Análise da Transparência de Dados Pessoais em Políticas de Privacidade de Dados

Thiago Adriano Coleti[1], Marcelo Morandini[2], Lucia Vilela Leite Filgueiras[1], Pedro Luiz Pizzigatti Corrêa[1]

[1]Escola Politécnica da Universidade de São Paulo
Departamento de Engenharia de Computação e Sistemas Digitais
Av. Prof. Luciano Gualberto, tv 3, 158 – 05508-010 – São Paulo – SP – Brasil

[2]Escola de Artes, Ciências e Humanidades da Universidade de São Paulo
Av. Arlindo Bettio, 1000 Ermelindo Matarazzo – 03828-000 – São Paulo - SP – Brasil

{thiagocoleti, mmorandini, lfilguei, pedro.correia }@usp.br

Abstract. *This paper presents a Personal Data Transparency evaluation conducted in applications widely used by traditional users. Transparency aims to provide information about how personal data are collected, used and disclosed among systems and thus, allows the subject to have knowledge about this process and became able to agency it. The research was performed with users that read and evaluated Privacy and Security Policies and answered a survey with 8 questions about issues that must provide transparency. Results presented that some issues were considered transparent, but other, usually related to computer infrastructure need improvements.*

Resumo. *Este artigo apresenta uma avaliação de Transparência de Dados Pessoais realizada em aplicações conhecidas e utilizadas por um grande número de usuários. A Transparência busca proporcionar informações de como os dados pessoais são coletados, utilizados e compartilhados entre sistemas e assim permitir que o indivíduo produtor tenha conhecimento e possa agir dentro deste processo. A pesquisa foi realizada com usuários tradicionais que avaliaram as políticas das aplicações e responderam a um questionário com 8 questões sobre aspectos que deveriam fornecer transparência. Os resultados mostraram que alguns elementos foram considerados transparentes, mas outros, normalmente relacionados à infraestrutura computacional, ainda requerem melhorias.*

1. Introdução

A Transparência de Dados Pessoais (TDP) é a capacidade que sistemas computacionais fornecem aos usuários de compreender como é ou como foi realizada a coleta e uso dos dados pessoais por uma aplicação, assim como os dados utilizados [Mortier et al. 2016]. Utilizar dados pessoais é uma ação realizada por diversos tipos de sistemas [Bonatti et al. 2017] e no século XXI o volume de dados pessoais aumentou significativamente devido ao uso de aplicações como Redes Sociais, GPS, *websites*, *smart devices* e *smartphones* e, portanto, a necessidade de mecanismos que favoreçam a TDP passou a ser fortemente considerada [Hamed Haddadi 2013, Schneier 2015].

A coleta e processamento de dados pessoais são comuns em aplicações de *software*, mas proporcionar informações ao indivíduo produtor dos dados ainda é um desafio e carece de melhorias e padronizações. Muitas das melhorias podem ser justificadas pela dificuldade de apresentar ao usuário de forma clara e compreensível as atividades envolvidas no uso dos dados [Hamed Haddadi 2013, Mortier et al. 2016, Murmann and Fischer-Hübner 2017].

Eventos recentes envolvendo o uso de dados pessoais, tais como divulgação de informações confidenciais, tentativas de influenciar eleições e quebra de sigilo chamaram a atenção de usuários, empresas e autoridades quanto a necessidade de regulamentar/controlar o uso de dados pessoais, principalmente a privacidade, controle e transparência [Mortier et al. 2016]. A Transparência integra essas discussões, pois a mesma, segundo [Murmann and Fischer-Hübner 2017] é um caminho para garantia da privacidade do indivíduo e segundo [Mortier et al. 2016] é um mecanismo para prover ao indivíduo produtor dos dados a capacidade de compreender, agir, negociar e intervir no uso de seus dados pessoais.

No que tange à TDP, pode-se observar duas características simples: (1) as informações sobre TDP são comumente alocadas nas Políticas de Privacidade e Segurança (PPS) que compreendem textos longos, complexos e muitas vezes com linguagens bastante jurídica/técnica; (2) a complexidade da forma de transmitir a TDP leva ao fato de um percentual baixo de pessoas que realizam a leitura dos mesmos. Uma pesquisa de opinião realizada antes deste artigo mostrou um percentual de 86% dos participantes nunca ou raramente leem as políticas, corroborando os achados de [Milne and Culnan 2004].

Assim, a falta de conhecimento sobre o uso dos dados pessoais pode levar o usuário a fornecer dados ou realizar tarefas (muitas vezes desconhecidas) que facilitam a produção e a coleta de seus dados por agentes interessados, neste artigo chamados de controladores, e consequente aprendizado sobre suas ações e/ou seus costumes.

Esta pesquisa teve como objetivo analisar as PPS de aplicações que são comumente utilizadas a fim de verificar como as mesmas empregavam a TDP em 8 aspectos inerentes ao uso de dados pessoais e desta forma analisar se informavam adequadamente ao produtor [1] o processo de uso dos dados. Para preservar a marca dos *softwares* avaliados, os mesmos foram nomeados de forma diferente da nomenclatura comercial. Foram avaliadas as aplicações:

- App-01: Site de compra e venda de veículos;
- App-02: Rede Social;
- App-03: Serviço de e-mail e computação em nuvem;
- App-04: Serviço de serviço de *streaming* de música e vídeo; e
- App-05: Web-Agenda

Destaca-se que as aplicações foram escolhidas devido à: ampla utilização; pela possibilidade de coletar e utilizar dados que de alguma forma reflitam ou identifiquem o seu usuário; e pela modificação recente em suas PPS, em função da entrada em vigor, na Europa, da *General Protection Data Regulation* (GDPR), o que se observou pelo envio de e-mails solicitando aos usuários que revalidassem a aceitação das PPS.

[1] O usuário será designado por indivíduo produtor dos dados ou como titular dos dados.

Para conduzir esta pesquisa as seguintes tarefas foram realizadas: (1) análise das aplicações popularmente conhecidas por um grupo de participantes; (2) resolução de um questionário a fim de identificar a adequabilidade da TDP nas aplicações; e (3) análise das respostas dos questionários;

Na próxima seção será apresentada a Revisão Bibliográfica realizada, enfatizando, mesmo que sumariamente, pontos que nortearam essa pesquisa e a análise dos resultados obtidos.

2. Fundamentação Teórica

Esta seção apresenta conceitos sobre pontos relacionados com a coleta e uso dos pessoais assim como a TDP. Dessa forma, são apresentados os principais conceitos e definições relacionados à Interação Humano Dados e a Transparência de Dados.

2.1. Interação Humano Dados

Pessoas/indivíduos se tornaram exímios produtores e consumidores de dados pessoais. Quando se pensa em dados pessoais, se pensa em qualquer registro digital que permite identificar uma pessoa ou torná-la identificável [Schneier 2015]. A produção destes dados se dá pelo uso de diversos meios tecnológicos que de alguma forma as pessoas utilizam e assim refletem suas preferências, comportamentos e ações [Epstein 2015].

Por outro lado, o consumo se dá pelo uso de um amplo volume de informações produzidas com base no dado do próprio (ou de outro) indivíduo [Crabtree and Mortier 2016]. Tais informações podem ser utilizadas para influenciar ações diárias como: qual estrada está menos congestionada? ou qual produto é mais comprado? ou qual o comportamento de um agente específico?

A produção e o consumo de dados e informações pessoais são apoiadas por áreas como a computação que envolve a Interação Humano Computador (IHC), Aprendizagem de Máquina e Banco de Dados, além de áreas de comportamento como Sociologia e Psicologia. O envolvimento de cada área é considerável e uma nova área de pesquisa/desenvolvimento chamada Interação Humano Dados ou *Human-Data Interaction* (HDI) surgiu com o propósito de estudar fenômenos de interação entre indivíduos e bases de dados [Hamed Haddadi 2013].

Com definições que variam pontualmente, de forma geral, a HDI propõe o estudo e o desenvolvimento de mecanismos para permitir o usuário interagir com grandes bases de dados. Esta interação compreende a capacidade de produção, compreensão da utilização dos dados, capacidade de ação, negociação e utilização de informações [Mortier et al. 2016].

Os desafios da área de HDI são vários e podem ser analisados em [Mortier et al. 2016], mas um deles é foco desta pesquisa e tem total relação com a área de IHC que é a Transparência de Dados Pessoais. A TDP visa proporcionar entendimento ao indivíduo produtor/titular dos dados de os mesmos serão utilizados, compartilhados e divulgados. Para [Bellamy and Alonso 2016] e [Hamed Haddadi 2013] esta divulgação deve ocorrer por intermédio de um ambiente visual que mostre não somente dados brutos e normalizados, mas informações legíveis e compreensíveis do ponto de vista de uma pessoa sem especialização na área de computação. Segundo [Mortier et al. 2013], neste

aspecto a IHC se apresenta como uma área complementar a HDI e responsável por facilita o TDP.

2.2. Transparência de Dados Pessoais

A TDP se tornou um requisito de sistemas que atuam com dados pessoais e deve ser vista como um suporte que visa proporcionar privacidade, segurança e controle do titular sobre os dados produzidos, considerando que, para que o indivíduo possa exercer seus direitos e agir sobre a utilização de seus dados, o mesmo precisa saber quais dados são utilizados e como são processados e/ou divulgados [Mortier et al. 2016, Murmann and Fischer-Hübner 2017].

O volume e a variedade de fins para os quais os dados pessoais são coletados, processados e distribuídos colocou a TDP em evidência como um requisito de sistema influenciando até mesmo o surgimento de leis/regulamentações que buscam propor meios de proporcionar e garantir aos titulares dos dados a capacidade de serem incluídos no fluxo de uso dos dados [Bellamy and Alonso 2016]. Um exemplo de regulamentação é a *General Data Protection Regulation* (GDPR) que é uma regulamentação da União Europeia, mas que pode abranger outros territórios dependendo da forma que os dados são tratados.

A GDPR disponibiliza quatro artigos voltados exclusivamente (ou com grande ênfase) para TDP: Artigos 12, 13, 14 e 15 que abordam direitos e deveres de titulares, controladores e processadores dos dados pessoais. Além destes artigos, a TDP ainda é citada como elemento básico do uso de dados pessoais em diversos outros artigos [Bonatti et al. 2017]. A GDPR entrou em vigor em 25 de Abril de 2018 para todas as organizações que coletam, armazenam, processam e/ou controlam dados pessoais dentro do território da União Europeia.

Considerando a necessidade de apresentar o mínimo ao indivíduo produtor de dados, os *websites* normalmente inserem informações sobre esta utilização em um documento conhecimento como PPS. Este documento que comumente apresenta textos longos e complexos são apresentados ao usuário no momento da aquisição, *download* ou execução de uma ação e seu conteúdo refere-se a práticas de coleta, uso e divulgação de dados pessoais [Earp et al. 2005] . O conteúdo, o detalhamento e a qualidade dos textos varia de acordo com a controladora dos dados que busca proporcionar maior ou menor divulgação destas informações, em muitos casos, somente textos genéricos e incompletos são apresentados.

3. Trabalhos Correlatos

Esta seção apresenta dois trabalhos correlatos que investigaram as PPS considerando o interesse dos usuários pela leitura, a qualidade e a facilidade de compreensão das mesmas.

3.1. *What happen with my data?*

No trabalho intitulado *What happen with my data?* de autoria de [van der Bergen and van der Hof 2012] foi questionado o conhecimento dos usuários em relação ao que é feito com seus dados e como poderia ser melhorada a experiência entre o indivíduo e o processo de utilização de seus dados.

Os autores destacam o fato de existirem leis que obrigam (ou orientam) controladores de dados a informarem seus usuários se existirá uma coleta de dados pessoais além de informar como os dados serão utilizados. Entretanto, as aplicações normalmente notificam o usuário por meio de textos longos, muito técnicos, difíceis de ler e que muitas vezes são ignorados.

Para conduzir a pesquisa um questionário foi aplicado pelos autores e mostrou que 50% dos entrevistados raramente (ou nunca) leem termos de privacidade e uso de dados e 41% nem mesmo verificam se existe. Para os dois casos, menos de 7% dos entrevistados realmente verificam se há regras de uso de dados em *websites* e fazem uma leitura adequada.

Segundos os autores, a justificativa é a falta de um mecanismo fácil de troca de informações sobre a privacidade dos dados, uma vez que as organizações normalmente esperam que os usuários se adaptem as leis enquanto os usuários finais esperam que as empresas proporcionem recursos para facilitar o entendimento dos dados. Foram identificadas técnicas como leitores de políticas, sistemas de rotulação e marcação e também sistemas baseados em ícones, mas concluiu-se que são muito pouco aplicados.

Os autores concluíram que as técnicas analisadas apresentavam falhas que dificultavam o entendimento do processamento dos dados pessoais e da privacidade dos dados. A conclusão foi baseada nos resultados dos questionários aplicados que mostravam que a vontade dos usuários entrevistados não era atendida pelas propostas analisadas, principalmente no que se referia à uma forma mais prática de ler e entender as políticas e ações com os dados.

3.2. *Examining Internet privacy policies within the context of user privacy values.*

O segundo trabalho é apresentado por [Earp et al. 2005] que discute o impacto dos textos das políticas de privacidade ao informar o usuário sobre as ações sobre seus dados e como tais informações podem aumentar a confiabilidade do usuário em relação ao sistema.

A pesquisa focou três questões: (1) qual era a organização mais regulamentada na área de saúde? (2) O que os usuários se preocupam nas políticas de privacidade? e (3) as políticas de privacidade fornecem informações que os usuários desejam saber?

Para condução desta pesquisa foram realizadas tarefas como: para responder a primeira questão foram feitas análises de declarações em políticas de 24 *website* com posterior classificação em uma tabela taxonômica na qual permitiu-se identificar o percentual de uso de determinadas palavras e assim determinar qual *website* apresentava uma política mais completa.

Para responder a segunda questão, os pesquisadores utilizaram de questionários que foram distribuídos para 385 participantes dentro e fora dos Estados Unidos. Após análise estatística os pesquisadores concluíram que as principais preocupações dos usuários estão relacionadas com a coleta (15% mencionaram) e a distribuição/compartilhamento (13 % mencionaram) de seus dados pessoais.

Os dados coletados permitiram responder a terceira questão da pesquisa na qual foi considerado que os *websites*, principalmente os norte-americanos, não disponibilizam PPS adequadas a *Fair Information Practice* (FIP) e que muito ainda deveria ser feito em busca de proporcionar políticas de privacidade mais adequadas para os usuários.

O trabalho discutido mostra o fato de que, em 2005, as políticas de privacidade eram uma preocupação de usuários em relação à coleta e compartilhamento de seus dados pessoais. Isso permite assumir que essa preocupação pode ter aumentado, com o aumento da coleta e uso de dados pessoais, o que pode interferir/comprometer a privacidade de um indivíduo.

3.3. Considerações dos Trabalhos Relacionados

Os trabalhos apresentados buscaram identificar como as PPS eram compreendidas pelos usuários, verificar se existia a preocupação das pessoas em ler as políticas, e identificar os pontos que causavam preocupações. Os resultados de ambos os trabalhos mostraram desinteresse dos indivíduos pela leitura e atribuíram a culpa aos textos técnicos e complexos. Mesmo assim, as organizações ainda não estavam de acordo com normas vigentes.

Entretanto, é possível identificar a preocupação dos indivíduos com o processo de coleta e compartilhamento dos dados. Desta forma, acredita-se que com o amplo uso de tecnologias móveis (*hardware/software*) os dados coletados venham a proporcionar insumos para um cenário muito próximo do realidade do indivíduo.

O presente trabalho procurou contribuir provendo uma avaliação da TDP em PPS. A realização das avaliações por usuários reais tiveram por objetivo verificar se as mesmas permitiam ao indivíduo compreender como será o uso de seus dados e como este uso poderia interferir no seu cotidiano além proporcionar maneiras do titular dos dados agir sobre o uso de seus dados.

4. Materiais e Métodos

A pesquisa foi realizada com 35 participantes com idades entre 18 e 40 anos, alunos dos cursos de Engenharia Elétrica e de Engenharia de Computação da Escola Politécnica da Universidade de São Paulo [2] que apresentavam conhecimentos avançados na área de Computação, mas a nível de iniciante nos assuntos de HDI e TDP. As atividades desta pesquisa ocorreram em Abril de 2018, 1 mês antes da obrigatoriedade da GDPR entrar em vigor. Considerando que todas as aplicações foram selecionadas a partir de email solicitando nova autorização do usuário, acredita-se que estivessem em processo de adequação.

O experimento foi iniciado com uma palestra em que foram apresentados pontos relevantes deste assunto e na qual foi apresentada a seguinte definição de TDP baseada em [Mortier et al. 2016]: *Transparência é a capacidade que uma aplicação tem de informar o usuário titular dos dados quais dados serão coletados, como os dados serão utilizados e/ou compartilhados e quais ações o usuário pode fazer durante o processo de uso dos dados*.

Posteriormente os participantes foram incentivados a escolher as aplicações para analisar suas PPS em relação a TDP. Foi recomendada a escolha de aplicativos e/ou *websites* populares os quais seu uso é considerado amplo e seu contexto de operação poderia permitir a coleta e processamento de dados pessoais para várias finalidades. Os participantes dividiram suas atenções em avaliar os sistemas apresentados na seção de Introdução no qual cada participante avaliou uma aplicação.

[2] https:\\pcs.usp.br

Em conjunto com o processo de avaliação os alunos responderam a um questionário com 8 questões com as possibilidades de respostas: (1) Transparência Inadequada: o usuário não conseguiu compreender quais dados seriam utilizados e/ou qual processo seria realizado; e (2) Transparência Adequada: o sistema conseguiu transmitir ao usuário informações sobre os dados utilizados e as ações realizadas com os dados pessoais. As questões sugeridas foram:

1. Q1: Quais informações são coletadas sobre você;
2. Q2: Como as informações são coletadas;
3. Q3: Como são usadas as informações coletadas;
4. Q4: Como são compartilhadas as informações coletadas;
5. Q5: Como são armazenadas as informações coletadas;
6. Q6: Como é tratada a segurança da sua informação;
7. Q7: Seu acesso à sua informação; e
8. Q8: Transferência da sua informação a terceiros.

No processo de análise dos dados, as questões aplicadas foram classificadas em 3 grupos que refletiam os objetivos de TDP deste trabalho: (1) Dados e mecanismos de coleta (Q1, Q2, Q3 e Q4); (2) Armazenamento e segurança (Q5 e Q6); e (3) Acesso a informação pessoal e Transferência para Terceiros (Q7 e Q8).

5. Análise dos Dados e Resultados

A análise dos dados foi conduzida com base na Análise Descritiva, um processo de estudo dos dados coletados em que os mesmos são resumidos e organizados em tabelas e gráficos para dar suporte suporte a discussão/comparação de aspectos importantes do conjunto de dados [Reis and Reis 2002]. As respostas foram tabeladas para cada pergunta e organizadas por aplicação avaliada. Para cada pergunta foi realizada uma avaliação da opinião dos participantes e realizadas inferências sobre cenários específicos. Os resultados serão apresentados nas Tabelas de 1 a 8 das próximas subseções.

5.1. Dados e Mecanismos de Coleta

Nas Tabelas de 1 a 4 são apresentadas informações relativas às quatro primeiras questões do questionário. Estas questões incentivaram os participantes a verificar se as aplicações forneciam uma visão/compreensão da intenção de uso dos dados pessoais pelos controladores. Os resultados mostraram que as aplicações forneceram informações sobre a intenção do uso dos dados dos indivíduos, pois as respostas dos participantes foram amplamente favoráveis a TDP neste aspecto.

Destaca-se ainda o App-04 que para as 4 questões discutidas apresentou respostas com percentuais entre 90% e 100% de Transparência Adequada o que permite inferir que o mesmo disponibilizou informações adequadas e claras em relação às intenções de uso dos dados. Situação semelhante pode ser vista no App-05, embora sem resultando tão significativo para a TDP Adequada, mas ainda assim, se mostrou bem avaliada.

Uma aplicação não apresentou bons resultados: O App-01 teve avaliação Não Adequada em 2 das 4 questões, tendo sido o único com avaliação negativa nestes aspectos. Acredita-se que a TDP Não Adequada identificada em Q3 e Q4 podem ter interferências nas questões comerciais, pois trata-se de uma aplicação comercial que pode utilizar dados

de pessoas a para melhorar a capacidade estratégica frente aos concorrentes e desta forma, detalhes do uso são omitidos.

Tabela 1. Respostas para Q1

Questão 01: Quais informações são coletadas sobre você.		
Aplicação/Resposta	**Transparência Inadequada**	**Transparência Adequada**
App-01	1	3
App-02	1	4
App-03	1	2
App-04	0	14
App-05	3	6

Tabela 2. Respostas para Q2

Questão 02: Como as informações são coletadas.		
Aplicação/Resposta	**Transparência Inadequada**	**Transparência Adequada**
App-01	1	3
App-02	3	2
App-03	1	2
App-04	0	14
App-05	2	7

Tabela 3. Respostas para Q3

Questão 03: Como são usadas as informações coletadas.		
Aplicação/Resposta	**Transparência Inadequada**	**Transparência Adequada**
App-01	3	1
App-02	1	4
App-03	1	2
App-04	2	12
App-05	2	7

Tabela 4. Respostas para Q4

Questão 04: Como são compartilhadas as informações coletadas.		
Aplicação/Resposta	**Transparência Inadequada**	**Transparência Adequada**
App-01	3	1
App-02	2	3
App-03	1	2
App-04	1	13
App-05	2	7

5.2. Armazenamento e segurança

Neste segundo grupo de questões, o objetivo foi avaliar como a TDP era apresentada no aspecto de segurança dos dados. Ou seja, a capacidade de informar ao usuário quais seriam as estratégias de armazenamento e segurança a fim de garantir a privacidade e evitar que agentes não autorizados tenham acesso aos dados. Os resultados destas questões são apresentados nas Tabelas 5 e 6.

Diferentemente do primeiro grupo de questões, estas apresentaram resultados apontando para Transparência Inadequada. Para a Q5, 100% das aplicações tiveram avaliação inadequada e em Q6, 80% tiveram avaliação inadequada sendo que os outros 20% apresentaram a mesma pontuação para Transparência Adequada e Inadequada.

Acredita-se que a avaliação inadequada pode ser justificada pela utilização de textos genéricos e pouco detalhados para informar sobre questões de armazenamento e segurança tais como: *we will securely store your information and isolate it from any further use until deletion is possible* ou *Este aplicativo utiliza técnicas avançadas para garantir a segurança de seus dados*. Nas frases apresentadas os controladores garantem a segurança, mas não informam qual ou quais as estratégias utilizadas por empresas e locais de armazenamento, assim como regulamentações que serão seguidas para manter os dados.

Outro ponto de interesse associado ao armazenamento e segurança foi o fato das empresas afirmarem que os dados não estão livres de roubo ou invasão (*hacker*) e que não podem garantir que os dados pessoais não serão compartilhados em caso de roubo. Acredita-se que estes fatores não apresentam ao usuário titular dos dados uma visão de segurança além de não fornecer mecanismos para ações em caso de roubo de dados ou em eventuais discordâncias do uso dos dados.

Tabela 5. Respostas para Q5

Questão 05: Como são armazenadas as informações coletadas.		
Aplicação/Resposta	**Transparência Inadequada**	**Transparência Adequada**
App-01	4	0
App-02	5	0
App-03	2	1
App-04	8	6
App-05	5	4

Tabela 6. Respostas para Q6

Questão 06: Como é tratada a segurança da sua informação.		
Aplicação/Resposta	**Transparência Inadequada**	**Transparência Adequada**
App-01	2	2
App-02	3	2
App-03	3	0
App-04	8	6
App-05	4	5

Um fator que pode ter contribuído para que os aspectos avaliados fossem considerados inadequados é a utilização de serviços em nuvem que podem, inclusive, estar em outro país. Desta forma, o controlador pode não ter detalhes técnicos da infraestrutura de segurança e armazenamento para fornecer. Além disto, o armazenamento e a segurança são elementos fortemente dependentes da infraestrutura que pode ser alterada/atualizada de acordo com necessidades, perigos ou custos e estas modificações não são transmitidas ou refletidas diretamente ao controlador e ao usuário o que é uma característica comum da Computação em Nuvem.

Desta forma, assume-se que aspectos de TDP voltados para o armazenamento e a segurança carecem de ações de melhorias.

5.3. Acesso a informação pessoal e Transparência a Terceiros

As questões Q7 e Q8 trataram a TDP para acesso às informações pelos usuários e também informações sobre transferência de dados para terceiros. Os resultados das respostas dessas questões essão apresentados nas Tabelas 7 e 8.

Para a Q7, exceto os App-01 e App-04 que receberam respectivamente uma avaliação Inadequada e um empate entre as avaliações. Demais aplicações foram consideradas Adequadas com 50% de indicações a mais que aquelas classificadas como Inadequadas. Ao realizar uma releitura do termos constatou-se que há explicações adequadas sobre como acessar, atualizar ou obter cópias dos dados.

Tabela 7. Respostas para Q7

Questão 07: Seu acesso à sua informação.		
Aplicações/Resposta	**Transparência Inadequada**	**Transparência Adequada**
App-01	4	0
App-02	1	4
App-03	0	3
App-04	7	7
App-05	3	6

O que tange a transferência de dados para terceiros somente o App-01 teve um empate na sua avaliação. Demais aplicações foram classificados como Adequadas com

destaque para o App-04 que teve mais de 80% de avaliação positiva. Uma avaliação das políticas mostrou que as aplicações destacaram suas relações com terceiros em que ocorrem compartilhamento dos dados, embora não detalhem quem são e quais objetivos levam a troca de dados. Acredita-se que fatores comerciais tenham forte influência nesta transferência assim como aspectos de infraestrutura devido ao fato que algumas empresas terceirizam ações de processamento e armazenamento.

Tabela 8. Respostas para Q8

Questão 08: Transferência da sua informação a terceiros.		
Aplicações/Resposta	**Transparência Inadequada**	**Transparência Adequada**
App-01	2	2
App-02	2	3
App-03	1	2
App-04	3	11
App-05	3	6

Na próxima seção serão apresentadas as considerações finais.

6. Considerações Finais

A Transparência de Dados Pessoais é um elemento fundamental para garantir a privacidade e conhecimento do indivíduo produtor de dados sobre a coleta e utilização de suas informações. A preocupação com este fator cresceu de forma a incentivar a elaboração de recomendações como a GDPR.

Desta forma, este artigo apresentou a avaliação de Políticas de Privacidade e Segurança de 5 aplicações populares, adequadas pelos fornecedores para atender aos requisitos da GDPR, de forma a ver se os mesmos estavam adequados ou não ao conceito de TDP apresentado aos participantes.

Como resultado, foi possível constatar que alguns aspectos foram considerados transparentes e bem avaliados pelos participantes, principalmente no que refere-se a informar que os dados serão coletados e utilizados. Por outro lado, fatores relacionados à infraestrutura e que são mais voláteis como armazenamento, segurança da informação e transferência e acesso ao dados foram avaliados como inadequados; em especial, as informações sobre armazenamento foram classificadas como totalmente inadequadas.

Assim, acredita-se que produtos de aplicações e controladores de dados pessoais estejam procurando proporcionar maior TDP principalmente com o surgimento de regulamentações, mas a Transparência continua transmitida por textos longos, vagos e complexos que compõem a Políticas de Privacidade e Segurança.

Portanto, coloca-se como trabalhos futuros a busca por melhorias na capacidade de transmitir e visualizar TDP de forma mais fácil e prática a fim de evitar a necessidade da leitura de complexos e infindáveis textos. Além disso, pretende-se realizar estudos que comparem numericamente os resultados obtidos com os observados nos trabalhos relacionados para que as avaliações da TDP em políticas de privacidade possam ser melhor fundamentadas e embasadas.

Referências

Ackerman, M. S. and Mainwaring, S. D. (2005). Privacy Issues and Human-Computer Interaction. *O'Reilly & Associates*, pages 1–19.

Bellamy, B. and Alonso, C. (2016). Reframing data transparency _. *Centre for Information Policy Leadership and Telefónica Senior Roundtable*, 1(June):1–20.

Bonatti, P., Kirrane, S., Polleres, A., and Wenning, R. (2017). Transparent Personal Data Processing : The Road Ahead. *Proceedings of International Conference on Computer Safety, Reliability and Secutity - Lecture Notes on Computer Science*, 10489(September):337–349.

Crabtree, A. and Mortier, R. (2016). Personal Data, Privacy and the Internet of Things: The Shifting Locus of Agency and Control. *SSRN Electronic Journal*, pages 1–20.

Earp, J. B., Antón, A. I., Aiman-Smith, L., and Stufflebeam, W. H. (2005). Examining Internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management*, 52(2):227–237.

Epstein, D. A. (2015). Personal Informatics in Everyday Life. (Figure 1):429–434.

Hamed Haddadi, R. M. D. M. J. C. (2013). Human-data interaction. *University of Cambridge*, (837):1–9.

Huang, D., Tory, M., Adriel Aseniero, B., Bartram, L., Bateman, S., Carpendale, S., Tang, A., and Woodbury, R. (2015). Personal visualization and personal visual analytics. *IEEE Transactions on Visualization and Computer Graphics*, 21(3).

Janic, M., Wijbenga, J. P., and Veugen, T. (2013). Transparency enhancing tools (TETs): An overview. *Workshop on Socio-Technical Aspects in Security and Trust, STAST*, (October 2014):18–25.

Milne, G. R. and Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, 18(3):15–29.

Mortier, R., Haddadi, H., and Henderson, T. (2013). Challenges & Opportunities in Human-Data Interaction. *Proceedings of DE2013: Open Digital - The Fourth Annual Digital Economy All Hands Meeting*, pages 4–6.

Mortier, R., Haddadi, H., Henderson, T., Mcauley, D., Crowcroft, J., and Crabtree, A. (2016). Human-Data Interaction: The Encyclopedia of Human-Computer Interaction. *The Encyclopedia of Human-Computer Interaction*, pages 1–48.

Murmann, P. and Fischer-Hübner, S. (2017). Tools for Achieving Usable Ex Post Transparency: A Survey. *IEEE Access*, 5:22965–22991.

Reis, E. A. and Reis, I. A. (2002). *Análise Descritiva de Dados de Pesquisa*. Departamento de Estatística da UFMG.

Schneier, B. (2015). *Data and Goliath. The hidden battles to collect your data and control your world*. Norton, New York.

van der Bergen, B. and van der Hof, S. (2012). What happens to my data? A novel approach to inform users of data processing practices. *First Monday*, 17(7):1–15.