V Simpósio de Iniciação Científica 2022
Ciência, Tecnologia e Inovação no Brasil

ANÁLISE DE ESTRATÉGIAS DE CONSENTIMENTO DE TRATAMENTO DE INFORMAÇÃO EM SISTEMAS DE IoMT (INTERNET OF MEDICAL THINGS)

Matheus Henrique Souza Araújo[1] (IC), Lina Garcés (PQ)[1]
[1]*Universidade Federal de Itajubá .*

Palavras-chave: LGPD; smartbands; compliance; IoMT; tratamento de informação.

Introdução

Em vigor desde 18 de setembro de 2020, a Lei Geral de Proteção de Dados, popularmente conhecida como LGDP (Brasil, 2018), nasce em um cenário internacional em que questões de regulamentação quanto ao uso de informações no meio digital emergem no debate público. Muito influenciada pela lei europeia "*General Data Protection Regulation*" (GPDR), a LGPD tem como objetivo regulamentar todo e quaisquer tipos de dados. Por atuar em todos os empreendimentos, seja público ou privado, a Lei também contempla os serviços de saúde. O emprego de meios digitais para arquivamento e consulta de dados, já se faz presente na vida de muitos residentes no Brasil, podem-se encontrar certos dados relativos à saúde em vários aplicativos. O cartão de vacina com as doses que protegem do COVID-19, fornecido pelo governo, pode ser consultado pelo aplicativo ConecteSUS.

Outra ação comum é consultar resultados de exames por meio de web apps. Entretanto, a LGPD trata de proteção de dados, não apenas no meio online. Então, papéis fornecidos, por exemplo, após uma consulta médica são considerados dados sensíveis de saúde e estão sob o rigor da lei. Outro ponto a se considerar é a emergente tecnologia conhecida como Internet das Coisas, de sigla IoT (*Internet of Things*).

IoT é um conjunto de variados dispositivos, imersos no dia-a-dia, como geladeira, tênis, etc, que juntos, geram uma quantidade imensurável de dados. Quando se trata de dispositivos que geram dados de saúde, como os *wearables* (dispositivos vestíveis), precisa-se de maior cautela.

Durante a exibição do *reality* show *Big Brother* Brasil, 2022, era perceptível o uso de pulseiras inteligentes, as smartbands, o que instigou o início desta pesquisa, visando entender como as empresas responsáveis tratam dados adquiridos por esse tipo de dispositivos de saúde e se tais aplicativos cumprem com os requisitos de adequação da LGPD.

As *smartbands*, são conectadas aos *smartphones* por meio de um aplicativo, geralmente indicado pela própria fabricante. Esses aplicativos contém os termos de serviço e privacidade, que informam aos usuários quais são as diretrizes de uso do mesmo. Todavia, essas informações precisam ser claras e de fácil entendimento ao usuário, além de cumprir todos os requisitos descritos na legislação brasileira.

Para o objetivo desta pesquisa, foram analisados três aplicativos de IoMT, sendo eles, *Google Fit* (*Google,* 2022), *Zepp* (*Huami*, 2021), *Samsung Health* (*Samsung*, 2018). Foi realizada uma análise crítica, determinando um grau de conformidade desses termos com a LGPD.

Metodologia

Para a execução e obtenção de dados nesta pesquisa, foi necessário utilizar um celular *Android* com capacidade de memória, possibilidade de conexão a uma *smartband* e acesso à *internet*.

Cada aplicativo foi analisado individualmente. Inicialmente, o aplicativo *Zepp* foi instalado utilizando a aplicação *PlayStore* do *Android*. Após a instalação, foram conduzidas as instruções do aplicativo para sua primeira utilização. Somente no momento da criação de conta foi possível acessar o termo de serviço do aplicativo. O termo foi salvo em formato PDF para facilitar a leitura. Esse procedimento foi realizado igualmente para os aplicativos *Google Fit* e *Samsung Health.*

O termo de cada aplicativo foi lido cuidadosamente várias vezes pelos pesquisadores. Com base na interpretação do termo de cada aplicativo foi definida a pontuação para cada um dos 32 critérios de avaliação de conformidade definidos em (Mendes, 2021). As avaliações foram registradas em tabelas. Por fim, para cada aplicativo, foi calculada a porcentagem de adequação do termo aos requisitos extraídos da LGPD. Os resultados detalhados das avaliações estão disponíveis em (Araujo 2022).

A análise realizada neste trabalho foi qualitativa, usando cálculos básicos e porcentagens para identificar a

quantidade de requisitos cumpridos por aplicativo.

Resultados e discussão

Os resultados das avaliações dos aplicativos de IoMT são apresentados em tabelas. Na primeira coluna se listam as categorias de requisitos de adequação, sendo elas: **TR** - Transparência; **CO** - Consentimento; e **DI** - Direito ao Titular. A segunda coluna descreve o critério a ser avaliado conforme o *checklist* em (Mendes, Viana, and Rivera 2021). Na última coluna, detalha-se o nível de cumprimento de cada um dos critérios, informando se o termo de serviço do *App* tem informações para considerar se o critério é cumprido totalmente **(C)**, parcialmente **(CP)** ou incumprido **(NC)**. Segue abaixo exemplos de critérios com seus respectivos identificadores utilizados para as avaliações. A lista completa dos 32 critérios e os resultados para cada aplicativo está disponível em (Araujo 2022).

- TR01 - O *software* utiliza os dados pessoais apenas para fins
- específicos, explícitos e legítimos para qual foi originalmente
- coletado e informado ao titular de dados?
- TR02 - O *software* realiza tratamento de dados previstos na lei de forma adequada e compatível com a finalidade para qual foi originalmente coletado?
- TR03 - O *software* permite acesso fácil e gratuito sobre às informações que estão sendo utilizadas, a forma e a duração do tratamento, sempre que o titular de dados requisitar?
- TR04 - O *software* mantém registros dos dados pessoais precisos e atualizados, sem demora, para cumprimento das suas finalidades?
- CO01 - O *software* permite que o titular de dados dê o seu
- consentimento de forma livre e clara aos termos e condições,
- políticas de privacidade, para realizar o tratamento de seus dados?
- CO02 - O *software* exige o consentimento específico do titular de dados para comunicar ou compartilhar os dados pessoais com outros controladores?
- CO03 - O *software* mantém registros para provar que o consentimento - foi obtido em conformidade com o disposto nesta lei, stendendo as condições de consentimento livre, específico, informado e presumido?
- CO04 - O *software* permite o titular de dados meios para recusar ouretirar o consentimento sem prejuízo a qualquer momento?
- DI01 - O *software* fornece ao titular o acesso aos seus dados pessoais que estão sendo utilizados de forma gratuita, sempre que requisitar?
- DI02 - O *software* armazena os dados pessoais em formato que facilite o titular de dados acessá-los?
- DI03 - O *software* fornece ao titular de dados, meios para registrar reclamações em relação a proteção e no processamento de seus dados pessoais?
- DI04 - O *software* fornece a cópia eletrônica integral dos dados pessoais para utilização subsequente em outras operações de tratamento previsto na lei, em caso de consentimento ou contrato?

Resultados

Tabela 1. Resumo da avaliação de adequação dos aplicativos de IoMT à LGPD

RESUMO DA ADEQUAÇÃO POR APLICATIVO			
ADEQUAÇÃO AOS CRITÉRIOS	***Zepp***	***Samsung Health***	***Google Fit***
Cumpre (C)	17	23	22
Cumpre Parcialmente (CP)	9	8	5
Não Cumpre (NC)	6	2	6
RESULTADO DA AVALIAÇÃO			
ADEQUAÇÃO à LGPD	*67,19%*	*81,82%*	*87,88%*
TR - Transparência	*88,89%*	*100%**	*88,89%*
CO - Consentimento	*75,00%*	*87,50%*	*87,50%*
DI - Direito ao Titular	*73,33%*	*86,67%*	*86,67%*

Analisando individualmente o *Zepp*, do ecossistema da *Xiaomi*, é possível concluir que seu termo de serviço é o menos adequado à LGPD, abordando somente o 67,19%

dos critérios de adequação. O *Zepp* incumpre (total ou parcialmente) 15 critérios de adequação, principalmente aqueles relacionados aos direitos do titular, no qual aborda somente o 73,33% dos requisitos. O aplicativo se saiu melhor nas questões de transparência. Nesse quesito, o termo do aplicativo conseguiu cumprir 88,89% dos requerimentos para transparência. Percebeu-se que o termo deste aplicativo é muito genérico, tentando se adequar a várias legislações de vários paises, o que não é o ideal já que cada legislação tem suas especificidades. Não é citado em momento algum no termo, que só é disponibilizado em inglês, a legislação brasileira. Durante a pesquisa, pode se notar aplicação de técnicas de usabilidade no aplicativo *Zepp*, como a criação de um menu dedicado às informações de tratamento de dados, mas as informações não foram suficientes para abordar todos os requisitos que a LGPD solicita.

Em relação ao *App Samsung Health*, este aborda um total de 81,82% dos critérios de compliance médio, sendo o segundo App no nível de adequação. Seu principal mérito foi, também, a transparência com 100% dos seus critérios abordados, mesmo que parcialmente. Possui um termo claro, de fácil acesso e com secções inteiras dedicadas a LGPD. Entretanto, um trecho específico do termo de serviço merece ser ressaltado por ser, do ponto de vista do usuário, bastante abusivo[...].

Do ponto de vista do pesquisador deste trabalho, trecho do termo de serviço do App *Samsung Health*, tenta, da perspectiva da legislação local, forçar ao usuário a abrir mão de todos os seus direitos em caso de danos. A na LGPD prevê a responsabilização do possuidor dos dados em caso de quaisquer danos. Isso demonstra, um termo genérico e/ou desatualizado e, sempre que possivel, evasivo de responsabilidade.

Por sua vez, o aplicativo *Google Fit*, possui o melhor índice de compliance em todos os critérios, destacando-se em todos os temas. Similarmente aos outros aplicativos, o critério de direito do titular é o assunto pior tratado. Percebeu-se que nenhum *App* “permite ao titular de dados meios para recusar ou retirar o consentimento sem prejuízo a qualquer momento". Também nota-se certa dificuldade ainda na portabilidade de dados aos outros fornecedores e serem mais explicidos sobre se irão notificar em caso de falhas de segurança, por exemplo.

O aplicativo com termo de maior conformidade a LGPD foi o *Google Fit* como ilustrado na Tabela 5, estando acima da média dos *Apps* avaliados nesta pesquisa. O acesso aos termos, linguagem e interface amigável ao público não técnico são os principais destaques desse app. Por estar dentro da conta *Google*, que um ponto comum entre os serviços da empresa, pode ter sido um facilitador, pois, como todo um ecossistema da mesma depende disso, tende a ter maior cautela na hora de elaborar os termos de serviço.

O termo de serviço com menor conformidade é o do *App Zepp*. Não possui uma interface amigável ao usuário final, tendo apenas um texto, mal formatado, na tela. Também não tem uma linguagem clara, soando ser uma tradução do termo. Outro problema é a falta de qualquer cuidado em estar em complaince com a LGPD. Entretanto, é importante destacar aqui o *Samsung Health*, que possui um termo bastante abusivo, termo esse que transfere a responsabilidade de algumas ações para o usuário. Devido a sua similaridade de conformidade com o *Google Fit*, foi considera que estão em um empate técnico.

Um dos pontos que mais falham é referente ao direito do usuário. Questões como "O *software* permite a portabilidade de dados a outro fornecedor de serviço ou produto mediante requisição expressa do titular?" e "O *software* informa o titular de dados quando uma decisão foi tomada unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a criação do seu perfil pessoal, possuindo o direito de contestar ou solicitar revisão da decisão?" não são respondidas ou os termos as abragem de maneira muito inconclusivas. Isso cria um ambiente de difícil visualização do que de fato usuários tem direito. De maneira geral, o critério que teve a maior média de conformidade foi o da transparência. Já em CO - Consentimento houve menos falhas, mas os pontos em que precisam de mais atenção são: "O *software* realiza o tratamento de dados pessoais de crianças e adolescentes somente com consentimento específico, de fácil compreensão e em destaque dado pelos pais ou responsável legal, e certifica que é o responsável legítimo que dar o consentimento e que somente ele pode atualizá-lo?" e ""O *software* fornece uma declaração de consentimento de forma inteligível e facilmente acessível, não contendo linguagem e termos abusivos?" que é um agravante já que legalmente, um menor não pode consentir e, por último, não basta apenas ter os termos, precisa está claro para usuário entender o que está consentindo.

Agradecimento

Desde o inicio, vem sido uma luta ardua para escrever a iniciação científica, já que passamos por uma pandemia a qual mexeu com o psicológico de todos. Somado a isso a dificuldade pessoais, a realização do processo parece ficar mais difícil. Agradeço a UNIFEI e as instituições publicas que permitiram essa iniciação. Visto que a universidade pública é financiada por todos

que habitam esse país, tenho profundo agradecimento a todos os cidadões brasileiro. Com muito pesar, também deixo aqui meu respeito aos mais de 700mil mortos pela Covid-19.
No mais, agradeço ao meu pai, Leison Araújo, a minha vó, Maria Geyza, e a minha namorada, Diullye por todo apoio dado durante o processo, além de me ajudar a ter perseverança para terminar a pesquisa. Muito obrigado!

Referências

BRASIL. **Lei no 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Presidência da República, 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm . Acesso em: 14 set. 2022.

GOOGLE. **“PRIVACIDADE & TERMOS“**, 2022. https://policies.google.com/privacy?hl=pt_BR Acessado em: 28 de maio de 2022.

HUAMI.. **“HUAMI PRIVACY POLICY. HUAMI“,** 2021. https://upload-cdn.huami.com/tposts/8192 Acessado em: 20 de maio de 2022.

ARAUJO, Matheus; GARCÉS, Lina. **Relatório: ANÁLISE DE ESTRATÉGIAS DE CONSENTIMENTO DE TRATAMENTO DE INFORMAÇÃO EM SISTEMAS DE IoMT (INTERNET OF MEDICAL THINGS).** 56 pp, 2022.

MENDES, João; VIANA, Davi; RIVERO, Luis. **Developing an Inspection Checklist for the Adequacy Assessment of Software Systems to Quality Attributes of the Brazilian General Data Protection Law: An Initial Proposal.** In: SIMPÓSIO BRASILEIRO DE ENGENHARIA DE SOFTWARE (SBES), 35. , 2021, Joinville. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2021. Acessado em 8 de setembro de 2022.

SAMSUNG. **“Aviso de privacidade do Samsung Health.”** Samsung Health, 2018a. https://samsunghealth.com/privacy. Acessado em 8 de setembro de 2022 .

SAMSUNG. **“TERMOS DO SERVIÇO DO SAMSUNG HEALTH.”** Samsung Health, 2018b. https://samsunghealth.com/terms. Acessado em 8 de setembro de 2022

SAMSUNG. **“Consentimento sobre o processamento de dados de saúde”** Samsung Health, 2018c. https://samsunghealth.com/lgpd?lc=pt&cc=BR&scv=6213001&platform=1&fqdn=samsunghealth.oobe&source=2 Acessado em 8 de setembro de 2022