Coordenação:
Eduardo Monguilhott Dalmarco
Izabel Galhardo Demarchi
Miliane Fantonelli
Raul Wazlawick

1ª Mostra Científica de Proteção de Dados na Saúde, Tecnologia e Poder Público

E-book dos melhores trabalhos da Mostra

Organização:
Laboratório Bridge

UFSC

1ª Mostra Científica de Proteção de Dados na Saúde, Tecnologia e Poder Público

E-book dos melhores trabalhos da Mostra

Laboratório Bridge
Organização

Eduardo Monguilhott Dalmarco
Izabel Galhardo Demarchi
Miliane Fantonelli
Raul Wazlawick
Coordenação

1ª Mostra Científica de Proteção de Dados na Saúde, Técnologia e Poder Público:

E-book dos melhores trabalhos da Mostra

Florianópolis
UFSC
2022

Comissão organizadora

Coordenação Geral:
Eduardo Monguilhott Dalmarco - Professor UFSC
Izabel Galhardo Demarchi - Professora UFSC
Miliane Fantonelli - Colaboradora do Laboratório Bridge
Raul Wazlawick - Professor UFSC

Comitê Organizador:
Célio Cunha - Colaborador do Laboratório Bridge
Jades Hammes - Colaborador do Laboratório Bridge
Daniel Scandolara - Doutorando UFSC
Ianka Cristina Celuppi - Doutoranda UFSC
Ranieri Alves dos Santos - Doutorando UFSC
Wagner L. Zanotto - Graduando UFSC

Capa:
Ana Júlia Lichtblau Bernardini

Realização:
Laboratório Bridge

Catalogação na fonte pela Biblioteca Universitária
da Universidade Federal de Santa Catarina

P953 1ª Mostra Científica de Proteção de Dados na Saúde, Tecnologia e Poder Público [recurso eletrônico] : e-book dos melhores trabalhos da mostra / organização, Laboratório Bridge ; coordenação, Eduardo Monguilhott Dalmarco ... [et al.]. – Florianópolis : UFSC, 2022.
38 p. : tab.

E-book (PDF)
Disponível em: https://doi.org/10.5007/978-85-8328-120-7
ISBN 978-85-8328-120-7

1. Proteção de dados. 2. Lei geral de proteção de dados pessoais (LGPD). 3. Saúde. 4. Tecnologia. 5. Poder público. I. Laboratório Brigde da Universidade Federal de Santa Catarina. II. Dalmarco, Eduardo Monguilhott.

CDU: 681.31.004.4

Elaborada pela bibliotecária Dênira Remedi – CRB-14/1396

Prefácio

O Laboratório Bridge – UFSC promoveu em agosto de 2022 a 1ª Mostra Científica de Proteção de Dados na Saúde, Tecnologia e Poder Público. O escopo da Mostra era viabilizar, dentro do espaço acadêmico e de forma gratuita, a discussão da privacidade e da proteção dos dados, nas respectivas áreas. Para isso, foi aberto edital de submissão de resumos expandidos sobre os assuntos, sendo que os melhores trabalhos seriam convidados a apresentar oralmente e publicar no e-book do evento.

Sob esse pano de fundo, o presente e-book é ator essencial que encerra a 1ª Mostra. Nele encontramos duas seções: uma de apresentação de cada área do evento - LGPD e Saúde, LGPD e Tecnologia e LGPD no Setor Público – escrita pelos próprios organizadores da Mostra; e outra seção com a seleção dos melhores trabalhos apresentados, sendo dois artigos de cada assunto.

Com este pequeno apanhado gostaríamos de frisar nossa satisfação, primeiro com os trabalhos selecionados, que contemplaram de Norte a Sul do Brasil e segundo em viabilizar um espaço democrático de diálogo sobre um assunto o qual ainda carece de mais estudos e pesquisas no território brasileiro, que é a proteção dos dados.

Apresentação

A privacidade e a proteção dos dados são assuntos que nos tocam diariamente, já que no mundo contemporâneo nós somos nossos dados e eles nos representam nos diversos meios, desde as redes sociais até os prontuários médicos, por exemplo. Nome, idade, CPF, condições de saúde, familiares, endereço são algumas das categorias que, em conjunto, perfazem cada um de nós.

Nesse sentido, em terras brasileiras, mesmo que já contássemos com a garantia constitucional à privacidade, ainda não contávamos com lei específica sobre como garantir tal privacidade. Assim, em 2018 a Lei Geral de Proteção de Dados (LGPD) foi promulgada. No entanto, apenas em 2020 que ela entrou em vigor, sendo que as sanções legais previstas, em caso de descumprimento, só passaram a vigorar em agosto de 2021. E, em 2022, a emenda constitucional 115 trouxe a proteção dos dados para o rol dos direitos e garantias fundamentais para a Carta Magna, no seu artigo 5º.

Tudo isso para dizer que é um assunto novo aqui, a despeito de outros países com tradições mais longevas sobre o assunto, como os países integrantes da União Europeia. Mas, fato é que o Brasil vem caminhando, mesmo que só agora no século XXI, para a garantia da privacidade, a partir especificamente da proteção dos dados. Não temos tanto material acadêmico sobre o assunto, tão pouco muitas experiências práticas de implementação da lei.

Contudo, o Laboratório Bridge - UFSC por entender que é um assunto essencial a ser estudado, discutido e implementado vem promovendo espaços para que seja possível a troca de conhecimentos, naquilo que chamamos na nossa cultura de #Compartilhar dá +XP.

Esse e-book traz experiências e estudos de diferentes regiões do país, demonstrando a diversidade e a complexidade do tema e a necessidade, portanto, de termos cada vez mais pesquisas sobre proteção dos dados. Acreditamos que assim será possível tratar do assunto com responsabilidade, implementar soluções viáveis seja na e pela tecnologia em variados setores, como a saúde e o Poder Público, temas explorados pela Mostra.

SUMÁRIO

PARTE I - SEÇÃO ESPECIAL DOS ORGANIZADORES DO EVENTO

POLÍTICAS DE *COOKIES* EM CONFORMIDADE COM A LGPD 9
Ranieri Alves dos Santos
Jades Fernando Hammes

PROTEÇÃO DE DADOS NO SETOR PÚBLICO 12
Miliane dos Santos Fantonelli
Wagner Luiz Zanotto

DESAFIOS TECNOLÓGICOS E ESTRATÉGIAS PARA O MANEJO SEGURO DOS DADOS EM SAÚDE NO SISTEMA ÚNICO DE SAÚDE 15
Fabiana Magarrote Fernandes de Melo
Ianka Cristina Celuppi
Eduardo Monguillhot Dalmarco
Célio Cunha

PARTE II - SEÇÃO DOS MELHORES TRABALHOS DA MOSTRA

A INCOMPATIBILIDADE DO USO DAS *DARK PATTERNS* NAS PLATAFORMAS DE MÍDIA SOCIAL COM A LEI GERAL DE PROTEÇÃO DE DADOS 19
Cecilia Araújo Santos Oliveira Veloso
Rodrigo Toledo Costa de Almeida

A LGPD E INTERNET DAS COISAS: A IMPORTÂNCIA DO PRINCÍPIO DA TRANSPARÊNCIA FRENTE ÀS NOVAS TECNOLOGIAS 22
Kethelen Severo Bacchi

A APLICAÇÃO DA LGPD NOS CARTÓRIOS EXTRAJUDICIAIS: UMA ANÁLISE ACERCA DA EXPEDIÇÃO DE CERTIDÕES EM REGISTRO DE IMÓVEIS DA BAHIA 25
Manuela de Oliveira Souza Brito

A LEI DE PROTEÇÃO DE DADOS PESSOAIS E A IMPLANTAÇÃO BRASILEIRA DA SAÚDE DIGITAL 28
Ruy Roberto Porto Ascenso Rosa

VAZAMENTO DE DADOS DO PRONTUÁRIO ELETRÔNICO DO CIDADÃO EM UM MUNICÍPIO DO CEARÁ – RELATO DE EXPERIÊNCIA 31
Manoel Lourenço da Silva

PERFIL DE UM ENCARREGADO DE TRATAMENTO DE DADOS EM SAÚDE NO SISTEMA ÚNICO DE SAÚDE DO BRASIL 34
Laíse Figueiredo Rolo de Oliveira
Lara Liz Freire
Vanessa Lora
Blanda Helena de Mello
Elen Ferreira Ramos de Azevedo
Thais Lucena de Oliveira

Seção especial dos organizadores do evento

COMPARTILHAR DA +XP

POLÍTICAS DE *COOKIES* EM CONFORMIDADE COM A LGPD

Ranieri Alves dos Santos[1]
Jades Fernando Hammes[2]

Introdução

Os *cookies* são como conjuntos de dados organizados em arquivos de texto baseados no endereço da aplicação de internet visitada. Estes dados são armazenados temporariamente no dispositivo do usuário, podendo ser excluídos ou expirar em até dois anos. A estrutura tecnológica dos *cookies* permite que estes sejam utilizados pela própria aplicação que os capturou livremente, inclusive disponibilizando estes dados para outras aplicações. Os *cookies* são comumente classificados como primários (*first-party data*), secundários (*second-party data*) e terciários (*third-party data*) (CAHN et al, 2016; DE LIMA, 2020).

Acerca dos *cookies* primários, estes são os dados armazenados no dispositivo do usuário, obtidos a partir dos cliques e interações do usuário com as aplicações. Estes *cookies* auxiliam na experiência do usuário nas aplicações, facilitando a personalização de preferências, como idiomas, senhas, recomendação de conteúdos, entre outras facilidades. Estes *cookies* primários são obtidos na própria aplicação e são utilizados para aprimorar o uso naquela aplicação. Já os *cookies* secundários são obtidos a partir de integrações entre aplicações, onde os dados obtidos como *cookies* primários de uma aplicação são disponibilizados para que uma outra aplicação os utilize. Por fim, os *cookies* terciários são os dados disponibilizados por provedores especializados no compartilhamento de informações de terceiros. Os *cookies* secundários e terciários são os originadores de estratégias e campanhas que podem não ter como foco o aprimoramento da experiência do usuário, trazendo riscos de segurança e possibilidades de rastreio mais avançadas (DE LIMA, 2020; CAVALCANTI, 2021).

Com a sanção da lei n.º 13.709, a Lei Geral de Proteção de Dados Pessoais (LGPD), as aplicações que utilizam dados no Brasil precisam se adequar quanto à transparência no armazenamento, privacidade e intenção ao capturar estes dados (BRASIL, 2018). A LGPD não é uma iniciativa isolada que visa garantir a experiência positiva do usuário, limitando excessos e aplicações maliciosas, o GDPR (*General Data Protection Regulation*), que é Regulamento Geral sobre Proteção de Dados na Europa, já tratava do consentimento do usuário quanto ao uso de *cookies*. A Apple, desde a versão do seu sistema operacional móvel iOS 14.5 já limita a coleta de dados, facilitando que o usuário bloqueie qualquer uso de *cookies* indesejados. Neste sentido, a partir de 2023 o Google já anunciou que em seus navegadores não serão mais aceitos os *cookies* terciários.

[1] Laboratório Bridge. e-mail: ranieri.santos@bridge.ufsc.br
[2] Laboratório Bridge. e-mail: jades@bridge.ufsc.br

Problema

Diante da necessidade de adequação dos produtos Web à LGPD, como utilizar coleta de dados e armazenamento em *cookies* de uma forma que atenda a legislação?

Objetivos

Revisar e listar as políticas que as aplicações Web devem adotar ao implementar a captura de *cookies* a partir das ações do usuário, bem como o seu futuro armazenamento no dispositivo.

Metodologia

O trabalho é baseado em uma revisão de literatura com foco na exploração de publicações na língua portuguesa que demonstrem suas interpretações acerca do uso de *cookies* segundo a LGPD. O trabalho teve foco qualitativo e não limitou os estudos apenas aos artigos científicos.

Resultados

A revisão culminou em uma série de publicações, entre artigos científicos, monografias, artigos de blogs e portais, resumos e textos de opinião. A seguir são apresentadas as formas com que estão sendo publicados os modos de se criar estratégias para o atendimento da LGPD no âmbito do uso de *cookies* em aplicações Web.

Na LGPD é necessário que os dados pessoais capturados tenham o livre consentimento do usuário (BRASIL, 2018). Neste sentido, os *cookies*, como podem conter dados relacionados com o comportamento, horários, detalhes do dispositivo, informações geográficas, entre outros, é necessário que o usuário concorde com esta captura. Porém, este consentimento deve ser detalhado. Antes de um momento de coleta de dados, o usuário precisa aceitar esta captura. Mesmo dados simples e indispensáveis para o uso da aplicação, é necessária a ciência do usuário deste uso, bem como o seu consentimento. Desta forma, não basta um simples aceite de que existem *cookies* sendo armazenados a partir da aplicação, é necessário o detalhamento de todos os dados que estão sendo capturados a partir daquela ação (PEREIRA, 2021; RAMOS, 2019).

Outro parâmetro que deve ser satisfeito para o atendimento da LGPD é que a finalidade do armazenamento daqueles dados deve ser informada. Sendo assim, a aplicação deve exibir previamente, de forma clara, qual é a finalidade do armazenamento daquele dado, impossibilitando o seu uso para outras operações que não sejam as explicitadas como finalidade do aceite. Desta forma, não haveria a possibilidade de tratamentos posteriores e o uso para outros fins dentro da aplicação atual, ou de terceiros (PEREIRA, 2021).

Acerca do uso de *cookies* secundários e terciários, é necessário que a aplicação disponibilize em sua política de privacidade o detalhamento de como os seus dados já capturados com o seu consentimento poderão ser compartilhados com outras aplicações através de parcerias comerciais e que o usuário seja capaz de novamente escolher quais dados gostaria de compartilhar para esta finalidade. Por fim, a política de privacidade deve conter informações sobre a privacidade, finalidade, duração e formas de entrar em contato com o responsável pela privacidade dos dados da aplicação (RIBEIRO, 2021; PEREIRA, 2021).

Conclusão

Como o objetivo do trabalho era buscar por interpretações sobre como o uso dos *cookies* à luz

ISBN 978-85-8328-120-7

da LGPD e listá-las, foi possível observar que diversos autores possuem visões semelhantes quanto ao tema. Porém, de acordo com a visão dos autores, fica evidente que diversas aplicações Web que operam no Brasil não estão completamente adequadas à LGPD. Poucas aplicações têm listado corretamente os dados capturados que serão armazenados em *cookies* e a finalidade deste armazenamento raramente fica explícita.

Para prosseguir com os estudos neste tema a partir deste trabalho, sugere-se que sejam analisadas aplicações Web gratuitas e utilizando ferramentas de análise de *cookies*, verificar se todos os dados ali listados foram realmente exibidos para o usuário, bem como se a sua finalidade também foi expressa.

Referências

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Institui a Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**: seção 1, Brasília, DF, p. 59, 15 ago. 2018.

BONNA, Alexandre Pereira; DE MOURA CAÑIZO, Amanda; CALZAVARA, Giovana Ferreira. CONSENTIMENTO E LGPD: DESAFIOS DIANTE DA HIPERVULNERABILIDADE DO CONSUMIDOR. **Revista de Direito e Atualidades**, v. 2, n. 3, 2021.

CAHN, Aaron et al. An empirical study of web cookies. **Proceedings of the 25th international conference on world wide web**. 2016. p. 891-901.

CAVALCANTI, Mario Felipe. COOKIES PARA QUEM? ENTRE O ESCAMBO DIGITAL E OS DIREITOS À PRIVACIDADE E PROTEÇÃO DE DADOS. **Revista Acadêmica da Faculdade de Direito do Recife** - ISSN: 2448-2307, v.93, n.2, p.96-1, 15 out. 2021.

DE LIMA, Ana Paula Moraes Canto; Aspectos gerais sobre a Lei Geral de Proteção de Dados que as empresas precisam saber. In; ALMEIDA, Dionice de; LIMA, Ana Paula Moraes Canto de; MAROSO, Eduardo Pereira. **LGPD**: Lei Geral de Proteção de Dados: sua empresa está pronta? São Paulo: Literare Books, 2020.

PEREIRA, Gustavo Nojosa. **O Direito Fundamental à Privacidade nos Meios Digitais**: Os Limites ao Comércio de Dados Pessoais por meio dos Cookies e a Impraticabilidade da Autodeterminação Informativa. 2021. Monografia (Bacharel em Direito) - Universidade Federal Fluminense, Volta Redonda, 2021.

RAMOS, Pedro Henrique Soares Melo. **A REGULAÇÃO DE PROTEÇÃO DE DADOS E SEU IMPACTO PARA A PUBLICIDADE ONLINE**: UM GUIA PARA A LGPD. 2019. Disponível em: https://baptistaluz.com.br/wp-content/uploads/2019/07/MP_guia_LGPD.pdf. Acesso em: 11 ago. 2022.

RIBEIRO, Paula Belleti. **A Proteção de Dados no Brasil**: Um Estudo Acerca da Legalidade dos Cookies da Publicidade Comportamental na Internet à Luz da Lei Geral de Proteção de Dados Pessoais (LGPD). 2021. Monografia (Bacharel em Direito) - Universidade do Sul de Santa Catarina, Palhoça, 2021.

Palavras-chave: LGPD; *cookies*; GDPR; consentimento; transparência.

PROTEÇÃO DE DADOS NO SETOR PÚBLICO

Miliane dos Santos Fantonelli[1]
Wagner Luiz Zanotto[2]

Introdução

No âmbito do que se convencionou chamar de Sociedade da Informação onde o fluxo de informações é elemento estruturante (BIONI, 2019), a proteção de dados alcançou uma dimensão sem precedentes a partir da introdução do uso da tecnologia da informática e da ampla digitalização que já assumiu um caráter onipresente e afeta todas as esferas da vida social, econômica e cultural contemporânea (SARLET, 2021a).

A crescente digitalização da sociedade e da economia vem acompanhada da transformação digital do próprio Estado que, com cada vez mais intensidade, tem adotado novas tecnologias para prestar serviços e para formular, monitorar e implementar políticas públicas nas mais diversas áreas. Na essência das atividades do Poder Público está o tratamento de dados pessoais pelo Estado, o que constitui condição indispensável para o cumprimento de sua missão (WIMMER, 2021).

O tratamento de dados pelo Setor Público produz uma complexidade que lhe é própria. Ainda que a racionalidade que move o Setor Público no tratamento de dados possa guardar semelhanças com aquela que move o setor privado, notadamente no que se refere à busca por maior eficiência e por alocação otimizada de recursos, as bases que garantem a legitimidade ao tratamento de dados pessoais pelos setores Público e Privado são inteiramente distintas. Na esfera pública o tratamento de dados pessoais não se inicia, em geral, a partir de uma decisão voluntária do titular, mas como decorrência das exigências do próprio pacto social, onde conhecer os seus cidadãos é pré-requisito para o desempenho das finalidades públicas do Estado (WIMMER, 2019).

Este cenário aponta para as tensões presentes na relação entre cidadão e Poder Público e que justificaram as primeiras regulamentações sobre a proteção de dados pessoais enquanto direito fundamental autônomo. Conforme a jurisprudência alemã, que orientou em grande medida tal movimento regulatório, o direito à autodeterminação informacional consiste, em suma, na prerrogativa de cada indivíduo decidir sobre a divulgação e utilização de seus dados pessoais. Não obstante, este direito não assegura a cada cidadão um controle absoluto sobre seus dados, dada a inserção e a responsabilidade comunitária e social do ser humano que o obriga a tolerar eventuais limitações ao seu direito particular quando em prol do interesse geral (SARLET, 2021b).

Com essas tensões de fundo, a complexidade do tratamento de dados na esfera Pública também reflete os múltiplos desafios da prestação de serviços à população, no cumprimento do papel constitucional do Estado. O Brasil é um país de dimensões continentais em que a Administração Pública

[1] Laboratório Bridge. e-mail: miliane@bridge.ufsc.br
[2] Graduando em Direito da Universidade Federal de Santa Catarina. e-mail: wzanotto@gmail.com

ISBN 978-85-8328-120-7

atua nas mais diversas frentes, a exemplo da educação, saúde, segurança pública e etc. Também é preciso analisar o enorme volume de dados pessoais necessários à promoção de políticas públicas e cumprimento das leis, de forma geral. Se a exigência de garantia do direito à confiabilidade e integridade dos sistemas técnico-informacionais já se faz presente em relação a qualquer conjunto de dados pessoais e está intimamente ligada ao dano em potencial que o seu uso indevido possa causar, muito mais alargada se encontra tal exigência na esfera pública também em razão do volume de informações processadas.

Neste sentido, a implementação de projetos de adequação à Lei Geral de Proteção de dados nos entes administrativos, visando efetivação dos princípios estabelecidos no art. 6º da referida lei e observância das regras por ela trazidas, requer uma análise de caso-a-caso que identifique as necessidades de utilização de dados por cada organização. Ademais, dada a descentralização da administração como estratégia adotada na gestão da coisa pública, que requer um diagnóstico apropriado sobre as particularidades da população em seu âmbito regional, se faz preciso também um movimento de verticalização da proteção de dados que faça com que o cuidado sobre as informações pessoais utilizadas pelos entes administrativos chegue a todas as regiões do país.

A promoção de uma mudança cultural sensível às exigências da privacidade e da proteção de dados encontra na conscientização um dos seus principais instrumentos, como vem apontando a literatura especializada na temática da adequação à LGPD. No Setor Público a mudança cultural, a partir da conscientização, que possui em certa medida um caráter generalista aplicável a todas as frentes de atuação do Poder Público, pode ser apontada como um elemento central para possibilitar a verticalização dos cuidados inerentes à proteção de dados. Neste sentido tem se destacado a atuação de órgãos como a Autoridade Nacional de Proteção de Dados (ANPD) e da Secretaria de Governo Digital (SGD).

A ANPD, como estipulado pela própria LGPD, possui competências normativas, fiscalizadoras e sancionadoras, além de cumprir um importante papel de interpretar a legislação de proteção de dados pessoais de forma definitiva na esfera do poder executivo. A partir de uma atuação colaborativa com outros órgãos do Setor Público e mesmo com entidades do Setor Privado tem atendido à sua vocação e buscado com essa articulação proporcionar a promoção de uma cultura de proteção de dados pessoais. Exemplo disso são as publicações editadas pela a ANPD, que contemplam temas relevantes como a definição dos agentes de tratamento ou ainda o tratamento de dados pelo Poder Público, que visam orientar aqueles que utilizam dados pessoais sobre o tema da proteção de dados.

No mesmo sentido, porém a partir de uma perspectiva mais pragmática tem atuado a Secretaria de Governo Digital pelo seu Departamento de Privacidade e Segurança da Informação que desde 2020 vem editando Guias Orientativos sobre boas práticas relacionadas à proteção de dados, além de outros guias que visam orientar e facilitar a implementação de medidas de adequação no Setor Público.

Problema

No processo de verticalização dos cuidados necessários à proteção de dados, através de quais mecanismos tem se dado a promoção da cultura de proteção de dados dentro do Setor Público?

Objetivos

A presente pesquisa é composta pelos seguintes objetivos: i) demonstrar a necessidade de tratamento de dados pelo Setor Público; ii) identificar as tensões de fundo da relação entre direitos dos titulares e prerrogativas do Estado no tratamento de dados pessoais; iii) indicar a relação entre os desafios da prestação de serviços públicos e a complexidade do tratamento de dados pelo Poder Público; iv) aponta a mudança cultural como elemento central que visa proporcionar a verticalização

do cuidado relativo à proteção de dados; v) identificar as ações do Setor Público centrais à promoção da mudança cultural.

Metodologia

O presente estudo é uma revisão de literatura, de caráter descritivo-discursivo, que tem como objetivo a construção de uma contextualização para o problema e a análise das possibilidades presentes na literatura consultada para a concepção do referencial teórico da pesquisa (ALVES-MAZZOTTI, 2002).

Conclusão

Frente aos desafios colocados pelo que se convencionou chamar de Sociedade da Informação, são atribuídas ao Poder Público maiores prerrogativas no que toca ao tratamento de dados pessoais, visando a efetivação de interesses de caráter geral. Dentre inúmeras questões, o tratamento de dados pessoais apresenta uma complexidade que lhe é própria também pela multiplicidade de frentes em que atua, o que acarreta em dificuldades em se traçar estratégias que abordem todo o setor. A mudança cultural, impulsionada por ações de conscientização, no entanto, apresenta esse caráter generalista e tem sido promovida por órgãos como a Autoridade Nacional de Proteção de Dados e a Secretaria de Governo Digital através de suas publicações.

Referências

BIONI, Bruno R. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019

SARLET, I. W.. Prefácio da coletânea **Lei Geral de Proteção de Dados e o Poder Público**. Porto Alegre, 2021

SARLET, I. W.. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: Laura S Mendes; Danilo Doneda; Ingo W Sarlet; Otavio Luiz Rodrigues Jr. (Org.). **Tratado de Proteção de Dados Pessoais**. 1ed.Rio de Janeiro: Forense, 2021, v. 1, p. 1-.

WIMMER, Miriam . Proteção de Dados Pessoais no Setor Público: incidência, bases legais e especificidades. **REVISTA DO ADVOGADO** , v. 144, p. 126-133, 2019.

WIMMER, Miriam. Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público.. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luis.. (Org.). **Tratado de Proteção de Dados Pessoais**. 1ed.Rio de Janeiro: Forense, 2021, v. 1, p. 271-288

Palavras-chave: proteção de dados; direitos fundamentais; Administração Pública; adequação; conscientização.

ISBN 978-85-8328-120-7

DESAFIOS TECNOLÓGICOS E ESTRATÉGIAS PARA O MANEJO SEGURO DOS DADOS EM SAÚDE NO SISTEMA ÚNICO DE SAÚDE

Fabiana Magarrote Fernandes de Melo[1]
Ianka Cristina Celuppi[2]
Eduardo Monguillhot Dalmarco[3]
Célio Cunha[4]

Introdução

A Lei Geral de Proteção de Dados (LGPD) brasileira entrou em vigor no ano de 2020, e com isso os serviços de saúde, sejam eles públicos ou privados, precisaram articular estratégias de adequação aos pressupostos legais instituídos. Os registros clínicos do prontuário do paciente são considerados dados sensíveis, portanto, seu tratamento requer o desenvolvimento de propostas de processos e tecnologias com foco no consentimento e segurança do paciente. Este cenário evidencia um processo de adequação e implementação de estratégias de *compliance* que se tornam ainda mais complexas à medida em que ocorrem avanços nos recursos tecnológicos.

Tal desafio se demonstra ainda mais complexo se analisarmos a estrutura de gestão e governança do Sistema Único de Saúde (SUS), pautado no federalismo tripartite brasileiro, que envolve a cooperação entre diferentes entes governamentais e sua relação com o setor privado de saúde. Tais elementos ressaltam a pertinência da reflexão proposta neste estudo.

Problema

Quais são os principais desafios tecnológicos e as estratégias recomendadas para a implementação de soluções para à conformidade com a LGPD no SUS?

Objetivos

Refletir sobre os desafios tecnológicos e estratégias do manejo seguro dos dados no SUS em conformidade com a LGPD.

Metodologia

Trata-se de um ensaio, fundamentado a partir de uma revisão integrativa da literatura juntamente as percepções dos autores.

[1] Laboratório Bridge, e-mail: fabiana@bridge.ufsc.br
[2] Laboratório Bridge, e-mail: ianka@bridge.ufsc.br
[3] Laboratório Bridge, e-mail: dalmarco@bridge.ufsc.br
[4] Laboratório Bridge, e-mail: celio@bridge.ufsc.br

Resultados

Os desafios da implementação da LGPD em cenários onde a informatização dos serviços de saúde e o uso de diferentes tecnologias já estão consolidados, são diferentes das vivenciadas em serviços onde o processo de trabalho em saúde ainda ocorre no papel. Com o acontecimento de algumas invasões de bases de dados por hackers, cresceu ainda mais a preocupação com o desenvolvimento de ambientes controlados e seguros para o tratamento dos dados dos pacientes. Portanto, é de extrema importância a implementação de prontuários eletrônicos que declarem conformidade com as mais atualizadas normas de segurança (BOTELHO; CAMARGO, 2021). Tal fato se caracteriza um desafio a ser enfrentado se consideramos a heterogeneidade dos sistemas de informação no Brasil (DE ARAGÃO; SCHIOCCHET, 2020). Nesta lógica, a Rede Nacional de Dados em Saúde (RNDS) se apresenta como uma proposta de solução para a interoperabilidade e o compartilhamento dos dados de saúde no SUS (FANTONELLI et al., 2021).

Também, percebeu-se a extrema importância da definição dos fluxos de informação entre os diferentes entes governamentais, que são união, estados e municípios, no tratamento dos dados dos sistemas de informação em saúde compartilhados entre eles (DE ARAGÃO; SCHIOCCHET, 2020). Esse "passo" pode se configurar um desafio ainda maior se analisarmos a interação e a troca de informações entre os serviços públicos e privados de saúde, como clínicas laboratoriais e diagnósticas, serviços hospitalares, prestadores de serviços, especialistas, ambulatórios, dentre outros.

Ainda, vislumbra-se que a LGPD terá um grande impacto nas bases de *big data*, visto que a obtenção de informações pessoais por meio do tratamento de dados poderão gerar danos aos pacientes, ferindo seus direitos à privacidade, liberdade e autonomia, além da coleta de dados de dispositivos periféricos, na modalidade *Internet of Things* (IoT) (LEME et al., 2020). Nessa perspectiva, a anonimização dos dados, que consiste no tratamento dos dados para a eliminação da associação direta ou indireta à uma pessoa, figura-se como essencial para o uso dos dados com finalidade de pesquisa e fomento/avaliação de políticas publicas (BOTELHO; CAMARGO, 2021). Por isso, recomenda-se que os novos sistemas deverão ser desenvolvidos baseados nos conceitos de *privacy by design* e *privacy by default* (LEME et al., 2020).

É notório observar as iniciativas relacionadas às diferentes formas de teleatendimentos na saúde que foram instauradas como proposta de enfrentamento à pandemia de Covid-19. Estas novas tecnologias expõem os pacientes a riscos maiores do que os usuais, na medida em que os sistemas não estão preparados, em termos de segurança, para o aumento súbito de tráfego de informações e usuários (JUNIOR; CAVET; NOGAROLI, 2020). Além disso, as teleconsultas configuram-se inovações para a prática dos serviços de saúde, mas, por terem sido implementadas sem haver uma preocupação com o uso de softwares adequados à esta finalidade (ao exemplo do uso do Whatsapp para realização de teleconsultas), necessitam de avaliação e consequentes melhorias em seus processos tecnológicos para à conformidade com a LGPD (LEME et al., 2020). Da mesma forma, evidencia-se os desafios da coleta e manejo dos dados em chatbots ou sistemas que realizam triagem virtual automatizada, e compõem sistemas de *business intelligence* e de inteligência artificial.

Além disso, existem desafios relacionados ao processo de trabalho de quem registra e tem acesso aos dados sensíveis dos pacientes. Com isso, estima-se que a adoção de medidas de segurança técnicas e administrativas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de tratamento inadequado dos dados (LEME et al., 2020), figura-se como essencial para a construção de uma cultura de segurança dos dados nas organizações de saúde.

Considerando todos estes desafios, destaca-se a necessidade de implementação de processos interdisciplinares de colaboração para a elaboração de planos de governança da informação, pautados

ISBN 978-85-8328-120-7

na transparência, gestão de riscos, adaptabilidade, discrição e mensuração das operações de tratamento de dados, práticas de governança, monitoramento, aplicação de boas práticas e elaboração de políticas e procedimentos operacionais padrão (LEME et al., 2020).

Conclusão

O setor saúde vive uma revolução em curso com a crescente e acelerada introdução de tecnologias nos processos de trabalho em saúde. Com isso, destaca-se a importância em considerar todos os desafios identificados e incorporá-los, na medida do possível, aos planos de governança e adequação à LGPD nos diversos serviços de saúde.

Referências

DE ARAGÃO, Suéllyn Mattos; SCHIOCCHET, Taysa. Lei Geral de Proteção de Dados: desafio do Sistema Único de Saúde. **Revista Eletrônica de Comunicação, Informação e Inovação em Saúde**, v. 14, n. 3, 2020.

BOTELHO, Marcos César; DO AMARAL CAMARGO, Elimei Paleari. A aplicação da lei geral de proteção de dados na saúde. **Revista de Direito Sanitário**, v. 21, p. e0021-e0021, 2021.

FANTONELLI, Miliane et al. Lei geral de proteção de dados e a interoperabilidade na saúde pública. **Journal of Health Informatics,** v. 12, 2021.

JUNIOR, José Luiz de Moura Faleiros. Telemedicina e Proteção de Dados: reflexões sobre a pandemia da covid-19 e os impactos jurídicos da tecnologia aplicada à saúde. **Revista dos Tribunais**. vol, v. 1016, 2020.

LEME, Renata Salgado et al. Lei Geral de Proteção de Dados e segurança da informação na área da saúde. **Cadernos Ibero-Americanos de Direito Sanitário**, v. 9, n. 3, p. 210-224, 2020.

Palavras-chave:
Lei Geral de Proteção dos Dados; Sistema Único de Saúde; Tecnologia; Governança.

Seção dos melhores trabalhos da Mostra

EXPLORAR NOVOS MUNDOS

A INCOMPATIBILIDADE DO USO DAS *DARK PATTERNS* NAS PLATAFORMAS DE MÍDIA SOCIAL COM A LEI GERAL DE PROTEÇÃO DE DADOS

Cecilia Araújo Santos Oliveira Veloso[1]
Rodrigo Toledo Costa de Almeida[2]

Introdução

A Em um cenário informacional, com constantes evoluções tecnológicas e a utilização da internet para conexões e transações cada vez mais necessárias, há também uma massiva produção de dados no meio digital. Dessa forma, os dados pessoais transformam-se em um amplo nicho de comercialização, que por vezes, extrapola limites fundamentais.

Dentro deste contexto virtual, as plataformas de mídias sociais elaboram estratégias que possam agregar ao usuário uma experiência positiva, tornando o serviço relevante para o seu público alvo, e assim, maximizando sua conversão em aquisições e fidelização. Nesse sentido, são utilizados recursos visuais e de *user interface* para promover um ambiente de fácil acesso, navegação e confiabilidade para o seu público. Entretanto, os direcionamentos empregados, por vezes, podem estar em conflito com a própria *user experience* fornecida.

As *dark patterns,* ou padrões obscuros, são interfaces implementadas nas plataformas de mídia social que influenciam o comportamento dos usuários na internet, levando-os a tomar ações não intencionais, com potencial de prejudicar seus dados pessoais (EDPB, 2020). Para tanto, a partir das diretrizes de experiências do usuário dentro das plataformas digitais, e com isso, há utilização de *design* e táticas experimentais para induzir que o usuário haja de acordo com os interesse das plataformas, sem que ele perceba ou possa evitar, maximizando a coleta de dados de forma menos transparente, a fim de atingir seus objetivos comerciais (BRIGNUL, 2010).

Tal prática ocorre, por exemplo, nas barras de *cookies*, quando há um maior destaque para a opção de aceitá-las, ao invés de apresentar a opção de personalizar ou rejeitá-los. Isso pode ocorrer a partir da utilização de elementos visuais, como cores, formas e fontes, que direcionam a escolha do usuário conforme os interesses da plataforma.

Nesse panorama, a Lei Geral de Proteção de Dados (Lei 13.709/18), responsável por regular, no Brasil, o tratamento de dados pessoais, define, em seu art. 5º, XII, o consentimento como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". Além disso, estabelece no art. 6º, VI, que a transparência consiste na "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial."

Assim, para considerar um consentimento livre, o titular de dados deve gozar de uma escolha

[1] Universidade Federal da Bahia. e-mail: velosoxz@gmail.com.
[2] Universidade Federal da Bahia. e-mail:toledorodrigo016@gmail.com.

real, significativa e genuinamente independente, sendo necessário garantir a ele um alto grau de autonomia para tomar a decisão de consentir. No que diz respeito ao consentimento informado, este ocorre quando o titular dos dados recebe, previamente ao ato de consentir, informações o suficiente que lhe permitam compreender como se dá, qual a finalidade do tratamento das informações fornecidas e quais as consequências do seu aceite, para então tomar a sua decisão.

Nesse contexto, utilização desse tipo de direcionamento intencional mácula não só o processo de obtenção de consentimento do titular, impedindo que ele seja informado, livre e manifesto, como também o princípio da transparência, tornando o tratamento de dados ilícito e, consequentemente, inválido (GOMES, 2022).

Desse modo, nota-se a importância de discutir a utilização das *dark patterns* nas plataformas de mídia social e sua incompatibilidade com a Lei Geral de Proteção de Dados diante da manipulação do consentimento dos titulares e a falta de transparência na captação desnecessária das informações dos usuários para fins comerciais.

Problema

Tendo em vista que algumas empresas, enquanto controladoras de dados, vêm escolhendo adotar métodos de experiências do usuário que produzem direcionamentos obscuros ou enganosos, não permitindo ao titular o controle sobre o fluxo informacional, e ainda, levando em consideração a excessiva utilização de recursos tecnológicos na construção das plataformas de mídia social, a presente pesquisa tem o intuito de responder o seguinte questionamento: existe compatibilidade entre o uso de *dark patterns* e os pressupostos previstos na Lei Geral de Proteção de Dados Pessoais no Brasil?

Objetivos

Nesse sentido, torna-se crucial analisar o uso de *dark patterns* na mídia social, e ainda, avaliar sua compatibilização com os pressupostos previstos na Lei Geral de Proteção de Dados e correlacionar sua legalidade a partir dos conceitos de consentimento e transparência.

Metodologia

Para tanto, o desenvolvimento deste trabalho qualitativo foi realizado a partir de uma pesquisa exploratória da bibliografia adequada e análise legislativa sobre a utilização de *dark patterns* nas plataformas de mídia social.

Resultados

A utilização de padrões obscuros e enganosos, chamados *dark patterns*, influencia o comportamento dos titulares de dados, violando a autodeterminação informativa. Isso porque, a aplicação dessas técnicas somadas às limitações cognitivas do ser humano, contribuem para a maximização da vulnerabilidade dos usuários ante o modelo econômico informacional. Assim, a tecnologia tem sido utilizada para neutralizar essa possível habilidade de controlar e gerenciar o fluxo informacional, fragilizando, ainda mais, o titular de dados (BIONI, 2020).

Nesse cenário, não há compatibilidade na utilização desses mecanismos com os pressupostos previstos na LGPD, uma vez que constitui elemento essencial para proteção dos dados pessoais o controle de suas próprias informações. A automação, bem como outras funcionalidades das plataformas de mídia social, através do estudo de experiência do usuário, deve ser usada para facilitar o exercício dos direitos, não sendo permitido a utilização de interfaces que beneficiam os interesses corporativos em detrimento do poder de escolha do titular de dados.

ISBN 978-85-8328-120-7

Conclusão

O presente resumo, portanto, visa discutir a problemática da incompatibilidade do uso das *dark patterns* nas plataformas de mídia social com a LGPD. Isso ocorre, em suma, pela prática violar os requisitos previstos na lei quanto ao consentimento e a transparência, tornando ilícito o tratamento de dados coletados com esse direcionamento intencional. A lei estabelece como essencial que os indivíduos tenham uma manifestação livre, informada e inequívoca no momento de concordar com o tratamento de seus dados pessoais, bem como a garantia que os titulares terão informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento. Desse modo, os chamados padrões obscuros ameaçam a autonomia da vontade, a autodeterminação informativa e a privacidade, tornando-se incompatíveis com a legislação brasileira para fins comerciais.

Referências

ARVIGO, MARU e CARBONI, Guilherme. **"Dark patterns" e proteção de dados pessoais**. Disponível em: <https://www.migalhas.com.br/depeso/367473/dark-patterns-e-protecao-de-dados-pessoais>. Acesso em: 19 de julho de 2022.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

BRIGNULL, H. Dark Patterns: dirty tricks designers use to make people do stuff. **90 Percent of Everything.** 2010. [Blog] Disponível em: <https://www.90percentofeverything.com/2010/07/08/dark-patterns-dirty-tricks-designers-use-to-make-people-do-stuff/>;. Acesso em: 20 de julho de 2022.

EUROPEAN DATA PROTECTION BOARD. **Guidelines 03/2022 on Dark patterns in social media platform interfadces**: How to recognise and avoid them. Versão 1.0 de maio de 2022. Disponível em: <https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf>. Acesso em: 15 de julho 2022.

GOMES, Andressa Delmondes. **O consentimento diante das interfaces maliciosas baseadas em vieses cognitivos.** In: TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (Coords.). Proteção de dados e tecnologia: estudos da pós-graduação em Direito Digital. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; ITS/Obliq, 2022, p.10-30.

LEAL, Martha. **Dark patterns e leis de proteção de dados**. Disponível em: <https://www.conjur.com.br/2021-nov-16/leal-dark-patterns-leis-protecao-dados>. Acesso em: 19 de julho de 2022.

Palavras-chave: Lei Geral de Proteção de Dados; Experiência do Usuário; Padrões Obscuros; Consentimento; Transparência.

A LGPD E INTERNET DAS COISAS: A IMPORTÂNCIA DO PRINCÍPIO DA TRANSPARÊNCIA FRENTE ÀS NOVAS TECNOLOGIAS

Kethelen Severo Bacchi[1]

Introdução

No ano de 2018, o Congresso Nacional aprovou uma nova legislação referente à proteção de dados no Brasil, essa lei – Lei 13.709 – entrou em vigência apenas em 2020. A Lei Geral de Proteção de Dados (LGPD) foi inspirada no Regulamento Geral de Dados (GPDR) que entrou em vigor na União Europeia em 2018, uma vez que legislações com esse viés estão se tornando cada vez mais comum por todo o mundo.

Nesse sentido, levando em consideração os avanços tecnológicos que presenciamos atualmente, caracterizando um período complexo, nomeado de "sociedade em rede" (CASTELLS, 1999), a lei tem como intuito fundamental a proteção, haja vista a vulnerabilidade dos dados pessoais nesse ambiente virtual. No que tange a essas novas tecnologias, este trabalho pretende estabelecer como foco principal a Internet das Coisas – *Internet of Things* (IoT).

O conceito para essas novas tecnologias traduz um arsenal de novas possibilidades que surgem a partir de dispositivos inteligentes conectados à internet que viabilizam de todo modo, a comunicação em qualquer lugar, a qualquer momento, através desses mecanismos (DINIZ, 2006). Do mesmo modo, a ideia de uma rede mundial de objetos que se conectam e permutam informações entre si não pode ser considerado um conceito fechado, uma vez que faz com que muitas tecnologias e aplicações diferentes correspondam pelo termo Internet das Coisas. No entanto, resta bastante claro sua funcionalidade: conectar objetos dotados da capacidade de agirem por conta própria, com ou sem supervisão humana (SINGER, 2012).

Por conta disso, observa-se uma grande exposição de dados no que tange as IoTs, pois a grande maioria desses dispositivos apenas poderão operar se estiverem vinculados a uma conta pessoal, a partir da troca de inúmeras informações por parte do usuário. Normalmente esses dados são transmitidos de forma espontânea e vinculada. Apesar disso, independentemente dos custos gerados, a empresa coletora desses dados deve garantir o armazenamento de todas as informações sobre o tratamento dos dados, além de manter efetiva governança e segurança sobre todo o tratamento realizado, conforme previsão da LGPD.

De forma complementar, a empresa deve delimitar quais são as atividades de tratamento que vai desempenhar, identificando sua viabilidade a partir da identificação de uma base legal para cada uma dessas atuações, além de ter documentada essa definição. Nesse viés, imprescindível a garantia de que todas as partes incluídas no tratamento (titulares, operadores e co-controladores) saibam quais informações estão sendo coletadas, para que estão sendo utilizadas e por quanto tempo serão armaze-

[1] Universidade Federal de Santa Maria. e-mail: kethelenbacchi@gmail.com.

ISBN 978-85-8328-120-7

nadas (DAVOLI, 2020).(DAVOLI, 2020).

Por essa razão, destaca-se um protagonismo do princípio da transparência, previsto no artigo 6º, inciso VI da LGPD, uma vez que se considera uma estratégia de mitigação de riscos. E para isso, é imprescindível a elaboração de Avisos e Políticas de Privacidade de forma objetiva e precisa em relação ao tratamento dos dados, a fim de evitar atitudes abusivas por parte das empresas. Convém, nesse sentido, salientar que nem sempre esses termos possuem uma linguagem acessiva e principalmente enxuta, passando, inúmeras vezes, despercebidos pelos usuários.

Nesse diapasão, no cenário brasileiro, especialmente no que se refere à internet das coisas, é necessária a observação de alguns critérios para que seja possível a identificação da aplicabilidade da transparência em relação ao tratamento dos dados dos usuários em relação a esses dispositivos. Alguns desses critérios podem ser classificados como a existência de mecanismos específicos para dados sensíveis, o cumprimento de todos os requisitos legalmente previstos pela política de privacidade, dentre alguns outros. Por tudo isso, é necessária a análise dessas novas tecnologias, dentro do espaço brasileiro, a fim de que seja possível identificar a presença primordial do princípio em questão.

Problema

Dado o exponencial crescimento das novas tecnologias e da regulamentação do tratamento dos dados através da LGPD, questiona-se: Em que medida o princípio da transparência é aplicado de forma eficaz no que se refere à Internet das Coisas?

Objetivos

Verificar a efetiva aplicabilidade do princípio da transparência, previsto na LGPD, especialmente no que se refere à Internet das Coisas, bem como investigar acerca de sua importância no tratamento de dados no Brasil.

Metodologia

Para elaboração deste trabalho, utilizou-se o método de abordagem dedutivo, haja vista que se analisou a LGPD, o princípio da transparência em seu contexto amplo e, posteriormente, reduziu-se ao contexto da Internet das Coisas. Com relação às técnicas de pesquisa, fez-se uso da análise legislativa, uma vez que se debruçou de forma enfática nos artigos da LGPD, assim como as pesquisas bibliográficas, aproveitando-se de alguns estudos de outros autores. Por fim, o estudo faz parte do desenvolvimento da pesquisa de dissertação no mestrado pelo Programa de Pós-Graduação em Direito, sendo que até o momento não foi publicado em revistas, eventos ou periódicos.

Resultados

Observou-se a partir da pesquisa realizada que as novas tecnologias, no caso em estudo, a Internet das Coisas, tem apresentado, na maioria dos dispositivos investigados, resultado eficaz no que tange a aplicabilidade da transparência, desempenhando um papel informativo e claro, especialmente no que se refere à elaboração de Avisos e Políticas de Privacidade.

Conclusão

A pesquisa se propôs analisar o tratamento de dados conforme a legislação brasileira em vigor – LGPD. Dentro desse panorama, observou-se uma tendência positiva no que tange à aplicabilidade

do princípio da transparência em relação às novas tecnologias, especialmente no contexto da Internet das Coisas (IoT). Dessa forma, constatou-se que as organizações do ramo devem a apresentar de forma clara e precisa os Avisos e Políticas de Privacidade, bem como elaborar mecanismos específicos para proteção de dados sensíveis e o cumprimento de todos os requisitos legalmente previstos pela política de privacidade. No decorrer do estudo, após a observação de muitos desses dispositivos, foi possível identificar, com base nos dispositivos analisados, que a grande maioria deles busca atender as exigências necessárias, corroborando para uma efetividade da aplicação da transparência dentro dessas tecnologias.

Referências

BRASIL. **Lei n.º 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. Acesso em: 10 de abr. 2022.

CASTELLS, Manuel. **A sociedade em rede**. Ed. São Paulo: Editora Paz e Terra, 1999.
DAVOLI, Gabriela Brum. Iot e seus Impactos à proteção de dados pessoais. Baptista Luz Advogados. Disponível em: https://baptistaluz.com.br/espacostartup/iot-protecao-de-dados-pessoais/. Acesso em: 24 abr. 2022.

DINIZ, Eduardo H. Internet das Coisas. **Revista GV Executivo**. v.5, n.1, p. 59, fev-abr/2016. Disponível em: https://bibliotecadigital.fgv.br/ojs/index.php/gvexecutivo/article/view/34372/33170. Acesso em: 16 abr. 2022.

SINGER, Talyta. Tudo Conectado: Conceitos e Representações da Internet das Coisas. **SIMSOCIAL – Simpósio em tecnologias digitais e sociabilidade: Práticas Internacionais em Rede**. 2ª edição, 2012. Disponível em: https://docplayer.com.br/1992460-Tudo-conectado-conceitos-e-representacoes-da-internet-das-coisas-1-palavras-chave-internet-das-coisas-objetos-inteligentes-ambientes-conectados.htm. Acesso em: 10 abr. 2022

UNIAO EUROPEIA. **Regulamento (UE) 2016/679 do parlamento europeu e do conselho de 27 de abril de 2016**. Regulamento Geral sobre a Proteção de Dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 10 de abr. 2022.

Palavras-chave
LGPD; Internet das Coisas; Princípio da Transparência.

ISBN 978-85-8328-120-7

A APLICAÇÃO DA LGPD NOS CARTÓRIOS EXTRAJUDICIAIS: UMA ANÁLISE ACERCA DA EXPEDIÇÃO DE CERTIDÕES EM REGISTRO DE IMÓVEIS DA BAHIA

Manuela de Oliveira Souza Brito[1]

Introdução

Esta pesquisa buscou entender sobre a aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD), também conhecida como Lei n.º 13.709/2018, no âmbito dos cartórios extrajudiciais de registro de imóveis do Estado da Bahia, em especial no que toca a concretização do princípio da publicidade registral, ou seja, a expedição de certidões imobiliárias independentemente de controle de finalidade específica.

De acordo com o artigo 17 da LRP "Qualquer pessoa pode requerer certidão do registro sem informar ao oficial ou ao funcionário o motivo ou interesse do pedido". Apesar do artigo 17 assegurar diversos direitos às partes e à sociedade – a exemplo do direito à propriedade e à prevenção de litígios – o surgimento da LGPD trouxe consigo uma problemática acerca da compatibilização entre o princípio da publicidade registral e o direito à proteção de dados pessoais dos usuários dos serviços registrais.

Dessa forma, o estudo buscou analisar se a expedição de certidões concernentes aos imóveis registrados – independentemente de controle de finalidade pelo oficial e seus prepostos – poderá (ou não) infringir o direito à proteção de dados pessoais das partes inscritas nas matrículas imobiliárias.

O artigo 6º, I, da LGPD dispõe que as atividades de tratamento de dados pessoais deverão ser realizadas para propósitos legítimos, específicos, explícitos e informados, sem a possibilidade de tratamento posterior de forma incompatível com essas finalidades. Entretanto, quando o oficial de registro realiza a expedição de uma certidão para um terceiro, este está tratando – "compartilhando" – dados pessoais (inclusive sensíveis) de um titular, ainda que de forma indireta. Contudo, o solicitante não precisa revelar a finalidade específica do tratamento, uma vez que a falta de motivação, teoricamente, está amparada no artigo 17 da LRP.

Ademais, o recorte espacial escolhido para análise desta questão foi o Estado da Bahia, pois a Corregedoria Geral de Justiça local possui Provimentos Extrajudiciais sobre o tema – os Provimentos Conjuntos n.º 03/2021 e 07/2021 – os quais regulamentam sobre o tratamento de informações pessoais pelos oficiais de notas e de registro, inclusive no que diz respeito ao escopo do presente trabalho.

Problema

Há conflito entre o princípio da publicidade registral, previsto no art. 16 e 17 da LRP, e o princípio da finalidade previsto no artigo 6º, I, da LGPD?

[1] Graduada pela Universidade Federal da Bahia. e-mail: manuelaosb@gmail.com.

Objetivos

De forma geral, a pesquisa visou responder se existe (ou não) conflito entre o princípio da publicidade registral e o princípio da finalidade.

De forma específica, a pesquisa visou: 1. Compreender como a LGPD se aplica no âmbito das serventias extrajudiciais, especialmente no âmbito da atividade finalística de serviço público; 2. Examinar as repercussões da publicidade imobiliária diante do novo cenário de proteção de dados pessoais do país; 3. Entender como a LGPD dialoga com as legislações vigentes, levando-se em conta a aplicação setorial do direito à proteção de dados pessoais; 4. Analisar a atuação das Corregedorias de Justiça locais diante do caráter geral da norma brasileira de proteção de dados; 5. Analisar as normas de foro extrajudicial que regulamentam sobre o tratamento de informações pessoais pelos oficiais de registro; 6. Analisar como as normas podem ser mediadas com base no Direito brasileiro.

Metodologia

O estudo é resultante de Trabalho de Conclusão de Curso (TCC), o qual será publicado no repositório da Universidade Federal da Bahia (UFBA) em breve. Foi utilizado o método hipotético-indutivo, consistindo na apresentação de teorias e premissas para o desenvolvimento e obtenção de resultados da presente pesquisa. Em relação aos procedimentos técnicos adotados, elegeu-se o bibliográfico e o documental. Ademais, a presente pesquisa possui natureza de abordagem aplicada, sob a forma qualitativa.

Resultados

Com o objetivo de analisar a aplicabilidade do princípio da finalidade, previsto na LGPD, no desempenho das atividades de registro público, especialmente no que toca à expedição de certidões, anota-se que os serviços registrais possuem o mesmo tratamento de dados pessoais dispensado às pessoas jurídicas de direito público, nos termos do art. 23, § 4º, da LGPD (MONTEIRO, 2021), pois estes entes atuam em colaboração com o Poder Público. Dessa forma, a adoção da finalidade pública e do interesse público para a realização do processamento de informações pode ser estendida a estas atividades, ainda que os cartórios extrajudiciais possuam natureza jurídica privada (TASSO, 2020).

Miranda (2020) entende que a finalidade do pedido de publicidade registral deve atender à finalidade mediata, ou seja, a finalidade específica do solicitante, uma vez que a LGPD determina que a finalidade para o tratamento de informações deve ser explícita e específica, bem como informada ao titular de dados. Por outro lado, a doutrina majoritária defende que a base legal que melhor se coaduna à atividade de registro é contida no art. 7º, II, da LGPD combinada com o art. 23, *caput*, da LGPD (VERDE e TEIXEIRA, 2021; CHEZZI, 2021; MARANHÃO, 2022; MONTEIRO, 2021).

Como tentativa de harmonizar os princípios da finalidade e da publicidade, a CGJ-BA dispôs que ficará a critério do oficial, e de seus prepostos, solicitar (ou não) a finalidade específica para o cartório publicizar as informações de natureza sensível; contidas nos indicadores e índices pessoais e; nos atos protocolares. Contudo, avalia-se que tal disposição pode provocar insegurança jurídica, pois deixa sob a responsabilidade do delegatário e de seus prepostos analisarem a legitimidade da finalidade específica indicada pelo requerente.

Já sobre a expedição de certidões agrupadas segundo critérios não usuais de pesquisa, a CGJ-BA entendeu que estas deverão ser negadas quando a motivação específica não for apresentada, o que tensiona, diametralmente, com os arts. 16, § 1º e 17, *caput*, contidos na LRP.

ISBN 978-85-8328-120-7

Conclusão

Conclui-se pela inexistência de conflito entre o princípio da publicidade registral, previsto na LRP, e o princípio da finalidade, previsto na LGPD, uma vez que a legislação especial deve ser priorizada (CHIASSONI, 2020). O tratamento de dados pessoais para o desempenho da atividade finalística de publicidade registral encontra-se amparado na finalidade pública, não sendo necessário o requerimento da finalidade específica para obtenção de certidões.

Diante do novo panorama de proteção de dados pessoais, faz-se necessária cautela no tratamento de dados no âmbito dos serviços registrais. Todavia, deve-se ter cuidado na aplicação de mitigações da LRP, uma vez que as normas regulatórias de foro extrajudicial não devem comprometer a prestação de função pública e a segurança jurídica existente.

Assim, a adequação dos serviços registrais à LGPD é um tema que merece discussões multiparticipativas, as quais devem abarcar as entidades de classe, o CNJ, as Corregedorias Estaduais, a ANPD e a própria sociedade (CHEZZI, 2021).

Referências

CHEZZI, Bernardo. A**plicação da LGPD ao registro de imóveis**. In: BRANDELLI, Leonardo; GALHARDO, Flaviano; NALINI, José; PARO, João (org.). Direito Registral e Novas Tecnologias. Rio de Janeiro: Forense, 2021.

CHIASSONI, Pierluigi. **Técnica da interpretação jurídica: breviário para juristas**. São Paulo: Revista dos Tribunais, 2020, p. 444.

MARANHÃO, Juliano. **Proteção de Dados e Registro Imobiliário**. Disponível em: <https://academia.irib.org.br/pdfjs/web/viewer.html?file=123456789/24047/2020-0362-BIR.pdf>. Acesso em: 15 de maio de 2022.

MIRANDA, Caleb. **Publicidade registral: considerações sobre a qualificação e a especialidade dos pedidos de publicidade**. Disponível em: <https://academia.irib.org.br/pdfjs/web/viewer.html?file=123456789/24184/2020-0088-RDI_0207-0225.pdf>. Acesso em: 29 de maio de 2022.

MONTEIRO, Janice. **A LGPD aplicada às serventias extrajudiciais brasileiras.** In: TEIXEIRA, Tarcísio et al. (org.). LGPD e cartórios: implementação e questões práticas. São Paulo: Saraiva, 2021.

TASSO, Fernando. **A Lei Geral de Proteção de Dados em debate - Proteção de dados e os registros públicos**. Disponível em: <https://academia.irib.org.br/xmlui/handle/123456789/24046>. Acesso em: 30 de maio de 2022.

VERDE, Hilda; STINGHEN, João; TEIXEIRA, Tarcisio. **Motivações para a adequação das serventias extrajudiciais à LGPD: mudança cultural e conscientização**. In: TEIXEIRA, Tarcísio et al. (org.). LGPD e cartórios: implementação e questões práticas. São Paulo: Saraiva, 2021.

Palavras-chave
privacidade; proteção de dados; publicidade registral; finalidade; cartórios.

A LEI DE PROTEÇÃO DE DADOS PESSOAIS E A IMPLANTAÇÃO BRASILEIRA DA SAÚDE DIGITAL

Ruy Roberto Porto Ascenso Rosa[1]

Introdução

No Brasil, a Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709) foi sancionada em 2018 (BRASIL, 2018). Dois anos depois, o Governo, por meio do Ministério da Saúde, apresentou o documento "Estratégia de Saúde Digital para o Brasil 2020-2028" (ESD28), onde prevê a implantação da Saúde Digital no território nacional, até o ano de 2028, utilizando, para isso, o Programa Conecte SUS (BRASIL, 2020a).

Percebe-se que a pandemia da COVID-19 impulsionou uma intensa utilização de recursos digitais para o seu enfrentamento (SCHMITZ et al., 2022), o que acelerou bastante a implantação de partes da ESD28. Por exemplo, dentro daquilo que é esperado com a instituição do Conecte SUS, a interoperabilidade entre os laboratórios públicos e privados e o Ministério da Saúde para notificação de resultados de testes diagnósticos para SARS-CoV-2, através da integração à Rede Nacional de Dados em Saúde (BRASIL, 2020b, 2020c), foi estruturada em tempo recorde (BRASIL, 2020d), a fim de responder à iminente demanda ocasionada pela pandemia, porém muitos outros projetos estruturantes ainda se encontram em desenvolvimento.

Problema

Frente ao plano de implantação da Saúde Digital no Brasil até 2028, faz-se necessário conhecer: quais as contribuições descritas na literatura que a Lei Geral de Proteção de Dados Pessoais pode oferecer ao processo de implantação nacional da Saúde Digital?

Objetivos

Sintetizar os achados científicos já publicados sobre a aplicação da Lei Geral de Proteção de Dados Pessoais dentro do contexto de implantação da Saúde Digital no Brasil.

Metodologia

Inicialmente, foi realizada uma busca por Descritores em Ciências da Saúde (DeCS/MeSH) utilizando os termos "Saúde Digital" e "Lei Geral de Proteção de Dados Pessoais" no site da Biblioteca Virtual em Saúde (BVS; https://decs.bvsalud.org/).

Na Base de Dados SciELO (https://scielo.org/en/) foi realizada a busca, utilizando a associação dos termos: (Saúde Digital) AND (Lei Geral de Proteção de Dados Pessoais), assim como, cada um dos termos de forma isolada. Foram adotados os seguintes critérios de inclusão: artigos publicados entre 2018 a 2022, publicados em português, inglês ou espanhol, que possuíam acesso livre e que abordassem tema referente aos objetivos propostos para essa pesquisa.

Conforme descrito em Ascenso-Rosa (2016), após a obtenção dos artigos, utilizando a estratégia de busca em Base de Dados, os artigos incluídos foram analisados individualmente, sendo

[1] Universidade do Estado do Amazonas. e-mail: ruyascenso@hotmail.com.

ISBN 978-85-8328-120-7

apresentada a síntese dos resultados obtidos em quadros.

Por utilizar dados secundários de livre acesso, não houve necessidade de submissão à Plataforma Brasil para apreciação por um Comitê de Ética e Pesquisa em Seres Humanos. Todavia, todas as demais orientações éticas e legais foram observadas na condução desta pesquisa (BRASIL, 2012).

Resultados

Ao realizar a busca por descritores na Biblioteca Virtual em Saúde para o termo "Saúde Digital", encontrou-se 5 descritores, apresentados no Quadro 1. Já para o termo "Lei Geral de Proteção de Dados Pessoais", a busca por descritores na referida biblioteca não retornou nenhum resultado.

Quadro 1 – Descritores retornados pela Biblioteca Virtual em Saúde para o termo "Saúde Digital".

n.	Português	Inglês	Espanhol
1	Bibliotecas Digitais	Libraries, Digital	Bibliotecas Digitales
2	Estratégias de eSaúde	eHealth Strategies	Estrategias de eSalud
3	Registros Eletrônicos de Saúde	Electronic Health Records	Registros Electrónicos de Salud
4	Sistemas Computadorizados de Registros Médicos	Medical Records Systems, Computerized	Sistemas de Registros Médicos Computarizados
5	Telemedicina	Telemedicine	Telemedicina

Fonte: BVS, 2022

A busca na Base de Dados SciELO não retornou nenhum resultado quando utilizando o operador boleano "AND". Contudo, ao utilizar na mesma base somente o termo "Saúde Digital" foram encontrados 668 artigos, dos quais apenas 376 atenderam ao critério de ano de publicação. Destes 376 artigos, somente 5 abordavam tema relevante aos objetivos desta pesquisa, sendo incluídos e apresentados no Quadro 2.

Quadro 2 – Artigos incluído para o termo "Saúde Digital".

AUTOR, ANO	REVISTA	TÍTULO	OBJETIVO
LOUREIRO; AZEVEDO; CORREIA, 2022	Revista Portuguesa de Medicina Geral e Familiar	Privacidade e confidencialidade em medicina: o que diz o Regulamento Geral de Proteção de Dados sobre o acesso a informação de saúde	Não declarado
SCHMITZ et al., 2022	SciELO Preprints	Eighteen years in two days: the next steps for remote consultation in Brazil	Subsidiar a discussão pós-pandemia da Doença causada pelo novo Coronavírus a respeito da regulamentação do atendimento por meio de recursos digitais.
ALMEIDA et al., 2020	Ciência & Saúde Coletiva	Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global	Não declarado
QUISPE-JULI et al., 2020	SciELO Preprints	COVID-19: una pandemia en la era de la salud digital	Describir cómo han sido utilizadas las tecnologías de la información emergentes para hacer frente al COVID-19.
CAETANO et al., 2020	Cadernos de Saúde Pública	Desafios e oportunidades para telessaúde em tempos da pandemia pela COVID-19: uma reflexão sobre os espaços e iniciativas no contexto brasileiro	Discutir os espaços de contribuição da telessaúde para o enfrentamento da epidemia pela COVID-19 e as iniciativas recentes desencadeadas no Brasil.

Fonte: SciELO, 2022

Para o termo "Lei Geral de Proteção de Dados Pessoais" a pesquisa na base de dados retornou apenas 5 artigos, sendo que, destes, apenas 2 atenderam a todos os critérios de inclusão, os quais foram incluídos na pesquisa, conforme Quadro 3.

Quadro 3 – Artigos retornados para o termo "Lei Geral de Proteção de Dados Pessoais".

AUTOR, ANO	REVISTA	TÍTULO	OBJETIVO
FICO; NOBREGA, 2022	Revista Direito e Práxis	The Brazilian Data Protection Law for LGBTQIA+ People: Gender identity and sexual orientation as sensitive personal data	Explorando a flexibilidade hermenêutica desta lei, este artigo argumenta que tanto "orientação sexual" como "identidade de gênero" são dados sensíveis, seja em virtude do termo "vida sexual", seja em virtude do termo "raça".
BINOTTO; PONCE, 2022	Revista de Economia Contemporânea	***Data portability: lessons from other sectoral experiences**	Investigar instrumentos legais e regulatórios já empregados para regulamentar direitos de portabilidade no Brasil.
GARCEL; MORO, 2021	Revista Internacional CONSINTER de Direito	Data protection law and its interactions with the anti-money laundering law	Analisar as interações da nova Lei Geral de Proteção de Dados Pessoais, Lei nº. 13.709, de 14 de agosto de 2018, com a lei de Lavagem de Dinheiro, Lei nº. 9.613, de março de 1998.
FORNASIER; KNEBEL, 2021	Revista Direito e Práxis	O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados na Lei Geral de Proteção de Dados	Caracterizar o regime jurídico da Lei Geral de Proteção de Dados sob os conceitos apresentados pelo capitalismo de vigilância, tendo como objetivos específicos: (I) descrever a economia política da vigilância e o papel do titular de dados/ usuário de serviços digitais e (II) identificar a inserção da LGPD no contexto da exploração econômica dos dados pessoais por meio do instrumento do consentimento do titular.
PIURCOSKY et al., 2019	Suma de Negocios	***A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos**	Descrever e compreender a realidade de organizações brasileiras quanto à adequação à Lei Geral de Proteção de Dados Pessoais (LGPD).

* Artigos que atenderam aos critérios de inclusão da pesquisa.

Fonte: SciELO, 2022

Conclusão

Inicialmente, percebe-se a necessidade da disponibilização, pela Biblioteca de Saúde Virtual, de descritores próprios para os termos "Saúde Digital" e "Lei Geral de Proteção de Dados Pessoais", a fim de promover uma melhor recuperação de publicações dessas áreas. Verifica-se, ainda, poucas publicações associadas aos temas pesquisados, todavia, é nítido que para os próximos anos há um grande campo de pesquisa a ser explorado, principalmente devido ao estímulo que as políticas públicas de Estado voltadas à implantação da Saúde Digital até o ano de 2028 provocarão. A análise dos artigos selecionados demonstra a escassez de publicações que abordam a Saúde Digital, e que menor ainda é a associação desse tema com a Lei Geral de Proteção de Dados Pessoais. A maioria das publicações sobre Saúde Digital até citam a necessidade de haver uma proteção dos dados sensíveis coletados pelos sistemas e/ou ferramentas utilizados no âmbito da Saúde Digital, mas somente um estudo faz referência à Lei 13.709/2018. Dessa forma, como resposta à problemática inicial, conclui-se que pouco há na literatura sobre as contribuições da Lei Geral de Proteção de Dados Pessoais para a implantação da Saúde Digital, contudo os estudos já apontam para a sua grande contribuição a este processo iminente de implantação da Saúde Digital, quando abordam questões acerca da necessidade de haver segurança para o uso dos dados coletados.

Referências

ASCENSO ROSA, R. R. P. Redução da morbimortalidade por câncer de colo uterino. **Revista de Epidemiologia e Controle de Infecção**, Santa Cruz do Sul, v. 6, n. 3, p. 131-137, jul. 2016. https://doi.org/10.17058/reci.v6i3.6633.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Institui a Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**: seção 1, Brasília, DF, p. 59, 15 ago. 2018. PL 4060/2012.

BRASIL. Ministério da Saúde. Conselho Nacional de Saúde. Comissão Nacional de Ética em Pesquisa. **Resolução n° 466/12**. 12p. Publicada no DOU n.º 12 jun. 2013, seção 1, p. 59. Disponível em: <http://conselho.saude.gov.br/resolucoes/2012/Reso466.pdf>. Acesso em: 28 jul. 2022.

BRASIL. Ministério da Saúde. Secretaria-Executiva. Departamento de Informática do SUS. **Estratégia de Saúde Digital para o Brasil 2020-2028**. 1. ed., Brasília: Ministério da Saúde, 2020. 128 p. Disponível em: < https://bvsms.saude.gov.br/bvs/publicacoes/estrategia_saude_digital_Brasil.pdf>. Acesso em: 28 jul. 2022.

BRASIL. Portaria n.º 1.068, de 17 de novembro de 2020. Institui o modelo de informação de resultado de exame laboratorial COVID-19. **Diário Oficial da União**: seção 1, p. 140, 19 nov. 2020.

BRASIL. Portaria n.º 1.434, de 28 de maio de 2020. Institui o Programa Conecte SUS e a Rede Nacional de Dados em Saúde. **Diário Oficial da União**: seção 1, p. 231, 29 maio 2020.

BRASIL. Portaria n.º 1.792, de 17 de julho de 2020. Dispõe sobre a obrigatoriedade de notificação ao MS de resultados de testes para SARS-CoV-2. **Diário Oficial da União**: seção 1, p. 41, 21 jul. 2020.

SCHMITZ, C. A. A. et al. Eighteen years in two days: the next steps for remote consultation in Brazil. **SciELO Preprints**, 2021. https://doi.org/10.1590/SciELOPreprints.3126.

Palavras-chave:Saúde Digital; Lei Geral de Proteção de Dados Pessoais; Sistema Único de Saúde.

ISBN 978-85-8328-120-7

VAZAMENTO DE DADOS DO PRONTUÁRIO ELETRÔNICO DO CIDADÃO EM UM MUNICÍPIO DO CEARÁ – RELATO DE EXPERIÊNCIA

Manoel Lourenço da Silva[1]

Introdução

Através da Portaria MS/GM n.º 2.488, de 21 de outubro de 2011, o governo brasileiro passou a investir em melhorias na captação e tratamento dos dados relacionados à saúde, em especial aos da atenção básica, com a implementação da estratégia e-SUS Atenção Primaria (e-SUS APS), que deu início ao desenvolvimento do e-SUS PEC e consolidou o uso do prontuário eletrônico do cidadão em todo território brasileiro, ficando a cargo da Universidade Federal de Santa Catarina (UFSC) e do Laboratório Bridge o seu desenvolvimento. O e-SUS PEC trata-se então de um sistema de informação com a finalidade de captação, gerenciamento, processamento, criação de fluxo de atendimento, e de facilitar a vida dos profissionais de saúde no atendimento e incentivar o uso de soluções de tecnologia no gerenciamento da atenção à saúde em todo território nacional.

Tomando-se a principal ferramenta da atenção básica na coleta de informações e melhoria no atendimento à população. Seu uso pelo município está condicionado ao download, instalação e ativação com contra chave gerada no e-gestor, sendo de responsabilidade do gestor municipal de saúde a sua implementação e manutenção (atualização) e segurança dos dados, bem como procedimentos de backups.

Uma das maiores preocupações das grandes empresas e governo do Brasil e do mundo são relacionadas aos vazamentos de dados e possíveis vulnerabilidades em seus sistemas. De acordo com Novaes (2021), MIT (Instituto de Tecnologia de Massachusetts), nos últimos anos o Brasil teve um aumento significativo em relação aos vazamentos de dados, com um aumento de 493% entre os anos de 2018 e 2019.

Com a aprovação da Lei Geral de Proteção de Dados Pessoais, Lei de n.º 13.709/2018, essa preocupação se tornou muito maior, tendo em vista que a LGPD trouxe punições e sanções para aqueles que a desrespeitam. Além de implementar a Autoridade Nacional de Proteção de Dados (ANPD) que tem como atribuições relacionadas a proteção de dados pessoais e da privacidade e, sobretudo, deve realizar a fiscalização do cumprimento da Lei n.º 13.709/2018.

Diante disso, podemos observar que o laboratório Bridge, que é o responsável pelo desenvolvimento do e-SUS PEC tem feito adoção de ferramentas consolidadas e de alta tecnologia e segurança no desenvolvimento de programas, além de protocolos de desenvolvimento e correções de bugs presentes no e-SUS PEC.

Infelizmente, em alguns municípios não observamos a adoção de protocolos de segurança de

[1] Discente da Faculdade Princesa do Oeste. e-mail: manoel.lourenco@alu.fpo.edu.br.

dados, bem como é possível notar a falta de profissionais da tecnologia da informação para a realização da instalação e manutenção do sistema, parte essa que é crucial para a segurança de dados.

Problema

Diante da preocupação acerca da segurança de dados é importante trazer uma nova perspectiva sobre o sistema de informação e-SUS PEC e a segurança de dados por parte dos municípios.

Objetivo

Trazer questionamentos e discussões sobre a segurança de dados em municípios sem suporte de tecnologia da informação (TI).

Metodologia

Trata-se de um estudo descritivo do tipo relato de experiência ocorrido nos meses de junho e julho de 2022. Nesse período foram realizados testes de segurança em servidores de um município no Ceará, onde foram encontradas vulnerabilidades e exposição de dados sensíveis do Prontuário Eletrônico do Cidadão - PEC.

Resultados

Ao visualizar publicações no *stories* do Instagram, acabei visualizando uma publicação que me chamou atenção: era mostrada na publicação a tela de login do e-SUS PEC, bem como uma legenda sobre um dia cansativo de trabalho de uma profissional da saúde. Na publicação era possível ver o IP público da aplicação na internet bem como a porta de acesso ao sistema. Movido pela curiosidade decidi realizar testes simples de segurança, onde fiz varredura de portas abertas no IP da aplicação. Tendo resultado positivo na porta 5433, porta padrão do banco de dados PostgreSQL do e-SUS PEC.

Diante disso, tentei realizar a conexão com o banco de dados utilizando credenciais padrão do sistema e-SUS PEC com o seguinte comando ($psql -h IP Público -p 5433 -U postgres – password esus) e, para minha surpresa, o sistema autenticou e liberou meu acesso com um login e senha padrão, que também era o administrador do sistema sendo possível realizar DROPDB (Exclusão) e DUMP (backup dos dados).

Infelizmente estava ali, acabava de descobrir um sério vazamento de dados onde estavam expostos na internet dados como nome, nome da mãe, nome do pai, data de nascimento, CPF, PIS, endereço, diagnósticos, consultas, procedimentos, vacinas e doenças. Eram cerca de 36 mil pessoas com seus dados expostos.

Imediatamente, me desesperei para reportar a falha de segurança, para tão logo ser corrigida. Na mesma rede social procurei pelo gestor responsável pelo município, onde não tive sucesso. Depois de muito procurar, consegui mandar mensagem via WhatsApp para o prefeito do município, onde reportei a falha. O gestor então me encaminhou o número do subsecretário adjunto de saúde, onde novamente reportei a falha de segurança. Diante disso fiquei com consciência limpa e pensei que o problema seria corrigido logo.

Passaram alguns dias, resolvi testar se a falha estava corrigida, para minha surpresa o banco continuava exposto. Novamente entrei em contato com o subsecretário para questionar sobre a falha, o mesmo relatou que a falha tinha sido corrigida e que na verdade não existia falha. Insistir em relatar que existia ali um vazamento de dados, o mesmo insistiu que não havia nenhuma anormalidade e que o pessoal do TI teria resolvido. Detalhei a falha e continuei insistindo e tentando explicar o que ocor-

ISBN 978-85-8328-120-7

ria, acabei sendo bloqueado no WhatsApp.

Conclusão

Diante do relato é possível identificar desconhecimento por parte do subsecretário e/ou do responsável pelo TI sobre as práticas de segurança da informação adotadas. O que provavelmente ocasionou a falha de segurança na realização da instalação e/ou configuração do sistema em seus servidores, tendo em vista que, por padrão, o banco de dados do e-SUS PEC é restrito ao servidor local. Se o mesmo está exposto foi devido a alteração de regras de segurança nas configurações do banco de dados, bem como abertura de portas do roteador de internet além de desativação do firewall do servidor. Também é possível que tenha sido realizada a abertura proposital do banco de dados para a realização de busca por programas de terceiros que fazem processamento de dados para calcular indicadores para o previne Brasil.

Com isso é possível fazer uma discussão sobre o vazamento de dados, onde a responsabilidade é do município e do gestor municipal, e não apenas dos desenvolvedores do sistema. Tendo em vista que o e-SUS PEC utiliza em seu desenvolvimento tecnologias de alto padrão, bem como protocolos de segurança, sendo o sistema e-SUS PEC de alta confiabilidade e alto nível de segurança.

Mas que devido seu formato instalação ser realizado pelos municípios que muitas das vezes não têm à disposição profissionais da TI para a realização da instalação bem como a devida configuração, levando assim a possíveis falhas de configuração onde acabam por ocorrer vazamentos de dados como o relatado.

Também é importante destacar que o município em questão está sujeito a sofrer com as penalidades impostas pela Autoridade Nacional de Proteção de Dados – ANPD. Tendo em vista a falta de adequação à Lei Geral de Proteção de Dados.

Minhas expectativas não foram alcançadas, tendo em vista não ter obtido retorno por parte do gestor, bem como pela não resolução do problema.

Referências

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Institui a Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**: seção 1, Brasília, DF, p. 59, 15 ago. 2018. PL 4060/2012.

FANTONELLI, Miliane et al. **Lei geral de proteção de dados e a interoperabilidade na saúde pública**. Journal of Health Informatics, v. 12, 2021.

NOVAES, Madnick et al. **Developing a Global Data Breach Database and the Challenges Encountered**. J. Data and Information Quality 13, 1, Article 3, 33 pag, 2021. https://doi.org/10.1145/3439873

Palavras-chave: Vazamento de dados; Prontuário Eletrônico do Cidadão; Lei Geral de Proteção de Dados.

PERFIL DE UM ENCARREGADO DE TRATAMENTO DE DADOS EM SAÚDE NO SISTEMA ÚNICO DE SAÚDE DO BRASIL

Laíse Figueiredo Rolo de Oliveira[1]
Lara Liz Freire[2]
Vanessa Lora[3]
Blanda Helena de Mello[4]
Elen Ferreira Ramos de Azevedo[5]
Thais Lucena de Oliveira[6]

Introdução

Embora as interfaces de cuidado estejam cada vez mais digitais, o fato de os dados de saúde não serem armazenados em um formato intercambiável de um serviço para outro, representa um desafio significativo para o Sistema Único de Saúde. Sistemas de informação independentes frequentemente propiciam interrupções na continuidade do cuidado ao longo da jornada do usuário, pois apresentam-se de forma fragmentada e frágil para gestão dos dados. Isso torna difícil a manutenção da assistência em saúde, uma vez que os dados de maior relevância têm caracterização sensível aos olhos da LGPD. Além disso, a falta do tratamento adequado dos dados, adotando um padrão formal para troca de dados intensificam a carga de trabalho dos profissionais de saúde e no retrabalho para manuseio dos distintos sistemas, os quais impactam diretamente na experiência dos usuários (paciente e equipe de saúde), e consequentemente na própria qualidade da assistência. Este cenário fragmentado facilita a hiperutilização de recursos em saúde, exacerbando custos ao longo de toda cadeia de cuidado em saúde, ocasionando gargalos no atendimento de pacientes com maiores demandas de assistência e, de maneira geral, gerando desperdícios, que impactam na eficácia do atendimento. O encarregado de dados em saúde, perfil que intermedia o acesso aos dados em um estabelecimento de saúde, seria responsável pelo gerenciamento dos dados coletados com o setor de políticas públicas, para possibilitar a tomada de decisões baseadas em dados. Assim, garantir que os dados coletados nas diferentes frentes de atenção, representem de forma fidedigna a realidade da saúde da população e orientem as políticas adotadas.

Problema

O grande volume de dados em saúde gerados diariamente tem sido um desafio nos últimos anos, cenário este destacado pelos autores (Martin-Sanchez e Verspoor, 2014), consequência da larga adoção de sistemas de registro eletrônico em estabelecimentos de saúde. A realidade no domínio da saúde tem seguido em direção a adoção de sistemas de informação e tecnologias *Big Data*, necessárias para realizar o armazenamento, processamento e análises neste grande volume de dados coletados

1 CGIIS/DATASUS/SE/MS. e-mail: laise.oliveira@saude.gov.br
2 CGIIS/DATASUS/SE/MS. e-mail: lara.freire@saude.gov.br
3 CGIIS/DATASUS/SE/MS. e-mail: vanessa.lora@saude.gov.br
4 CGIIS/DATASUS/SE/MS. e-mail: blanda.mello@saude.gov.br
5 CAOFI/DATASUS/SE/MS. e-mail: elen.azevedo@saude.gov.br
6 COGISS/CGIIS/DATASUS/SE/MS. e-mail: thais.lucena@saude.gov.br

ISBN 978-85-8328-120-7

(NASEEM et al., 2020). A partir deste contexto, evidencia-se a falta de capacitação técnica para manejar os dados, com uma abrangência insuficiente das regulamentações técnicas sobre o tema, bem como a inexistência de definições e procedimentos adequados para a guarda dos dados. Consequentemente, este cenário é intensificado, uma vez que o crescimento exponencial dos dados em formato digital tem sido uma realidade para registros de saúde, denominados sistemas de registros eletrônico de saúde (RES). Portanto, quais seriam as atribuições de um perfil de encarregado de dados em saúde, observando as necessidades impostas pelo volume de dados coletados, as leis de proteção e privacidade estabelecidas, mas atentando-se às necessidades de permitir o acesso às informações para definição de políticas públicas, vigilância e cuidado?

Objetivos

O intuito dessa pesquisa é buscar os caminhos que definam a figura do encarregado de dados em saúde, partindo do pressuposto que um profissional técnico com conhecimento específico, amparado do esqueleto regulatório adequado, tem capacidade para viabilizar o melhor aproveitamento desses dados, possibilitando melhores análises das informações e evidências clínicas. O que permite às instâncias tomar decisões mais assertivas baseadas em dados (*Data Driven*) e reduz os custos nas políticas públicas (exames em duplicidade). Nesse contexto, atualmente o SUS já conta com capilaridade em atender a população nas diferentes regiões em um cenário físico, contudo, ao trazer este cenário de capilaridade aos dados estruturados de qualidade é possível representar essa capilaridade também para decisões em políticas públicas, decisões técnicas e fomentar a disseminação. O encarregado de dados tem o objetivo de passar o conhecimento sobre recursos que podem ser extraídos a partir dos dados.

Metodologia

Os aspectos metodológicos considerados nesta pesquisa estão alinhados conforme a abordagem de Köche (2011) onde a presente pesquisa caracteriza-se como descritiva, porque visa à identificação e análise das características, fatores ou atribuições que se aplicariam com a criação de um perfil encarregado de dados em saúde, como cargo/função em estabelecimentos de saúde (SUS). Com o objetivo de analisar as relações entre as ações previstas deste perfil, a fim de verificar seus respectivos efeitos resultantes na proposição de novas políticas públicas, ações e políticas de vigilância.

Resultados

No que tange às definições aplicadas pela LGPD, o perfil elaborado para o encarregado de dados tem contexto genérico, o qual permite uma abstração das atividades previstas e posteriores aplicações em cenários específicos. O encarregado de dados em saúde seria um profissional de atuação a nível assistencial, responsável por acompanhar e gerir os dados de saúde do cidadão através do prontuário eletrônico, fortalecendo um cuidado longitudinal. Atualmente, o Ministério da Saúde disponibiliza regulamentações sobre o tratamento de dados de saúde, a exemplo, a Portaria n. 234, de 18 de julho de 2022, referente ao modelo Informação Registro de Atendimento Clínico (RAC). Neste sentido, verificou-se que não há uma regulamentação que combine as necessidades de controle de privacidade de informações como a lei geral de proteção de dados, as regras e modelos de tratamento dos dados de saúde e de acordo com os padrões nacionais brasileiros.

Em consequência, as atribuições do que seria um encarregado do tratamento de dados em saúde também não são apresentadas concretamente. Por outro lado, o Conselho Federal de Química, através da portaria n. 93 de agosto de 2021, adiciona diversas outras expectativas ao cargo. Observando este

cenário, é necessário promover a regulamentação e criação de um perfil do encarregado de tratamento de dados em saúde, atento aos padrões de interoperabilidade estabelecidos a nível nacional, acompanhar e verificar os dados coletados constantemente e identificar cenários de atenção às autoridades, conhecer e compreender as leis e regulamentações que prevalecem sobre os dados pessoais coletados.

Conclusão

Para garantir o melhor uso e controle da proteção de dados sensíveis de saúde é imprescindível a criação de um perfil responsável pelo tratamento desses dados. O volume de dados gerados e processados tem aumentado exponencialmente, assim como a complexidade da aplicação do tratamento destes. Dentre os dados pessoais sensíveis estão os dados de saúde, eles necessitam de cuidados específicos que podem ser descritos nas atribuições do perfil proposto. Dentre eles, destaca-se a importância de orientar os envolvidos no processo através de boas práticas de utilização da LGPD e nas normas de utilização dos modelos de informações de saúde e adotar providências. Espera-se que com a implementação desse perfil estratégico, os estabelecimentos de saúde otimizem seus protocolos de tratamentos de dados, qualificando as informações reunidas a fim de gerar melhores decisões para saúde da população de forma coletiva e para o atendimento individual ao cidadão.

Referências

AYUSO, Juan Francisco Rodríguez. **Control de la privacidad por parte de las autoridades sanitarias ante situaciones de emergencia**. Revista de bioética y Derecho, v. 50, p. 353-368, 2020.

BRASIL. Ministério da Saúde. Gabinete do Ministro. **Portaria no 234, de 18 de julho de 2022**. Brasília, 2022. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-234-de-18-de-julho-de-2022-416506215. Acesso em: 04 ago. 2022.

CONSELHO FEDERAL DE QUÍMICA. **Portaria no 93, de 26 de agosto de 2021**. Brasília, 2021. Disponível em: http://cfq.org.br/wp-content/uploads/2021/09/Portaria_93-de-26-de-agosto-de-2021-Disp%C3%B5e-sobre-a-indica%C3%A7%C3%A3o-de-Encarregado-pelo-Tratamento-de-Dados-Pessoais-no-CFQeh.pdf. Acesso em: 04 ago. 2022.

KÖCHE, José Carlos. **Fundamentos de metodologia científica: teoria da ciência e iniciação à pesquisa**. Editora Vozes, 185 p., 2011.

MARTIN-SANCHEZ, Fernando; VERSPOOR, Karin. **Big data in medicine is driving big changes**. Yearbook of medical informatics, Georg Thieme Verlag KG, v. 23, n. 01, p. 14–20, 2014.

TAMBOSI, Paulo Vitor Petris. **Responsabilidade civil pelo tratamento de dados pessoais conforme a Lei Geral de Proteção de Dados (LGPD)**: subjetiva ou objetiva? Repositório Institucional, Universidade Federal de Santa Catarina, 115 p., 2021.

Palavras-chave: Saúde Pública; Agente Público; Proteção de Dados; Encarregado de Dados em Saúde.

ISBN 978-85-8328-120-7

1ª Mostra Científica de Proteção de Dados na Saúde, Tecnologia e Poder Público

laboratoriobridge Laboratorio Bridge

www.portal.bridge.ufsc.br

1ª Mostra Científica de Proteção de Dados na Saúde, Tecnologia e Poder Público

E-book dos melhores trabalhos da mostra

bridge_

UNIVERSIDADE FEDERAL DE SANTA CATARINA