



Princípios de informação equitativa nas políticas de privacidade online de empresas brasileiras

Principles of equitable information in Brazilian firms' online privacy policies

Patricia Zeni Marchiori*

Jaqueline Lopes**

RESUMO

A presente investigação objetiva apresentar os princípios de informação equitativa nas políticas de privacidade dos sites das principais empresas brasileiras (segundo lista da revista americana *Forbes* do ano de 2014). A verificação e análise apoiaram-se em um *checklist* elaborado a partir de documentos emanados pela Federal Trade Commission e pela Organization for Economic Co-operation and Development. O levantamento envolveu 14 empresas selecionadas de um universo de 25, considerando-se o critério de imediatez de acesso à política de privacidade nos respectivos sites. O princípio de segurança é o fundamento mais difundido nas políticas de privacidade das empresas selecionadas (existente em 8 das 14 políticas analisadas), e o princípio de responsabilidade é o de menor aderência, pois não está contemplado em quaisquer das políticas de privacidade *online* examinadas. A Sabesp apresenta a política de privacidade da *web* mais completa diante dos princípios de informação equitativa, se comparada às outras políticas analisadas, enquanto que a WEG não apresenta qualquer um dos

ABSTRACT

This article aims to present the Fair Information Principles in the privacy policies of the websites of major Brazilian companies (according to the 2014 Forbes Magazine list). The research and analysis were supported by a checklist compiled from documents issued by the Federal Trade Commission and the Organization for Economic Co-operation and Development. The study selected fourteen companies from a universe of twenty-five, considering the immediacy criterion of access to the privacy policy on their websites. The security (safeguards) principle is the most widespread foundation in the privacy policies of the companies selected (existing in eight of the fourteen analyzed policies); and the principle of responsibility receives less adherence since it is not covered in any of the examined online privacy policies. The Sabesp Company presents the most complete privacy policy, considering the compliance with the Fair Information Principles when compared to the others perused, while WEG does not present any of the principles identified in the documental survey. As for e-commerce, the number of companies that assume some of the Principles is even smaller. For

* Doutora em Ciências da Comunicação pela USP. Professora titular da Universidade Federal do Paraná. Endereço: Av. Prefeito Lothário Meissner, 632, Campus III, Jardim Botânico, CEP 80210-170, Curitiba, PR. Telefone: (41) 3360-4421. E-mail: pzeni@ufpr.br

** Bacharel em Gestão da Informação. Analista de Controle – Logística na Ambev CDD Curitiba. Endereço: Rua Alfredo Pinto, 1.124, Afonso Pena, CEP 83065-150, São José dos Pinhais, PR. Telefone: (41) 3283-8204. E-mail: jaqe_lopes@hotmail.com

princípios identificados no levantamento documental. Quanto ao comércio eletrônico, o número de empresas que assume algum princípio é ainda mais reduzido. Conclui-se que, para o universo selecionado, a adesão aos princípios de informação equitativa é incipiente ainda que se ressalte a sua não obrigatoriedade. A discussão aberta do projeto de lei de proteção de dados pessoais no Brasil deverá ter um papel importante na criação de orientações mais completas na temática. Propõem-se estudos adicionais envolvendo a percepção de usuários de tais sites, assim como um recorte de empresas voltadas diretamente ao comércio eletrônico, considerando-se que este contexto pode exigir o alinhamento efetivo aos princípios e outras orientações voltadas à proteção da privacidade e dos dados pessoais no ambiente *web*.

Palavras-chave: Princípios de Informação Equitativa; Política de Privacidade *Online*; Proteção de Dados Pessoais.

the selected universe, adherence to the Fair information Principles is still incipient, and its use is not mandatory. An open discussion of the proposed Brazilian law about personal data protection should play an important role in creating further guidance on the subject. Additional studies in this subject should involve the perception of users, as well as a cutout of companies which target e-commerce, considering that an effective alignment with these principles and other guidelines are required in order to protect the user's privacy and personal data in the web environment.

Keywords: Fair Information Principles; Privacy Policies; Personal Data Protection.

INTRODUÇÃO

Desde o início das operações comerciais da internet, no final de 1995, o número de usuários no Brasil vem crescendo a taxas elevadas (ENDLER, 2000). Segundo dados da Pesquisa Nacional por Amostra de Domicílios (PNAD) – do Instituto Brasileiro de Geografia e Estatística (IBGE) –, mais de 50% dos brasileiros estavam conectados à internet em 2013, e a proporção de internautas subiu de 49,2% para 50,1% entre os anos 2012 e 2013 (GRUPO GLOBO, 2014).

Para Ciglio (2013), o ambiente em rede – especialmente no âmbito das transações *online* – resulta na coleta e manipulação de quantidades significativas de dados que, não raro, incluem informações pessoais de clientes ou usuários. Mesmo em organizações que tradicionalmente não pertencem ao ramo da tecnologia, agravam-se problemas de privacidade e de segurança digital, o que pode impactar não apenas diretamente nos negócios, mas também na confiança dos consumidores diante de tais organizações (CIGLIO, 2013).

A coleta de informações de clientes e usuários de um *site* comercial, por exemplo, pode ser identificada sob duas condições iniciais, e não mutuamente exclusivas: a) na recolha e retenção de dados para cadastro/acesso a páginas restritas ou como resposta a pesquisas/levantamentos feitos no *site*; e b) nas transações de comércio eletrônico. Assim, as questões de privacidade, confiabilidade e segurança tornam-se mais críticas com o crescente dinamismo no trâmite de dados quando comparados com formas tradicionais de cadastro e comercialização (PEREIRA; PRADO, 2009).

Nas últimas décadas, o assunto privacidade de dados pessoais tem sido discutido de forma mais intensa. Lins (2000) esclarece que são essencialmente três os fenômenos que vêm contribuindo para uma maior atenção ao tema: 1) a estruturação de bases

de dados que possibilitam o cruzamento de informações com facilidade, rapidez e baixo custo e – não raro – sem a ciência dos envolvidos; 2) a disseminação dos recursos informáticos, que estimulam a transposição e a guarda de informações em formato digital; e 3) a padronização de equipamentos e sistemas que facilitam a coleta de informações em distintas instâncias, inclusive sem o conhecimento do fornecedor dos dados (LINS, 2000). Esse fato tem alterado toda a estruturação do direito à privacidade e mostrado como os sistemas de proteção à privacidade são frágeis (MAIA, 2011).

Termos de uso e políticas de privacidade de sites – quando existentes – normalmente apresentam responsabilidades de uso/navegação e, idealmente, deveriam esclarecer, respaldar e sustentar vínculos de transparência entre as organizações e seus clientes/usuários, em especial quanto à amplitude da proteção de dados pessoais.

Bonner e Chiasson (2005) esclarecem que governos e empresas/organizações têm, historicamente, se baseado em um conjunto de preceitos formais/processuais (p. ex., limitação de uso) e materiais/substantivos (p. ex., consentimento) – conhecido como *Fair information principles/practices* (Princípios/práticas de informação equitativa/FIPs) – e entendido como uma garantia mínima da privacidade, da autonomia e da não interrupção do fluxo de dados nos ambiente tecnológicos típicos da sociedade contemporânea (ROTENBERG, 1998; CATE, 2006). Os FIPs, na visão de Gellman (2011), são um conjunto de práticas reconhecidas internacionalmente, que abordam as condições em que se dá a privacidade das informações sobre os indivíduos. De acordo com o autor, os FIPs são importantes porque fornecem uma política subjacente a leis nacionais que tratam de questões de privacidade e proteção de dados, sendo sua evolução proveniente de diferentes formulações de diversos países e de variadas fontes ao longo das décadas (GELLMAN, 2011).

Da mesma forma que para os governos, os FIPs passaram a ser reconhecidos como um alicerce para as políticas de privacidade de empresas na ausência de legislações que tratem especificamente da questão da privacidade de dados pessoais, sendo que os atuais esforços para estabelecer a proteção da privacidade na ambiência *web* geralmente se concentram na aplicação de tais princípios (ROTENBERG, 1998).

Portanto, considerando-se a (ainda) ausência, em território brasileiro, de uma lei relativa à proteção de dados pessoais, e a importância de uma relação simétrica e de transparência entre empresas com presença na *web* junto a seus clientes, a investigação se propôs a responder a seguinte questão de pesquisa: as políticas de privacidade *online* de empresas brasileiras expressam os princípios de informação equitativa (FIPs)?

PROCEDIMENTOS METODOLÓGICOS

Os seguintes critérios foram aplicados para se identificarem – das 25 empresas brasileiras de capital aberto do mundo –¹ aquelas a serem examinadas quanto às FIPs: a) existência do *link* de acesso à política de privacidade na *homepage* do *site* da empresa (descartaram-se aquelas cujo acesso ao *link* exigia dois ou mais cliques); b) existência, no *site* da empresa, de páginas que ofereciam/exigiam algum tipo de

¹ Listadas no *ranking* das maiores companhias públicas globais (FORBES, 2014).

entrada de dados pelo usuário/visitante; tal entrada de dados é entendida, no contexto desta pesquisa, como tendo algum grau de retenção de dados pessoais.

Das 25 empresas listadas pela Forbes (2014), 14 tiveram suas políticas de privacidade examinadas em detalhe. São elas (por ordem de posição no *ranking*): Petrobrás, Vale, JBS, Grupo Pão de Açúcar, BRF Brasil Foods, Oi, Cemig, Eletrobrás, Sabesp, CPFL Energia, Braskem, Metalúrgica Gerdau, Porto Seguro, WEG.

Os parâmetros FIP que fundamentam este estudo foram desenvolvidos por duas instituições internacionais: a Federal Trade Commission (FTC) e a Organization for Economic Co-operation and Development (OCDE). A FTC² lista quatro princípios de informação equitativa, enquanto a OCDE,³ oito. Ainda que o domínio de aplicação seja distinto em cada uma dessas organizações, ambos os conjuntos de FIPs respaldam a elaboração de políticas de privacidade, respeitando os dados pessoais do usuário de informação, em especial quando este navega e/ou insere dados em *sites*.

Ao se analisarem tais parâmetros, três princípios de cada organização foram considerados similares em seu conteúdo e finalidade de aplicação, a saber:

- a) “Segurança” da FTC e “Salvaguardas de segurança” da OECD. Tais princípios estipulam que a organização toma medidas complementares – contra riscos de perda ou acesso não autorizado, destruição, divulgação ou alteração –, de forma a garantir a segurança das informações coletadas dos consumidores. Ambos foram identificados como “Segurança”.
- b) “Acesso” da FTC e “Participação individual” da OECD. Tais princípios visam esclarecer aos usuários que estes têm pleno acesso às informações recolhidas sobre eles, incluindo oportunidades para que eles as analisem, complementem, corrijam imprecisões ou excluam informações. Para fins de análise, ambos são identificados como “Acesso”.
- c) “Nota” da FTC e “Abertura” da OECD. São princípios que definem que a organização se obriga a fornecer avisos claros e visíveis no *site*, quanto às práticas relativas aos dados pessoais de seus consumidores. Materializadas como parte de uma política, devem incluir alertas sobre o tipo de informação/dados coletados, a forma de coleta, os tipos de uso, as garantias de acesso e segurança a essas informações; e se estas são repassadas a outras entidades/parceiros (e de que forma). Ambos foram identificados como “Abertura”.

O princípio “Escolha” da FTC implica que as organizações são obrigadas a oferecer aos consumidores condições de escolha quanto à forma como suas informações de identificação pessoal são utilizadas para além do uso para os quais elas foram fornecidas inicialmente. Usos secundários internos, tais como o *marketing* de retorno a tais consumidores, e usos secundários externos – tais como a divulgação de dados a outras entidades/parceiros – devem ser passíveis de escolha explícita por parte do usuário.

² Disponível em: <<https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf>>.

³ Disponível em: <<http://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>>.

Os demais princípios da OCDE são: a) limitação de coleta: definição de um limite para a coleta de dados pessoais, assim como da sua obtenção por meios legais e justos e, quando apropriado, com o conhecimento do sujeito dos dados; b) qualidade de dados: os dados pessoais coletados/armazenados devem ser relevantes para os propósitos para os quais serão utilizados e, na extensão necessária desses propósitos, devem ser precisos, completos e atualizados; c) especificação de propósito: os propósitos para os quais dados pessoais são coletados devem ser especificados *a priori* ou no momento da coleta, e a subsequente utilização deve se limitar ao cumprimento desses propósitos. Demais propósitos que sejam incompatíveis com os definidos inicialmente devem ser especificados a cada mudança (de propósitos); d) limitação do uso: dados pessoais não devem ser divulgados, tornados disponíveis ou usados em desacordo com os propósitos declarados, a não ser que isso seja realizado com o consentimento do sujeito dos dados ou pela autoridade da lei; e) responsabilidade: exige-se que se aponte um controlador de dados responsável pelo cumprimento e medidas de efeito aos demais princípios.

Da compilação definida, nove princípios foram então listados para serem identificados conforme sua presença ou ausência nas políticas de privacidade das empresas selecionadas. Em um segundo momento, verificou-se se estas oferecem serviços e práticas de comércio eletrônico, entendidos como sendo "a compra e a venda de informações, produtos e serviços através de redes de computadores" (ALBERTIN, 1998, p. 57). Para a compilação dos dados, criou-se uma matriz (Quadro 1)

Quadro 1 – Matriz de verificação da existência de FIPs nas políticas de privacidade online de empresas brasileiras listadas no ranking das maiores companhias públicas globais, segundo a Forbes, 2014.

EMPRESA	Comércio eletrônico	PRINCÍPIOS DE INFORMAÇÃO EQUITATIVA								
		FTC e OECD			FTC	OECD				
		Segurança	Acesso	Abertura	Escolha	Limitação de coleta	Qualidade de dados	Especificação de propósito	Limitação do uso	Responsabilidade
1 Petrobrás										
2 Vale										
3 JBS										
4 Grupo Pão de Açúcar										
5 BRF - Brasil Foods										
6 Oi										
7 Cemig										
8 Eletrobrás										
9 Sabesp										
10 CPFL Energia										
11 Braskem										
12 Metalurgia Gerdau										
13 Porto Seguro										
14 WEG										

Fonte: Elaborado pelas autoras [Dados coletados no primeiro semestre de 2015].

Na coluna "Comércio eletrônico", buscou-se verificar o oferecimento dessa modalidade via seu *site*, indicando-se três opções de preenchimento: a) direto: quando é evidente que a instituição oferece a possibilidade de se efetivar transações comerciais através de seu *site*; b) indireto: aplicável quando as empresas analisadas são caracterizadas como grupos organizacionais que têm diversas corporações e marcas em sociedade, e que estas oferecem opções de comércio eletrônico (o "Grupo Pão de Açúcar", p. ex., não promove venda de produtos e serviços pelo seu *site* institucional, mas via a marca de varejo "Extra"); c) inexistente: quando a empresa não viabiliza qualquer forma de comércio eletrônico em seu espaço *web*.

A leitura das políticas de privacidade exigiu nova codificação no preenchimento da matriz, a saber: a) utilização da cor preta para a evidência explícita/nítida do uso do princípio de informação equitativa. Ou seja, o princípio é verificado como "palavra-chave". Indicou-se, nesses casos, o parágrafo no qual o termo ocorre; b) utilização da cor cinza para uma evidência implícita, ou seja, apesar do termo que caracteriza o princípio de informação equitativa não estar exposto na política de privacidade, verifica-se um conceito similar de sua aplicação; e c) não preenchimento, quando não se localizou explícita ou implicitamente o princípio na política de privacidade *online* da empresa.

Além do levantamento, procedeu-se a uma análise relativa às condições e consequências da incorporação (ou não) dos FIPs, assim como uma reflexão sobre o atual cenário da proteção de dados pessoais no País.

OS PRINCÍPIOS DE INFORMAÇÃO EQUITATIVA E SUAS CONTRADIÇÕES

Ao assumir que a internet oferece uma série de oportunidades para as empresas reunirem um vasto leque de informações pessoais dos consumidores, a FTC considera que é possível estabelecer um nível básico de proteção da privacidade para todos os visitantes de sites comerciais, assim como reconhece que o acolhimento dessas práticas pode variar de acordo com a natureza das informações recolhidas e os usos a que se destinam, bem como com o aparato tecnológico envolvido. Por esta razão, a Comissão responsável redigiu, no ano 2000, os princípios em termos gerais (e tecnologicamente neutros) e de forma ampla o suficiente para proporcionar flexibilidade para a organização que pretender aplicá-los (FTC, 2000)

Anteriormente à FTC, a OCDE desenvolveu e aprovou, em 23 de setembro de 1980, oito princípios que podem ser complementares à legislação de um país ou servir de base a nações que carecem de amparos legais no âmbito da proteção de dados pessoais. As orientações, na forma de recomendações da Organização – e entendidas como princípios que auxiliam na divulgação e no uso de informação equitativa em transações no ambiente *web* – foram impulsionadas a partir do reconhecimento de que o processamento automático de dados permite que quantidades significativas deles sejam transmitidas em frações de segundos por fronteiras internacionais, exigindo, assim, movimentos voltados à proteção dos dados pessoais. Tal esforço existe para evitar violações à privacidade – como direito humano fundamental –, que podem ser exemplificadas como o armazenamento ilegal e inexato de dados pessoais; e o abuso e divulgação não autorizada de tais dados. Vale ressaltar que as recomendações estabelecidas pela OCDE visam estabelecer medidas de proteção à privacidade e liberdade individuais, instituir normas e práticas compatíveis com um novo cenário mundial e, ainda, preservar a livre circulação de dados (OECD, 2013).

A OECD definiu o contexto de aplicação de seus princípios, não apenas ao ambiente informatizado, mas ao processamento de dados em geral, independentemente da tecnologia empregada. Os princípios assumem que há uma relação entre a coleta e a utilização de dados pessoais, quer para a tomada de decisão, quer para pesquisas (ou fins semelhantes), que, dependendo da forma de tratamento, de sua natureza ou de seu contexto, podem oferecer perigo à privacidade e ao direito individual (OECD, 2013).

Outras entidades realizaram esforços no quesito privacidade de dados pessoais. A comissão de Informação e Proteção da Vida Privada de Ontário/Canadá, dr^a. Ann Cavoukian, desenvolveu o conceito do *privacy by design* (PbD) na década de 1990,

com o objetivo de enfrentar os progressivos efeitos sistêmicos das TICs e das redes, e o consequente crescimento no tráfego de dados pessoais (PBD, [2014]). Contudo, esse recorte não será utilizado para fins deste estudo.

Bonner e Chiasson (2005) esclarecem que vários países e governos criaram legislações relativas à privacidade com base nos FIPs, e que empresas privadas já assumiram a necessidade de indicar tais princípios em suas políticas de privacidade e termos de uso em seus sites. No entanto, os autores consideram, com base em uma análise histórica de legislações de privacidade, que os FIPs paradoxalmente levam à redução da privacidade, em vez de protegê-la (BONNER; CHIASSON, 2005). Os autores explicam que isso se deve a três pontos-chave:

[...] First, FIP has come to assume multiple and even contradictory meanings, despite its narrow constitution [...]. Second, early ICT has played a critical role in the construction of the privacy problem and its solution, while the evolving constitution has invalidated many of the assumed protective features of FIP. Finally, we must address the asymmetrical concept of balance embedded in the dominant discourse, in practice (BONNER; CHIASSON, 2005, p. 283).⁴

Os autores afirmam que, pelo menos por parte da OECD, os princípios de informação equitativa foram assumidos pela conveniência dos envolvidos – tais como os meios de comunicação, partidos políticos e grupos de interesse – e via ações coercitivas, em vez de serem gerados por meio de debate público (BONNER; CHIASSON, 2005).

A mudança nas TICs, desde a criação dos FIPs, é outra condição destacada pelos autores. Segundo eles, o surgimento de recursos de computação descentralizados e o aumento da mobilidade e portabilidade de dados colocaram em dúvida o direito de um indivíduo de poder controlar o uso de suas próprias informações e, assim, a suposta facilidade de monitoramento decorrente do uso dos FIPs. Por exemplo, o princípio de abertura (princípio 6/OECD) considera que as pessoas estão cientes da localização e detenção de dados sobre si mesmos. Porém, com a computação descentralizada, os indivíduos têm pouca chance de saber onde essa informação efetivamente reside, pois podem existir replicações e cópias em diferentes repositórios. Isso limita a capacidade dos indivíduos para exercer controle sobre o uso subsequente da informação (princípio 4/OECD), e sua capacidade em identificar o destino de seus dados para: a) poder, eventualmente, alterá-los (princípio 7/OECD); b) conhecer o responsável pela base que detém seus dados (princípio 8/OECD); e c) ter conhecimento quanto à precisão e segurança desses (princípios 5 e 2/OECD) (BONNER; CHIASSON, 2005). Bonner e Chiasson (2005) sugerem que o papel dos FIPs – como resposta à questão de como proteger a privacidade individual – é questionável, devido à volatilidade e replicação dos conteúdos em distintos contextos/sistemas/repositórios.

⁴ [...] Em primeiro lugar, os FIPs têm assumido significados múltiplos e até mesmo contraditórios apesar de sua estruturação restrita [...]. Em segundo lugar, desde o início, as TICs têm desempenhado um papel fundamental nos contornos do problema de privacidade e de sua solução, ainda que a evolução do entorno tenha invalidado muitas das características de proteção assumidas pelos FIPs. Finalmente, temos de abordar, na prática, o conceito assimétrico do equilíbrio embutido no discurso dominante. [tradução livre]

Cate (2006), não obstante, concorda que o atual uso dos FIPs tem fracassado, pois a abordagem desses princípios, especificamente os desenvolvidos pela FTC, transformou as indicações de limitação de coleta, de finalidade de uso e de transparência em meros avisos e solicitação de consentimento. Para a autora, o sistema de proteção de dados baseada nos FIPs não está funcionando, pois apesar dos avisos concederem aos indivíduos uma ilusão de maior privacidade, estes não reforçam sua proteção. Os indivíduos e as empresas criam/acessam documentos de efeito burocrático enquanto falham em oferecer melhores alternativas (CATE, 2006). O descontentamento com a efetiva utilidade de tais “avisos” deve-se ao fato de que estes – ainda que tenham sido elaborados para facilitar a participação do usuário quanto aos seus próprios dados pessoais – são geralmente ignorados pelo público, quer por desconhecimento ou porque tais informes não conseguem provocar qualquer resposta (negativa ou positiva) dos seus destinatários (CATE, 2006). Ainda para Cate (2006), as organizações podem ser motivadas a apresentar um “bom comportamento” quanto ao processo de informar os usuários sobre as condições de coleta e uso de seus dados pessoais. Porém, se o gasto de obtenção do consentimento dos usuários é comparativamente mais alto do que a percepção econômica do uso dos dados, o consentimento perde valor (CATE, 2006).

Como uma crítica geral aos FIPs, o equívoco estaria na adoção – pelos legisladores, políticos e organizações em geral – de tais princípios como um conjunto de normas mínimas que, na prática, são tratados como máximas (BONNER; CHIASSON, 2005).

Para Cate (2006), as FIPs falharam na prática, pois os

[...] data protection regimes built on them are not delivering a high standard of effective, predictable, and efficient data protection, or meaningful consistency among nations or regions. [...] FIPs have been used to glorify individual choice as if that, and not appropriate privacy protection, were the goal of data protection. While privacy advocates and policymakers cling tenaciously to FIPs, at least in their rhetoric, the reality is that FIPs as applied today largely disserve both privacy and other important societal interests (CATE, 2006, p. 27).⁵

No entanto, apesar das contradições quanto ao uso dos FIPs, os documentos que retratam os princípios de informação equitativa ainda são relevantes para o atual esforço de preservar a privacidade na sociedade da informação, pois não há, ainda, alternativa que venha a substituí-los (ROTENBERG, 1998).

DISCUSSÃO E ANÁLISE DOS RESULTADOS

Após a verificação do uso dos princípios de informação equitativa nas políticas de privacidade *online* de cada uma das empresas selecionadas para a pesquisa, procedeu-se ao preenchimento da matriz (Quadro 2). Ressalta-se, inicialmente, que a política de privacidade *online* da empresa JBS não estava disponível durante o

⁵ [...] regimes de proteção de dados desenvolvidos a partir [de tais princípios] não resultam em um nível eficaz, previsível e eficiente de proteção de dados, ou trazem uma consistência significativa entre as nações ou regiões. [...] Os FIPs têm sido usados para enaltecer a escolha individual, como se isso, e não a efetiva proteção da privacidade fosse o objetivo de proteção de dados. Enquanto os defensores da privacidade e os responsáveis políticos se apegarem tenazmente aos FIPs (pelo menos retoricamente), a realidade é que os FIPs, como aplicados hoje, prestam um desserviço aos interesses relativos à privacidade e outros socialmente importantes [tradução livre].

período de coleta de dados (primeiro semestre de 2015). Identificou-se um *link* de acesso, mas a página não apresentava conteúdo, não se podendo afirmar se tal dificuldade era temporária. A política de privacidade da WEG voltava-se única e exclusivamente às condições relativas aos direitos autorais de textos e imagens expostos no *site*.

Quadro 2 – FIPs declarados implícita ou explicitamente nas políticas de privacidade online das empresas brasileiras listadas no ranking das maiores companhias públicas globais, segundo a Forbes, 2014.

EMPRESA	Comércio eletrônico	PRINCÍPIOS DE INFORMAÇÃO EQUITATIVA								
		FTC e OECD			FTC	OECD				
		Segurança	Acesso	Abertura	Escolha	Limitação de coleta	Qualidade de dados	Especificação de propósito	Limitação do uso	Responsabilidade
1 Petrobrás	Inexistente							§ 14		
2 Vale	Inexistente									
3 JBS	Indireto									
4 Grupo Pão de Açúcar	Indireto									
5 BRF - Brasil Foods	Indireto									
6 Oi	Direto									
7 Cemig	Inexistente	§ 5								
8 Eletrobrás	Inexistente									
9 Sabesp	Inexistente	§ 15								
10 CPFL Energia	Inexistente	§ 12								
11 Braskem	Inexistente									
12 Metalurgia Gerdau	Inexistente									
13 Porto Seguro	Direto	§ 15								
14 WEG	Inexistente									

Legenda: ■ Princípio explícito; ▒ Princípio implícito; □ Princípio não encontrado.

Fonte: Elaborado pelas autoras.

Nas políticas de privacidade da Braskem e da CPFL Energia, foram constatadas a existência de seis dos nove princípios; e nas políticas da Petrobrás e Porto Seguro, há um alinhamento com sete FIPs. A Sabesp tem a política de privacidade *online* mais completa se comparada às outras 13 políticas analisadas, ainda que se ressalte que o princípio "responsabilidade" – que dita que um controlador de dados deve ser o responsável pela implantação e controle dos demais princípios de informação equitativa na política de privacidade – não tenha sido identificado nas políticas de privacidade das empresas selecionadas. Ou seja, em nenhuma dessas políticas havia a indicação de uma pessoa física responsável pelo documento *online* e seu cumprimento.

O princípio "escolha" foi identificado apenas na política de privacidade da Sabesp, e o princípio "acesso" existe de forma implícita em políticas de privacidade *online* de quatro empresas (Sabesp, Petrobrás, Braskem e Porto Seguro). Tais empresas, portanto, assumem o compromisso de garantir o acesso às informações recolhidas dos usuários, incluídas aí as oportunidades para que o indivíduo as analise, complementemente, corrija imprecisões ou mesmo exclua informações sobre si mesmo.

Os princípios "especificação de propósito" (que dita que os sites devem especificar os propósitos da coleta de dados e se limitar a estes) e "limitação do uso" (que dita que os dados pessoais não devem ser divulgados, tornados disponíveis ou usados em desacordo aos propósitos declarados de coleta) estão presentes em sete políticas de

privacidade das empresas. A “especificação de propósito” encontra-se explicitada apenas na Petrobrás, ainda que tenha sido identificada, implicitamente, em outras seis organizações (Vale, Sabesp, CPFL Energia, Braskem, Metalurgia Gerdau e Porto Seguro). Quanto à “limitação de uso”, esta aparece de forma implícita nas políticas de privacidade *online* de sete empresas: Petrobrás, BRF Brasil Foods, Eletrobrás, Sabesp, CPFL Energia, Braskem, e Porto Seguro.

Petrobrás, BRF Brasil Foods, Oi, Sabesp, CPFL Energia, Braskem, Metalurgia Gerdau e Porto Seguro se comprometem em suas políticas de privacidade *online* a coletar apenas dados pessoais relevantes para a finalidade declaradas de uso (princípio da “qualidade de dados”).

Os princípios “abertura” e “limitação de coleta” estão presentes – de forma implícita – em nove políticas de privacidade *online*. As mesmas empresas⁶ que atenderam ao princípio de “abertura” igualmente respeitam o princípio da “limitação de coleta”. Pode-se considerar que, ao atenderem ao princípio “abertura”, as empresas tenham aderência também ao princípio de “limitação de coleta” dos dados pessoais.

O princípio “segurança” é o fundamento mais difundido quando comparado aos demais princípios de informação equitativa. De um total de quatorze, quatro empresas tratam desse conceito em suas políticas de privacidade de forma explícita (Cemig, Sabesp, CPFL Energia e Porto Seguro), e outras quatro de forma implícita (Petrobrás, Vale, Grupo Pão de Açúcar e BRF Brasil Foods). Assim, tais empresas se comprometem a efetivar medidas complementares para garantir a segurança das informações que coletam de seus consumidores, especialmente contra riscos de perda ou acesso não autorizado, destruição, divulgação ou, ainda, alteração indevida.

Ao assumir que o comércio eletrônico tramita dados de natureza “mais delicada” – tais como informações bancárias e de endereço, por exemplo –, esperava-se que as empresas que operam com o comércio de serviços e produtos via *web* mostrassem maior comprometimento com os dados pessoais.

Nesse particular, a pesquisa apontou que, das quatorze analisadas, duas empresas oferecem diretamente comércio eletrônico, mas diferem quanto à aplicação dos FIPs em suas políticas de privacidade *online*. A Porto Seguro explicita sete dos nove princípios equitativos de informação no documento, demonstrando um maior alinhamento a estes, quando comparada com a Oi (um FIP explicitado).

Das três empresas que oferecem o comércio eletrônico de forma indireta (via suas redes de comércio), a JBS não apresenta quaisquer dos princípios, o Grupo Pão de Açúcar se compromete com apenas um (princípio de segurança), e a BRF Brasil Foods com cinco princípios.

Causa espécie o fato de as políticas de privacidade de três empresas, das cinco que disponibilizam funcionalidades de comércio eletrônico, estarem desalinhadas com os princípios de informação equitativa. A existência dos princípios poderia auxiliar na percepção, pelos usuários/clientes, de que a empresa oferece um serviço *online* de forma responsável e ética, com preservação de direitos fundamentais aos envolvidos nas transações eletrônicas, resultando em uma vantagem competitiva.

⁶ Petrobrás, Vale, BRF Brasil Foods, Cemig, Sabesp, CPFL Energia, Braskem, Metalurgia Gerdau e Porto Seguro.

CONSIDERAÇÕES FINAIS

Os princípios de informação equitativa – principalmente em ambientes de presença e serviços *online* – se traduzem em diretrizes que sustentam uma política de privacidade voltada ao compromisso ético na troca de informações, e que vem em auxílio à percepção de uma relação respeitosa entre empresa e cliente, pautada por vínculos de transparência. No entanto, devido às contradições ressaltadas, os FIPs não devem ser tratados de forma absoluta, ainda que sirvam como uma base inicial para a elaboração de políticas de privacidade objetivas, claras, acessíveis e críveis.

Ainda que não se possa confirmar, no escopo deste estudo, se as empresas adotam os FIPs a partir do efetivo reconhecimento destes – pois nenhuma empresa revela explicitamente que segue alguma normativa relativa a eles em seu espaço *web* –, os dados da pesquisa permitem afirmar que as políticas de privacidade das empresas analisadas apresentam, à exceção da Sabesp, um comprometimento mínimo com a aplicação dos princípios de informação equitativa. No entanto, não se pode alegar que a falta de alinhamento de tais políticas de privacidade com os princípios se configura em desrespeito quanto à privacidade e segurança de dados pessoais de seus consumidores, pois os FIPs – entendidos como parâmetros de boas práticas e de utilização não obrigatória – podem não ter sido estimulados no cenário brasileiro.

Porém, para empresas que oferecem comércio eletrônico – e, portanto, têm uma relação de coleta de dados mais intensiva e aprofundada com o usuário –, os resultados são preocupantes. Contudo, no primeiro semestre de 2015, o Brasil enfim propôs um debate público⁷ voltado às questões de privacidade de dados da esfera privada. Promovido pelo Ministério da Justiça, está em discussão o anteprojeto de lei de proteção de dados pessoais, que tem por objetivo garantir e proteger, no âmbito do tratamento desses dados, a dignidade e os direitos fundamentais da pessoa, particularmente em relação à sua liberdade, igualdade e privacidade pessoal e familiar, nos termos do art. 5º, incisos X e XII da Constituição Federal. Considera-se tal medida passo importante para que o comprometimento dos envolvidos na troca, coleta e uso de informações possa ser respaldado e assegurado por autoridades de lei no país. Por conseguinte, a aplicação dos FIPs – como é recomendável – pode servir como elemento complementar à aplicação de uma legislação, sensibilizando os usuários de ambientes *online* para os seus direitos nesse particular.

Outras questões que não foram abordadas diretamente nesta pesquisa podem estimular estudos subsequentes na temática, tais como o envolvimento e a percepção dos usuários quanto ao entendimento dos princípios de informação equitativa (e os avisos e escolhas colocados à sua disposição). Sugere-se, igualmente, a continuidade dos levantamentos, incluindo-se os termos de uso dos sites das empresas selecionadas e se aprofundando a análise de outras condicionantes às políticas de privacidade. Ainda como indicação para trabalhos futuros, recomenda-se o estudo com empresas – não necessariamente classificadas quanto a estratos de produtividade/lucros – que concentram suas atividades em comércio eletrônico, nas quais os FIPs já tenham sido incorporados.

Artigo recebido em 16/01/2016 e aprovado em 27/04/2016.

⁷ Acesso e informações do debate público do anteprojeto de lei de proteção de dados pessoais disponíveis no link: <<http://participacao.mj.gov.br/dadospessoais/>>. Acesso em: 21 dez. 2015.

REFERÊNCIAS

ALBERTIN, A. L. Comércio eletrônico: benefícios e aspectos de sua aplicação. *Revista de Administração de Empresas*, v. 38, n. 1, p.52-63, jan./mar. 1998. Disponível em: <<http://www.scielo.br/pdf/rae/v38n1/a06v38n1.pdf>>. Acesso em: 21 dez. 2015.

BONNER, W.; CHIASSON, M. If fair information principles are the answer, what was the question? An actor-network theory investigation of the modern constitution of privacy. *Information and Organization*, v. 15, n. 4, p.267-293, Oct. 2005. Disponível em: <<http://doi.dx.org/10.1016/j.infoandorg.2005.03.001>>. Acesso em: 21 dez. 2015.

CATE, F. H. The failure of fair information practice principles. In: WINN, Jane K. (Edit.). *Consumer protection in the age of the "Information Economy"*. Farnham, UK: Ashgate, 2006. p. 1-32. Disponível em: <https://www.hunton.com/files/Publication/4100e953-8ce7-47f8-bd91-2338a896a138/Presentation/PublicationAttachment/cca74554-612c-41e0-934f-1372b8a6afcf/Failure_of_Fair_Information_Practice_Principles.pdf>. Acesso em: 21 dez. 2015.

CIGLIO, M. O. Levando em conta os riscos do big data. *Big Data Brasil*. 5 ago. 2013. Disponível em: <<http://www.bigdatabrasil.net/levando-em-conta-os-riscos-do-big-data/>>. Acesso em: 21 dez. 2015.

ENDLER, A. M. Governo eletrônico: a internet como ferramenta de gestão dos serviços públicos. *Revista Eletrônica de Administração*, v. 6, n. 2, p.1-14, mar./abr. 2000. Disponível em: <<http://www.egov.ufsc.br/portal/conteudo/governo-eletronico-internet-como-ferramenta-de-gestao-dos-servicos-publicos-0>>. Acesso em: 21 dez. 2015.

FORBES. Global 2000: the world's biggest public companies. Forbes, 2014. Disponível em: <[http://www.forbes.com/global2000/list/#page:1_sort:0_direction:asc_search:_filter:All industries_filter:All countries_filter:All states](http://www.forbes.com/global2000/list/#page:1_sort:0_direction:asc_search:_filter:All%20industries_filter:All%20countries_filter:All%20states)>. Acesso em: 21 dez. 2015.

FTC [FEDERAL TRADE COMMISSION]. *Privacy online: fair information practices in the electronic marketplace*. May 2000. Washington: Bureau of Consumer Protection, 2000. Disponível em: <<https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf>>. Acesso em: 21 dez. 2015.

GELLMAN, R. Fair information practices: a basic history. *Bobgellman.com*, versão 2.13, p. 1-32, fev. 2011. Disponível em: <<http://bobgellman.com/rg-docs/rg-FIPShistory.pdf>>. Acesso em: 21 dez. 2015.

GRUPO GLOBO. G1 [Portal de Notícias da Globo]. Mais de 50% dos brasileiros estão conectados à internet, diz Pnad. Set. 2014. Disponível em: <<http://g1.globo.com/tecnologia/noticia/2014/09/mais-de-50-dos-brasileiros-estao-conectados-internet-diz-pnad.html>>. Acesso em: 21 dez. 2015.

LINS, B. F. E. Privacidade e internet. *Consultoria Legislativa*, Brasília, p.1-13, mar. 2000. Disponível em: <<http://www2.camara.leg.br/documentos-e-pesquisa/publicacoes/estnottec/arquivos-pdf/pdf/001854.pdf>>. Acesso em: 21 dez. 2015.

MAIA, L. S. A privacidade e os princípios de proteção do indivíduo perante os bancos de dados pessoais. In: ENCONTRO NACIONAL DO CONPEDI/FUMEC, 20., 2011, Belo Horizonte. *Anais eletrônicos...* Belo Horizonte: Anpad, 2011. p. 453-466. Disponível em:

<http://www.publicadireito.com.br/conpedi/manaus/arquivos/anais/bh/luciano_soares_maia.pdf>. Acesso em: 21 dez. 2015.

OECD [ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT]. Guidelines on the protection of privacy and transborder flows of personal data. OECD, 2013. Disponível em: <<http://www.oecd.org/internet/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm#part1>>. Acesso em: 21 dez. 2015.

PBD [PRIVACY BY DESIGN]. History. [2014]. Disponível em: <<https://www.privacybydesign.ca/index.php/about-pbd/applications/>>. Acesso em: 21 dez. 2015.

PEREIRA, A. P.; PRADO, A. A. Comércio eletrônico: vantagens competitivas para empresas no B2C (Empresa-para-Consumidor). *Revista de Administração da Fatea*, v. 2, n. 2, p. 95-106, jan./dez. 2009. Disponível em: <<http://publicacoes.fatea.br/index.php/raf/article/viewFile/220/177>>. Acesso em: 21 dez. 2015.

ROTENBERG, M. Preserving privacy in the information society. In: INFOETHICS 1998: ETHICAL, LEGAL AND SOCIETAL CHALLENGES OF CYBERSPACE, 2., 1998, Monte Carlo. *Anais eletrônicos...* Monte Carlo: Unesco, 1998. p.167-182. Disponível em: <<http://unesdoc.unesco.org/images/0012/001204/120452M.pdf>>. Acesso em: 21 dez. 2015.