-content/uploads/sites/2/2015/04/23-Alemanha.pdf.> Acesso em 15 de setembro de 2022.

Em 2014, entrou em vigor o Marco Civil da Internet, que previa inúmeros princípios reguladores do uso da internet no Brasil, inclusive a proteção da privacidade e dos dados pessoais. Tal diploma legal representou grande avanço em termos de garantia de uma maior segurança para as relações existentes na internet, que aumentavam exponencialmente à época.

Em 2018, ocorreu um escândalo de vazamento de dados da empresa Cambridge Analytica, que expôs uma utilização inapropriada de dados recolhidos através do Facebook. Os dados, que começaram a ser recolhidos pela Cambridge Analytica em 2014, foram utilizados por políticos para influenciar campanhas eleitorais pelo mundo, inclusive nas eleições norte-americanas de 2016 e na votação da saída do Reino Unido da União Europeia ("BREXIT").

Tal evento de repercussão internacional, somado à entrada em vigência da GDPR na Europa, influenciaram o Brasil a aprovar a Lei Geral de Proteção de Dados no mesmo ano, com previsão de entrada em vigor após 18 meses.

Entretanto, como muitas empresas e órgãos públicos entenderam que seria necessário um tempo maior para se adequarem às novas disposições legais e com a chegada da pandemia de COVID-19, em junho de 2020, foi aprovada a Lei 14.010, que definiu, em seu artigo 20, que as sanções administrativas relacionadas ao descumprimento da lei entrariam em vigor apenas a partir de agosto de 2021.

Dessa forma, a partir de referida data, a Autoridade Nacional de Proteção de Dados (ANPD) já poderia definir instruções para o cumprimento e fiscalizar as regras; o Procon e o Ministério Público já poderiam fiscalizar a aplicação da Lei e o Judiciário já poderia decidir sobre casos que a envolvam.

A Lei Geral de Proteção de Dados regula, principalmente, o tratamento de dados, definido no artigo 5º, X, que diz respeito a qualquer atividade que utiliza um dado pessoal na execução da sua operação. O ordenamento exige que o agente informe de forma clara e explícita a finalidade da operação, bem como os propósitos especificados e informados ao titular dos dados.

O artigo 6º da Lei traz alguns princípios importantes do tratamento de dados, como o da finalidade, o da transparência, o da necessidade, entre outros. No entanto, para

assegurar um tratamento de dados adequado, um princípio de grande importância é o da prevenção, previsto no inciso VIII.

De fato, quando se fala na implementação da Lei dentro de um sistema de tratamento de dados, seja público ou privado, o trabalho a ser feito visa justamente à prevenção do vazamento de dados ou de uma destinação inadequada a eles.

Largamente utilizado no Direito Ambiental, o princípio da prevenção versa sobre a adoção de medidas para prevenir a ocorrência de danos.

De acordo com Rony Vainzof[12], a prevenção esperada pela disposição do inciso VIII do artigo 6º é a pautada no conceito de Ann Cavoukian chamado *Privacy by Design*, que prevê a existência de sete princípios fundamentais no tratamento de dados em sistemas de TI, práticas negociais responsáveis e em uma infraestrutura de rede.

O primeiro, Proactive not Reactive; Preventative not Remedial, versa sobre a importância da proatividade para adotar medidas que previnam incidentes de violação de privacidade, de modo a afastar ao máximo a necessidade de medidas remediativas.

O segundo, Privacy as the Default Setting, prevê a necessidade de uma prévia implementação de um padrão de proteção no sistema desde o recebimento dos dados, de modo que a tutela deve estar embutida no sistema como proteção automática antes do tratamento.

Numa linha similar, o Privacy Embedded into Design visa à incorporação da privacidade na própria arquitetura do sistema e nos modelos de negócio.

O Full Functionality – Postive-Sum, not Zero-Sum versa sobre a transparência da relação de tratamento de dados, em que os interesses e objetivos das partes devem ser acomodados, de modo que há uma relação de "ganha-ganha", com a possibilidade de garantir todos, como a privacidade e a segurança, ao mesmo tempo.

End-to-End Security – Full Lifecycle Protection é o princípio que assegura as medidas de proteção e segurança de dados ao longo de todo o tratamento, uma vez que a Privacy by Design já incorporou tais medidas antes mesmo da coleta do primeiro

[12] LGPD: Lei Geral de Proteção de Dados Pessoais comentada / coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. 3. Ed. Ver., atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2021.

elemento de informação. Esse princípio assegura, inclusive, a destruição do dado de forma segura e eficaz ao longo do tempo.

O Visibility and Transparency – Keep it Open, por sua vez, é o princípio que assegura que todos os envolvidos sejam informados com suficiente transparência acerca dos componentes e do modelo de operação de tratamento de dados.

Por fim, o princípio Respect for User Privacy – Keep it User-Centric foca na necessidade dos agentes de tratamento de dados manterem respeito aos interesses dos usuários, com a manutenção de altos padrões de privacidade.

Apesar de não ser diretamente mencionado, o Privacy by Design tem bastante utilidade na adequação aos artigos 46 e 47 da lei:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.
>
> [...]
>
> § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.
>
> Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

No entanto, apesar de todos esses princípios embutidos na Lei brasileira de Proteção de Dados, o cenário de tratamento de dados no país está longe de estar adequado e conforme à lei.

1.4. O problema da tratativa dos dados na atualidade

De acordo com o perito em crimes digitais Wanderson Castilho, em entrevista à CNN[13], em 2021, o Brasil ficou no topo de vazamentos de informações no mundo.

Em comento ao vazamento de dados de mais de 227 milhões de brasileiros, o especialista destacou o episódio ocorrido no Ministério da Saúde, que expôs 16 milhões de pacientes que tiveram COVID-19 no fim do ano de 2020.

---

[13] Em 2021, Brasil ficou no topo de vazamento de informação no mundo, diz especialista. CNN Brasil, 2021. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/em-2021-brasil-ficou-no-topo-de-vazamento-de-informacao-no-mundo-diz-especialista/>. Acesso em 18 de Agosto de 2022.

Ainda, segundo dados da Check Point Research, do site Medicina S.A[14], divulgados no início de 2022, golpes virtuais na saúde aumentaram 64%. O segmento é o segundo alvo preferencial dos cibercriminosos, ficando atrás apenas do varejo.

Esses episódios de grandes vazamentos de dados no Brasil são sintomas da dificuldade e da falta de compromisso por parte dos setores privado e público na implementação da LGPD.

Após o início da vigência da Lei Geral de Proteção de Dados, tanto o setor privado como o público tiveram até o mês de julho de 2021 para implementarem as novas regras legais nos seus sistemas internos de tratativa de dados. Caso contrário, poderiam ser aplicadas multas de até 50 milhões de reais. No entanto, devido à complexidade dessa tarefa, muitos operadores de dados ainda não conseguiram cumprir todas as disposições legais.

Segundo notícia veiculada no site de notícias CNN Brasil[15], mais de dois terços das empresas ainda não implementaram nem mesmo a primeira etapa, que é a criação de políticas de proteção de dados, aquela que deve ser incluída nos sites das companhias para explicar como as informações dos usuários são capturadas e como serão usados esses dados, entre outras questões básicas exigidas pela lei

Os números ainda apontam uma maior dificuldade de adequação à Lei por parte do setor público. De acordo com o site Capital Digital, uma auditoria realizada pelo Tribunal de Contas da União (TCU), através da Secretaria de Fiscalização de TI (Sefti) em relatório final aprovado pelo plenário da Corte e relatado pelo Ministro Augusto Nardes, apresentou dados alarmantes: 76,7% em um contingente de 382 órgãos federais não adotam a LGPD; somente 45% das organizações concluíram a iniciativa de mapeamento e planejamento das medidas necessárias à adequação e apenas 18% das organizações possuem Política de Proteção de Dados Pessoais ou documento similar.[16]

---

[14] Vazamento de dados na saúde coloca pacientes na mira de golpes. Medicina S/A, 2022. Disponível em: <https://medicinasa.com.br/vazamento-dados saude/#:~:text=Vazamento%20de%20dados%20na%20sa%C3%BAde%20coloca%20pacientes%20na%20mira%20de%20golpes,-Seguran%C3%A7a%20Digital&text=A%20privacidade%20e%20a%20seguran%C3%A7a,de%20pacientes%2C%20cl%C3%ADnicas%20e%20profissionais.>. Acesso em 26 de setembro de 2022.

[15] Empresas não conseguem se adaptar à lei de proteção de dados, aponta pesquisa. CNN Brasil, 2021. Disponível em: < https://www.cnnbrasil.com.br/business/empresas-nao-conseguem-se-adaptar-a-lei-de-protecao-de-dados-diz-pesquisa/>. Acesso em 26 de setembro de 2022.

[16] QUEIROZ, Luis. TCU: 76,7% de 382 órgãos federais não adotam a LGPD. 24% não têm sequer Política de Segurança da Informação. Capital Digital, 2022. Disponível em: < https://capitaldigital.com.br/tcu-767-

Esses resultados podem indicar certa negligência de ambos os setores em cumprir as determinações legais e em criar um sistema de segurança que evite o acesso a dados por hackers, por exemplo.

Especialista em segurança digital na empresa Kzarka, Gwin, em entrevista dada ao site Tecnoblog[17], expõe a falta de interesse de empresas em gastar com a chamada redundância, algo que seria essencial para qualquer sistema de segurança. Ele a explica da seguinte forma:

> Você precisa de uma muralha bem construída na empresa, uma segurança que consiga suportar qualquer intempérie, sistemas que são redundantes…
> Então, se um sistema falha, você tem outro, e ele segura o primeiro.
> É como se fosse um castelo na Idade Média: se a muralha de fora falha – recebe uma pedrada de uma catapulta e cai – você tem as muralhas internas para proteger. Você tem os soldados para proteger. Você tem torres de vigia para proteger. Enfim, você tem uma multiplicidade de sistemas de segurança que são redundantes.

Para Gwin, o problema é que a LGPD não força essa redundância e, devido ao alto preço da implementação, muitos preferem não implementar. O especialista afirma que isso é visto como algo desnecessário, todavia, a segurança é a única área em que você precisa de redundância.

Outro fator que pode ter influenciado no atraso da implementação da LGPD pelas empresas e pelo setor público são as poucas penalidades aplicadas até hoje frente ao descumprimento da Lei. De acordo com o site Escritório de Contabilidade[18], especialistas apontam que a Autoridade Nacional de Proteção de Dados (ANPD) tem efetuado ações mais educativas e menos punitivas nesse primeiro momento.

De fato, o Planejamento Estratégico da ANPD[19] para os anos de 2021 a 2023 tem três objetivos estratégicos: promover o fortalecimento da cultura de proteção de dados

---

de-382-orgaos-federais-nao-adota-a-lgpd-24-nao-tem-sequer-politica-de-seguranca-da-informacao/>. Acesso em: 01 de setembro de 2022.

[17] Problema da LGPD é depender demais de confiança no Brasil, diz especialista. Tecnoblog, 2022. Disponível em: <https://tecnoblog.net/especiais/problema-da-lgpd-e-depender-demais-de-confianca-no-brasil-diz-especialista/> . Acesso em 26 de setembro de 2022.

[18] ANPD - Pesquisa aponta que maioria das empresas não conseguem se adaptar à LGPD. Escritório de Contabilidade, 2021. Disponível em: <https://www.sitecontabil.com.br/view/C1601/noticias-ler.php?id=6097&p=1&regiao=brasil>. Acesso em 26 de setembro de 2022.

[19] Brasil, Autoridade Nacional de Proteção de Dados. Planejamento Estratégico 2021-2023. Disponível em: <https://www.serpro.gov.br/lgpd/noticias/2021/anpd-agenda-regulatoria-lgpd.> Acesso em 26 de setembro de 2022.

pessoais, estabelecer ambiente normativo eficaz para a proteção de dados pessoais; e aprimorar as condições para o cumprimento das competências legais.

Apesar de ser inquestionável a extrema relevância das ações educativas às empresas e ao setor público, igualmente importante é a aplicação de penas para quem deixa de implementar a Lei.

Fabrício da Mota Alves[20], ao lecionar sobre a fiscalização da aplicação da LGPD, destaca:

> Contrapondo-se ao pensamento sofista – o qual pregava que a persuasão e a razão seriam suficientes para o governo de "muitos", privilegiando, assim, a onipotência do discurso retórico na política -, Xenofonte defendia uma visão mais realista da filosofia política: para ele, seriam necessárias "leis com dentes", ou seja, dotadas de elementos coercitivos, para a manutenção da coesão da cidade e do bem comum.
>
> (...) Por isso, a coercitividade das leis tem sido muito associada à instrumentalização das administrativa que o legislador confere aos órgãos de fiscalização notadamente componentes do Poder Executivo, a quem compete, por excelência, segundo o modelo aristotélico-platônico aprimorado pela visão maquiavélica de Estado tripartite, o exercício do poder de polícia.

Nesse sentido, seja pela dificuldade dos procedimentos tecnológicos específicos; pelos preços elevados dos sistemas de informática e da contratação de compliance; ou pela falta de aplicação de multas coercitivas pela ANPD nesse momento, os setores público e privado ainda não se adequaram à Lei.

No entanto, a partir de 2021, ao não implementar práticas de proteção de dados, o controlador desses dados estará ferindo um direito fundamental e pode sofrer consequências jurídicas seríssimas e muito onerosas caso haja qualquer vazamento ou tratamento inadequado.

Por exemplo, em julho de 2019, a GDPR (a regulação geral de proteção de dados da União Europeia) multou a companhia aérea inglesa British Airways no maior valor da história da lei: 230 milhões de dólares. O motivo foi uma falha de segurança no sistema interno, que possibilitou o desvio, por hackers, de cerca de 500 mil clientes que acessavam

[20] LGPD: Lei Geral de Proteção de Dados Pessoais comentada / coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. 3. Ed. Ver., atual. e ampl. –São Paulo: Thomson Reuters Brasil, 2021.

o site da companhia aérea para uma plataforma fraudulenta, no qual dados pessoais como nomes, informações de login, endereços e detalhes de pagamento foram roubados.[21]

Por isso, ainda que, no primeiro momento, a ANPD não esteja aplicando muitas sanções, não há dúvidas de que deixar de implementar a LGPD será muito mais oneroso do que implementá-la da forma adequada, de forma a criar uma verdadeira cultura de segurança de dados.

[21] Por roubo de dados pessoais, British Airways é multada em R$ 230 milhões. LGPDbrasil.com.br, 2019. Disponível em: <https://www.lgpdbrasil.com.br/por-roubo-de-dados-british-airways-e-multada-em-us230-milhoes/#:~:text=Close-,Por%20roubo%20de%20dados%20pessoais%2C%20British%20Airways,multada%20em%20US%24230%20milh%C3%B5es&text=As%20autoridades%20brit%C3%A2nicas%2C%20muito%20por,dos%20passageiros%20no%20ano%20passado.> Acesso em 28 de setembro de 2022.

CAPÍTULO 2: PROTEÇÃO E SEGURANÇA DE DADOS

2.1 Conceitos de Proteção e de Segurança

O dicionário Oxford Languages define "proteção"[22] como cuidado com algo; defesa contra um agente exterior, um invólucro. Na etimologia da palavra, tem-se *protectĭo,ōnis*, de *protegĕre* 'cobrir, esconder'.

Já o termo "segurança"[23] é definido como "estado, qualidade ou condição de quem ou do que está livre de perigos, incertezas, assegurado de danos e riscos eventuais; situação em que nada há a temer". Também como "a condição ou caráter do que é firme, seguro, sólido, ou daquele com quem se pode contar ou em quem se pode confiar."

Os desenvolvedores de softwares e códigos também distinguem os dois conceitos: "segurança significa que nenhum dano é causado, seja ele deliberado ou não, já proteção significa que nenhum dano deliberado é causado." [24]

Para eles, em termos mais específicos, a proteção do código trata da prevenção de atividades indesejadas ou ilegais no software criado ou utilizado. Isso ajuda a garantir que os sistemas estejam seguros durante um ataque, impedindo a entrada de invasores.

Já, a segurança do código é um termo mais amplo, capaz de indicar se um software é confiável e seguro de utilizar.

Para David Zanetti, Sócio-Fundador da ProMove - Business Innovation, empresa que presta consultoria em melhoria de processos de software em organizações no Brasil, a proteção é um meio para chegar-se à segurança.

---

[22] Proteção. *In*: Oxford Languages, Dicionário Online Oxford Languages. Disponível em: < https://languages.oup.com/google-dictionary-pt/>. Acesso em: 03/10/2022

[23] Segurança. *In*: Oxford Languages, Dicionário Online Oxford Languages. Disponível em: < https://languages.oup.com/google-dictionary-pt/>. Acesso em: 03/10/2022

[24] Segurança vs Proteção em Desenvolvimento de Software: Entenda as diferenças! ProMove, 2022. Disponível em: < https://promovesolucoes.com/seguranca-vs-protecao-em-desenvolvimento-de-software-diferencas/>. Acesso em 03 de outubro de 2022.

Nesse sentido, muito além da proteção de dados, isto é, de adotar um conjunto de processos e ferramentas que previnam um vazamento interno e externo de informações pessoais, deve-se almejar verdadeira segurança de informações.

No site da Rastek Soluções[25], outra empresa especializada na implementação de LGPD, esclarecem que a segurança da informação não trata apenas de dados pessoais e sensíveis, mas sim da segurança de toda a informação do negócio.

Para alcançar essa segurança, de acordo com a empresa, "é necessário criar um Sistema de Gestão da Segurança da Informação (SGSI), que define uma estrutura para que as informações de uma empresa sejam protegidas. Isso inclui uma série de processos, controles, políticas e estratégias para realizar o monitoramento, analisar e definir ações necessárias para estabelecer a segurança da informação dentro do negócio."

Ainda, o site elenca quatro tipos de segurança cibernética, com um foco de atuação particular a cada contexto: a segurança defensiva; a segurança ofensiva; a segurança forense e a segurança avaliatória.

A primeira, com foco na proteção, visa à redução de possibilidade de ataques por meio de tecnologias e de instrumentos internos de segurança eficazes.

A segunda tem como objetivo testar a segurança do ambiente, por meio da utilização das mesmas técnicas de hackers de grandes organizações, com o fim de verificar se eles conseguiriam ou não adentrar o sistema de informação interno.

A terceira, forense, além do apoio na elaboração de medidas preventivas, objetiva investigar um incidente, utilizando técnicas de coleta, recuperação e análise de evidências digitais para entender como ocorreu um ataque.

Por fim, a segurança avaliatória busca avaliar a funcionalidade dos sistemas, bem como identificar possíveis vulnerabilidades, instabilidades ou falhas que facilitem possíveis ataques.

O próprio artigo 46 da Lei Geral de Proteção de Dados prevê a necessidade da adoção de "medidas de segurança":

---

[25] Diferenças entre Privacidade, Proteção de Dados e Segurança da Informação. Rastek Soluções, 2022. Disponível em: < https://rasteksolucoes.com.br/2022/01/diferencas-entre-privacidade-protecao-de-dados-e-seguranca-da-informacao/>. Acesso em 03 de outubro de 2022.

> Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.

Com o uso do termo "medidas de segurança", após os conceitos supramencionados, verifica-se que a interpretação a ser dada ao texto legal é a necessidade de criação de um sistema complexo, sólido e bem estruturado dentro das instituições para o tratamento de dados, que previna danos deliberados ou não.

Além do artigo 46, a segurança também se apresenta como princípio no artigo 6º, inciso VII da LGPD. De acordo com a autora Camilla do Vale Jimene[26],

> [...] o art. 6º da LGPD estabelece no inc. VII a segurança como princípio a ser observado nas atividades de tratamento de dados pessoais, definindo o vocábulo "segurança" como a 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.

Portanto, no tocante ao tratamento de dados pelos operadores e controladores, a Lei Geral de Proteção de Dados visa a um movimento que passa pela proteção para chegar à segurança. Ou seja, além de se adotar medidas para evitar uma invasão de agentes exteriores, hackers, objetiva criar um sistema que se auto sustenta, confiável e seguro, com uma redução significativa na possibilidade de vazamento interno e externo e de tratamento inadequado de dados.

2.2 Tipos de dados

A Lei nº 13.709/2018 regulamenta o tratamento de dados pessoais, que, segundo o artigo 5º, I, é qualquer "informação relacionada a pessoa natural identificada ou identificável"[27]. São exemplos de dados pessoais: nome e sobrenome; data e local de nascimento; RG; renda; hábitos de consumo; entre outros.

O autor Danilo Doneda ressalta ser "importante distinguir dados gerais de dados pessoais, pois estes últimos possuem um vínculo objetivo com a pessoa, justamente por revelar aspectos que lhe dizem respeito".[28]

---

[26] LGPD: Lei Geral de Proteção de Dados Pessoais comentada / coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. 3. Ed. Ver., atual. e ampl. –São Paulo: Thomson Reuters Brasil, 2021.
[27] BRASIL. Art. 5º, I, LGPD, 2018.
[28] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. P. 157.

Ademais, Rony Vainzof[29] destaca que

> O Brasil adotou o conceito expansionista de dado pessoal, pelo qual não somente a informação relativa a pessoa diretamente identificada estará protegida pela Lei, mas também aquela informação que possa – tem o potencial de – tornar a pessoa identificável.

Além dos dados pessoais, são também objeto de disciplina pela Lei os dados pessoais sensíveis, que, de acordo com o artigo 5º, inciso II, são os dados pessoais:

> 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[30].

Sobre os dados pessoais sensíveis, a autora Gabrielle Bezerra Sales Sarlet escreve:

> O conjunto dessas informações compõe os perfis ou as identidades digitais, possuindo valor político e, sobretudo, econômico, vez que podem ser a matéria prima para as novas formas de controle social, especialmente mediante o uso de algoritmos. Os perfis são composições, ou melhor dizendo, são mosaicos compostos pelas informações fornecidas pelos usuários em uma formatação igualmente constituída e emoldurada pelo que é advindo das pegadas digitais e pelos vazamentos de dados [31]

Por serem dados íntimos e com bastante valor social, econômico e político, é extremamente importante que gozem de uma segurança especial. É o que defende Sarlet:

> Tratando-se de dados sensíveis, reafirma-se a exigência de uma proteção especial alicerçada no princípio da dignidade da pessoa humana, cuja fundamentalidade radica e sustenta a democracia e o atual molde de Estado de Direito. Este reforço antropológico encontra ainda amparo, e.g., no artigo segundo do Tratado da União Europeia, no qual se consagra, a dignidade humana, a liberdade, a democracia, a igualdade, o Estado de direito e o respeito pelos direitos humanos.

Além dos dados pessoais sensíveis, a Lei também traz o conceito de dados anonimizados, que, segundo o inciso III do artigo 5º, são os "dados relativos a titular que não possam ser identificados, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento".

De acordo com o artigo 12 da Lei, uma vez anonimizados, os dados já não são mais considerados pessoais, mas tal característica não é necessariamente permanente. Por

---

[29] LGPD: Lei Geral de Proteção de Dados Pessoais comentada / coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. 3. Ed. Ver., atual. e ampl. –São Paulo: Thomson Reuters Brasil, 2021.
[30] BRASIL. Art. 5º, II, LGPD, 2018.
[31] SARLET, Gabrielle Bezerra Sales. Notas sobre a Proteção dos Dados Pessoais na Sociedade Informacional na Perspectiva do Atual Sistema Normativo Brasileiro in: LIMA, Cíntia Rosa Pereira D. Comentários à Lei Geral de Proteção de Dados. São Paulo: Grupo Almedina (Portugal), 2020. E-book. ISBN 9788584935796. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584935796/. Acesso em: 06 out. 2022.

exemplo, se, com a aparição de uma nova tecnologia de processamento ou base de dados, houver o cruzamento com um dado anonimizado, ele perderá tal característica.[32]

Para a LGPD, o dado está anonimizado quando (i) é impossível identificar o titular ou associar o dado diretamente ao indivíduo; (ii) é utilizado meio técnico razoável e disponível na ocasião do seu tratamento; e (iii) o processo de anonimização não pode ser revertido por meios próprios ou por esforços razoáveis.

O "esforço razoável" previsto no artigo 12, caput, da LGPD, está definido no parágrafo 1º do mesmo artigo, como "fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios."[33]

Por fim, existe o dado pseudonimizado, definido como

> dado pessoal, que, por meio de tratamento, perde a possibilidade de ser associado direta ou indiretamente a um indivíduo, a menos que o controlador use uma informação adicional que era mantida separadamente em ambiente seguro. Exemplo: dados criptografados e uso de *hash* como autenticação. [34]

No presente trabalho, o foco de estudo são os dados sensíveis, mais especificamente relacionados à saúde e quais são as diretrizes de tratamento a serem dadas pelo Conselho Nacional de Saúde.

2.3 Tratamento de dados relativos à saúde.

Os dados referentes à saúde são dados sensíveis, conforme esclarece inciso II do artigo 5º e, portanto, conforme observado, merecem tratamento diferenciado.

O tratamento de dados de forma geral está descrito no inciso X do artigo 5º como

> toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação,

[32] LGPD: Lei Geral de Proteção de Dados Pessoais comentada / coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. 3. Ed. Ver., atual. e ampl. –São Paulo: Thomson Reuters Brasil, 2021.
[33] BRASIL. Art. 12, §1º, LGPD, 2018.
[34] LGPD: Lei Geral de Proteção de Dados Pessoais comentada / coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. 3. Ed. Ver., atual. e ampl. –São Paulo: Thomson Reuters Brasil, 2021.

> avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração[35]

De forma mais específica, o artigo 11, que dá início à Seção II da Lei Geral de Proteção de Dados, disciplina o tratamento dos dados pessoais sensíveis e elenca as hipóteses em que ele pode ocorrer.

Na primeira hipótese, a lei exige o consentimento do titular ou do seu responsável legal, de forma específica e destacada, para finalidades específicas.

A segunda deixa de exigir o consentimento do titular quando for indispensável fazer o tratamento de dados em hipóteses taxativas.

Nos termos da lei, é possível fazer o tratamento de dados pessoais sensíveis sem consentimento do titular quando for necessário: (a) para o cumprimento de obrigação legal ou regulatória pelo controlador; (b) por meio de tratamento compartilhado de dados, à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; (c) realizar estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; (d) o exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral; (e) para a proteção da vida ou da incolumidade física do titular ou de terceiro; (f) para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (g) para a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.[36]

A partir da leitura desses artigos, observa-se que o tratamento de dados de saúde, regra geral, exige o consentimento do titular. No entanto, quando, por exemplo, o tratamento de dados for necessário para a tutela da saúde, em procedimento realizado por profissionais da área, ou em serviços de saúde ou por autoridade sanitária, não há necessidade de consentimento.

Nesse momento, fica evidente um grande desafio a ser enfrentado no âmbito de tratamento de dados de saúde.

---

[35] BRASIL. Artigo 5º, X, LGPD, 2018.
[36] BRASIL. Artigo 11, II, LGPD, 2018.

Primeiro, por ser necessária a adoção de práticas de segurança em todas as instâncias dos serviços de saúde, vez que existe um ecossistema interligado, que passa pela clínica médica, pelo laboratório, pela farmácia e chega até o Pronto Socorro de um hospital, por exemplo. Além disso, esse processo engloba tanto clínicas privadas, agentes de saúde e também toda a esfera pública - o Sistema Único de Saúde (SUS).

Segundo, porque o tratamento de dados de saúde, na grande maioria das vezes ocorrerá por meio do consentimento do titular, o que implica na necessidade da aplicação do princípio da transparência, reforçado pela LGPD e que tem conexão inclusive com a legislação consumerista.[37]

Conforme afirma José Luiz de Moura Faleiros Júnior,

> Tudo parte da necessidade de um "novo olhar" sobre a informação. Na medida em que o consentimento passa a ser o critério fundamental para a coleta, torna-se essencial que o indivíduo saiba discernir os limites e os riscos que enfrentará ao fornecer seus dados a determinado agente.[38]

Ainda que a Lei trate da autodeterminação informativa e do consentimento para permitir um tratamento de dados, importa pontuar que a responsabilidade, caso haja um tratamento inadequado dos dados, jamais será do titular que os forneceu. O consentimento está ligado à coleta apenas. Não se nega a importância de o titular analisar os riscos e e estar ciente da destinação dos seus dados, porém não se deve responsabilizá-lo por qualquer vazamento, com base na autodeterminação informativa.

Inclusive, diversos serviços médicos, para serem efetuados, têm como premissa a coleta e o tratamento de dados, o que implica na obrigação de investir na adequação dos seus sistemas internos à LGPD.

Se não forem definidas medidas de segurança que garantam o sigilo e o 'bom uso' dos dados coletados e armazenados nas bases das três esferas da federação, a possibilidade de lesar os titulares e, consequentemente, de sofrer responsabilizações civis e administrativas aumentam.

---

[37] PINHEIRO, Patrícia Peck. LGPD e saúde: os fins justificam os meios? SerPro, 2019. Disponível em: < https://www.serpro.gov.br/lgpd/noticias/2019/paciente-no-comando-lgpd-dados-sensiveis-saude> . Acesso em 10 de outubro de 2022.

[38] JÚNIOR. José Luiz de Moura Faleiros. O Tratamento de Dados relativos à saúde: breves reflexões. Contraditor.com, 2021. Disponível em: < https://www.contraditor.com/o-tratamento-de-dados-relativos-a-saude-breves-reflexoes/>. Acesso em 10 de outubro de 2022.

Um tratamento mais efetivo e seguro de dados no âmbito do Sistema Único de Saúde tem sido feito no âmbito da pesquisa, pela regulamentação dos Comitês de Ética em Pesquisa, definida na Resolução MS/CNS n° 466/2012, a qual tem sido posta em prática. Dentre as definições da Resolução, encontram-se disposições similares às da LGPD, como no item IV.7:

> Na pesquisa que dependa de restrição de informações aos seus participantes, tal fato deverá ser devidamente explicitado e justificado pelo pesquisador responsável ao Sistema CEP/CONEP. Os dados obtidos a partir dos participantes da pesquisa não poderão ser usados para outros fins além dos previstos no protocolo e/ou no consentimento livre e esclarecido.[39]

Ainda que o setor de pesquisa esteja fazendo um tratamento de dados exemplar, esse não é o caso da área de saúde como um todo, que ainda está bastante defasada na implementação da LGPD.

Nesse sentido, as práticas vigentes no âmbito da pesquisa devem ser importadas para as demais ações e serviços disponibilizados pelo SUS e também pelos prestadores privados de serviço de saúde.

Oportuno consignar que o Plano Diretor de Tecnologia da Informação 2019/2021 do DATASUS cita a necessidade de implantar a LGPD no Ministério da Saúde por meio da preparação para o compliance. Ante o exposto, evidente a necessidade de ágil ação por parte de gestores do SUS de modo a adequar-se com brevidade às exigências técnicas, organizacionais e legais que defluem da LGPD.

[39]BRASIL. Resolução nº 466, 2012. Disponível em: <https://conselho.saude.gov.br/resolucoes/2012/Reso466.pdf>.

CAPÍTULO 3: O PAPEL DO CONSELHO NACIONAL DE SAÚDE NA IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS NO SETOR DA SAÚDE.

3.1 O Conselho Nacional de Saúde

Segundo o site oficial do governo[40], o Conselho Nacional de Saúde (CNS) é parte integrante da estrutura organizacional do Ministério da Saúde, criado em 1937. Instância colegiada, deliberativa e permanente do Sistema Único de Saúde (SUS), o CNS tem a missão de fiscalizar, acompanhar e monitorar as políticas públicas de saúde nas suas mais diferentes áreas, levando as demandas da população ao poder público, ou seja, ele faz um controle social da saúde.

As atribuições atuais do CNS estão regulamentadas pela Lei n° 8.142/1990. O seu §2º do artigo 1º define:

> § 2° O Conselho de Saúde, em caráter permanente e deliberativo, órgão colegiado composto por representantes do governo, prestadores de serviço, profissionais de saúde e usuários, atua na formulação de estratégias e no controle da execução da política de saúde na instância correspondente, inclusive nos aspectos econômicos e financeiros, cujas decisões serão homologadas pelo chefe do poder legalmente constituído em cada esfera do governo.[41]

Ainda sobre o tema, o site oficial complementa:

> a atuação na formulação de estratégias diz respeito a uma postura combativa/ofensiva/criadora de construção do novo modelo, e a atuação ao controle da execução das políticas, a uma postura defensiva, contra os desvios e distorções. Essas duas visões devem ser relativizadas: a atuação na formulação não deve ser "vanguardista" e isolada, mas sempre que possível, articulada e sinérgica com o Gestor do SUS (que tem assento no Conselho de Saúde), e o Poder Legislativo, sem qualquer prejuízo da autonomia e agilidade próprias do Conselho.[42]

Observa-se que o Conselho Nacional de Saúde tem a prerrogativa de atuar de forma direta no setor de saúde, inclusive com a elaboração de políticas públicas. Dessa forma, é inquestionável a necessidade de intervenção do CNS no âmbito da

---

[40] Conselho Nacional de Saúde. Apresentação. Disponível em: <https://conselho.saude.gov.br/apresentacao/apresentacao.htm#:~:text=A%20presid%C3%AAncia%20do%20%C3%B3rg%C3%A3o%20%C3%A9,o%20Plano%20Nacional%20de%20Sa%C3%BAde.> Acesso em: 11 de outubro de 2022.

[41] BRASIL. Lei 8.142, 1990.

[42] Conselho Nacional de Saúde. Disponível em: < http://conselho.saude.gov.br/pratica/pratica.htm>. Acesso em: 14 de outubro de 2022.

implementação da Lei Geral de Proteção de Dados nas diversas esferas de atendimento à saúde no País e principalmente no setor público.

No mais, conforme estabelece o artigo 21, inciso XXVI, da Constituição Federal de 1988, "compete à União organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei." Nesse sentido, o Conselho Nacional de Saúde, enquanto ramificação do Ministério da Saúde, possui a competência constitucional para organizar e criar políticas públicas.

Dentre as possíveis políticas públicas a serem implementadas, o foco de estudo no presente trabalho será o Compliance. Da análise que se fez ao longo dos capítulos anteriores, é indubitável a importância da contratação de empresas e profissionais especializados para a criação de um sistema virtual que garanta verdadeira segurança para a tratativa de dados relacionados à saúde no âmbito público. Logo, o investimento no compliance é eficaz solução, que deverá ser motivado e financiado pelo Conselho Nacional de Saúde e pelo Ministério da Saúde, instância federal da saúde no Poder Executivo.

3.2 O compliance como importante política pública para a criação de segurança de dados.

Com origem no termo inglês "to comply", que significa "estar em conformidade com", a atividade do compliance objetiva garantir o cumprimento de atos, regimentos, normas e leis estabelecidos interna e externamente.[43]

Muito utilizado em empresas privadas, o compliance no Brasil passou a ganhar maior notoriedade com a Lei Anticorrupção, promulgada em 2013 e regulamentada pelo pelo Decreto nº 8.420/15.

No entanto, o compliance pode e deve ser utilizado em diversas instituições, privadas ou públicas, e para implementar qualquer norma, com o objetivo de prevenir problemas e litígios.

De acordo com Franciso Mendes e Vinícius Carvalho:

> Um programa de compliance visa estabelecer mecanismos e procedimentos que tornem o cumprimento da legislação parte da cultura corporativa. Ele não

[43] BOBSIN, Arthur. Compliance: conceito, tipos, benefícios e como colocar em prática. Disponível em: < https://www.aurum.com.br/blog/compliance/>. Acesso em: 15 de outubro de 2022.

> pretende, no entanto, eliminar completamente a chance de ocorrência de um ilícito, mas sim minimizar as possibilidades de que ele ocorra, e criar ferramentas para que a empresa rapidamente identifique sua ocorrência e lide da forma mais adequada possível com o problema.[44]

A Lei Geral de Proteção de Dados opera justamente no âmbito da prevenção de vazamentos e de tratamento inadequado de dados. Ainda, para se criar um ambiente virtual seguro para os milhões de dados pessoais sobre saúde que estão sob o controle do poder público, é necessário conhecimento técnico em informática e sistemas de segurança específicos.

Dessa forma, o compliance se mostra como política pública extremamente eficaz no que diz respeito à criação de um ambiente efetivamente seguro para o tratamento de dados pessoais sensíveis.

Para Ariana Quintanilha,

> A relação entre o compliance e a LGPD é permeada pela noção de controle e transparência, visto que a LGPD permite que o titular de dados tenha total controle de todo ciclo de vida dos seus dados dentro de uma empresa, permitindo entender o objetivo e finalidade daquele determinado tratamento. Portanto, na sociedade e no mercado atuais, o controle e transparência são peças-chaves.[45]

Dentre os responsáveis pela área de compliance, o profissional de compliance é aquele que atua na implementação e gestão de programas da área em empresas e instituições. Fica, assim, responsável por institucionalizar processos de conformidade dentro da sua expertise. Inclusive, os profissionais de compliance podem ter diferentes formações, como engenharia, administração, ciências contábeis, tecnologia da informação.

Ainda, atua na área o advogado de compliance, que fica responsável pela implementação de programas de conformidade. “Por meio da consultoria jurídica, garante o cumprimento das normas internas e da legislação estabelecida pelo poder público, minimizando riscos e evitando danos.” [46]

---

[44] MENDES, Francisco Schertel; CARVALHO, Vinícius Marques de. Compliance: concorrência e combate à corrupção. São Paulo: Trevisan Editora, 2017, p. 31.

[45] QUINTANILHA, Ariana. Opinião: A LGPD como um pilar do compliance. Disponível em: <https://www.conjur.com.br/2022-mai-17/ariana-quintanilha-lgpd-pilar-compliance#:~:text=A%20rela%C3%A7%C3%A3o%20entre%20o%20compliance,e%20finalidade%20daquele%20determinado%20tratamento>. Acesso em: 15 de outubro de 2022.

[46] BOBSIN, Arthur. Compliance: conceito, tipos, benefícios e como colocar em prática. Disponível em: < https://www.aurum.com.br/blog/compliance/>. Acesso em: 15 de outubro de 2022.

Nesse sentido, enquanto política pública, o governo federal deve investir na contratação desses profissionais especializados para atuarem nas diversas instituições de saúde, com o objetivo de criar uma sistema de segurança de dados e uma nova cultura na tratativa deles.

3.3 A implementação do compliance pelo Conselho Nacional de Saúde.

Até o presente momento, a maior incidência do compliance nas próprias empresas e nos órgãos públicos tem envolvido a Lei Anticorrupção, que versa sobre o programa de integridade.

O artigo 7º dessa Lei define o programa de integridade como um conjunto de:

> mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e na aplicação efetiva de códigos de ética e de conduta no âmbito da pessoa jurídica[47]

Nesse sentido, seriam criadas políticas e diretrizes com objetivo de detectar e sanar desvios, fraudes, irregularidades e atos ilícitos praticados contra a administração pública, nacional ou estrangeira.[48]

Ainda que a Lei Geral de Proteção de Dados não estabeleça uma estratégia similar ao programa de integridade previsto na Lei Anticorrupção, é possível importar o conceito e as diretrizes para a implementação da LGPD em qualquer âmbito.

O artigo 50 da LGPD, em início à Seção das Boas Práticas e da Governança, prevê:

> Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Na saúde, o Conselho Nacional de Saúde, com auxílio do Conselho Nacional de Proteção de Dados e da Autoridade Nacional de Proteção de Dados devem debater a

---

[47] BRASIL. Art. 7º, Lei 12.846/2013.

[48] Lei Anticorrupção - Programas de Integridade (Compliance). Gov.br. Disponível em: <https://www.gov.br/corregedorias/pt-br/assuntos/perguntas-frequentes/lei-anticorrupcao-programas-de-integridade-compliance#:~:text=Segundo%20a%20Lei%20Anticorrup%C3%A7%C3%A3o%2C%20consiste,de%20detectar%20e%20sanar%20desvios%2C.> Acesso em 15 de outubro de 2022.

melhor estratégia para implementar o compliance nas instituições públicas de saúde, bem como para contratar os profissionais de compliance.

Até o presente, o Conselho Nacional de Saúde tem se mostrado ativo em debates e atento às políticas realizadas pelo Ministério da Saúde.

Em setembro de 2022, o CNS e a Fiocruz realizaram um seminário online em formato de "live" sobre a Lei Geral de Proteção de Dados e suas implicações no Sistema Único de Saúde, no qual debateram a importância da segurança de dados referentes à saúde. Posteriormente, o conteúdo foi publicado no Youtube, de modo a conferir acesso à informação para toda a população.[49]

Já, em 04 de fevereiro de 2022, o CNS editou a Recomendação nº 002, frente à intenção do Ministro da Saúde, Marcelo Queiroga, de promover uma plataforma de compartilhamento de dados e informações de saúde no setor suplementar, o Open Health, que consistiria na possibilidade de usuários de planos privados de saúde autorizarem que seus dados pessoais de saúde fossem compartilhados entre empresas do setor para oferta de produtos personalizados.

Dentre as recomendações feitas ao Ministério da Saúde sobre a questão, tem-se:

> I - Que a consolidação da saúde digital no Brasil seja uma prioridade do Ministério da Saúde, feita, no entanto, por meio do fortalecimento do SUS, da proteção dos dados pessoais dos usuários (tanto contra vazamentos quanto de uso indevido pelo setor privado) e principalmente pela busca da melhoria da qualidade da atenção à saúde ao usuário do SUS;
>
> II - Aprimorar a Política Nacional de Informação e Informática em Saúde (PNIIS) e ampliar a participação social no debate da saúde digital, uma vez que estas são demandas urgentes a serem trabalhadas priorizando-se a sintonia com a sociedade brasileira, acima dos interesses privados de setores empresariais e financeiros;
>
> III - Que os avanços das tecnologias de informação e comunicação sejam focados no sistema público e com uma política robusta de segurança, com transparência e que assegure a proteção de dados pessoais dos usuários, incluindo a autodeterminação informativa dos titulares de dados; e

[49] Conselho Nacional de Saúde. Em seminário do CNS e Fiocruz, especialistas debatem relações da "proteção de dados" na Europa, EUA e Brasil. Disponível em: <http://conselho.saude.gov.br/ultimas-noticias-cns/2048-em-seminario-do-cns-e-fiocruz-especialistas-debatem-relacoes-da-protecao-de-dados-na-europa-eua-e-brasil.> Acesso em: 15 de outubro de 2022.

> IV - Que uma medida desse calibre não deve, em hipótese alguma, tramitar por meio de Medida Provisória, devendo ser precedida de amplo debate público e participação social.[50]

Não se discute a importância da atuação do Conselho Nacional de Saúde nesse sentido, porém, também é essencial que, em conjunto ao Ministério da Saúde, discutam quais as políticas públicas necessárias implementar a Lei Geral de Proteção de Dados no sistema público de saúde, com o fim de pôr essas recomendações em prática.

De fato, a melhor opção para garantir uma implementação efetiva da Lei nesse âmbito é a contratação de profissionais de compliance habilitados, que devem desenvolver um software capaz de armazenar os dados pessoais de saúde de forma segura.

O compliance a ser feito nessa seara deve se pautar nos mesmos princípios do conceito de *Privacy by Design*, elaborado por Ann Cavoukian, com a criação de uma infraestrutura de rede, sistemas de tecnologia e cultura baseados na prevenção.

Nesse sentido, ressalta-se a importância da proatividade para adotar medidas que previnam incidentes de violação de privacidade; da implementação de um padrão de proteção no sistema desde o recebimento dos dados e da incorporação da privacidade na própria arquitetura do sistema.

Além disso, é importante que os profissionais responsáveis pelo controle e tratamento de dados sejam ensinados a, além de operar o sistema virtual de forma ótima, informar aos titulares dos dados, com suficiente transparência, acerca dos componentes e do modelo de operação de tratamento de dados, bem como a respeitarem os interesses dos usuários, com a manutenção de altos padrões de privacidade.

Repassadas essas diretrizes para o governo federal, o Conselho Nacional de Saúde e o Ministério da Saúde devem entrar com um processo de licitação para contratar o melhor serviço para atuar na elaboração de um sistema tecnológico seguro o suficiente para o tratamento de dados, bem como na instrução dos profissionais responsáveis por esse tratamento – controladores e operadores de dados - a utilizarem referido sistema.

---

[50] BRASIL, Recomendação nº 002 do Conselho Nacional da Saúde, de 04 de fevereiro de 2022. Disponível em: < http://conselho.saude.gov.br/recomendacoes-cns/2322-recomendacao-n-002-de-04-de-fevereiro-de-2022>.

Sabe-se que o investimento em medidas que garantam uma segurança de dados não é uma opção. A proteção de dados pessoais, inclusive nos meios digitais é, agora, direito fundamental de todo cidadão brasileiro.

Caso as instituições públicas e privadas não se adequem às disposições da Lei Geral de Proteção de Dados e ocorra qualquer problema com o tratamento dos dados pessoais, elas estão sujeitas a multas elevadíssimas e a demais responsabilizações jurídicas.

Desse modo, no âmbito público, conforme o texto constitucional, a adequação à Lei Geral de Proteção de Dados compete à União, na medida em que ela deve organizar e fiscalizar a proteção e o tratamento de dados pessoais, ou seja, possui um papel ativo na implementação de políticas públicas nesse sentido.

Por isso, no âmbito da saúde pública, é imprescindível que o Conselho Nacional da Saúde e o Ministério da Saúde invistam em um programa geral e efetivo de compliance a ser trabalhado nas diversas instituições públicas de saúde, como em hospitais, unidades de pronto atendimento, institutos e até fundações.

CAPÍTULO 4: CONSIDERAÇÕES FINAIS

Frente à vigência da Lei Geral de Proteção de Dados, bem como das sanções administrativas decorrentes do seu descumprimento, é imprescindível que qualquer pessoa, física ou jurídica, responsável pelo tratamento de dados pessoais, garanta ao titular meios seguros para fazê-lo.

Além da lei específica, a proteção de dados agora alcançou patamar de direito fundamental por meio da Emenda Constitucional nº115/2022, que além da inclusão desse direito no artigo 5º, fixou a competência da União para organizar e fiscalizar a proteção e o tratamento de dados pessoais, bem como a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

Os diversos vazamentos de dados que ocorreram no Brasil durante os últimos anos, em especial na seara da saúde, denunciam a falta de compromisso das mais diversas instituições em implementar os ditames da lei.

Embora, até o presente, nenhuma multa vultosa tenha sido aplicada no Brasil pela ANPD, sabe-se que elas podem chegar até cinquenta milhões de reais, sem contar o risco de eliminação, bloqueio e suspensão das atividades de coleta das informações de empresas e as demais responsabilizações jurídicas.

Para evitar tais sanções e, mais importante, o desrespeito ao direito fundamental de todo cidadão de ter os seus dados pessoais protegidos, urge o investimento em programas de compliance, com o fim de que sejam criados sistemas virtuais seguros, com risco mínimo de vazamento e que apenas sejam acessados pelos responsáveis pelo tratamento dos dados.

Ainda que o compliance seja majoritariamente utilizado em empresas, o setor público também deve se utilizar desse método eficaz dentro de suas instituições.

No que tange às instituições públicas de saúde, a organização, a elaboração, o investimento, bem como a posterior fiscalização competem ao Conselho Nacional de Saúde em conjunto com o Ministério da Saúde, que representam a União na seara, em conformidade com o que prevê a Lei n° 8.142/1990, bem como com a competência disposta no artigo 21, inciso XXVI, da Constituição Federal.

Uma vez que os dados referentes à saúde são sensíveis, os sistemas tecnológicos de armazenamento de dados no setor de saúde devem seguir as regras de tratamento dispostas no artigo 11 da LGPD. Não obstante, devem também seguir os princípios elencados pelo conceito de Privacy by Design, elaborado por Ann Cavoukian, que foca na criação de uma cultura de prevenção e de um padrão de proteção no sistema desde o recebimento dos dados, de modo que a tutela deve estar embutida no "design" do sistema como proteção automática antes mesmo do tratamento.

CAPÍTULO 5: REFERÊNCIAS BIBLIOGRÁFICAS

Alemanha – Informações sobre a Regulamentação da Internet. Disponível em: <http://pensando.mj.gov.br/marcocivil/wp-content/uploads/sites/2/2015/04/23-Alemanha.pdf.>.

ALONSO, Felix Ruiz. Direito à privacidade. Porto Alegre: Síntese, 2004. p. 457

ANPD - Pesquisa aponta que maioria das empresas não conseguem se adaptar à LGPD. Escritório de Contabilidade, 2021. Disponível em: <https://www.sitecontabil.com.br/view/C1601/noticias-ler.php?id=6097&p=1&regiao=brasil>.

BALDISSERA, Olívia. O que é Privacy By Design, uma solução para se adequar à LGPD. Disponível em: < https://posdigital.pucpr.br/blog/privacy-by-design>.

BOBSIN, Arthur. Compliance: conceito, tipos, benefícios e como colocar em prática. Disponível em: < https://www.aurum.com.br/blog/compliance/>.

Brasil, Autoridade Nacional de Proteção de Dados. Planejamento Estratégico 2021-2023. Disponível em: <https://www.serpro.gov.br/lgpd/noticias/2021/anpd-agenda-regulatoria-lgpd.>

BRASIL, Recomendação nº 002 do Conselho Nacional da Saúde, de 04 de fevereiro de 2022. Disponível em: <http://conselho.saude.gov.br/recomendacoes-cns/2322-recomendacao-n-002-de-04-de-fevereiro-de-2022>.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2016]. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/ Constituiçao.htm.>.

BRASIL. Lei 8.142, de 28 de dezembro de 1990. Dispõe sobre a participação da comunidade na gestão do Sistema Único de Saúde (SUS) e sobre as transferências intergovernamentais de recursos financeiros na área da saúde e dá outras providências. Disponível: <http://www.planalto.gov.br/ccivil_03/leis/l8142.htm> .

BRASIL. Lei nº 12.846, de 1º de agosto de 2013. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm>.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>.

BRASIL. Resolução nº 466, de 12 de dezembro de 2012. Disponível em: <https://conselho.saude.gov.br/resolucoes/2012/Reso466.pdf>.

Conselho Nacional de Saúde. Apresentação. Disponível em: <https://conselho.saude.gov.br/apresentacao/apresentacao.htm#:~:text=A%20presid%C3%AAncia%20do%20%C3%B3rg%C3%A3o%20%C3%A9,o%20Plano%20Nacional%20de%20Sa%C3%BAde.> Acesso em: 11 de outubro de 2022.

Conselho Nacional de Saúde. Disponível em: <http://conselho.saude.gov.br/pratica/pratica.htm>.

Conselho Nacional de Saúde. Em seminário do CNS e Fiocruz, especialistas debatem relações da "proteção de dados" na Europa, EUA e Brasil. Disponível em: <http://conselho.saude.gov.br/ultimas-noticias-cns/2048-em-seminario-do-cns-e-fiocruz-especialistas-debatem-relacoes-da-protecao-de-dados-na-europa-eua-e-brasil.>.

Diferenças entre Privacidade, Proteção de Dados e Segurança da Informação. Rastek Soluções, 2022. Disponível em: < https://rasteksolucoes.com.br/2022/01/diferencas-entre-privacidade-protecao-de-dados-e-seguranca-da-informacao/>.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. P. 157.

Em 2021, Brasil ficou no topo de vazamento de informação no mundo, diz especialista. CNN Brasil, 2021. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/em-2021-brasil-ficou-no-topo-de-vazamento-de-informacao-no-mundo-diz-especialista/>.

Empresas não conseguem se adaptar à lei de proteção de dados, aponta pesquisa. CNN Brasil, 2021. Disponível em: < https://www.cnnbrasil.com.br/business/empresas-nao-conseguem-se-adaptar-a-lei-de-protecao-de-dados-diz-pesquisa/>.

GARRIDO GÓMEZ, María Isabel. Art. Cit., p. 82. "Liberdade de exercer um direito de controle sobre os dados pessoais de alguém, que já deixaram a esfera pessoal para se transformar em parte de um arquivo eletrônico".

JIMENE, Camilla do Vale. Capítulo VII: Da Segurança e das Boas Práticas in: LGPD: Lei Geral de Proteção de Dados Pessoais comentada / coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. 3. Ed. Ver., atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2021.

JÚNIOR. José Luiz de Moura Faleiros. O Tratamento de Dados relativos à saúde: breves reflexões. Contraditor.com, 2021. Disponível em: < https://www.contraditor.com/o-tratamento-de-dados-relativos-a-saude-breves-reflexoes/>.

Lei Anticorrupção - Programas de Integridade (Compliance). Gov.br. Disponível em: <https://www.gov.br/corregedorias/pt-br/assuntos/perguntas-frequentes/lei-anticorrupcao-programas-de-integridade-compliance#:~:text=Segundo%20a%20Lei%20Anticorrup%C3%A7%C3%A3o%2C%20consiste,de%20detectar%20e%20sanar%20desvios%2C.>

MENDES, Francisco Schertel; CARVALHO, Vinícius Marques de. Compliance: concorrência e combate à corrupção. São Paulo: Trevisan Editora, 2017, p. 31.

MENDES, Laura S. Série IDP - Linha de pesquisa acadêmica - Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental, 1ª Edição, São Paulo: Editora Saraiva, 2014. E-book. ISBN 9788502218987. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502218987/.

PINHEIRO, Patrícia Peck. LGPD e saúde: os fins justificam os meios? SerPro, 2019. Disponível em: < https://www.serpro.gov.br/lgpd/noticias/2019/paciente-no-comando-lgpd-dados-sensiveis-saude> . Acesso em 10 de outubro de 2022.

Por roubo de dados pessoais, British Airways é multada em R$ 230 milhões. LGPDbrasil.com.br, 2019. Disponível em: <https://www.lgpdbrasil.com.br/por-roubo-de-dados-british-airways-e-multada-em-us230-milhoes/#:~:text=Close-,Por%20roubo%20de%20dados%20pessoais%2C%20British%20Airways,multada%20em%20US%24230%20milh%C3%B5es&text=As%20autoridades%20brit%C3%A2nicas%2C%20muito%20por,dos%20passageiros%20no%20ano%20passado.>

Problema da LGPD é depender demais de confiança no Brasil, diz especialista. Tecnoblog, 2022. Disponível em: <https://tecnoblog.net/especiais/problema-da-lgpd-e-depender-demais-de-confianca-no-brasil-diz-especialista/>.

Promulgada emenda constitucional de proteção de dados. Agência Senado, 2022. Disponível em: <https://www12.senado.leg.br/noticias/materias/2022/02/10/promulgada-emenda-constitucional-de-protecao-de-dados>.

Proteção. *In*: Oxford Languages, Dicionário Online Oxford Languages. Disponível em: < https://languages.oup.com/google-dictionary-pt/>.

QUEIROZ, Luis. TCU: 76,7% de 382 órgãos federais não adotam a LGPD. 24% não têm sequer Política de Segurança da Informação. Capital Digital, 2022. Disponível em: < https://capitaldigital.com.br/tcu-767-de-382-orgaos-federais-nao-adota-a-lgpd-24-nao-tem-sequer-politica-de-seguranca-da-informacao/>.

SARLET, Gabrielle Bezerra Sales. Notas sobre a Proteção dos Dados Pessoais na Sociedade Informacional na Perspectiva do Atual Sistema Normativo Brasileiro in: LIMA, Cíntia Rosa Pereira D. Comentários à Lei Geral de Proteção de Dados. São Paulo: Grupo Almedina (Portugal), 2020. E-book. ISBN 9788584935796. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584935796/.

Segurança vs Proteção em Desenvolvimento de Software: Entenda as diferenças! ProMove, 2022. Disponível em: < https://promovesolucoes.com/seguranca-vs-protecao-em-desenvolvimento-de-software-diferencas/>.

Segurança. *In*: Oxford Languages, Dicionário Online Oxford Languages. Disponível em: < https://languages.oup.com/google-dictionary-pt/>.

VAINZOF, Rony. Capítulo I: Disposições preliminares in: LGPD: Lei Geral de Proteção de Dados Pessoais comentada / coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. 3. Ed. Ver., atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2021.

Vazamento de dados na saúde coloca pacientes na mira de golpes. Medicina S/A, 2022. Disponível em: <https://medicinasa.com.br/vazamento-dados saude/#:~:text=Vazamento%20de%20dados%20na%20sa%C3%BAde%20coloca%20pacientes%20na%20mira%20de%20golpes,Seguran%C3%A7a%20Digital&text=A%20privacidade%20e%20a%20seguran%C3%A7a,de%20pacientes%2C%20cl%C3%ADnicas%20e%20profissionais.>.